Lecture Notes in Networks and Systems 521

Lalit Garg · Dilip Singh Sisodia · Nishtha Kesswani · Joseph G Vella · Imene Brigui · Peter Xuereb · Sanjay Misra · Deepak Singh *Editors*

Information Systems and Management Science

Conference Proceedings of 4th International Conference on Information Systems and Management Science (ISMS) 2021

Springer

Lecture Notes in Networks and Systems

Volume 521

The series "Lecture Notes in Networks and Systems" publishes the latest developments in Networks and Systems—quickly, informally and with high quality. Original research reported in proceedings and post-proceedings represents the core of LNNS.

Volumes published in LNNS embrace all aspects and subfields of, as well as new challenges in, Networks and Systems.

The series contains proceedings and edited volumes in systems and networks, spanning the areas of Cyber-Physical Systems, Autonomous Systems, Sensor Networks, Control Systems, Energy Systems, Automotive Systems, Biological Systems, Vehicular Networking and Connected Vehicles, Aerospace Systems, Automation, Manufacturing, Smart Grids, Nonlinear Systems, Power Systems, Robotics, Social Systems, Economic Systems and other. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution and exposure which enable both a wide and rapid dissemination of research output.

The series covers the theory, applications, and perspectives on the state of the art and future developments relevant to systems and networks, decision making, control, complex processes and related areas, as embedded in the fields of interdisciplinary and applied sciences, engineering, computer science, physics, economics, social, and life sciences, as well as the paradigms and methodologies behind them.

Indexed by SCOPUS, INSPEC, WTI Frankfurt eG, zbMATH, SCImago.

All books published in the series are submitted for consideration in Web of Science.

For proposals from Asia please contact Aninda Bose (aninda.bose@springer.com).

More information about this series at https://link.springer.com/bookseries/15179

Lalit Garg · Dilip Singh Sisodia ·
Nishtha Kesswani · Joseph G Vella ·
Imene Brigui · Peter Xuereb ·
Sanjay Misra · Deepak Singh
Editors

Information Systems and Management Science

Conference Proceedings of 4th International Conference on Information Systems and Management Science (ISMS) 2021

Springer

Editors
Lalit Garg
Department of Computer Information Systems
University of Malta
Msida, Malta

Nishtha Kesswani
Central University of Rajasthan
Ajmer, Rajasthan, India

Imene Brigui
EMLYON Business School
Écully, France

Sanjay Misra
Department of Computer Science and Communication
Ostfold University
Halden, Norway

Dilip Singh Sisodia
Computer Science and Engineering
National Institute of Technology
Chhatisgarh, India

Joseph G Vella
Computer Information Systems Department
University of Malta
Msida, Malta

Peter Xuereb
Faculty of Information and Communication Technology
University of Malta
Msida, Malta

Deepak Singh
Computer Science and Engineering
National Institute of Technology
Chhattisgarh, India

ISSN 2367-3370 ISSN 2367-3389 (electronic)
Lecture Notes in Networks and Systems
ISBN 978-3-031-13149-3 ISBN 978-3-031-13150-9 (eBook)
https://doi.org/10.1007/978-3-031-13150-9

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

The Sentiment Analysis for Hindi Language Using Convolution Neural Network and Deep Belief Network

Manish Rao Ghatge(✉) and Snehlata Barde

MATS University, 492004 Raipur, India
ghatge.manish@gmail.com, drsnehlata@matsuniversity.ac.in

Abstract. It is simple for people to share their ideas, feelings and thoughts on the widespread social media network. The changes in technology and the creation of social platforms have allowed individuals to express their ideas both in the English language and in the mother tongue for such platforms as Hindi, Marathi etc. These are good, negative and neutral ideas. These phrases function as a reservoir of information that may be used to obtain knowledge. In the analysis of sentiment from regional language such as Hindi, study becomes vital and motivating. The goal is therefore to utilize Neural Networks (NNs) to analyses the feelings of Hindi words. The Machine Learning (ML) model will be formed and compared with the use of Deep Belief Network (DBN), Convolution Neural Network (CNN) and Long Short Time Memory (LSTM) to organize the data into constructive and undesirable feelings in Hindi.

Keywords: CNN · DBN · LSTM · ML · NNs · Sentiment analysis

1 Introduction

Due to the fast expansion of information technology, the Internet has become a vital aspect of people's lives. Most individuals exchange views about various entities such as products, service on various platforms such as blogs, and on other social online sites. These sites include significant data from business to political and societal applications on a range of fields [1]. It is tough to manually analyze this large volume of data. SA was highly beneficial in this situation. Basically, it gets a sense of how you feel and how you communicate. SA is becoming a prominent issue in the Natural Language Processing (NLP) area. The aim is to extract subjective information that is transmitted by a transcript automatically. It shelters the extraction of the split or the identification of the target or opinion holder. The function, sentence, and document level can be used for the SA. In many other applications, SA is used, for example, to anticipate consumer patterns, marketing plans and stock market predictions, teacher training and learning [2]. One of the key requests made by SA is to help political parties or the government obtains a sense of how much they can win in the upcoming elections, and how happy the community stays with the guidelines they forecast in the 2016 US election.

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 1–14, 2023.
https://doi.org/10.1007/978-3-031-13150-9_1

In the discipline of NLP, scientists conduct SA through experiments using various tools and techniques like rules or ML. It is a word that refers to instances of computers. ML models are numerous and enable learning, such as Naïve Bayes (NB), Support Vector Machine (SVM), Logistic Regression (LR) and Random Forest (RF). ML models are numerous. NNs are one aspect of ML. NNs is an area that grows extremely fast and further expands under many forms, such as the CNN and Recurrent Neural Networks (RNN). The number of layers in which the NNs is comprised is deep study. Input, hidden and output were specified as early NNs. The addition of additional hidden layers allows the NNs to 'deep' and to understand subtler and more complicated connections. How high the network is determined by the number of "hidden layers." Deep learning is therefore an ML area that employs profound neural networks. Recently, across many disciplines of NLP such as computer vision, entity identification and speaker recognition, deep learning approaches have shown tremendous gains over other existing ML technology. Improvement of accuracy is the main reason behind the adoption of profound learning model with the present ML algorithms [2]. The precision of an ML algorithm depends nevertheless significantly on the good data display feature. One major benefit that profound learning models rely on substantial feature engineering over conventional ML models. While conventional ML algorithms are handmade, it takes time and also misses features. Though, in comparison to standard ML methods, the profound learning needs significant computational power and storage, due to the rise in hidden layers. This encouraged us to use profound learning to do SA in Hindi.

Hindi language is one of the most spoken languages in the world. There are millions of speakers of this language, covering around 41% of India's entire population. In recent years, web sites in the Hindi language have significantly increased with the advent of Unicode standards. Our study analyses sentiments for the Hindi material using CNN.

The paper might summaries the key contributions. The study provides the examination of feelings for low resource Hindi. Three instinctive speakers of Hindi used a Deep Learning Model for manually recording the dataset of the Hindi Reviews. This collection of data was marked in three types of feeling, that is, positive, negative and neutral. The review data set was then analyzed with a deep learning model, which is CNN. Several experiments were carried out in order to assess the exactness and training times of the models by defining various restrictions, like numbers of convolution layers, number of hidden layers, number of filters, output dimension, regulator, drop out and filter size. The prior study by SA researchers utilizing ML and profound language learning approaches. Section 3 briefly discusses the CNN and the different CNN models are implemented as per requirements. The other sections deal with experimental configuration and Sect. 6 discusses the findings of the proposed system as well as the comparison of the results with current work and conventional ML algorithms.

2 Related Work

A complete study of SA for Hindi is conducted utilizing both machine and lexical based approaches, some of them are given as follows.

A Corpus of Hindi reviews and blogs on the use of subjective lexicons and N-grams were performed by Aroa P. [3]. Joshi et al. [4] initially tried to create his own lexicon resource Hindi SentiWordNet (HSWN) for SA in Indian languages and attained a precision of 78.14%. Subsequently Mittal et al. [5] conducted HSWN film reviews with an accuracy of 80.21%. A New system was suggested for SA by utilizing a vocabulary method which is unattended. The unchecked, lexical based approach to SA was taken by Sharma et al. [6]. Akhtar et al. [7] has recently carried out product assessments on aspect-based SA by establishing their own, and 54.05% accuracy, annotated datasets on Hindi.

Nowadays profound learning has become popular due to its precision and automated engineering, researchers have experimented with profound learning models to analyse feelings. The following is the summary of some of the research projects employing deep learning methods. Santos and Gattti [8] presented deep CNN and achieved 85.7 and 86.4% accuracy respectively. Shirani-Mehr[9] evaluated several algorithms for deeper learning such RNN and CNN on a data set for film reviews using NB. In order to conduct SA film evaluation and Twitter messages. Singhal et al. [10] tested several variants of profound learning model, such basic NNs, CNN, RNN and LSTM to different ML methods. Ouyang et al. [11]. In order to enhance the model accuracy, they utilized parametric corrected linear unit (PReLU), normalizing and dropout technologies. Zhang et al. [12] has been offered in Chinese text. They determined that only word embedding characteristics improve their model. The performance of Twitter's CNN for SA has been analyzed by Stojanovsky et al. [13], and the F1 score was 64.85% on 2015 on Twitter, which is equivalent to the conventional ways that SA has taken with regard to. The CNN framework, utilizing Word2Vec to conduct SA, has been suggested by Zhang and Chen [14] performed SA on CNN in China, and assessed the performance of CNNs in comparison with classical ML technology. CNN architecture for SA was proposed in short texts by Hassan and Mahmood [15], with a precision of 88.3% for binary and 47.5% for five-class problem arrangement.

It was found through a literature study that researchers tried utilizing alternative ingredient representations, either word embedding or lexicon sentimental characteristics, in different types of NNs, such as CNN, RNN and the LSTM. The majority of study has also been carried out in English and Chinese, which is rich in resources. Research into poor-resource languages like as the Hindi language is limited since there are not many suitable resources such as lexicons, lexical instruments and annotated corporations. Until date, mostly lexicon based and other standard ML techniques have been utilized by academics to conduct SA for Hindi. A feeling analysis system for Hindi was created in this work. Due to its inexistence, a corpus of Hindi reviews was manually annotated for testing, which was labeled with a polarity data set.

In this study, CNN was used to conduct SA of Hindi text. The motive behind using CNN is that recent advances to CNN and NLP have been seen. As with the CNN, we just have to artificially label the complete phrases, avoiding the enormous labor compared to more profound learning models such as the RNN. With the convolution function, CNN is possible to extract a range of characteristics from global information. Data may be extracted together as features and can take the relation between these features into consideration. The same procedure may thus be employed on transcript to provide the input characteristics for the model, which can be effectively skilled for feeling analysis in another method. For experiments, 12 CNN models were designed to assess the performance of the model using factors such as number of overlay layers, number of filters and filter size. In addition, the performance of the CNN model was evaluated using known ML approaches. A short discussion on the neural and CNN networks is provided in the next section.

3 Concept Behind Neural Networking

A neural network is a cataract of neuron coats with a layer production passed into the next layer. In order to encourage more informative features, each layer transmits the changed version of the data to the next level. NNs are unable to comprehend words, but they work on word embedding, or feature vectors expressing those words more explicitly [11]. As NNs learn from the task they can adapt to any domain. They can adapt.

3.1 Convolutions Neural Network

Nearly the same as conventional NNs are CNN. Like regular NNs, CNN neurons accept input, analyses and further spread it. The distinction is that CNNs accept input as pictures directly. This is why they are employed to analyses picture data explicitly. NNs regularly do not extend well to complete pictures [12]. These can be managed for small sizes, but additional neurons and parameters resulting to a problem of over fitting are necessary as the dimensions increase. The CNN is a four-layered feed forward neural network. The input layer represents the phrases of nxk dimension, the second is convolutional layer and the global max layer of poolization as illustrated in Fig. 1. This figure illustrates Architecture of CNN [15]. The principal component of a CNN is Convolutional layer, as most calculations are done on that layer [16, 17]. It is a functionality extraction layer that extracts local features via the filters, and creates a function map that is calculated with a kernel converting function.

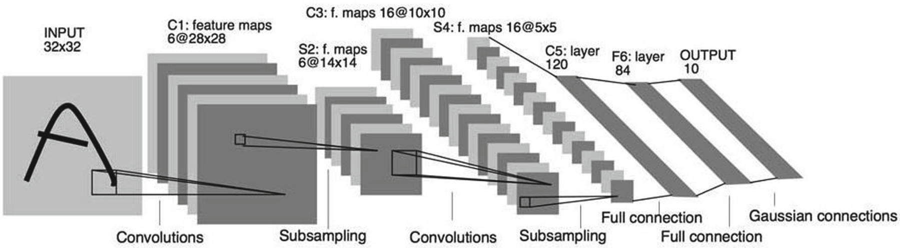


Fig. 1. Architecture of CNN

The CNN inputs are either matrix-represented sentences or documents. Each matrix row is a token, usually a word, although it might be a character. In other words, every row is a vector representing a word. These vectors are often word embedding systems such as Word2vec or GloVe, but may also become one-hot, vocabulary-indexing vectors. For visual recognition jobs, CNN is great. The popular vision networks are available like VGG, LeNet, AlexNet, Inception, ResNet. These NNs are usually developed to recognize images. These networks contain many NNs that extract abstract picture functions these networks. These networks demand a large amount of memory and computer training while requiring more computational networking to achieve more accuracy depending on the layers being employed. AlexNet consists of five layers of convolution and three completely linked layers, for instance. The component LeNet-5 is made up of seven layers; GoogleNet (Beginning) comprises of deep CNN 22 levels; VGG 16 and VGG 19 are composed of 16 and 19 layers. It is difficult to train these deep networks, as they need a huge amount of memory and calculation. However, using our suggested CNN model, the tests with two or three convolution layers were done and it was analyzed that the number of convolutionary layer rises, rather than improves the accuracy.

4 Implementation

4.1 Tool Used

As a development environment for experimenting, we have utilized Jupyter Notebook [20]. It allows building and sharing codes, text, equations and visualizations of documents. They also involve machine education, data cleansing, processing, statistical modeling, etc. CNN models were created using the Python TFLearn (the deep learning library) [18] package built on the top of Tensorflow [19], which accelerates the creation of profound learning models. All strings in the phrases are changed to a sequence list by utilising a TFLearn vocabulary processor as NNs do not handle strings.

4.2 Working of the System

Figure 2 shows the working of the system suggested. It includes three phases: data collection and preparation, system training and testing, and the display of the outcome. The description of above figure is given as follows:

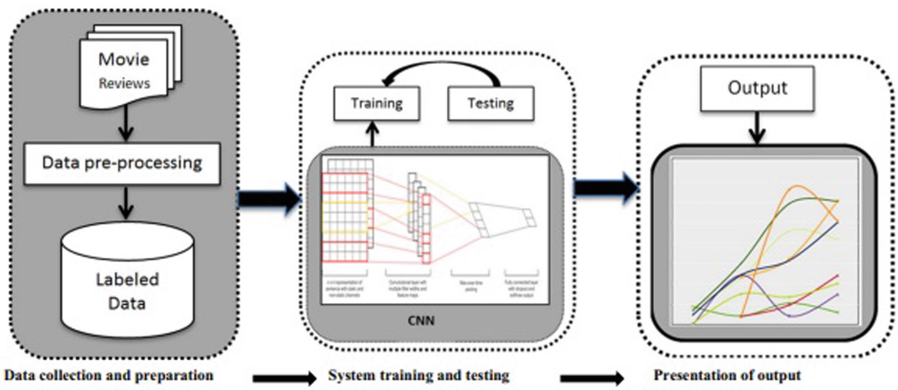


Fig. 2. Workflow of system

Explanatory Data Analysis: The data collected will be pre-processed to provide a rich collection of features by eliminating unnecessary data. Google API will transliterate the romanized text to Hindi text. The dots, URLs, etc. are eliminated using normal Python expressions. A mapping dictionary of 250 often used reviews with associated terms, comprising a mapping of Hinglish to Hindi words, has been developed for the problem of Hinglish wording. The dataset was personally recorded in three classifications, positive, negative and neutral, by three native Hindi speakers.

The collection consists of 7354 reviews, which includes 2341 pp, 2037 pp and 2976 pp. Table 1 provides some sample dataset phrases.

Table 1. Sample sentence of dataset

Type	Some sample sentences of the dataset	Transliteration
Negative	कहानी को ठीक से समेटा नहीं गया है ।	Kahaani Ko Theek Se Sameta Nahi Gaya Hai
Positive	आमिर बशीर स्टेज के बेहतरीन कलाकार हैं ।	Amir Basher Stej Ke Behtareen Kalakaar Hain
Neutral	उन्हें रास्ते में सैमुअल जैक्सन मिलते हैं ।	Unhe Raste Men Samual Jakson Milte Hain

CNN Model Training and Testing: The system is made using a four-layer CNN model, i.e., input layer, convolution layer, worldwide max pond layer and fully connected layer. The following is a short description of these strata.

Input Layer; The CNN input layer should incorporate image data. Image data is represented as a three-dimensional matrix. It will be needed to be resized so that it fit into a solitary column. If you have an image with the dimensions 28X28 = 784, you must convert it to 784 $\times$ 1 before inserting it into the input. The input dimension will be "m" if you have "m" training samples (784, m). Because it extracts visual characteristics, the convolution layer is also known as a feature extractor layer. A part of the picture is linked to the Convolution layer, which performs convolution operations and calculates the dot product between the receptive field (a local section of the input image the same size as the filter) and the filter, as we saw before. The output volume is represented by a single integer as a result of the operation. The filter is then moved across the next receptive field of the same input image using a Stride, and the process is repeated. We'll keep doing this till we've gone through the whole image. The following layer's input will be the output.

Convolution Layer; a set of m filters in this layer is applied over each sentence to a sliding window of length h. These filters are applied to each word window in the sentence, and an enhancement is created. There is a distinct bias in each filter. Multiple maps are generated by these m filters running in simultaneously.

Max pooling Layer; the max pooling layer illustrates the map of the convolution layer and its optimal local characteristics. This layer adds the data and lowers the display.

Presentation of the Output: The output findings are displayed by creating line diagrams and these diagrams contribute to the comparison of CNN models. The next section provides the various parameter settings for conducting the experiment.

5 Experimental Setup

Due to multiple parameters for each layer, various CNN models were developed in this project. Table 2 specifies the parameters for the CNN model such as vocabulary size, vector size, number of convolutionary layers, hidden layers, fully connected layers, number of filters, filter size, activation function.

Table 2. Parameters for the CNN

Parameter	Value
Size of the Vocabulary	13,400
Size of the Input Vector	110
CNN Layer	2,3
Hidden Layer	7,6
Activation Function	ReLu, Softmax
Filter	10,50,60,100,128,256
Size of the filter	3,4,5,7
Connected Layer	1
Dimension of the output	128
Regulizer	L2
Drop Out	0.5
Epochs	50
Batch Size	32

For experimentation there were either 2 or 3 layers of convolution, and there were 10 to 256 filters. In addition, several filter sizes such as 3 to 3, 4 to 4, 5 to 5 and 7 to 7 were used in tests. By evaluating research carried out by other writers in this field, the values of these factors were determined. As the modification in these parameters did not demonstrate any increase in model precision, the other parameters such as the output dimension, regularize, dropout and number of periods and batch size have now been fixed. In all models, together with other parameters such as filters number and filters size, the number of convolutionary layers has been changed. All 12 CNN models are presented in Table 3 for setup.

Table 3. Parameter setting for CCN

CNN Layer Name	Convolution Layer	Hidden Layers	Number of Filter	Size of the filter
1	2.0	6.0	09	3.40
2	2.0	7.0	10	3.50
3	2.0	6.0	50	3.39
4	2.0	7.0	49	3.49
5	2.0	6.0	60	3.39
6	2.0	7.0	59	3.50
7	3.0	6.0	99	3.4.5
8	3.0	7.0	100	7.4.3
9	3.0	6.0	128	3.4.5
10	3.0	7.0	128	7.4.3
11	3.0	6.0	256	3.4.5
12	3.0	7.0	256	7.4.3

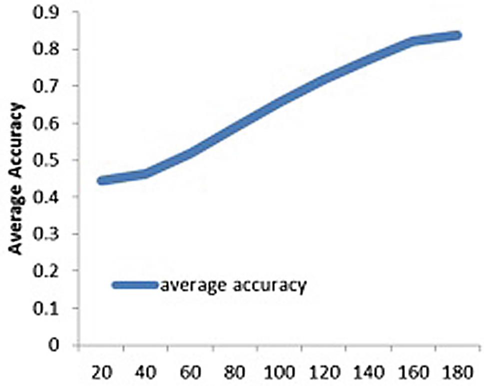
6 Result and Discussion

All CNN models are given in Table 4 with their validation and loss ratings and their period of training (in seconds).

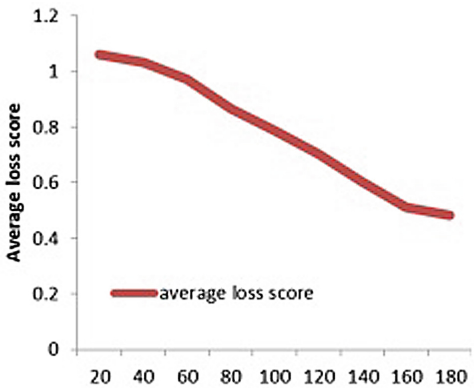
Table 4. Accuracy and loss of CNN model

CNN Layer Name	Val_Accuracy	Val_Loss	Training Time (sec)
1	92.62	22.1	16.73
2	95.32	14.2	16.87
3	95.44	15.5	24.02
4	88.41	29.8	25.07
5	93.28	16.5	25.53
6	94.21	18.3	26.12
7	73.72	67.3	46.40
8	85.49	33.1	53.43
9	92.20	23.5	61.22
10	93.24	16.5	67.11
11	92.27	23.5	166.84
12	93.24	20.5	169.83

After experimenting with various parameter setters, it became clear that the CNN model outperforms the others in two convolution layers and filter sizes 3, 4, with 95.4% accuracy. A CNN model with three convolutive layers achieved the highest accuracy of 93.44%. It was discovered that increasing the number of convolutional layers and filters improves the training time of the models. Figure 3 depicts the average precision and loss of all CNN models. In Fig. 3a, b, the number of iterations is indicated on the X-axis, while the exactness and loss score percentages are shown on the Y-axis.



(a)



(b)

Fig. 3. (a) Training iteration (average accuracy). (b) Training iteration (average loss score)

In Fig. 3a, the average study curve indicates that the accuracy % is gradually increased as the training increases. The model learns from data. The total number of mistakes predicted by the model is the loss value. Figure 3b illustrates a number of mistakes at the beginning and that the number of training steps decreased. Since most models had a decent non-linear curve, they dropped fast at first and were mainly below 0.6. For each CNN model, the additional performance characteristics such as accuracy, reminder, F-method, Kappa score, MAE and RMSE are presented in Table 5.

Table 5. Other performance measures

CNN Layer Name	Precision (%)	Recall	F-Measure (%)	Kappa	MAE	RMSE
1	93.10	92.61	92.60	88.92	0.08	0.304
2	95.40	95.32	95.34	93.21	0.05	0.239
3	95.40	95.42	0.954	93.21	0.06	0.297
4	88.50	88.40	88.43	82.66	0.117	0.347
5	93.90	93.82	93.13	90.11	0.076	0.322
6	95.23	94.01	94.23	91.00	0.065	0.277
7	75.31	73.63	71.66	60.22	0.365	0.754
8	86.35	85.91	95.62	78.83	0.143	0.383
9	92.15	92.03	82.31	92.21	0.11	0.413
10	93.12	73.43	93.23	88.13	0.073	0.298
11	93.00	92.43	92.52	89.21	0.076	0.286
12	93.54	93.45	93.62	90.12	0.068	0.265

The accuracy, memory, and F-measure of all 12 CNN models are represented in Fig. 4. The CNN models with various parameter settings are represented on the X-axis, while the accuracy, recall, and F-measure for each CNN model are represented on the Y-axis. Figure 5 shows how CNN models calculate error rates in terms of MAE and RMSE. In Figs. 4 and 5, it can be shown that CNN3 is the best model, while CNN7 is the foulest of wholly models; with an exactness of less than 80%.Best model CNN3's confusion matrix is as follows.

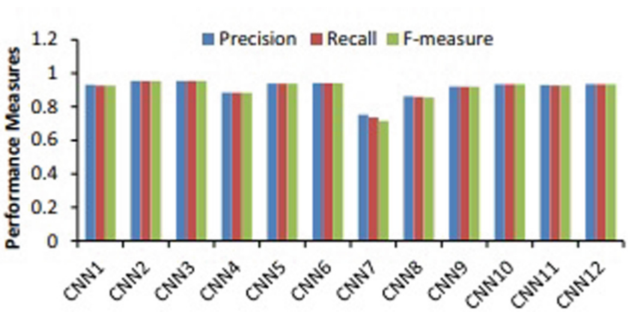


Fig. 4. Different model with different parameter settings

Figure 6 illustrate the precision and loss score learning curves for the best-performing model CNN3. The model's accuracy improves as the number of training iterations

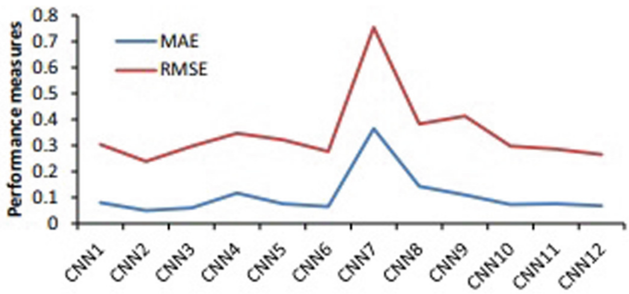
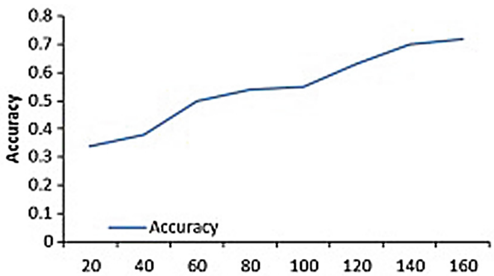


Fig. 5. CNN model with different parameter settings

increases, as seen in Fig. 6(a). The accuracy, however, stabilizes after 130 repetitions. In Fig. 6(b), the loss score learning curve for CNN model CNN3 falls fast and falls below 0.2, suggesting that this model has the fewest mistakes.



(a)

(b)

Fig. 6. (a) The accuracy learning curves. (b) The accuracy and loss score learning curves

6.1 Comparison

In this part, the results of our system are compared to the accuracy of baseline ML approaches. On the same dataset, basic ML techniques such as KNN, NB, ME, and SVM were tested Support Vector Machine. The dataset is transformed after preprocessing, and the file encoding parameter is adjusted to ‘UTF-8’. The filter ‘String To Word Vector’ and the features TF Transform, IDF Transform, and tokenizer are used to convert the string input into numerical matrices. The system uses KNN, NB, ME and SVM classifiers, and unigram feature model bag-of-words. The training portion of the dataset is utilized, whereas the testing portion is used. On the tested dataset, the accuracy achieved using ML techniques for comparison applied our model, as shown in Fig. 7.

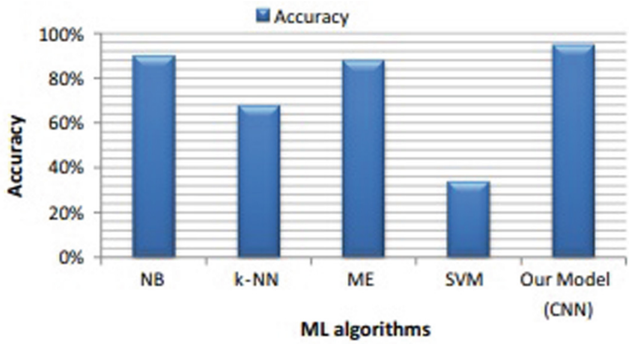


Fig. 7. Comparative analysis of accuracy with baseline ML Algorithm with CNN

After experiment on various parameter adjustments of CNN models, it was discovered that 9/12 CNN models were capable to reach an accuracy of greater than 90%. This accuracy is superior to that of standard ML algorithms. NB achieves the highest accuracy (i.e., 90%) among baseline ML algorithms.

In addition, utilizing HSWN, an experiment was conducted on the recommended method. The HSWN is a divergence lexicon that includes sentimental words and a pre-calculated divergence score. In this situation, the presenting word as an n-dimensional, xRn, where n indicate feature number and the word vector is constructed from the emotion attribute feature of the given word. Three-word emotion attribute qualities, namely whether the word is positive, negative, or neutral, were employed for this. Each dimension has a one or zero value, with one indicating the existence of a feature and zero indicating the lack of one.

A sentence’s characteristics matrix is X Rkn, and it’s used as input to the CNN for a specific phrase with k words. The recommended CNN model’s findings on the reviews dataset are underwhelming since the HSWN comprises both broad sentiment words and sentiment words with restricted coverage. As previously noted, there is only a little amount of effort on Hindi language SA because to a lack of annotated corpora. In addition, the majority of research for English and Chinese languages has been conducted on SA using CNN.

7 Conclusion and Future Work

We did tests using different shapes and settings from CNN and conducted SA of Hindi reviews from websites and online newspapers, because to the popularity of profound learning models. A dataset was manually annotated by three Hindi speakers in preparation for the model training. The tests are run with a variety of convolution layers and filter sizes and numbers, with 80% of the data set being trained and 20% of the remaining dataset being tested. For review datasets, the results of our CNN model are compared to traditional ML approaches and state-of-the-art discoveries. With 95% accuracy, our model outperforms traditional ML approaches.

The findings of the experiments show that adequately trained CNNs can outperform basic ML systems when it comes to sentiment classification. The sentences of reviews are divided into three categories in our model: favorable, negative, and neutral. All of the experiments were conducted with various parameter values for all CNN models, and it was discovered that the CNN model with two convolutional layers and filter sizes 3 and 4 performs the best across all models and achieves a 95% accuracy rate.

Experimenting with multiple deep learning models as well as increasing the data set to include other domain reviews, goods, political analysis, and social media analysis will be part of future work in order to build a system that can be used in a number of applications for the benefit of society.

References

1. Almatrafi, O.; Parack, S.; Chavan, B.: Application of location based sentiment analysis using Twitter for identifying trends towards Indian general elections 2014. In: Proceedings of the 9th International Conference on Ubiquitous Information Management and Communication. ACM, Bali, Indonesia, pp. 1–5 (2015)
2. Rani, S., Kumar, P.: A sentiment analysis system to improve teaching and learning. Computer **50**(5), 36–43 (2017)
3. Arora, P.: Sentiment Analysis for Hindi Language. MS Thesis. International Institute of Information Technology, Hyderabad, India (2013)
4. Joshi, A., Balamurali, A.R., Bhattacharyya, P.: A fall-back strategy for sentiment analysis in Hindi: a case study. In: Proceedings of the 8th International Conference on Natural Language Processing, pp. 1–6 (2010)
5. Mittal, N., Agarwal, B., Chouhan, G., Bania, N., Pareek, P.: Sentiment analysis of Hindi review based on negation and discourse relation. In: proceedings of International Joint Conference on Natural Language Processing, pp. 45–50 (2013)
6. Sharma, Y., Mangat, V., Kaur, M.: A practical approach to sentiment analysis of Hindi tweets. In: Proceedings of 1st International Conference on Next Generation Computing Technologies, pp. 677– 680 (2015)
7. Akhtar, M.S., Ekbal, A., Bhattacharyya, P.: Aspect based sentiment analysis in Hindi: resource creation and evaluation. In: International Conference on Language Resources and Evaluation, pp. 1–7 (2016)
8. Dos Santos, C.N., Gatti, M.: Deep convolutional neural networks for sentiment analysis of short texts. In: Proceedings of 25th International Conference on Computational Linguistics, pp. 69–78 (2014)
9. Shirani-Mehr, H.: Applications of deep learning to sentiment analysis of movie reviews. Technical rep

10. Singhal, P., Bhattacharyya, P.: Sentiment Analysis and Deep Learning: A Survey [Online]. http://www.cfilt.iitb.ac.in/resources/surveys/sentiment-deeplearning-2016-prerna.pdf (2016)
11. Ouyang, X., Zhou, P., Li, C.H., Liu, L.: Sentiment analysis using convolutional neural network. In: International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), pp. 2359–2364 (2015)
12. Zhang, L., Chen, C.: Sentiment classification with convolutional neural networks: an experimental study on a large-scale Chinese conversation corpus. In: Proceedings of 12th International Conference on Computational Intelligence and Security (CIS), pp. 165–169 (2016)
13. Stojanovski, D., Strezoski, G., Madjarov, G., Dimitrovski, I.: Twitter sentiment analysis using Deep Convolutional Neural Network. In: International Conference on Hybrid Artificial Intelligence Systems, pp. 726–737 (2015)
14. Zhang, Y., Chen, M., Liu, L., Wang, Y.: An effective Convolutional Neural Network model for Chinese sentiment analysis. In: AIP Conference Proceedings, vol. 1836, number 1, pp. 1–6 (2017)
15. Hassan, A., Mahmood, A.: Deep learning approach for sentiment analysis of short texts. In: 3rd International Conference on Control, Automation and Robotics (ICCAR), pp. 705–710 (2017)
16. Singh, D., Singh, S.: Realising transfer learning through convolutional neural network and support vector machine for mental task classification. Electron. Lett. **56**, 1375–1378 (2020). https://doi.org/10.1049/el.2020.2632
17. Pisda, K., Jain, P., Sisodia, D.S.: Deep networks for brachial plexus nerves segmentation and detection using ultrasound images. In: Garg, L., et al. (eds.) Information Systems and Management Science. ISMS 2020. Lecture Notes in Networks and Systems, vol 303. Springer, Cham (2022). https://doi.org/10.1007/978-3-030-86223-7_13
18. Tensorflow [Online]. https://www.tensorflow.org/
19. TFLearn: Deep learning library featuring a higher-level API for TensorFlow [Online]. http://tflearn.org/
20. Jupyter [Online]. http://jupyter.org/

An Empirical Review on Brain Tumor Classification Approaches

Mutkule Prasad Raghunath(✉) and B. Ankayarkanni

Sathyabama Institute of Science and Technology, Chennai, India
mutkuleprasad000@gmail.com

Abstract. Cancer or malignant growth is the significant medical issue that shatters the world due to higher mortality rate. Cancer is regarded as the second most deadliest disease after cardiovascular disease as it kills one sixth of people in the world. There are different sorts of cancers such as colon cancer, lung cancer, breast cancer, blood cancer and brain tumor. The Brain tumor prevails as the most destructive cancer due to its low survival rate, assorted characteristics and combative nature. The brain is the crucial part of the human body as it controls the whole activity such as breathing, muscle movement and inducing the senses with the help of tissues and neural cells. Each and every cell has their own abilities; a few cells develop with their own usefulness, and some lose their ability, oppose, and develop distortions. These mass assortments of unusual cells from the tissue are called cancer. Harmful brain tumors are uncontrolled and unnatural development of synapses (brain cells). It is quite possibly the most dangerous and deadly malignant growth, which forces the requirement for programmed recognition techniques. There are so many methods existing in the literature to facilitate effective brain tumor classification methods. Hence, in this survey, we analyze 30 literature works concentrating on classification problems associated with the brain tumor using MRI, bringing into light the various shortcomings of the existing methodologies for classification problems. Here, the analysis of various methods will be facilitated based on several factors, such as performance metrics, datasets used etc. On the other hand, the analysis of the methods with respect to the merits and demerits of the methods are presented. Finally, the paper elaborates the prospective future research directions and provocations in obtaining the better classification accuracy for the MRI brain tumor categorization.

Keywords: Brain tumor classification · Computer assisted determination (CAD) · Magnetic resonance ımaging (MRI) · Machine learning (ML) · Deep Learning (DL)

1 Introduction

Brain tumor is the deadliest and dangerous malignant growth mostly prevails among children and the adolescence [1]. Brain tumor is categorized as an incurable disease due to the complex interconnection of tissues and the perplexing structure [2]. Precise and brief recognition of brain tumor is indispensable for executing a successful therapy

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 15–27, 2023.
https://doi.org/10.1007/978-3-031-13150-9_2

of this sickness. The decision of a treatment methodology relies upon the phase of the cancer at the time of determination, the curative types, and grade of the growth. As per the characterization guidelines of World Health Organization (WHO), cancerous tissue growth or cancers of the focal sensory system is additionally separated into grades of threat grade I (harmless) to grade IV (highly dangerous) [1]. Glioblastomas also termed by WHO as grade IV cancers are viewed as the most deadly kind of growth conveying inauspicious visualization even with numerous headways in restorative administration [3]. The essential technique for separating grade IV cancers from different grades by pathology. Introductory separation can be made based on microvascular multiplication, necrosis and vascular apoplexy components of grade IV tumors [1, 4]. Early recognition and characterization of malignant growth with particular grade is vital to treat the cancer adequately [1].

Computer Assisted Determination (CAD) strategies have been accommodating neurologists from numerous points of view. Computer aided design applications in neurocytology incorporate cancer identification, arrangement, and categorization [1]. CAD design framework [5–7] or order of the brain tumor is set up to assist the neurologists in representation [8] and characterizing growth types [9–11]. Evaluating glioma, which is a significant class of threatening cancers, is another examination issue in this area [3]. The previously mentioned CAD frameworks depend on Magnetic Resonance Image (MRI) pictures of the cerebrum. This is a direct result of the potential of MRI to give a higher difference to delicate tissues in cerebrum contrasted with Computed Tomography (CT) pictures [1]. With Deep neural organizations, elevated level of attributes removed from the MRI filters are used to order various kinds of grades that may assist neurologist in decision making about the prior determination and future diagnosis strategy. This arrangement introduced by various specialists, gives insight regarding the harm of growth by different rates [3]. CAD design based brain tumor is categorized into harmless and threatening growths is a broadly investigated theme [1].

Ongoing research on CAD clinical analysis gives further developed exhibitions attributable to the approach of Deep Learning (DL) techniques. DL systems have been widely utilized in the clinical picture investigation of cancer disease [4] and cellular breakdown in the lungs determination [12]. Nawab et al. [13] presented a DL algorithm for the recognition of human epidermis, which is a representation of dermatology diagnostics. Deepak et al. [1] utilized a Deep Convolutional Neural Network (DCNN) organization) to screen the cerebrum metastases. In the recent strategy, an unique class of DL, also called as deep transfer learning, overwhelmed the investigations on visual arrangement, object acknowledgment and picture order issues [1, 6]. In this review article a portion of the traditional DL procedures used for the cerebrum cancer categorization is assessed.

In this review article, various literature works concentrating on classification problems associated with the brain tumor are analyzed using MRI, bringing into light the various shortcomings of the existing methodologies for classification problems. Here, the analysis of various methods will be facilitated based on several factors, such as performance metrics, datasets used and so on. On the other hand, the analysis of the methods with respect to the merits and demerits of the methods are presented.

The organization of the review article is as follows: The review of the literature associated with the brain tumor categorization model is enumerated in Sect. 2. The analysis and discussion of various brain tumor categorization models is elucidated in Sect. 3 and the research gaps and challenges are deliberated in Sect. 4. Finally, the paper is concluded in Sect. 5. In this subsection, the review of 30 papers are elucidated.

2 Review of Some Existing Methods

This section elucidates the review of some techniques, which are related to brain tumor recognition. The review articles are basically classified into the techniques which are represented as below:

1) Machine learning technique, 2) Fuzzy logic techniques, 3) Ensemble techniques and 4) Hybrid techniques 5) DL techniques (see Fig. 1).These techniques involved in the recognition of brain tumors for MR images. These techniques are represented according to the core area of their year of evolution.

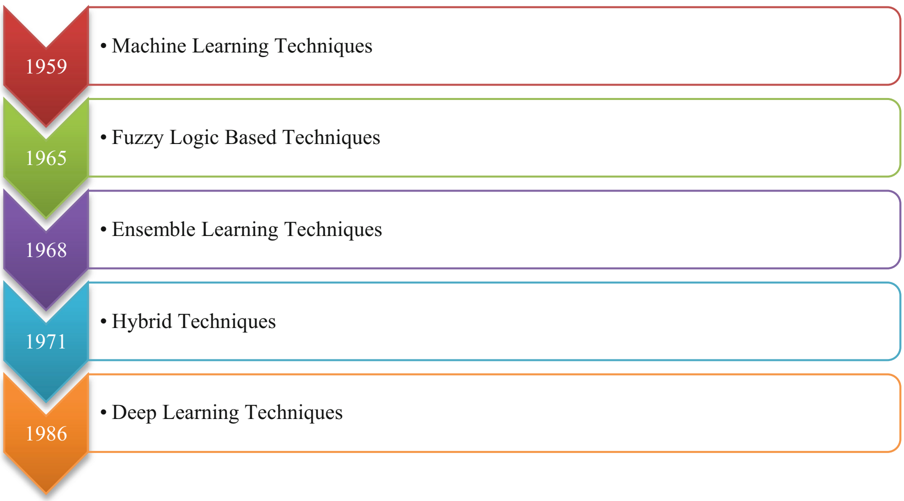


Fig. 1. Brain tumor detection techniques

2.1 Brain tumor detection based on Machine-learning techniques

Amin et al. [12] preferred a computerized strategy for the effective discrimination among destructive and non-malignant MRI of the cerebrum. Various strategies have been used for the fragmentation of applicant contusion. Then, at that point an attribute set is selected for each candidate lesion utilizing surface, intensity and shape. By then, SVM classifiers are associated with various cross approvals on the attribute set to enhance the accuracy of the categorization system. The technique is approved on three standard datasets like RIDER, Local and Harvard. The technique accomplished normal 97.1% precision, 91.9% affectability and specificity of 98.0%. It is utilized to recognize the growth all the more precisely in less computing time when contrasted with existing techniques.

Usman and Rajpoot [2] presented the novel algorithm for the categorization of tumor categorization. The novel algorithm utilized MICCAI BraTS data depending on the magnitude-connected attributes and the wavelet pattern attributes. This model is utilized to categorize the cancerous tissue into three sectors such as core tumor, intensifying tumor and the entire tumor.The potential, the locale, potential variation and the wavelet attributes are extricated and used on the multi-modal MRI with different classifiers. The wavelet-based attributes utilized RF classifier has enhanced the accuracy.

Rafia et al. [8] utilize the K-Nearest Neighbor classifier to commutatively evaluate the MRI images. The edema T1 and T2 tumor categorization is devised to recognize the tumor to label and categorize the type of tumor. Data presentation of the device is utilized to categorize the brain tumor. The brain tumor is classified into three types such as Gliblastoma, oligodendroglioma and Astrocytoma. To determine the cancerous region the image processing strategy is established, which consists of image binarization, image augmentation, watershed and the morphological image.

Amin et al. [9] presented novel strategies, in which the progression of the MRI is combined at distinct stages by utilizing WT so as to attain the comprehensive information and to detect the tumor. The combined images are exposed to CNN for the automated feature selection and the tumor categorization.

Chandan and Foisal [15] utilized the strategies for the categorization normal and the cancerous tissues from the MRI utilizing the SVM, NSCT and K-means congregating. The K-means clustering ensures the rapid categorization using the K-means clustering.

2.2 Brain Tumor Detection based on Fuzzy Approach

Roy et al. [4] presented the modified classifier along with the ANFIS for the characterization of the cancerous tissue. The classifiers utilized in the system attain the highest accuracy for the standard Harvard dataset. The feature extractions are utilized in the technique so as to boost the performance of the classifier. The overfitting issue along with high computational time is the main drawback of the system.

2.3 Brain Tumor Detection based on Ensemble-Learning Techniques

Deepak and Ameer [16] concentrated on designing an appropriate algorithm so as to effectively categorize the brain tumor. While comparing CNN along with softmax classifiers the organization of CNN and SVM provides better categorization outcomes. The method is widely utilized for the medical image categorization. The high memory and fine tuning are the main advantages of the system. High computational time is the main drawback of the system.

2.4 Brain Tumor Detection based on Hybrid Approach

Cinar and Yildirim [17] presented effective hybrid techniques to categorize the tumor images. The Resnet50 framework is utilized as the basic unit of this hybrid technique.

The endmost 5 layers of the hybrid technique are replaced with the other 10 layers. The highest accuracy is obtained by the proposed strategies.

2.5 Brain Tumor Detection based on Deep-Learning Techniques

Deepak and Ameer [1] suggested a precise and completely programmed framework, with least pre-processing, for the categorization of the brain tumors. The categorization framework applied the idea of Deep transfer learning out how to extricate attributes from MRI pictures of the brain. The elements were utilized with demonstrated classifier models for a further revamped interpretation. The framework recorded the best categorization exactness contrasted with all connected works. The presentation was assessed utilizing different measurements additionally, to find out the effectiveness of the framework. Furthermore, the framework demonstrated an efficient attitude with fewer training representation. In spite of the accomplishments revealed in this paper, a few upgrades stay conceivable: First, to the somewhat terrible showing of the exchange the gained model as an independent classifier. Subsequently, there was extensive miscategoraization of representation from the grade meningioma. Moreover, the procedure of overfitting with more modest training information.

Sajjad et al. [3] suggested a dynamic DL based multi-grade framework of the categorization of the brain. The framework is triple extend: 1) the cancer areas from the dataset are fragmented through a CNN model, 2) the fragmented information is additionally expanded utilizing several extremities to enhance the quantity of information samples, and 3) a pre-processed VGG-19 CNN model is calibrated for multi-grade cerebrum growth categorization. This framework worked on precision by using information expansion and DL. The experimental outcomes demonstrate the adequacy of the CNN based CAD framework, for aiding the neurologist in taking an exact choice for categorization multi-grade cancer growths into four grades. Later on, the research plan to expand the work for fine-grained grouping of each grade with examination of light-weight CNN models to adjust the proficiency and exactness.

Bahadure et al. [5] fragmented cerebrum tissues into ordinary tissues like white matter, dim matter, cerebrospinal liquid, and cancer affected tissues. The method utilized pre-preparing to lessen the impact of undesirable commotion caught during the procurement of MR pictures and utilized upgrade dependent on auto-upgrade FCM procedure to work on the nature of un-processed MR pictures. The unwanted cerebral tissues, for example, fat and epidermis are eliminated utilizing skull stripping dependent on threshold strategies. Further, to get the most ideal characterization results, the method enhances the similar methodology for looking at four division strategies dependent on FCM, watershed, BWT, and DCT. Further select the pre-eminent features by contrasting their division score. To enhance the precision for grouping of the growth stage, the attribute vector is removed and furthermore upgraded and characterized utilizing the genetic algorithm. The experimental outcome demonstrates that the approach can enhance the precise, and ideal recognition of brain cancer.

Parnian et al. [6] utilized a CapsNet framework that integrates both the un-processed MRI brain pictures and the cancerous growth limits to categorize the cancers. The CapsNet design has two primary advantages: (I) First, the requirement for cancerous growth is terminated, and; (ii) Second, it assists the CapsNet with concentrating on the principal region, and simultaneously, contemplating its connection with encompassing tissues. The experimental outcomes demonstrate that the approach is suitable for expanding the classification precision, contrasted with CapsNets and CNNs. At last, it is worth focusing on the fact that CapsNets are equipped with assets that expand their interpretability, e.g., the yield insanitation attributes of the genuine class can clarify whether the organization has caught the right components. Lavanyadevi et al. [7] suggested the strategy incorporates precisely perceiving semantically significant full regions in a picture. As mentioned in the outcomes, by the relationship of each pixel in the picture alongside the sticker signifying a semantically significant fragment, the doctor and radiologist can recognize danger and determination. The attributes of adjoining twofold models and dark level co-events are eliminated from brain pictures with harmless or threatening or typical pictures. In the processing mode the eliminated includes alongside semantic provisions are prepared utilizing PNN classifiers. In categorization mode similar components are separated from test brain pictures and concealed with processed models utilizing PNN classifiers. PNN is considered to enjoy significant benefits. It is because of reality that PNN gains from preparing information promptly. As PNN has a high rate of learning ability, it can adjust its learning progressively. Mohsen et al. [10] suggested a productive approach which consolidates the discrete wavelet change (DWT) along the DNN to categorize MRIs into Normal and 3 sorts of harmful cerebrum cancers: metastatic bronchogenic carcinoma, glioblastoma and sarcoma. The DWT-DNN approach design is similar to the convolutional neural organizations (CNN) strategies yet demands less equipment determinations and takes a preferable season of handling for huge size pictures. Moreover utilizing the DNN classifier shows high precision contrasted with conventional classifiers. Abdelaziz et al. [11] presented an improved DL model for categorization of the brain from MRI pictures. This model was processed on a standard brain cancer MRI pictures dataset composed of 3064 numbers of MRI pictures. This strategy upheld different information expansion strategies which expanded the dataset size and improved the precision. The methods have utilized flat and vertical flips, turn, moving, ZCA brightening, zooming, shearing, and splendor control as increased procedures. The strategy utilized Residual Networks (ResNet), a sort of CNN framework which obtained ahead of everyone else at the ImageNet Large Scale Visual Recognition Challenge (ILSVRC) 2015. The advanced ResNet permits the processing of incredibly deep neural organizations by presenting the idea of alternate route associations to avoid at least one layer, in this manner tackling the issue of degenerated exactness and vanishing gradient. ResNet-50 were modified to the real time picture dataset by altering the completely associated layer to have 3 neurons, then, at that point, tweaked the attributes of ResNet-50 via processing of the dataset. Nawab et al. [13] presented a dynamic methodology for cancerous growth picture categorization dependent on fine-tuning along with transfer learning move. The tumor categorization methodology of block-wise fine tuning along with the transfer learning with recommends an elective methodology, which is unique in relation to utilizing pre-prepared CNN as an off-the-rack attribute extractor (without preparing) that process the different strategy for categorization, (for example, SVM, Random Forest and Decision Trees). It additionally exhibits the adaptability of knowledge from normal pictures to clinical cerebrum MR pictures. This approach might be utilized to enhance the grouping framework for other MRI pictures and other clinical imaging areas, for example, PET, CT and X-rays. The technique is more conventional; it requires least initialization for 2D MR pictures and fails to utilize handmade components.

Rehman et al. [14] enforced an transfer learning strategies utilizing normal pictures of ImageNet (source assignment) dataset and categorized the brain cancer phase from meningioma, pituitary, and glioma utilizing Figshare dataset known as target task. This technique employed three incredible DCNN structures such as GoogleNet, VGGNet and AlexNet on MRI fragments of Figshare to distinguish the cancerous sorts. To assess and investigate the attitudes of deep organizations, two investigations from transfer learning such as freeze and fine-tune are directed to remove the perspective visual attributes and representation from MRI cuts.

Table 1 gives the summary of all the techniques used.

Table 1. Summary of techniques used in the different papers

Title of paper and authors	Year	Technique used	Specifications
Deepak and Ameer [1]	2019	Deep Learning	Suggested a precise and completely programmed framework, with least pre-processing, for the categorization of the brain tumors
Sajjad et al. [3]	2020		Suggested an dynamic DL based multi-grade framework of the categorization of brain
Bahadure et al. [5]	2019		The method utilized pre-preparing to lessen the impact of undesirable commotion caught during the procurement of MR pictures and utilized upgrade dependent on auto-upgrade FCM procedure to work on the nature of un-processed MR pictures
Parnian et al. [6]	2020		A CapsNet framework that integrates both the un processed MRI brain pictures and the cancerous growth limits to categorize the cancers
Lavanyadevi et al. [7]	2017		Suggested the strategy incorporates of precisely perceiving semantically significance full regions in a picture

(*continued*)

Table 1. (*continued*)

Title of paper and authors	Year	Technique used	Specifications
Mohsen et al. [10]	2017		Suggested a productive approach which consolidates the discrete wavelet change (DWT) along the DNN to categorize MRIs into Normal and 3 sorts of harmful cerebrum cancers: metastatic bronchogenic carcinoma, glioblastoma and sarcoma
Abdelaziz et al. [11]	2019		Presented an improved DL model for categorization of brain from MRI pictures
Nawab et al. [13]	2019		Presented a dynamic methodology for cancerous growth picture categorization dependent on fine-tuning along with transfer learning move
Rehman et al. [14]	2019		Enforced an transfer learning strategies utilizing normal pictures of ImageNet (source assignment) dataset and categorized the brain cancer phase from meningioma, pituitary, and glioma utilizing Figshare dataset known as target task
Amin et al. [12]	2017	Machine Learning	Preferred a computerized strategy for the effective discrimination among destructive and non-malignant MRI of the cerebrum
Usman and Rajpoot [2]	2017		Presented the novel algorithm for the categorization of tumor categorization
Rafi et al. [8]	2019		Utilize the K-Nearest Neighbor classifier to commutatively evaluate the MRI images
Amin et al. [9]	2019		Presented the novel strategies, which the progression of the MRI are combined at distinct stages by utilizing WT so as to attain the comprehensive information and to detect the tumor

(*continued*)

Table 1. (*continued*)

Title of paper and authors	Year	Technique used	Specifications
Chandan and Foisal [15]	2017		Utilized the strategies for the categorization normal and the cancerous tissues from the MRI utilizing the SVM, NSCT and K-means congregating
Deepak and Ameer [16]	2020	Ensemble Learning	Concentrated on designing an appropriate algorithm so as to effectively categorize the brain tumor. While comparing with CNN along with softmax classifier the organization of CNN and SVM provides better categorization outcome
Cinar and Yildirim [17]	2020	Hybrid Technique	Presented a effective hybrid techniques to categorize the tumor images. The Resnet50 framework is utilized as the basic unit of this hybrid technique
Roy et al. [4]	2016	Fuzzy Technique	Presented the modified classifier along with the ANFIS for the characterization of the cancerous tissue. The classifiers utilized in the system attain the highest accuracy for the standard Harvard dataset

3 Analysis and Discussion

This section deliberates the evaluation and the discussion of performance metrics and the dataset used in the research papers and the outcomes of the analysis indicates the importance of the number of implementation strategies of brain tumor classification method.

3.1 Analysis Based on Dataset

Figure 2 illustrates the evaluation of the research papers in accordance with the data set utilized for the determination of brain tumor. The database such as MRI dataset (figshare), Publically available data, Brain tumor dataset, Radiopaedia, Harvard dataset, RIDER dataset, Local dataset, MICCAI BraTS dataset, Digital Imaging and Communications in Medicine (DICOM) dataset, contrast-enhanced magnetic resonance images (CE-MRI) dataset, T1-weighted contrast-enhanced images data were commonly utilized in the review papers. The MRI data is the commonly utilized data set among the different brain tumor detection methods. Among the 30 papers 11 papers utilize the MRI dataset, 1 paper utilizes the publicly available dataset, 5 papers utilize the brain tumor dataset, 4 papers utilize the BraTS dataset. Figure 2 depicts the chart based on the analysis of the datasets for the determination of brain tumor.

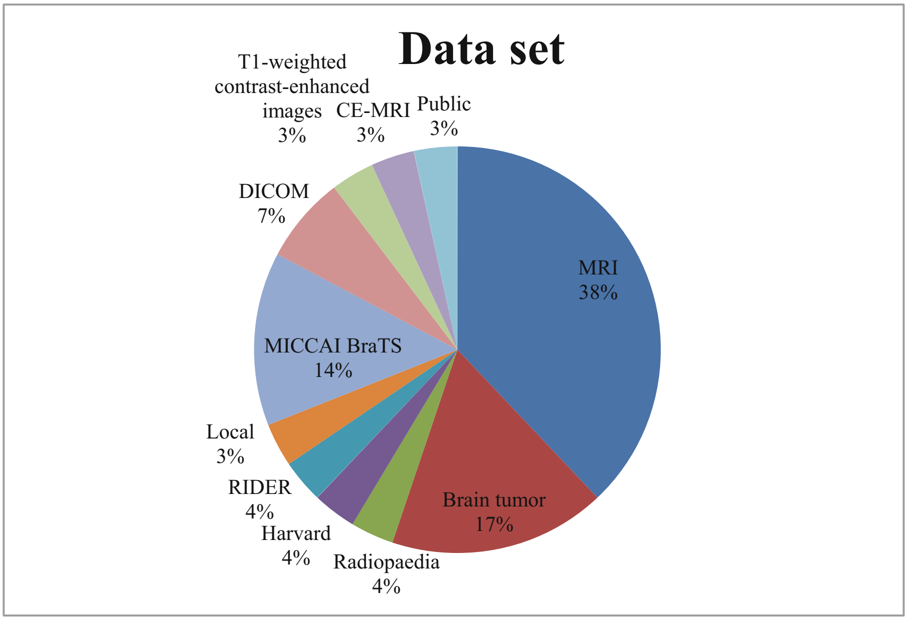


Fig. 2. Analysis based on different datasets

3.2 Analysis based on Performance Metrics

In this the evaluation of the research papers in terms of performance indices utilized in the brain tumor classification method is demonstrated. The Mean absolute error (MAE), Mean Absolute Percentage Error (MAPE), Relative Absolute Error (RAE), Root Relative squared Error (RRSE), Mean Percent Error (MPE), False Acceptance Ratio (FAR), and False Rejection Rate (FRR) are the commonly utilized performance metrics. The Accuracy is the widely accepted parameters utilized for the brain tumor classification technique. Figure 3 shows the evaluation with respect to the performance metrics.

4 Existing Gap and Challenges

The challenges and the limitations experienced in the convolutional brain tumor detection method mentioned in the review article are demonstrated in this section.

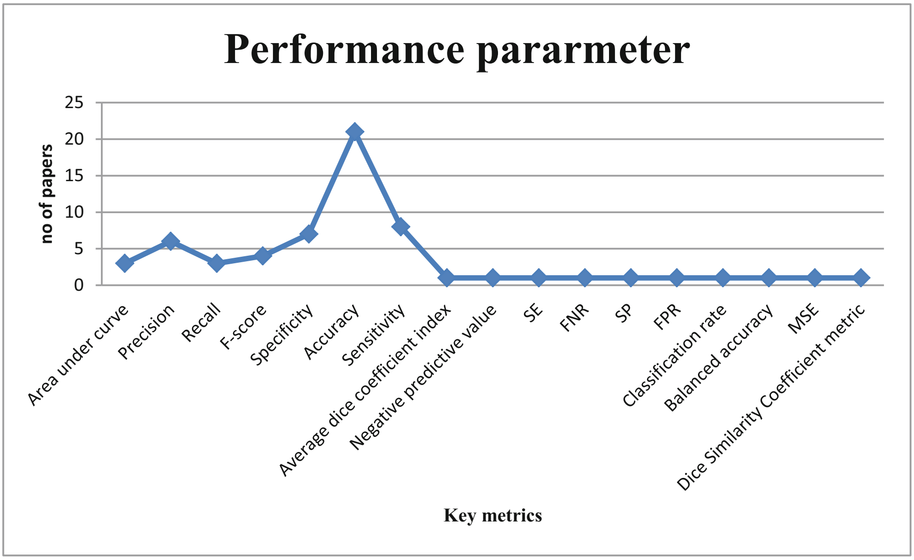


Fig. 3. Analysis based on performance indices

4.1 Challenges Experienced in Deep Learning Techniques

Shortcomings

Some of the DL techniques such as transfer learning experience poor performance due to the lack of self-sustained classifiers. Their improper data in the DL techniques will lead to miss- categorization of the samples. The overfitting issue due to insufficient data is one of the hectic challenges experienced in DL techniques.

Future Work

Need to develop an effective data augmentation technique so as to handle the problems such as overfitting, mis-classification and poor performance of the classifier the aforementioned issues.

4.2 Challenges Experienced in Machine Learning techniques

Shortcomings

The ML techniques established for brain tumor classification techniques show low accuracy as it is not suitable for large datasets. The high computational complexity and large execution time due to the high dimensional data.

Future Work

The selective strategy needs to be developed so as to combine more than one classifier to enhance the effectiveness of the classifier. A dynamic algorithm is needed to be developed which increases the performance of the classifier by reducing the computational complexity and the execution time.

5 Conclusion

In this survey, various literature works evaluated concentrating on classification problems associated with the brain tumor using MRI, bringing into light the various shortcomings of the existing methodologies for classification problems. Here, the analysis of various methods facilitated based on several factors, such as performance metrics, the dataset used in the research papers and so on. In the above methods, enhanced deep learning model proven better accuracy than any other method. On the other hand, the analysis of the methods with respect to the their merits and demerits are presented. Finally, the paper elaborates the prospective future research directions and provocations in obtaining the better classification accuracy for the MRI brain tumor categorization.

References

1. Deepak, S., Ameer, P.: Brain tumor classification using deep CNN features via transfer learning. Comput. Biol. Med. **111**, 103345 (2019)
2. Usman, K., Rajpoot, K.: Brain tumor classification from multi-modality MRI using wavelets and machine learning. Pattern Anal. Appl. **20**, 871–881 (2017)
3. Sajjad, M., Khan, S., Muhammad, K., Wu, W., Ullah, A., Baik, S.: Multi-grade brain tumor classification using deep CNN with extensive data augmentation. J. Comput. Sci. **30**, 174–182 (2019)
4. Roy, S., Sadhu, S., Bandyopadhyay, S., Bhattacharyya, D., Kim, T.: Brain tumor classification using adaptive Neuro-Fuzzy inference system from MRI. Int. J. Bio-Sci. Bio-Technol. **8**, 203–218 (2016)
5. Bahadure, N., Ray, A., Thethi, H.: Comparative approach of MRI-based brain tumor segmentation and classification using genetic algorithm. J. Digit. Imaging **31**, 477–489 (2018)
6. Parnian, A., Konstantinos, N., Arash, M.: Capsule networks for brain tumor classification based on MRI images and coarse tumor boundaries. In: IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 1368–1372 (2019)
7. Lavanyadevi, R., Machakowsalya, M., Nivethitha, J., Kumar, A.: Brain tumor classification and segmentation in MRI images using PNN. In: IEEE International Conference on Electrical, Instrumentation and Communication Engineering (ICEICE), pp. 1–6 (2017).
8. Rafia, H., Entin, M. Tita, K.: Brain tumor classification using MRI images with K-nearest neighbor method. International Electronics Symposium (IES), pp. 660–667. IEEE (2021)
9. Amin, J., Sharif, M., Gul, N., Yasmin, M., Shad, S.: Brain tumor classification based on DWT fusion of MRI sequences using convolutional neural network. Pattern Recognit. Lett. **129**, 115–122 (2020)
10. Mohsen, H., El-Dahshan, E., El-Horbaty, E., Salem, A.: Classification using deep learning neural networks for brain tumors. Future Comput. Inf. J. **3**, 68–71 (2018)
11. Abdelaziz Ismael, S., Mohammed, A., Hefny, H.: An enhanced deep learning approach for brain cancer MRI images classification using residual networks. Artif. Intell. Med. **102**, 101779 (2020)
12. Amin, J., Sharif, M., Yasmin, M., Fernandes, S.: A distinctive approach in brain tumor detection and classification using MRI. Pattern Recognit. Lett. **139**, 118–127 (2020)
13. Nawab, Z., Swati, K., Zhao, Q., Kabir, M., Ali, F., Ali, Z., Ahmed, S., Lu, J.: Brain tumor classification for MR images using transfer learning and fine-tuning. Comput. Med. Imaging Graph. **75**, 34–46 (2019)

14. Rehman, A., Naz, S., Razzak, M., Akram, F., Imran, M.: A deep learning-based framework for automatic brain tumors classification using transfer learning. Circuits, Syst., Signal Proces. **39**, 757–775 (2019)
15. Chandan, S., Foisal, H.: MRI brain tumor images classification using K-means clustering, NSCT and SVM. In: 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON), pp. 329–333 (2017)
16. Deepak, S., Ameer, P.: Automated categorization of brain tumor from MRI using CNN features and SVM. J. Ambient Intell. Humanized Comput. **12**, 8357–8369 (2020)
17. Çinar, A., Yildirim, M.: Detection of tumors on brain MRI images using the hybrid convolutional neural network architecture. Med. Hypotheses **139**, 109684 (2020)
18. Osman, A.A.A, W.: MRI brain image classification using neural networks. In: Proceedings of İnternational Conference on Computing, Electrical and Electronic Engineering (ICCEEE), pp. 253–258. IEEE (2013)
19. Kumar, S., Dabas, C., Godara, S.: Classification of brain MRI tumor images: a hybrid approach. Procedia Comput. Sci. **122**, 510–517 (2017)
20. Arunkumar, N., Mohammed, M.A., Mostafa, S.A., Ahmed Ibrahim, D., Rodrigues, J.J.P.C., de Albuquerque, V.H.C.: Fully automatic model-based segmentation and classification approach for MRI brain tumor using artificial neural networks. Concurrency Comput.: Pract. Experience **32**, e4962 (2020)
21. Narmatha, C., Eljack, S., Tuka, A., Manimurugan, S., Mustafa, M.: A hybrid fuzzy brain-storm optimization algorithm for the classification of brain tumor MRI images. J. Ambient Intell. Humanized Comput. (2020)
22. Varuna Shree, N., Kumar, T.: Identification and classification of brain tumor MRI images with feature extraction using DWT and probabilistic neural network. Brain Informatics. **5**, 23–30 (2018)
23. Sultan, H., Salem, N., Al-Atabany, W.: Multi-classification of brain tumor images using deep neural network. IEEE Access **7**, 69215–69225 (2019)
24. Gumaei, A., Hassan, M., Hassan, M., Alelaiwi, A., Fortino, G.: A hybrid feature extraction method with regularized extreme learning machine for brain tumor classification. IEEE Access **7**, 36266–36273 (2019)
25. Pereira, S., Pinto, A., Alves, V., Silva, C.: Brain tumor segmentation using convolutional neural networks in MRI images. IEEE Trans. Med. Imaging **35**, 1240–1251 (2016)
26. Verma, K., et al.: Latest tools for data mining and machine learning. Int. J. Inno. Tech. Exp. Engi. **8**, 24–28 (2019)
27. Pathan, S., Bhushan, M., Bai, A.: A study on health care using data mining techniques. J. Crit. Rev. **7**, 7877–7890 (2020)
28. Singh, V.J., Bhushan, M., Kumar, V., Bansal, K.L.: Optimization of segment size assuring application perceived QoS in healthcare. Lect. Notes Eng. Comput. Sci. **2217**, 274–278 (2015)
29. Arya, R., Kumar, A., Bhushan, M.: Affect recognition using brain signals: a survey. Adv. Intell. Syst. Comput. **1257**, 978–981 (2021)
30. Odusami, M., Maskeliunas, R., Damaševičius, R., Misra, S.: Comparable study of pre-trained model on alzheimer disease classification. In: Gervasi, O., et al. (eds.) Computational Science and Its Applications – ICCSA 2021: 21st International Conference, Cagliari, Italy, September 13–16, 2021, Proceedings, Part V, pp. 63–74. Springer International Publishing, Cham (2021). https://doi.org/10.1007/978-3-030-86976-2_5

Obstacle Finding and Path Planning of Unmanned Vehicle by Hybrid Techniques

Varsha Dubey, Snehlata Barde(✉), and Brijesh Patel

MSIT, MATS University, Raipur, C.G 492004, India
v.snehabarde@gmail.com

Abstract. With the wide application of unmanned vehicles (UV) in a complex environment, the research on path optimization and obstacle detection system has gradually become an important research part in the field of unmanned vehicle (UV) systems. The basic concept of path planning methods has always been a basic and difficult problem, especially in complex environments, in the effect of the dynamic environment, the safety, smoothness, and real-time requirement. To perform the task in a different environment and follow the exact movement and find the accurate path as well as remove the minimum human hurdle. In this research paper to find the shortest path with the avoidance of human obstacles with optimization techniques with meta-heuristic algorithms such as A*, fuzzy logic, GA, etc. we compare A* and fuzzy logic algorithms with the terms of processing time and path length with obstacle detection for high traffic areas. This research paper was practically implemented by the MATLAB software to simulate UV traversing from starting to endpoints.

Keywords: Unmanned vehicle · A* · Fuzzy logic · Navigation

1 Introduction

In the recent era Path planning is the new concept of the research area. In path planning, we find the shortest path between starting point to the ending point [1, 2]. It is recent time to find the destination path in a different way to find the path to navigate the path root. As unmanned vehicles (UV) have to define different parameters used in traversing like path, path planning, and navigation it's an important parameter of UV, they allow them to perform intelligently and compute the shortest optimum path between a starting position to an end position to fulfill their task with specific parameters such as path length, timing, and obstacle detection, etc., as path planning is also related to obstacle avoidance. In recent times Path planning process concept development has rapid growth and the path planning problem has been solved especially with the help of various genetic and meta-heuristic algorithms happening in recent days, such as the gray-wolf algorithms, ant colony advance algorithm, swarm intelligence, firefly, etc.

In recent researcher various meta-heuristic algorithms used to find an optimal solution such as the firefly algorithm which gives the accurate result provide, for example,

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 28–36, 2023.
https://doi.org/10.1007/978-3-031-13150-9_3

ants, bees, glowworms, etc. to provide optimum results. An inspirational swarm intelligence algorithm that was inspired by the behavior of ant colonies for solving combinatorial optimization problems is ant colony optimization (ACO), which provides optimal results for an effective environment. ACO works cooperatively to reach the optimal solution to a problem on the basis of effective environment colonies of artificial ants. Ant colony optimization to communicate with other ants accepted ants through.

A Fuzzy algorithm has been evolved the decision based on the environment. It evolved in the path optimization techniques of UV but the limited possibilities have to be compared and analyzed [3].

In AI different metaheuristic algorithm concepts were used in this paper we used the A* algorithm. In A* algorithm is a metaheuristic type of algorithm. We execute the A* algorithm in high configuration processors were used to execute starting nodes to ending nodes and checking various nodes in respectively. If the finding the root note to destination node involves and compare to starting nodes to adjacent node one after another then increasing the processing time [4].

In this paper, we introduced the concept of A hybrid path planning algorithm is proposed to optimum path planning techniques. A hybrid technique is used for global path planning and local path planning to optimization is used continuously. Path planning is a combination of navigation and path optimization. We see several types of research related to path optimization techniques [5].

In this paper, we make a new A*-fuzzy–based hybrid approach for finding a property such as shortest path planning and obstacle detection for UV in various environments and analyze and compared it to a performance of individual algorithm performance and execute hybrid controller. Secondly, we compare path length and time was done for the hybrid algorithm in different environments. In this paper sections 3 and 4 explain the A* and Fuzzy logic are described. In Sect. 5, describe the practically implemented work and experimental analyses on the results of the individual algorithm and develop a new hybrid algorithm. In Sect. 6, the results and conclusion part are described.

2 A* Methodology

A In AI techniques we execute the path finding mechanism to use the A* algorithm. A* techniques to use the traversing the starting point to ending point and finding the best shortest path. To find the shortest path we used different applications to it is used in various applications, such as maps. or tree traversing in maps we used finding the shortest distance between the initial state to final state.

Here we explain a small square grid which shows the many obstacles, and hurdles in this grid we show the starting and ending cell is indicated. The main purpose of this grid cell is to reach the final cell in a little amount of time. Here A* Search Algorithm techniques shown in Fig. 1:

2.1 Parameters of A* Algorithm

g: is the calculating the cost moving initial cell to current cell. And finally, we calculate the sum of all the cells that have been visited and leaving the first cell.

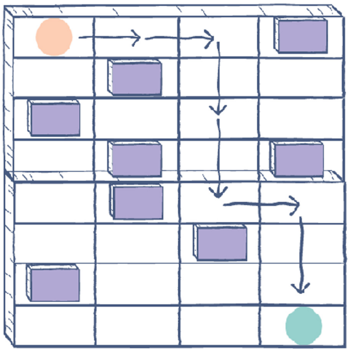


Fig. 1. Process of A* algorithm

h: is represent the heuristic value, it is the calculated cost of o moving from the current cell to the final cell. The actual cost will be calculated throw the traversing of the last cell. Hence, h is the estimated cost to be found.

f: it is the sum of all the cell(g) and heuristic value(h). Then we make one formula so, f = g + h.

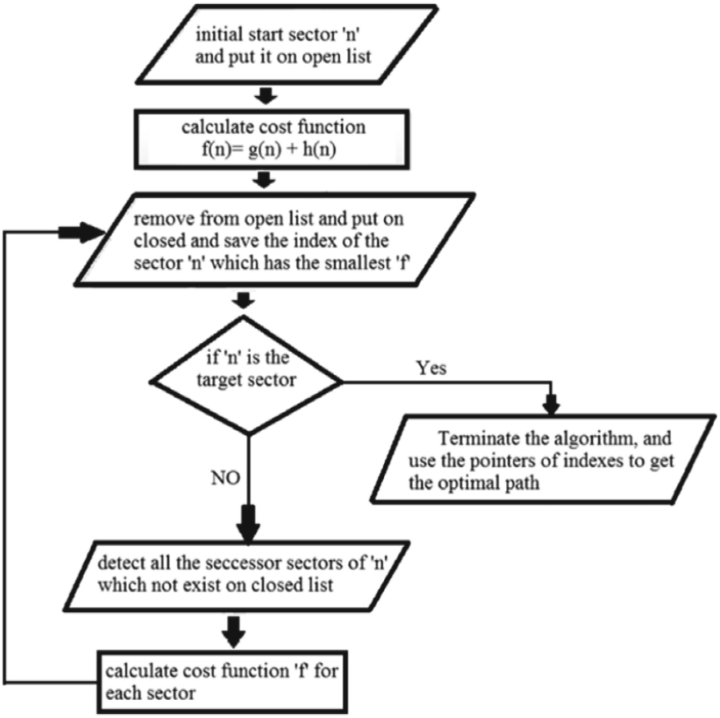


Fig. 2. Flowchart of A* algorithm

This parameter of this algorithm makes its result is by taking the f-value into account. The algorithm selects the smallest f-valued cell and moves to that cell. This process continues until the algorithm reaches its goal cell. Figure 2 shows the A* algorithm model is from the flow chart.

3 Fuzzy-Logic Algorithm

Firstly introduced the concept or origin of Fuzzy logic methods and it was developed by Lotfi Zadeh in the year 1965 [7], and explain their mechanism based on human decisions like yes or no or if-else. Fuzzy logic concept of the various factors that are dilemma and it gives a real decision representation by its if-else, rule-based mechanism. Its working depends on unclear and randomly partial data for different problems. Fuzzy logic models complex data problems with maximum uncertainty to the linear one. The basic fuzzy logic working model is explained in given below in the form of a flowchart (Fig. 3).

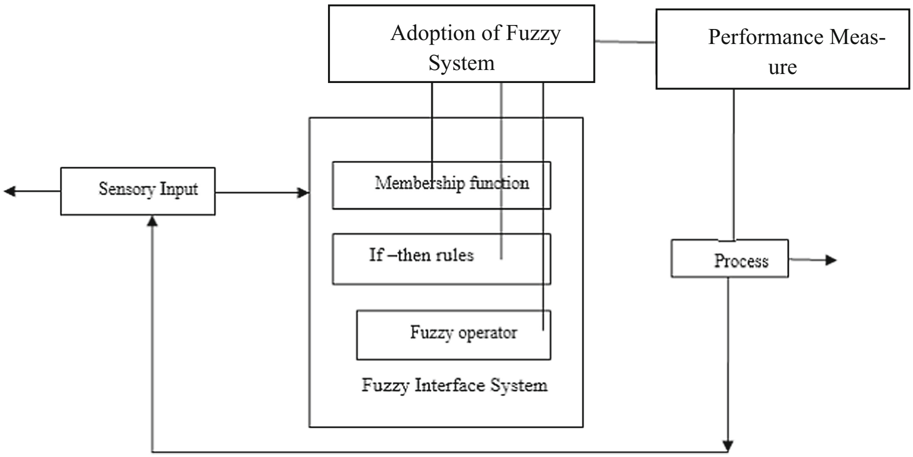


Fig. 3. Flow chart of fuzzy system

Basic Parameters of fuzzy logic are given as follows:

Fuzzification: It is represented the input variables are defined by a membership function.
Inference and Aggregation: Its parameter shows the Final output to the fuzzy rules.
Defuzzification: Its Crisp value converted from fuzzy-based output will be found.

4 Fuzzy Inference Parameter

The concept of fuzzy inference basic mapping techniques use the input data with the output variables, In fuzzy inference basically, the if–then rule is used. It is also the base for its decision-making. Let them calculate the different objects(x) denoted by X and x be the fuzzy set A to known ordered pair.

$$A = \{(x, \mu A(x) e X\} \tag{1}$$

For Eq. (1), μA (x) defines the fuzzy membership function provided for set A. In other, the membership values used to measure x will be 0 to 1. In the concept of basic fuzzy logic problem to solved by two types of function, i.e., trapezoidal and triangular.

The triangular membership function is explained below as follows.

$$\begin{cases} 0, x < p \\ \frac{x-p}{q-p} \quad p \le x \le q \\ \frac{r-x}{r-q} \quad q \le x \le r \\ 0, r \le X \end{cases} \tag{2}$$

As per the given equation to explain the principle of maxima and minima, Equation (2) can be represented by

$$\text{Triangle(x, p, q, r)} = \max(\min.\{\frac{x-p}{q-p}, \frac{r-x}{r-q}\}, 0) \tag{3}$$

Similarly, the given trapezoidal function can be explained by using the four-parameter {p, q, r, s} as represented in Equation (4) is given below.

$$\begin{cases} 0, x < p \\ \frac{x-p}{q-p} \quad p \le x \le q \\ \frac{s-x}{s-r} \quad 1, q \le x \le r \\ \quad\quad r \le x \le s \\ 0, s \le X \end{cases} \tag{4}$$

Here with four variables (p, q, r, s) determines the values of the x-coordinates(with p < q < r < s) of the corners of the defuzzification-trapezoidal membership function will be explained.

4.1 Concept of Defuzzification

The concept of the Defuzzification mechanism to explain the basic concept of mathematically represented as in the equation given below, which works to explain the center of gravity concept and converts the fuzzy set into a crisp value.

$$\mu^{crisp} = \frac{\sum ibi \int \mu \mathrm{i}}{\sum i \int \mu \mathrm{i}} \tag{5}$$

The above crisp value output is defined by and the definition and explains the center of the membership function is given by bi. Consequently, rules i and μ (i) give the area under the given in membership function.

5 Concept of Hybrid A*-Fuzzy Controller

In this section, we explain the basic concept of A*-fuzzy controller is a hybrid controller using A* and fuzzy mechanism for optimizing different parameters in a different way.

Here we explain the concept of the A* search algorithm used for pathfinding to navigate the best path root. The A* algorithm to traversing the starting node to the destination node to calculate the weight of the positioning node and traverses the next node and calculates the cost of a node in the traversal.

The above equation to calculate the total fitness can be expressed as:

$$F(n) = g\ (n) + h\ (n) \ldots\ldots (1)$$

Here are explain the given variables as g(n) = the total distance between the starting position to the current location and h (n) = the distance from the current position to the goal point.

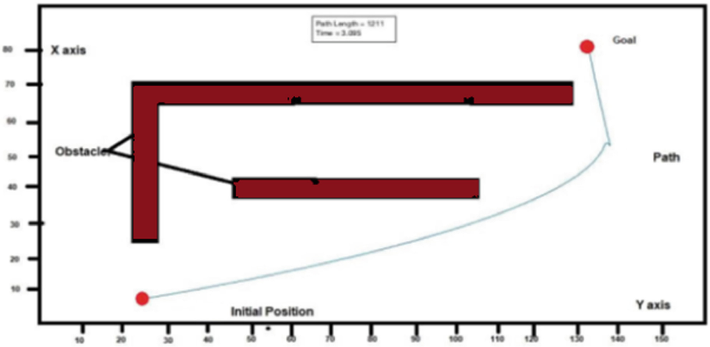
This is the concept of the sum of the cost of the path planning from starting to current nodes position and an estimation of the cost and defines the current node to the final node. The average cost must always be less or equal to the actual cost or it cannot be classed as an admissible heuristic.

In this section we explain the new concept of path finding to hybrid method. And combine the A* and fuzzy logic method and design the new concept of hybridization.

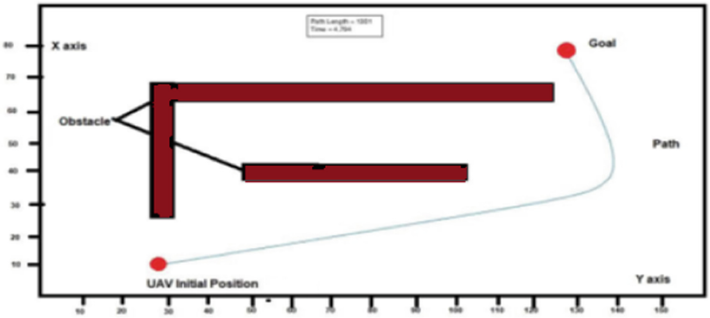
6 Analysis and Result of A*-Fuzzy Hybrid Controller

The A*-Fuzzy Hybrid Controller was executed by experimental work which was simulation through MATLAB software, for the execution of controller work, and execution platform MATLAB software was used and the result was provided for both static and dynamic obstacles in different environmental parameters.

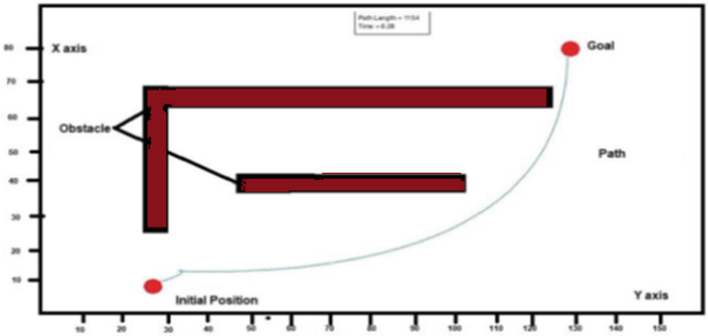
In the below figures, the executed grid maps are plotted according to parameters. The obstacles are shown with black circles and the red-dotted line indicates the best path. The blue and green points are presented in the original and moved aim points when necessary. The starting point path of the vehicle which is executed finally is shown as a red as destination solid line. When following the path generated in the high-level model in Figs. 4. The below three figures show simulations with individual controllers along with hybrid controllers (Table 1).



(a)



(b)



(c)

Fig. 4. Simulation results using (a) A* hybrid controller(A1), (b) Fuzzy controller(A2), (c) A* fuzzy hybrid controller (A3)

In the above table we show the performance of three algorithms with time and distance parameters.

Table 1. The results of the simulation

Performance	*A1*	*A2*	*A3*
Times (ms)	116	151	100
Distance (m)	9352	9126	8556

Also, the simulation was done using the A*hybrid controller for moving obstacle, whose simulation results is given in Fig. 5.

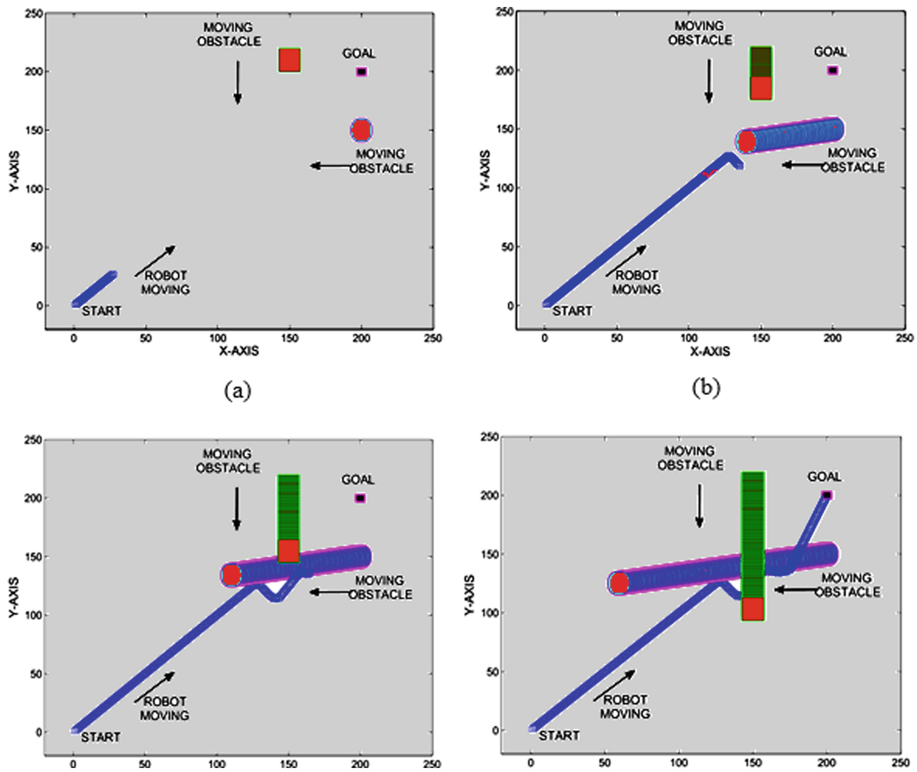


Fig. 5. Simulation of A*Fuzzy hybrid controller with moving obstacle

7 Conclusion and Future Work

In this research paper, we execute the experiment and simulation result was found and there are many possibilities to found and developing a hybrid controller to find optimal results, in this paper through the successful execution of A*-Fuzzy Logic-based new controller for navigating of a UV in the started obstacle detection and pathfinding with respect to time and distance parameter per with a static environment. In the simulation section and experimental result are found the path obtained by the new hybrid controller to compare a standalone controller for both static and dynamic environments. A1 covered 9352 m in 116 ms, A2 covered 9126 m in 151 ms, and covered 8556 m in 100 ms.

In this result we found future work, like more metaheuristic and genetic algorithms like a binary gray wolf; gray wolf etc. can be tested for more optimal results. In this research, this experimental work was done with a static obstacle so for future work the hybrid controller would be tested for the dynamic obstacle.

References

1. Hutchinson, S.A., Kak, A.C.: Planning sensing strategies in a robot work cell with multi-sensor capabilities. IEEE Trans. Robot. Autom. **5**, 765–783 (1989)
2. Alexopoulos, C., Griffin, P.M.: Path planning for a mobile robot. IEEE Trans. Syst., Man, Cybern. **22**(2), 318–322 (1992). https://doi.org/10.1109/21.148404
3. Ferdaus, M.M., Anavatti, S.G., Pratama, M., Garratt, M.A.: Towards the use of fuzzy logic systems in rotary wing unmanned aerial vehicle: a review. Artif. Intell. Rev. **53**, 257–290 (2018)
4. Guruji, A.K., Agarwal, H., Parsediya, D.K.: Time-efficient A* algorithm for robot path planning. In: 3rd International Conference on Innovations in Automation and Mechatronics Engineering vol. 23, issue 3, pp. 144–149. ICIAME (2016)
5. Abbas, N.H., Saleh, B.J.: Design of a kinematic neural controller for mobile robots based on enhanced hybrid firefly-artificial bee colony algorithm. Al-Khwarizmi Eng. J. **12**(1), 45–60 (2017)
6. Abbas, N.H., Ali, F.M.: Path planning of an autonomous mobile robot using enhanced bacterial foraging optimization algorithm. Al-Khwarizmi Eng. J. **12**(4), 26–35 (2016)
7. Zadeh, L.A.: Fuzzy sets. Inform. Control **8**, 338–353 (1965)
8. Singh, K.K., Barde, S.: Fuzzy logic in terms of biometrics. i-manager's J. Image Process. **7**(4), 17–23 (2020)
9. Ranade, S., Manivannan, P.V.: Quadcopter obstacle avoidance and path planning using flood fill method. In: 2019 2nd International Conference on Intelligent Autonomous Systems (ICoIAS), pp. 166–170 (2019). https://doi.org/10.1109/ICoIAS.2019.00036.
10. Ali, Z.A., Wang, D., Aamir, M.: The Fuzzy-based hybrid control algorithm for the stabilization of a Tri-Rotor UAV. Sensors **16**, 652 (2016)
11. Barde, S., Singh, K.K.: Role of fuzzy in multimodal biometrics system. Int. J. Res. Appl. Sci. Eng. Technol. (IJRASET) **8**(IV), 1041–1047 (2020)
12. Pochmara, J., Grygiel, W., Koppa, R., Kamiński, K.: Mobile robot platform for real-time search algorithms. In: Proceedings of the 20th International Conference Mixed Design of Integrated Circuits and Systems - MIXDES 2013, pp. 615–620 (2013)
13. Kala, R.: Mobile robot navigation control in moving obstacle environment using genetic algorithm, artificial neural networks and A* Algorithm. In: Proceedings of the IEEE World Congress on Computer Science and Information Engineering, Los Angeles/Anaheim, USA, pp. 705–713 (2009)

Simulation of Internet of Things Network for Big Data Analytics

B. C. Manujakshi[1](✉), K. B. Ramesh[2], Lalit Garg[3], and T. M. Shashidhar[4]

[1] Department of Computer Science and Engineering, Presidency University, Bengaluru, Karnataka, India
manujakshibc@gmail.com

[2] Department of Electronics and Instrumentation Engineering, RV College of Engineering, Bengaluru, Karnataka, India

[3] Department of Computer Information Systems, University of Malta, Msida, Malta

[4] Department of Computer Science and Engineering, Acharya Institute of Technology, Bengaluru, Karnataka, India

Abstract. In recent years there has been a tremendous amount of data generated from various wireless sensor networks. These sensor networks generate a large volume of data. Traditional data processing systems do not process these data. An effective analytical model is required for efficient design and implementation of WSN's and the data collection, processing, and analytics to process this type of data. The complex data collected from the sensors can be called big data. Drawing the insights from the data collected is a challenging task in real-time analysis. This paper discusses big data characteristics, types of data analytics and their applications in the IoT environment. All the WSN's consist of sensing devices associated with few resources, and they are connected wirelessly. As a part of IoT analysis, in this paper Contiki operating system is used along with the Cooja simulator to simulate an IoT network. The number of motes can be used to communicate with each other. This paper focuses on IoT generation and its analysis using Hadoop framework tools.

Keywords: Big data · Data Analytics · IoT · IoT Analytics · Mapreduce

1 Introduction

There is a massive data generation with the emerging trend and modernised world and ubiquitous of various commercial applications. The information generated from many digital sources is growing very fast and shared on the internet [1]. Modern sensor applications like IoT are evolving tremendously. This data is of concern in every sector. Big data is a term used when there is a requirement to handle nontraditional data. As big data evolves, there is a large complex volume of data generated from multiple sources. There is a networking evolvement due to which it is becoming challenging to store the big data. All the engineering, medical domains are generating an enormous amount of data [2]. Big data is a combination of structured, semi- structured and unstructured data. A big

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 37–48, 2023.
https://doi.org/10.1007/978-3-031-13150-9_4

data system can be used to analyse and get insights from them. The big data evolution leads to a few new challenges like data storage, processing, and analysis, leading to the growth of cloud computing and the Internet of Things (IoT) [3]. It always gives good decisions and strategic business ideas. Big data for any organisation can be mined for any information as per the requirements of the end-users.

The raw data generated from any network is not helpful for any of the predictions and decisions. This data needs to be analysed on the collected data. Big data analytics should extract large datasets to predict, visualise and optimise the data. This helps to make proper decision making and acquire the knowledge [4]. In any wireless sensor network, sensors gather complex data. It is not easy to understand how it helps data analysis because of its complexity in size, heterogeneity etc. It leads to many problems for sensor data analytics in the cloud environment [5]. In [6], An IoT environment is built based on localised data processing and decision making. This framework provides efficient management for the local sensor network.

Internet of things provides the platform for sensors to communicate in the network area. It helps to share the information effectively. IoT is an emerging technology in wireless and internet technology. There is a lot of applications for the internet of things. The smart city is one among them. The IoT can be applicable for other applications like healthcare, transportation, agriculture etc. All the organisations are interested in extracting meanings from the collected raw data. So the data analytics plays a significant role in industries and organisations.

2 Importance of Bigdata

Nowadays, in day-to-day life, we can see a large amount of data generated by various sources. This large data set can be accumulated in the systems, improving its operations and providing better customer services. This data set provides the companies or business sectors with valuable insights about the customers that can refine the business marketing by adopting still better techniques to increase customer engagement. A massive amount of data is generated by smart city applications. Big data systems utilise this type of data to provide information to enhance smart city applications. The big data frameworks are used to store, process and mine the stored data efficiently to produce information to improve the services [7].

According to [8], there is a tremendous demand for big data analytics in the transportation sector like railway. Every passenger wants any service to be reliable, service-oriented. This can be made possible by adopting big data services. Usage of big data technology benefits the companies for taking proper decisions.

Few more remarkable applications of bigdata are,

- It enables companies to give customer-centric services.
- It gives the historical, real-time data analysis that can be used to assess the consumers' requirements.
- It enables business people to adopt various business strategies to meet the customer's desires and needs.
- Many medical researchers can use big data analysis to understand the different types of diseases and their risk factors which doctors can use to diagnose illness.

- Financial companies use big data systems for real-time analysis of data and other risk management.
- Different government sectors may use big data for immediate and emergency responses, preventing crimes and other smart city applications.

3 Characteristics of Bigdata

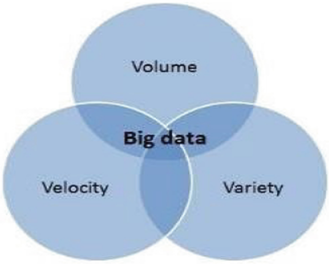


Fig. 1. Three V's in Bigdata

The big data term is used for nontraditional strategies and techniques which gather, organise and process the data. The gathered insights from a massive dataset of data with different types will be used for future decisions. It is required to have enormous computing power to work with such a large dataset. The traditional tools cannot store and process large dataset on a single computer. The characteristics should describe the requirement of big data technologies.

As the data is growing very fast, every company or organisation is facing few significant issues. The issues are related to data, its storage, processing and how to manage it. Proper storage techniques need to be adopted. The processing of the data may relate to how to analyse the data as per the requirement. What kind of algorithms are to be applied. The management issues related to the architectures to be used and infrastructures to be adopted [9].

The data which is to be processed by the analytics is not similar to the traditional data. Because of the type of data we call variety, the data volume means the data generation speed [10]. The three V's describe the main characteristics that make big data different from other data processing techniques.

3.1 Volume

The large scale of the information that needs to process the work required exceeds the single computer capabilities can be referred to as a large volume of data. The groups of computers help process the large volume of data.

3.2 Velocity

Big data makes its way different from other databases is because of the speed through which the information is obtained. From multiple sources, the data will be flowing continuously in real- time. This real-time data needs to be analysed to gain insights from it. The best example of this could be in the IoT system.

3.3 Variety

Big data systems are always unique compared to other systems. It involves a wide range of sources being processed and collected. This data can be collected from various applications like social media data. Physical device sensors provide big data seeds to handle such large datasets having a variety of data. It may consist of structured, semi-structured and unstructured data. But all such data storing and processing is not possible by traditional data processing. So there is a challenge to handle such types of data.

The other characteristics that differentiate big data from normal data are veracity, variability and value. The veracity includes the various sources and the level of complexity involved in processing the data. The variability defines the variation in data quality. The main goal of the data is to extract knowledge. So the delivery of value is the primary concern in any big data system.

4 Data Analytics and its Types

Big data analysis examines an enormous volume of data about the hidden patterns, correlation and market trends. The customer preferences can be checked, and it helps the organisations to make better business decisions. The analysis helps to perform complex applications with elements like predictive models. Data analytics gives positive business outcomes by enhancing effective marketing and better customer services. The analysis exists because of its variety and velocity from various sources.

The entire process of analysing the data involves collecting the data, organising the data, and analysing large data sets to discover different data patterns and other information. Any data analysis involves technologies and techniques that require collecting large values from large data sets, complex and large in scale.

Once there is an enormous amount of data, then getting insights from it is a significant concern. Data analytics is the science involved in analysing the raw data to extract valuable conclusions and decisions. Many companies depend on this analytics to make better business decisions and verify or approve or disapprove of the existing models [12]. There are mainly four types of data analytics.

4.1 Descriptive Analytics

It is the first stage of data processing. It generates a set of historical data. Data mining methods used to organise the data and make the patterns to give insights out of it. This type of analysis provides different probabilities, trends and offers future analysis.

4.2 Diagnostic Analysis

It takes the descriptive analysis insights and observes and understands its causes, events, and behavioural changes.

4.3 Predictive Analysis

In this method, past data is used to predict the future. That means forecasting can be done. Data mining techniques are adopted to perform this analysis. AI techniques are used to analyse the data and extract knowledge from it.

4.4 Prescriptive Analysis

This analysis always uses the descriptive and predictive analysis outcome and uses it to find the best solutions.

5 Data Analytics in IoT: Simulation using Contiki OS and Cooja Emulator

As discussed in the above section, IoT and data are invariably linked together. Nowadays, data consumed and produced is kept growing at an exponential rate. IoT is an interconnection of several devices, network technologies that generates a large volume of data. The data generated from these devices will always be helpful if it is analysed. This brings the data analysis into an IoT system. The meaningful conclusions have drawn from the data analysis always acts as actionable insights. These conclusions are often valuable for trends, statistics, and patterns that aid business organisations in using these insights and effectively implementing efficient decision-making processes.

According to [13], big data is generated from many web-enabled things. The query processing on such unstructuredness in the data is a complicated task. So the organisations will be expecting a better analytical platform for the data analysis to gain valuable insights and make quick decisions.

IoT Sector is emerging very fast. The applications of IoT can be seen in all fields. Each and everything can be made smarter with the use of IoT. This happens because devices communicate with each other, carry the work independently and give the expected results. An IoT application using Contiki OS and Cooja emulator for a network is shown in Fig. 2. It offers an energy- efficient solution by collecting the data and managing it as per the requirement. The Contiki OS is a lightweight open-source operating system for the Internet of Things [14]. The OS is written in a C programming language. The Contiki is highly portal. It is ported to many platforms [15]. The Cooja is the network simulator in the Contiki operating system [16]. Many IoT projects need to understand sensors working, generate the data using Contiki, and use the collected data for analysis.

In this proposed simulation work using Contiki operating system and Cooja emulator, it is possible to simulate the data collected and transmitted using any sensors. We can see how the network nodes will be communicated to each other and transfer the required information. The Contiki operating system with the Cooja emulator acts as an

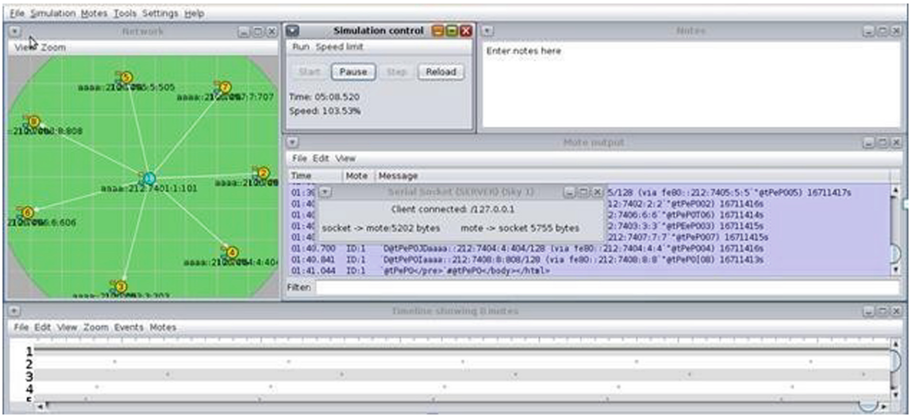


Fig. 2. IoT Simulation to get the temperature

open-source simulation for any smart device, not being expensive. It gives low power consumption and collects a large amount of data.

Figure 2 shows the simulation with the Cooja emulator with many windows. In the left corner of the simulation, we can see the "Network" window. In this, we can see the network topology. This window will notify that there will be access to every other node in the network to configure it and do the measurement. The second window in Fig. 2 is the simulation control window, used to control the simulation, like start, pause, move a step forward, and reload the simulation. In this top right corner, we can find another window called the "Notes" window used to write any notes regarding the simulation. The middle window is the "Mote Output" window, which gives all the serial ports' nodes. The last window is the "Timeline" window, and it will be created when a new simulation is initiated.

The sensors measure the temperature, humidity, pressure, light movement. A cloud server helps to manage the building or home and store the information from the sensors. The motion sensor analysis makes it easy to see and understand a home or a building's requirement to fulfil the person's needs or a thing at home or a building. This simulation is carried out to build an energy- constrained IoT environment using 'n' number of sky motes and RPL border router as a routing protocol for low power networks. This RPL border router use made visible at the edge of any network. This RPL border router is mainly used to route data between any wireless sensor network, i.e. RPL network and the IP network acting as an external network.

Simulation is done using the Cooja simulator to detect the temperature at each node. This simulation can be kept for a long duration to read all the sensors data and analyse it. The address of the border router has to be set using the ping command. Ping can be used for any one of the nodes in the network. Figure 3 shows the IPv6 addresses to be used to get the routes of each node. Figure 4 describes the temperature and light analysis for the selected node. Selecting the particular node address makes it possible to view and analyse the sensor data as per the requirement.

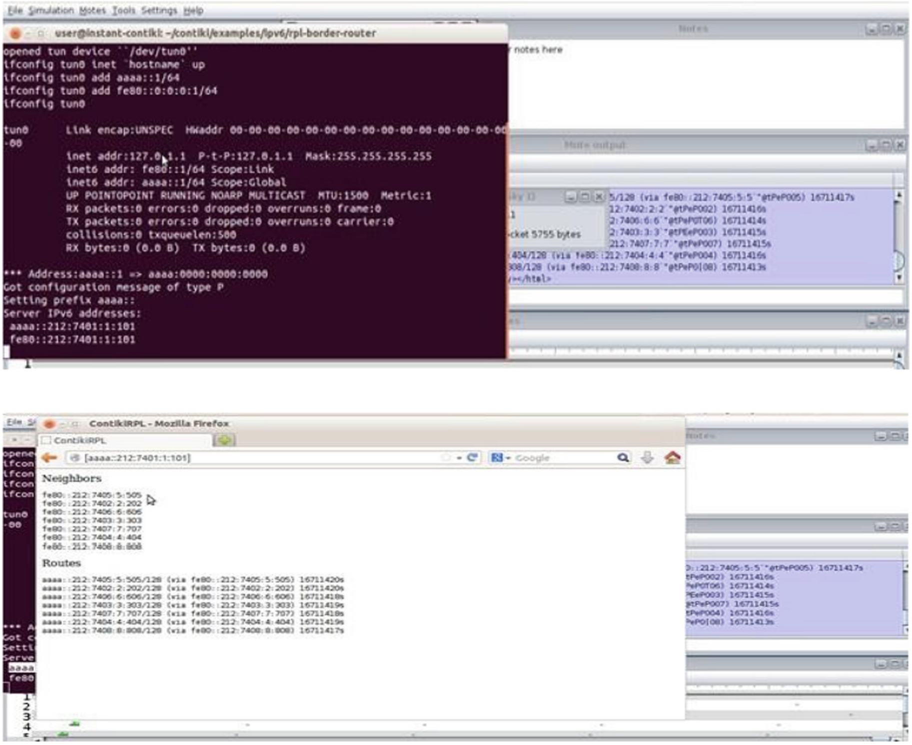


Fig. 3. IPv6 Server Address and neighbouring routes in the simulation.

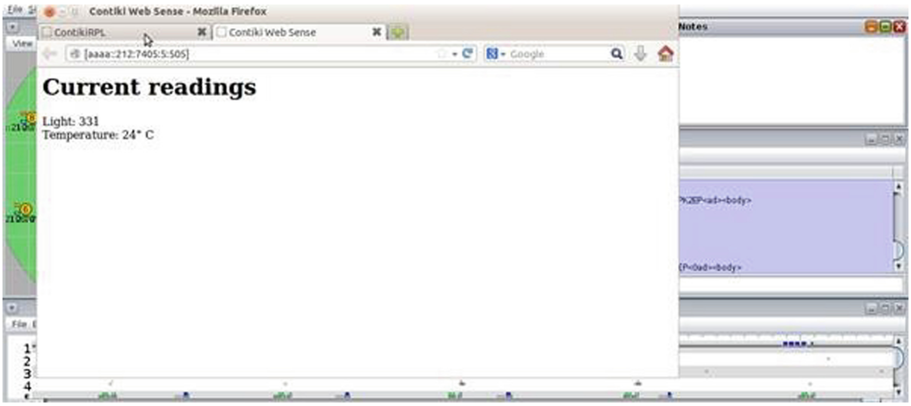


Fig. 4. Temperature analysis for the selected node

5.1 Data Analytics using Hadoop MapReduce

The Contiki OS and Cooja simulator help to build the IoT network. IoT network analysis can be done for every node in the simulation platform, as shown in Fig. 4. The data collected with this type of IoT network can be used to analyse the data. Knowledge extraction is a significant task for stored data. A sample one year climatic data is considered for the analysis in this paper to illustrate this work. The analysis is carried out using Hadoop distributed framework. The map-reduce tool is used to analyse the dataset.

In today's digital world, more data is created every day. Every business companies and organisations try to know the value of the data, which is considered useless. Hadoop is efficient in handling all such types of data which is structured, semi-structured or unstructured. The types of data can be audio, video, images, emails, log files etc. The Hadoop cluster can able to store all the types of data in the cluster format. It doesn't need any schema as required in traditional data handling [11]. Data analytics is done for an unstructured dataset using Hadoop MapReduce. All the states' historical data is collected, and that data file is stored in the Hadoop distributed file system. Hadoop distributed file system is used for faster processing. The analysis can be done in various stages.

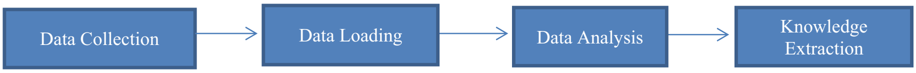


Fig. 5. Steps involved in Data analysis

5.2 Data Collection

This involves the collection of real-time data for analysis. This data can be experimental data or any real-time historical data as considered here for the analysis.

5.3 Data Loading

The collected dataset is loaded into Hadoop distributed file system for analysis. Hadoop is a great platform to store many large volumes of data in a distributed environment. From the HDFS, the data feed goes to MapReduce.

5.4 Data analysis

The Hadoop MapReduce algorithm is used to analyse the climatic data, and it helps predict the weather conditions in the located areas.

5.5 Knowledge Extraction

After the data analysis using Hadoop tools, the required decisions can be taken.

5.6 Input data

The input dataset considered for analysis is historical data collected monthly for different countries, and within each country, various states' climatic temperature is considered.

5.7 Mapreduce Implementation

A MapReduce tool is a Hadoop framework tool that is used to analyse the dataset. The most important of the MapReduce function is its scalability. It takes the data from the HDFS. In the Hadoop distributed file system, the data is stored in a cluster of computers. When the request comes from Hadoop ecosystem tools, then the HDFS sends the data for further processing.

The MapReduce paradigm has mainly two phases, the mapper phase and the reducer phase. A large volume of the data file can be processed on multiple computing devices. In the MapReduce operation, the data processing tasks will be called mappers and reducers. The mapper phase filters the matching records in the dataset. The mapper breaks the individual data elements into tuples. This stores the data in the form of key-value pairs. In the map phase, the data will be in the form of a directory in the HDFS. The line by line data is passed to the mapper from the input file. The mapper phase will process the data and create the small chunks of the reducer task.

The reducer is the second phase of the MapReduce function. The reducer operation takes the output of the map as input. This step involves the shuffle operation and reducer operation. Reduce operation is the second phase of the MapReduce operation. It processes the data of the mapper and produces a new set of outputs. This output will be stored in Hadoop Distributed File System. The Hadoop framework tools manage the complete data collection, storing it in HDFS by copying the data between the clusters of nodes. All the computing tasks will be placed on the nodes.

In Fig. 6, we can see data loading into HDFS and initiating the MapReduce task. As the data is loaded into the mapper, it will show the completion percentage of data analysis. Once the analysis is done, the output file is generated it is stored in the HDFS. The content of the output file is shown in Fig. 7. The maximum and minimum temperature recorded for each state is analysed for the entire dataset. This is shown in Fig. 8 and Fig. 9.

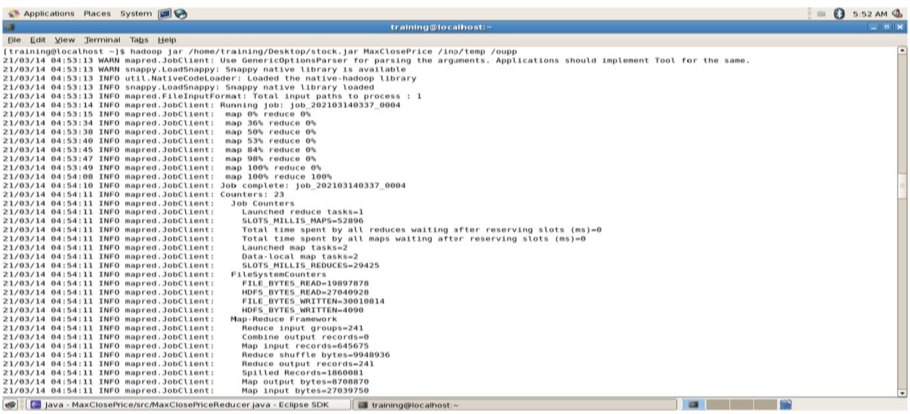


Fig. 6. Data loading using into HDFS to initiate Mapreduce operation

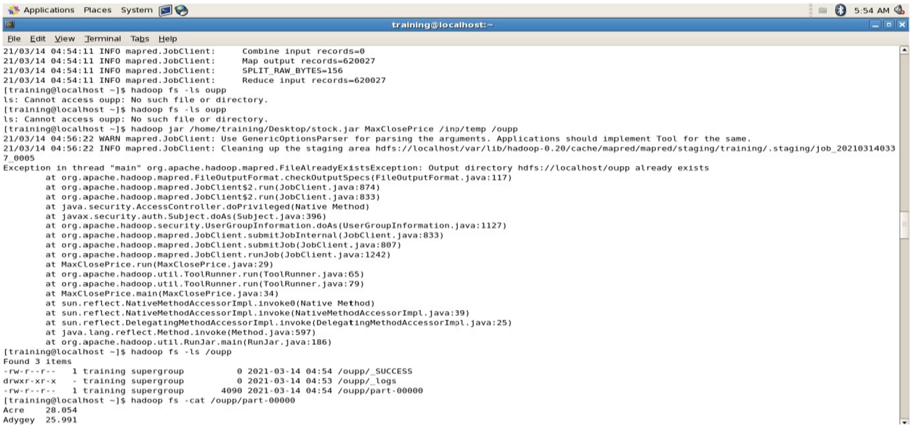


Fig. 7. The output file generated and stored in the HDFS

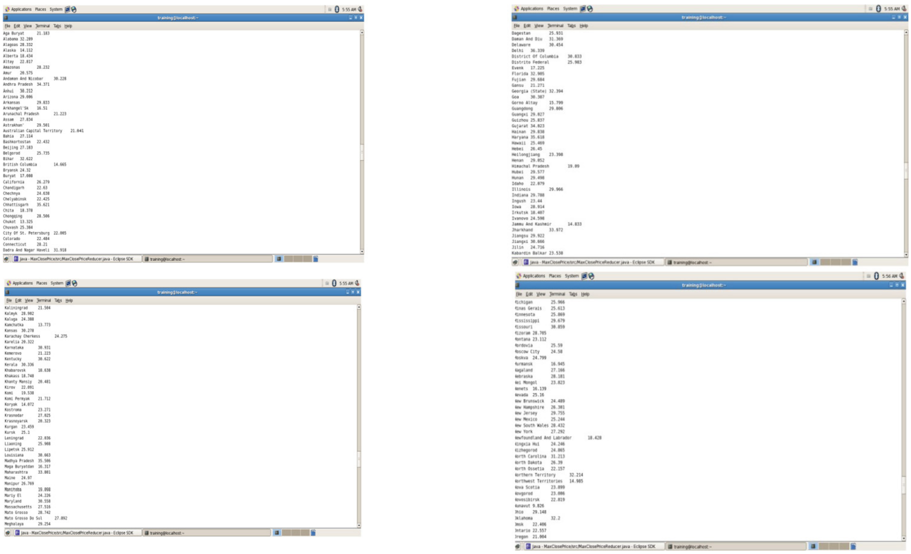


Fig. 8. State-wise maximum temperature using MapReduce analytics

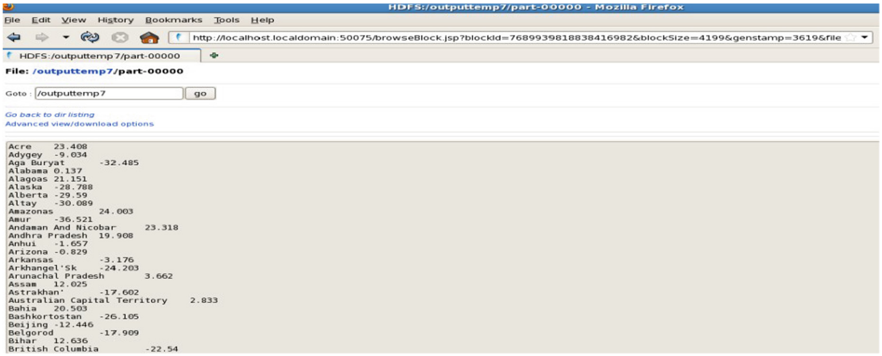


Fig. 9. State-wise minimum temperature using MapReduce analytics

6 Conclusion

This paper discusses the fundamental concepts of big data, its storage and its analytics. Big data is a field that is evolving rapidly. Many organisations are expecting to use big data for their work-loads and analyse using business tools. These numerical data produced by the new technologies help to examine the data to obtain hidden patterns. Based on the customer requirements, preferences and market trends, other useful information can be fetched to get the right decisions for the business improvement. Big data Analysis is a fast-growing technology. Many industries adopt to extract the knowledge from it. Analysing this data leads to data science. The connected things, called IoT, generates a large amount of data. IoT and big data act as the two faces in the field of data analytics. The analytics has to be applied to this stored data, and an organisation or company can draw meaningful insights to make decisions whenever needed.

This paper discusses real-time data generation using Contiki OS and Cooja simulator. It detects the temperature of a sensor in a particular node. The simulator illustrated that the sensor data collection in an energy-constrained device is made easier. The weather data analysis is also carried out using the Hadoop MapReduce. The paper gives future analysis scope using other Hadoop tools to analyse better performance in terms of response time.

References

1. Tsai, C.-W., Lai, C.-F., Chao, H.-C., Vasilakos, A.V.: Big data analytics: a survey. J. Big Data **2**(1), 1–32 (2015). https://doi.org/10.1186/s40537-015-0030-3
2. Wu, X., Zhu, X., Wu, G., Ding, W.: Data mining with big data. IEEE Trans. Knowl. Data Eng. **26**(1), 97–107 (2014)
3. Chen, M., Mao, S., Liu, Y.: Big data: a survey. Mob. Netw. Appl. **19**(2), 171–209 (2014). https://doi.org/10.1007/s11036-013-0489-0
4. Han, H., Wen, Y., Chua, T.-S., Li, X.: Toward scalable systems for big data analytics: a technology tutorial. Access IEEE **2**, 652–687 (2014)
5. Manujakshi, B.C., Ramesh, K.B.: Review of techniques used for sensory data analytics over cloud. In: 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, pp. 1244–1248 (2016)

6. Choubev, P.K., Pateria, S., Saxena, A., SB, V.P.C., Jha, K.K., PM, S.B.: Power efficient, bandwidth optimized and fault tolerant sensor management for IOT in smart home. In: Advance Computing Conference (IACC), 2015 IEEE International, 12-13 June 2015, Banglore, India
7. Al Nuaimi, E., Al Neyadi, H., Mohamed, N. et al.: Applications of big data to smart cities. J. Internet Serv. Appl. **6**, 25 (2015). https://doi.org/10.1186/s13174-015-0041-5
8. Ghofrani, F., He, Q., Goverde, R.M., Liu, X.: Recent applications of big data analytics in railway transportation systems: a survey. https://doi.org/10.1016/j.trc.2018.03.010
9. Géczy, P.: Big data characteristics. Macrotheme Rev. **3**(6), 94–104 (2014)
10. Akter, S., Wamba, S.F.: Big data analytics in E-commerce: a systematic review and agenda for future research. Electron. Mark. **26**(2), 173–194 (2016). https://doi.org/10.1007/s12525-016-0219-0
11. Ularu, E.G., Puican, F.C., Apostu, A., Velicanu, M.: Perspectives on big data and big data analytics. Database Syst. J. **3**(4), 3–14 (2012)
12. Mujawar, S., Joshi, A.: Data analytics types, tools and their comparison. Int. J. Adv. Res. Comput. Commun. Eng. **4**(2), 488–491 (2015)
13. Marjani, M., Nasaruddin, F.: Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges
14. Contiki: The Open Source OS for the Internet of Things. http://www.contiki-os.org/. Accessed 28 Mar 2016
15. Farooq, M.O., Kunz, T.: Operating systems for wireless sensor networks: a survey. Sensors **11**(6), 5900–5930 (2011)
16. Roussel, K., Song, Y.Q., Zendra, O.: Using cooja for WSN simulations: some new uses and limits, kay roemer. EWSN 2016 - nextmote workshop, Feb 2016, Graz, Austria. Junction Publishing. In: Proceedings of the 2016 International Conference on Embedded Wireless Systems and Network - EWSN 2016 - NextMote workshop, pp. 319–324 (2016)

Mirai Botnet Attacks on IoT Applications: Challenges and Controls

G. Sripriyanka and Anand Mahendran(✉)

School of Computer Science and Engineering, Vellore Institute of Technology, Vellore 632014, Tamil Nadu, India
manand@vit.ac.in

Abstract. IoT is rapidly developing technology to enhance the quality of human life with embedded technologies. IoT can control and access daily usable devices and equipment with an internet connection. Smart technology provides a connected infrastructure to heterogeneous devices like IP cameras, cell phones, cars, home appliances, and industrial equipment for autonomous communication and interaction. The great perspective of IoT infrastructure comes with more security challenges. The multiplication of IoT gadgets it can be more easily negotiated than personal computers has led to intensification in the IoT-based botnet attacks. These IoT devices need to ensure the security and privacy of sensitive information and network communication. In the public channel, an adversary can damage the transferred information for unauthorized activities on applications. To moderate this hazard, there is a necessity for new procedures that diagnose the threats dispatched from exchanged IoT appliances and that are dispersed amongst all IoT-based attacks. We discuss the bio-inspired-based attack discovery techniques for IoT botnet attacks and network traffic from hacked IoT gadgets. This paper aims to review the existing attack detection approaches that have been used to address the security issues on IoT applications. In this work, bio-inspired computing models were independently trained to detect and mitigate the Mirai botnet attacks on IoT applications. The bio-inspired computing framework shows the high accuracy and high detection rate over the IoT environment. And also we are exploring details of the bio-inspired models for improving security measures in different scenarios on smart technology.

Keywords: Internet of Things · Mirai botnet · Machine learning · Cryptography · Bio-inspired computing

1 Introduction

The word "Internet of Things (IoT) was coined by Kevin Ashton of Procter & Gamble, later MIT's Auto-ID Center in 1999". Internet of Things (IoT) is smart technology and facilitates that interconnect with all things including

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 49–67, 2023.
https://doi.org/10.1007/978-3-031-13150-9_5

software, hardware, sensors, and actuators for generating and exchanging information through the internet. The development of smart things is increasing tremendously with billions of connected devices through internet communication. The tremendous opportunities create new interactions for new smart services. Without requiring human support these smart devices are communicating with each other by using international networks. With the high processing speed and unique identification, digital devices are generating a huge amount of confidential data. The fabulous growth of heterogeneous objects is reaching 75.44 billion by 2025 [1,2]. This smart technology is using things, it includes data centers (DC), end-users, chips, sensors, RFID tags, WiFi networks, NFC, and so on. A wide variety of IoT smart applications are smart wearables, smart cars, smart homes, smart agriculture, smart farming, smart healthcare, and so on. An important feature of IoT technology is sensing, analyzing, connectivity, automation, and integrating [6]. IoT connecting any smart users with anyplace, anytime, anything, any network is explained in Fig. 1 [11].

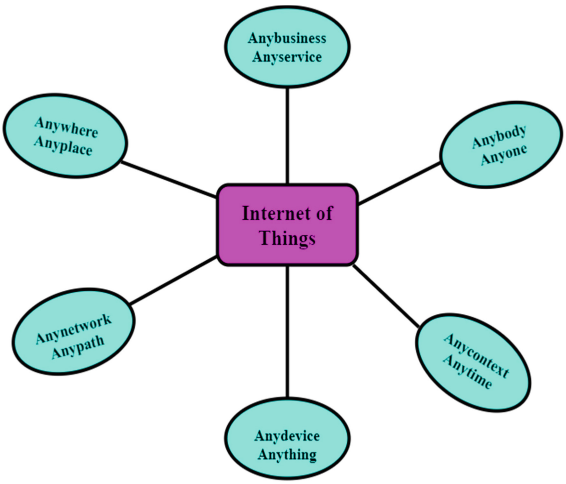


Fig. 1. Features of IoT

In IoT objects, attackers can create a severe threat to personal privacy and security. The IoT applications are becoming more critical to detect threats like DDoS, jamming, tag killing, spoofing, data leakage, unauthorized access, data leakage. This rapidly developing technology comes with numerous security privacy challenges. Such as insecure networks, improper use of confidential information, increase security privacy risks and spreading attacks from other devices. The framework accomplished the inconsequential environment and the greatest identification precision by spread over the component choice methodology. The crossbreed grouping possibly will likewise significantly help with accomplishing the best precision with quick recognition [7,8]. The highest intention of our article is to deliver a current state of IoT security privacy issues with countermeasures. This paper provides a broad discussion about smart technology, with particular motivation on the areas of privacy security threats, vulnerabilities, attack surfaces, and solutions.

2 Literature Survey

Exposure and mitigation of the attacks on modern technology are some of the most interesting matters these days. Many researchers and IoT application developers focus to detect botnet attacks.

The paper [7] stated the IoT gadgets come to be very modest to customary up for individual utilization, as now independent venture then savvy family machines. These aggressors stayed dispatching the assaults towards the casualty hubs later tainting the robot nets scheduled these gadgets. A botnet assaults discovery structure with successive engineering dependent on machine learning. ML calculations are proposed for managing assaults in IoT conditions. An associated highlight determination approach is received for decreasing the insignificant highlights, which creates this framework inconsequential. In this proposition, classifieds dependent on various machine learning calculations might be functional in various assault identification substitute motors, it prompts better recognition execution and more limited preparing times also, a lightweight execution.

The authors in [14] explain IoT security presents novel difficulties, for example, the relative straightforwardness and size of assaults just as the absence of progressed security highlights. This underscores the significance of discovering more successful and useful arrangements that can encourage the plan and improvement of secure IoT frameworks. As featured, halfway, in the presentation, the significant inquiries and worries of non-security specialists associated with the plan and improvement of IoT gadgets and shrewd applications may include: (1) how to distinguish the security prerequisites of an IoT framework, (2) what explicit security best practice rules to follow for the plan of a specific IoT framework, (3) which security instrument to decide for a given security necessity, and (4) what cryptographic calculations give the privilege systems for a given arrangement of safety necessities.

In paper [15], discuss the oblivious usage, and gadgets are lacking in updates have enlarged the security challenges and control of access towards the hacked applications in the smart technology's confidential information. These incongruous privacy methods increase the ways for the information crack and former dangers. Utmost the safekeeping experts deliberate the IoT is considered as the socket of attacks with the pathetic security procedures and strategies. Although a huge number of security techniques are established and deployed towards the protection of IoT gadgets from cyber threats, safekeeping guidelines are not properly acknowledged. In this way, smart application users can't exploit defensive methods to avoid information threats. Attackers established dissimilar varieties of spyware towards contaminating smart appliances. They deliberate numerous hacking techniques towards these organizations and personalities to segment confidential information. These smart Individual gadgets and commercial workstations are facing secrecy damages due to the serious attacks and challenges. If the gadget establishers and safety experts need to consider the security attacks properly. Also, they need to deploy a productive defense technique towards averting or deactivating the risks and vulnerabilities (Table 1).

Table 1. Comparative analysis of IoT attack detection techniques

References	Data_Set	Approach	Performance Metrics	Accuracy
[33]	Two common IDS data sets	Double Particle Swarm Optimization (PSO)-based algorithm	Accuracy, recall, precision, specificity	Increased DR by 4% to 6%
[34]	KDD Cup 99 and CIC-IDS 2017	GOIDS	AUC, specificity, false-positive rate	Low false positive rate.
[35]	Own collected	Immune Genetic Algorithm	Average standard deviation	85% of prediction accuracy
[36]	NSL-KDD and ISCXIDS2012	Anomaly network-based IDS (A-NIDS)	TP, FP, FN, TN	Gained enhanced detection accuracy
[37]	Public data sets	IoT-based IDS	FPR and DR	Obtained satisfactory results
[38]	NSL-KDD	Network intrusion detection system (NIDS)	FPR, FNR, TPR, TNR	Low false alarm rates (FARs)

In paper [39], the widespread use of the Internet of Things and related machinery such as interacting, information loading, administration, and analytics puts it at the risk of Ransomware assaults. As the international network becomes more completely integrated into our company processes through the smart internet platform, the necessity for a safe and creative construction develops. Once assaults happen, it drives have long-term also debilitating consequences for the internet of things expansion. The safekeeping of internet devices can't be overstated, given the rising frequency of devices in our information central culture and network-connected strategies. Some internet of things device that is successfully hacked can be held to redemption. For example, the scenario of Ransomware enslaving every device and limiting admission to or making evidence unavailable for usage in the internet of things atmosphere might have a negative impact scheduled the progression, causing industries to lose their reputation and causing significant financial loss.

Cloud computing [40] is a new paradigm that enables on-demand, metered access to computational resources (processes, memory, storage, and so on) while also supporting geographically distributed applications. The author gives a thorough assessment of computing paradigms and technologies, as well as the impact of the trifecta (blockchain, IoT, and AI) on the growth of cloud computing, The evolution of computing paradigms and technologies has been designed after the history and backdrop of computing paradigms and technologies, have been presented. In addition, cloud computing research fields have been identified, explored, and research concerns and challenges have been emphasized.

Author [41] describes fraudulent activities and characteristics of phishing attacks, website security from the cybercriminals (phishing attacks) in the cyber world, and proposed anti-phishing mechanism to detect the phishing sites. This detection solution follows the pre-filtering stage (pre-processing) and classification stage (feature extraction). This approach development for digital forensics methods in communication networks domains. The author shows an accuracy of 99.1% effective in detecting different forms of phishing attacks by using the Phish Detect Method.

The author in [42], the goal of this research is to look into previous techniques for software distributed denial of service (APDDoS) outbreak protection utilizing the following criteria: exposure approaches or procedures, violence plan, and feature consideration of prevailing APDDoS appliances. Numerous researches ensure not deliberate an outbreak form when positioning their clarification, according to a calculation established on occurrence approach. Established on current structures, the appeal torrent through a handler assembly and envelope outline yielded the best results for the APDDoS appreciation performance. According to the data, a substantial percentage of APDDoS outbreak recognition elucidations included structures grounded on appeal crick through consumer assembly and container configuration. The accurateness of recognition will be upgraded by optimizing characteristics. Our findings suggest that investigators should use deep learning algorithms to exploit all attack tactics, resulting in the more active discovery of APDDoS attacks launched by various botnets.

In this paper, we intend towards giving an outline of the smart solicitations, advantages, and prospective changes. Furthermore, towards fabricating a structure toward examining and additionally grow the superlative safekeeping rehearses by whichever carrying out besides investigating contemporary surviving plans otherwise growing novel ones. Because of these discoveries, we'll provide suggestions towards maintaining a strategic distance from such dangers and curing conceivable security weaknesses. This work will direct administrative organizations to keep implementing strategies, instructing end clients and substances, and partners engaged with the Internet of Things towards creating then relating new fitting safety and protection procedures.

3 Internet of Things Layer Architecture

The Internet of things gives captivating answers for most issues that the labor force is confronting. The methodology of achieving an answer depends on how the data innovation segments were coordinated with correspondence gadgets with the best equipment and programming union. IoT, the product and equipment segments performance and exertion commonly through the learned result established ideas before needs assumed by this proprietor to looks for an arrangement. The design of IoT is to impose security attacks and prevent the IoT applications from attackers [12]. To sum things up the product characterized equipment framework helps in handling the crude data to prepared information, from where the putting away, recovering, and examination of information is finished utilizing progressed registering apparatuses considering remains the coordinated through smart IoT framework. This correspondence framework advantages to giving each correspondence frequencies besides permit conventions concerning the items are possessions or every segment of this technology [11].

The greatest, quick, dependable, besides protected intermingling about these data innovations with correspondence innovation spirit possibly occur while a successful internet engineering level is constructed. Such strategy surfaces used to differ contingent upon these necessities also assignments towards deal with. Though, many scientists have proposed various designs which are as per the following. This segment gives the outline of the generally concurred and acknowledged design of IoT [10]. IoT works in the base-to-top methodology. Sensors accumulate information utilizing the smart gadgets, cycle this information utilizing regulators to make choices, and later impart to the gadgets or people for execution. Client or applications are in the highest layer and the innovation, appointing addresses to keen items, and correspondence media utilized are in the base layer. Brilliant articles, sensors, and programming like micro regulators used to handle information are in the center layer. The engineering of IoT comprises four layers as demonstrated in Fig. 2 [12]. The functionalities of each layer have been momentarily talked about underneath [9,16].

3.1 Application Layer

This layer is accountable for delivering the application's precise services to the users. IoT can be deployed in many applications to the real world. For example, smart grid, smart home, smart city, smart healthcare, and so on. The application layer deals with all application interactions dependent on data acquired from the middleware layer. This application includes sending messages, enacting caution, security framework, and turning on or off gadgets [9].

3.2 Middleware Layer

At this level, IoT modules are interfaced for potential connection with the elements. It has various processes, namely filtering the information received from the hardware gadgets, access control is provided to the strategies, information collection and detection of information is performed on smart expertise. It is used to hide the network details from solicitations, supported the mobility, statistics controlling, and distribution of nets. This layer stocks the index details of the smart gadget report and appellation that provides proper information towards the gadgets for interconnection [10].

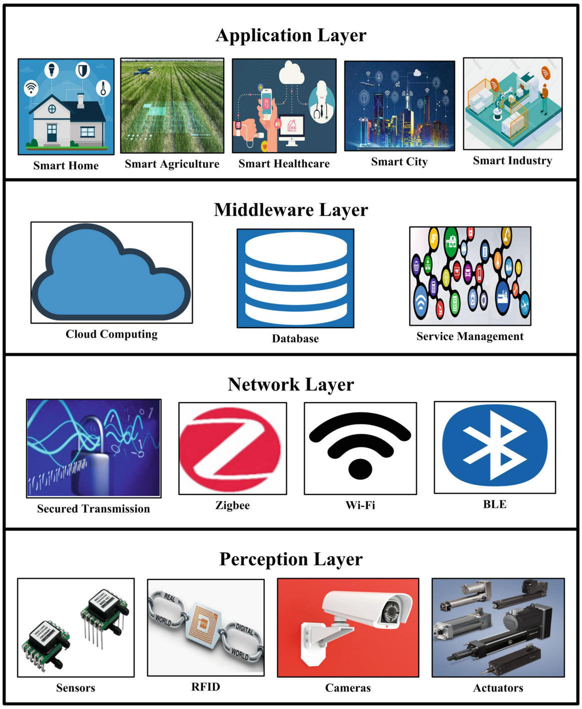


Fig. 2. IoT layer architecture

3.3 Network Layer

At this level, smart objects, servers, and network devices are connecting for sensed data processing and transmitting. This layer is also called a communication layer. It acts like a scaffold that conveys and communicates information assembled from actual articles through sensors. The medium can be remote or wire-based. It additionally associates the organization's gadgets and organizations with one another. Consequently, it is amazingly delicate to assault the aggressors. It has significant security issues in regards to trustworthiness and validation of information that is being sent to the organization [11].

3.4 Perception Layer

The sensor layer should perceive things and assemble the information from them. There are numerous sorts of sensors associated with the items to assemble data like RFID, sensors, and standardized identification. The sensors are chosen according to the prerequisite of utilizations. The information that is gathered by these sensors can be about area, changes noticeable all around, climate, and so on In any case, they are the fundamental point of assailants who wish to utilize them to supplant the sensor with their own [13].

4 IoT Applications

Possible uses of the IoT are various and different, pervading into essentially all territories of consistently people's life, speculations, and overall humanity in real solicitations. The internet technology solicitation shelters "savvy" situations and universes now the expanses for sample, Farming, City, Shipping, Supply Chain, Construction, Emergency, Factory, Routine, Healthcare, Client collaboration, Principles and the transportable production, surroundings, and dynamism. The subsequent are the portions of the smart internet solicitations [16].

4.1 Smart Home

Probably the biggest market for IoT gadgets is the savvy home market. Universally, there are more than 120 new IoT gadgets that make an association with the Internet each second. In the US, every individual midpoints eight associated gadgets for each family, and that number is projected to increment by 2022. Keen home gadgets comprise a wide reach of gadgets from cameras to voice collaborators to indoor regulators to lights. The availability of the IoT gadgets and the administrations they give establish keen home conditions. For instance, consider a situation of a family where the guardians are observing their youngsters after school while they are busy working. Amazon's keen home items, e.g., Amazon Cloud Cam, Amazon Key (with lock), Amazon Echo (with Alexa voice right hand), and Amazon Fire TV, are utilized to achieve this. The guardians would utilize the cameras and keen lock to give the children access to the house. The children could turn on the lights and TV utilizing the voice collaborator while the guardians screen the children's exercises furthermore, set parental controls on their cell phones. The computerization of these orders, assignments, and administrations, through the help of associated keen IoT gadgets, gives simplicity and solace to property holders [17].

4.2 Smart City

The progressive expansion in urbanization presents different experiences for the leaders in proposing various offices to the occupants of these urban communities. The ICT [Information and Communication Technologies] are utilized to make the urban areas savvy enough by conveying and advancing manageable advancement rehearses for tending to the developing difficulties of urbanization. A strong establishment is offered for the Internet of Things (IoT) with headway in the field of keen urban communities' sensors by empowering them to interconnect Smart city information calculation and inescapable knowledge open the organizations to security assaults, malware, and other digital breaks. The between network necessities of regular actual gadgets would likely add various noteworthy and clever malignant models to IoT information registering. The presence of vindictive gatecrashers may create manufactured information to control the detected data of genuine gadgets. The gatecrashers may antagonistically influence the administrations and dynamic in a pervasive climate. Moreover, these noxious elements may take off assaults like forswearing of administration by disturbing the transmission and detecting of an omnipresent climate to diminish the greatness of shrewd administrations [18].

4.3 Smart Agriculture

Countless advances are being utilized in IoT rural arrangements because of which it is difficult to make an unequivocal of each one of those because of which our conversation zeroed in on a few center advances which have assumed an indispensable part to modernize the IoT farming administrations. Information examination comprises of two principles includes that are checking and controlling. Checking includes three principle applications in brilliant agribusiness that is Live Stock Monitoring, Field Monitoring, and Greenhouse Monitoring. IoT empowers ranchers to screen domesticated animals utilizing numerous sensors which are utilized to screen distinctive animal's illnesses like temperature, pulse, and absorption, and so forth Though field checking applications mean to report various states of the field like soil extravagance, temperature, mugginess, gas, pressure (pneumatic force and water pressing factor), and yield infection observing. A shrewd nursery configuration wipes out the manual mediation and measures diverse environment boundaries by canny IoT gadgets and sensors as per plants' necessities [19].

4.4 Smart Industry

Interfacing a huge number of modern gadgets will alter organizations by expanding measure productivity, dependability, and security. A few organizations like Honeywell, Cisco, Emerson, Uptake, Yokogawa, and GE are giving completely incorporated savvy production lines frameworks utilizing smart industry stages; however, their extension is to cover enormous scope exercises like railroad coordination, power age and circulation, oil and gas tasks, and flight armada. A captivating report depicts the accomplishments of mechanical information investigation dependent on progress in the regions of AI, IoT, and modern information examination (IDA). Ongoing progressions in detecting, activation, and correspondence advancements have empowered undertakings to procure, communicate, store, and interact with continuous information for describing manufacturing plant conduct. There are various control frameworks accessible to gain the monstrous modern information, including circulated control frameworks, administrative control and information securing frameworks, and programmable rationale regulators [21].

4.5 Smart Transport

Smart transportation framework applications in our nation are for the most part packed in rush hour gridlock (particularly crossing point) the executives, traffic security, and programmed charge assortment. As of late, it has gone to the plan that the utilizations of the metropolitan districts to help public transportation frameworks. As per International Road Federation (IRF), points of savvy transportation framework are resolved as; Safe streets and safe driving, accomplishing maintainable street transport, information assortment, information move, handling and examination, and cognizant choice making. In the light of these reasons, there are various immediate and aberrant advantages anticipated from the keen transportation framework, which are lessening auto collisions, expanding the well-being and security of streets, drivers, and walkers, improving the exhibition of the vehicle framework, and decreasing gridlock, observing, direction and continuous administration of traffic, improvement of transportation times and commitment to the economy by diminishing transportation costs, expanding administration quality and efficiency, expanding individual versatility and solace, limiting the harm done to the climate and saving energy; these advantages likewise shows the significance of the system [22].

4.6 Smart Healthcare

Smart wellbeing observing could be utilized to screen non-basic patients at home instead of in a medical clinic, lessening the strain on clinic assets like specialists and beds. It very well may be utilized to give better admittance to medical care to those living in rustic zones or to empower old individuals to live autonomously at home for more. It can improve admittance to medical services assets while lessening the strain on medical services frameworks and can give individuals better authority over their wellbeing consistently. It is desirable to carry out all fundamental sensors as little, convenient, and remotely wearable hubs. This would furnish patients with a non-meddling and agreeable arrangement that is fit for checking their wellbeing any place they go. This would make patients more open to utilizing wellbeing checking innovation than they would be if implantable sensors or cameras were required. Furthermore, fixing or supplanting remotely wearable hubs would be basic when contrasted with embedded sensors or vision-based sensors introduced in the home [20].

5 Attacks on IoT Applications

This scalable IoT technology is highly concerned with security and privacy attacks. Current smart applications come with a lot of vulnerabilities, it includes default authentication credentials, spoofing, eavesdropping, ransomware, and so on. The collection of data can be affected by information leakage, data breach, and authentication attacks. The processing of data is vulnerable to DDoS attacks, confidential data modification, attacks on integrity, attacks on access control, impersonation, and so on. Possibilities of attacks on data transmission are hijacking, flooding, routing attacks, channel attacks, and so on [6,44].

5.1 Mirai Botnet

This scalable IoT technology is highly concerned with security and privacy attacks. Current smart applications come with a lot of vulnerabilities, it includes default authentication credentials, spoofing, eavesdropping, ransomware, and so on. The collection of data can be affected by information leakage, data breach, and authentication attacks. The processing of data is vulnerable to DDoS attacks, confidential data modification, attacks on integrity, attacks on access control, impersonation, and so on. Possibilities of attacks on data transmission are hijacking, flooding, routing attacks, channel attacks, and so on [6,44].

5.2 DDoS

Distributed Denial-of-Service, more known as DDoS presents perhaps the most hazardous dangers for the Web. The measure of these kinds of assaults expands in size every year. To perform DDoS assault, three stages should be applied here, and they are. Filtering is the initial step, where the assailant examines the weak machine by various checking procedures. The following stage is spread, where the aggressor initiates the machine to produce a stream of bundles that will play out the assault onto the weak machine [24].

5.3 Malicious Code Injection

This sort of assault centers around genuinely infusing the IoT hub with noxious code that assists with accessing the IoT framework. The aggressor acquires the admittance to touchy data by genuinely working another malevolent hub between conveying hubs of the IoT framework, which permits the assailant to control all information stream between different hubs [25].

5.4 Ransomware

Ransomware has been around for some time. It's a type of malware that secures admittance to your records by scrambling them and sells you the unscrambling key that will give you back admittance to the documents. IoT ransomware is generally new. Lamentably, however, IoT ransomware isn't being given sufficient consideration, or not being taken a gander at from the correct point of view, which can prompt its underestimation and heartbreaking results that could result in monetary misfortunes, yet in death toll too., ransomware aggressors should fall back to the more seasoned type of ransomware, the one that bolts your gadget and payoffs you for recapturing admittance to its usefulness. Furthermore, that is as inconsequential to defeat as resetting the gadget and putting in new fixes and updates, which is considerably simpler to achieve with IoT gadgets than Personal Computers [26].

6 Mirai Botnet Attacks on IoT

Malware is a major threat to network communication between IoT devices. The smart devices are operated by various standards and protocols but active traffic observing is quite harder in real-time [4]. Generally, botnets are a net of bargained IoT pieces of machinery, below the regulator to a single foundation. For the command and control process, they try to communicate with the bot admin or master shown in Fig. 3 [5]. The DDoS attacks aim to incapacitate the service-based environments it provides several services to the users through the internet with malicious traffic for service denial [5]. Botnet attacks are developing continuously on IoT applications and are too hard to discover by using traditional or signature-based anomaly detection techniques. At last, a strong consistency score can be utilized by huge associations to guarantee organization usefulness and breaking point the effect that undermined gadgets may have on the organization. That is, security strategies probably won't permit the association of IoT gadgets with low consistency scores to their organizations, since they present troubles in assault identification [8,26].

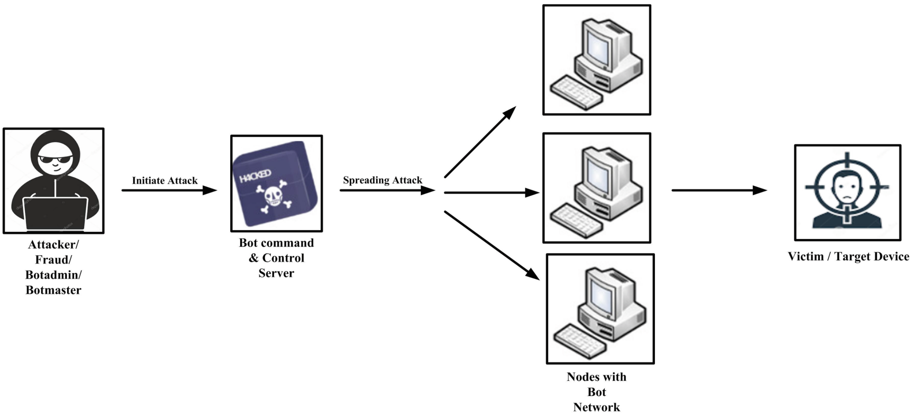


Fig. 3. Mirai botnet attack

7 Detection Methods

The development of detection mechanisms is applied to ensuring the confidentiality, security, integrity, and privacy of users' information and IoT devices from malware. The process of authentication is used to identify unauthorized users in the public network and allow access to the authorized user [3]. Learning algorithms are the most appropriate for attack detection in internet infrastructure. Bio-inspired algorithms are making something perfect to find the proper solution. It has more advantages than traditional attack detection techniques [4].

The Primary Check is answerable for examining the approaching traffic and choosing whether the approaching parcel is dubious or not. Every one of the parcels coming from the outside network is gotten at the boundary switch and afterward, they go through the Primary Check [43]. The Secondary calculation checks the dubious bundles. On the off chance that the flood of suspected bundles are beginning from a similar IP and have comparable attributes, at that point denial of service (DoS) assault is identified then this starting Internet Protocol is auxiliary towards the banned Internet Protocol. Then again, if these surges of bundles have comparable trademarks yet are beginning from various IPs, at that point, a Distributed Denial of Service (DDoS) and Mirai botnet assault is recognized [28].

7.1 Machine Learning

In the Internet of Things environment, traditional attack detection methods are not fixed to protect and mitigate the smart devices in conventional networking. More attacks are detected on the traditional devices with network delay, data theft, data loss, and so on. Presently more security faults occur in the smart infrastructure because, less memory and low computation resources for robust protection. Machine Learning-based attack detection methodology can use an efficient feature selection method for implementing the high-performance-based lightweight botnet attack detection and isolating the compromised gadgets [7].

Machine Learning models, while requiring critical time furthermore, endeavors to prepare and test, can be effortlessly conveyed to lead essential induction. Also, ML models are fundamentally improved via preparing bigger, more delegate datasets. As a territory of a specific requirement for dynamic examination and disclosure, interruption identification is required to keep up secure frameworks and to tell framework clients, what's more, directors of unintended access with the goal that further activities (attribution, relief, and evacuation) can be conveyed out. In the accompanying, we research the subtleties of utilizing distinctive ML methods to distinguish interruption assaults [13].

7.2 Cryptography

This report introduced an overview of different strategies identified with LB-PKC for the IoT infrastructure. With the far and wide reception of IoT sensors in the keen foundation, security and protection have become significant difficulties over the most recent couple of years. The conventional cryptographic strategies and calculations are not effective to deal with the security challenges in the IoT climate since they are not strong to quantum assaults. Subsequently, to address a portion of the inadequacies of conventional cryptographic methods, LB-PKC has been proposed to give assurance against quantum assaults. In the initial segment of this paper, we have introduced a portion of the significant NP-difficult issues of cross-sections followed by as of late proposed grid-based ways to deal with tackle a portion of the issues in a polynomial time. At last, we examined different grid-based encryption and verification strategies [27].

The IoT gadgets like RFID, keen cards, sensors hubs assume a significant part of the organization. These gadgets have restricted memory and are battery-worked gadgets. The standard cryptography calculations (like AES) give great security however their presentation isn't adequate on these gadgets due to huge memory prerequisites to store s-boxes, enormous squares, and key sizes. To determine these issues, NIST suggested favoring lightweight calculations which give the same degree of safety and their exhibition is likewise worthy on these gadgets. There can be different arrangements at the individual layers of IoTs utilized eventually to end correspondence. The cryptography calculations are taken for information security. Cryptography is a method where we can scramble information into figure text for its protected transmission. Cryptographic codes are of two sorts, symmetric and asymmetric approaches. Symmetric key encryption utilizes the same key for both encryption and unscrambling of information. This technique for encryption is very secure and moderately quick. The significant hindrance of symmetric key encryption is sharing of the key between the conveying parties. On the off chance that the key gets in hands of some malignant gathering, the scrambled information gets bargained [29,30].

7.3 Bio-Inspired Computing Techniques

Artificial natural immune frameworks are applied in an assortment of regions and are especially praised for their achievement in IDS. Resistant identifiers decide the exhibition of the location part of the safe framework, a center segment of the insusceptible framework. A few works including give some examples utilize safe enlivened methodologies for creating PC security instruments dependent on the self-versatile, self-learning, self-sorting out, equal handling, and dispersed coordination credits of AISs. Moreover, the creators in microbes; youthful Tlymphocytes life cycle. By producing memory identifiers from a static preparing informational index and youthful indicators through transformation, the proposed framework identifies approaching phishing messages through memory finders, while the juvenile locators distinguish phishing messages with obscure marks. Tooth et al. place the idea that their proposed frameworks performed well in phishing recognition [31].

Bio-inspired intelligent calculations that can deal with these restrictions on the internet are required, as is supporting organizations and correspondence frameworks to secure against assaults, cybercriminals, programmers, and inconsistencies proficiently. Organically motivated frameworks have many engaging qualities, for example, adjusting to different natural conditions and self-versatility toward harm. Conveyed, self-coordinated, bumblebee motivated calculation for early oddity location in an associated framework over a remote organization. The calculation is determined by noticing the settlements of bumblebees and mirrors the way that honeybees use to scavenge productively. Essentially, the members characterized the objective (assets, for example, PC organizations) and experienced them dependent on dynamic and data extraction strategies to distinguish and alleviate assaults, for example, SYN flooding assaults [32].

8 Bio-Inspired Computing Framework for IoT Botnet Attacks

In this work, a bio-inspired computing methodology that is aligned with mathematics, computer science, and biology is all used to create tools for storing, analyzing, and interpreting biological statistics. It's also utilized to handle real-world issues including biological data sequencing, data clustering, and optimization. Swarm intelligence is a new type of biologically inspired artificial intelligence technology based on social insect behavioral models.

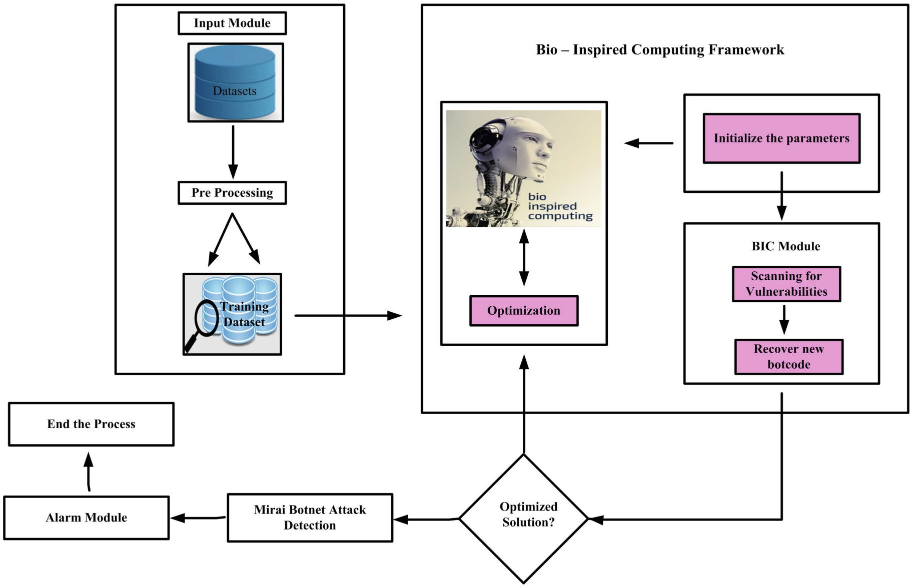


Fig. 4. Bio-inspired computing framework for IoT botnet attacks

The identification of internet of things Mirai botnet assaults in real-time can improve IoT safety by inevitably disconnecting infected IoT strategies from the grid, preventing the spread of these outbreaks. IoT Mirai botnet discovery approaches have traditionally relied on controlled erudition, which has several drawbacks. To begin, a vast amount of storage is required to store numerous instances of malicious packets as well as numerous examples of benign packets. Another, a specialist is required to classify packets as malevolent or benevolent. As a result, this will take a long time. Next, due to the high number of IoT Mirai botnet spasms performed every day; existing technologies are unable to precisely detect them. The demand for bio-inspired and faster ways to detect IoT Mirai botnets grows as a result of these concerns. As a result, the goal of this research is to create an evolutionary bio-inspired computing-based algorithm that can solve these difficult detection problems.

The fundamental contribution of this work is to create a framework that uses a powerful bio-inspired computing model to discover numerous unexpected patterns from smart things to effectively and efficiently Mirai detect botnet assaults from various types of internet of things devices. Figure 4 shows a high-level diagram that illustrates the sequencing of the main phases of the proposed bio-inspired computing-based Mirai botnet detection method which consists of the following main phases: (a) Initialize the input module, (b) understanding the collected information, (c) preprocess and train the data (d) bio-inspired computing framework for scanning and detecting the vulnerabilities with better optimization methods (e) process the alarm if the attack is detected and finally end the communication.

9 Performance Evolution

We are using five-concert methods to appraise the enactment of the bio-inspired computing model. These appraisal metrics include accuracy, precision, recall, f1-score, and sensitivity. The recall is calculated by dividing the number of true positives by the number of false negatives plus true positives. True positives are independent variables that the bio-inspired computing classifies as positive but are positive. While false negatives are independent variables that bio-inspired computing classifies as negative but are truly positive. Accuracy can be defined as follows:

$$Accuracy = \frac{TruePositive + TrueNegative}{FalsePositive + FalseNegative + TruePositive + TrueNegative} \times 100\% \quad (1)$$

Precision is calculated by dividing the number of true positives by the number of false positives plus true positives. False positives are independent variables that the bio-inspired computing model classifies as positive but are negative. Precision and F1-Score can be defined as follows:

$$Precision = \frac{TruePositive}{TruePositive + FalsePositive} \times 100\% \quad (2)$$

$$F1 - Score = 2 * \frac{Precision \times Sensitivity}{Precision \times Sensitivity} \times 100\% \quad (3)$$

Sensitivity can be defined as follows:

$$Sensitivity = \frac{TruePositive}{TruePositive + FalseNegative} \times 100\% \quad (4)$$

Recall can be defined as follows:

$$Recall = \frac{TruePositive}{TruePositive + FalseNegative} \times 100\% \quad (5)$$

10 Conclusion

Huge numbers of devices are connected with the internet for collecting and exchanging information for enhanced smart services to the user. Leaving things without human interaction for a long period can lead to the theft of confidential information about smart technology users. The IoT security attacks are observed and include DDoS, MIMA, malicious code injection, Spoofing attacks, sniffing, and jamming. On the other hand, privacy attacks are observed and include identification attacks, tracking, profiling, and interaction. We determined the IoT application user is heavily affected by security and privacy harms. The existing solution techniques are centralized and deal only with DoS attacks. The fundamental theoretical impact is needed to redefine the nature of botnet attacks on the internet and smart devices. Bio-inspired techniques are most promising to address the security issues in the IoT environment and recover the Mirai botnet attacks. The model results display that the Mirai botnet attack detection can achieve a net accurateness of as high as around 99%. This research should strive to reproduce results in a broader system to detect hacked end-points and retrain models with more recent data to address network performance anomalies. In the future, we plan to implement bio-inspired lightweight techniques on real-time IoT applications with less computation, more efficiency, and high accuracy.

References

1. Ogonji, M.M., Okeyo, G., Wafula, J.M.: A survey on privacy and security of internet of things. Comput. Sci. Rev. **38**, 100312 (2020)
2. Butun, I., Österberg, P., Song, H.: Security of the internet of things: vulnerabilities, attacks, and countermeasures. IEEE Commun. Surv. Tutor. **22**(1), 616–644 (2019)
3. Hassan, W.H.: Current research on internet of things (IoT) security: a survey. Comput. Netw. **148**, 283–294 (2019)
4. Procopiou, A., Komninos, N.: Bio/nature-inspired algorithms in AI for malicious activity detection(2019)
5. Ogu, E.C., Ojesanmi, O.A., Awodele, O.: A botnets circumspection: the current threat landscape, and what we know so far. Information **10**(11), 337 (2019)
6. Damghani, H., Damghani, L., Hosseinian, H., Sharifi, R.: Classification of attacks on IoT. In: 4th International Conference on Combinatorics, Cryptography, Computer Science and Computation (2019)
7. Soe, Y.N., Feng, Y., Santosa, P.I., Hartanto, R., Sakurai, K.: Machine learning-based IoT-botnet attack detection with sequential architecture. Sensors **20**(16), 4372 (2020)
8. Meidan, Y., et al.: N-BaIoT-network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Comput. **17**(3), 12–22 (2018)
9. Singh, J.: IoT: architecture, technology, applications, and quality of services. In: Hu, Y.C., Tiwari, S., Mishra, K., Trivedi, M. (eds.) Ambient Communications and Computer Systems. Advances in Intelligent Systems and Computing, vol. 904, pp. 79–92. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-5934-7_8
10. Kumar, N.M., Mallick, P.K.: The Internet of Things: insights into the building blocks, component interactions, and architecture layers. Proc. Comput. Sci. **132**, 109–117 (2018)

11. Sethi, P., Sarangi, S.R.: Internet of things: architectures, protocols, and applications. J. Electr. Comput. Eng. (2017)
12. Burhan, M., Rehman, R.A., Khan, B., Kim, B.S.: IoT elements, layered architectures and security issues: a comprehensive survey. Sensors **18**(9), 2796 (2018)
13. Liang, F., Hatcher, W.G., Liao, W., Gao, W., Yu, W.: Machine learning for security and the internet of things: the good, the bad, and the ugly. IEEE Access **7**, 158126–158147 (2019)
14. Sfar, A.R., Natalizio, E., Challal, Y., Chtourou, Z.: A roadmap for security challenges in the Internet of Things. Digit. Commun. Netw. **4**(2), 118–137 (2018)
15. Tawalbeh, L.A., Muheidat, F., Tawalbeh, M., Quwaider, M.: IoT privacy and security: challenges and solutions. Appl. Sci. **10**(12), 4102 (2020)
16. Patel, K.K., Patel, S.M.: Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. Int. J. Eng. Sci. Comput. **6**(5) (2016)
17. Davis, B.D., Mason, J.C., Anwar, M.: Vulnerability studies and security postures of IoT devices: a smart home case study. IEEE Internet Things J. **7**(10), 10102–10110 (2020)
18. Zhang, H., Babar, M., Tariq, M.U., Jan, M.A., Menon, V.G., Li, X.: SafeCity: toward safe and secured data management design for IoT-enabled smart city planning. IEEE Access **8**, 145256–145267 (2020)
19. Farooq, M.S., Riaz, S., Abid, A., Abid, K., Naeem, M.A.: A survey on the role of IoT in agriculture for the implementation of smart farming. IEEE Access **7**, 156237–156271 (2019)
20. Baker, S.B., Xiang, W., Atkinson, I.: Internet of things for smart healthcare: technologies, challenges, and opportunities. IEEE Access **5**, 26521–26544 (2017)
21. Saqlain, M., Piao, M., Shim, Y., Lee, J.Y.: Framework of an IoT-based industrial data management for smart manufacturing. J. Sens. Actuator Netw. **8**(2), 25 (2019)
22. Finger, M., Audouin, M.: The Governance of Smart Transportation Systems. Springer, Berlin (2018). https://doi.org/10.1007/978-3-319-96526-0
23. Kolias, C., Kambourakis, G., Stavrou, A., Voas, J.: DDoS in the IoT: Mirai and other botnets. Computer **50**(7), 80–84 (2017)
24. Džaferović, E., Sokol, A., Abd Almisreb, A., Norzeli, S.M.: DoS and DDoS vulnerability of IoT: a review. Sustain. Eng. Innov. **1**(1), 43–48 (2019)
25. Atlam, H.F., Wills, G.B.: IoT security, privacy, safety and ethics. In: Farsi, M., Daneshkhah, A., Hosseinian-Far, A., Jahankhani, H. (eds.) Digital Twin Technologies and Smart Cities. IT, pp. 123–149. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-18732-3_8
26. Zahra, S.R., Chishti, M.A.: Ransomware and internet of things: a new security nightmare. In: 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), pp. 551–555. IEEE (2019)
27. Chaudhary, R., Aujla, G.S., Kumar, N., Zeadally, S.: Lattice-based public key cryptosystem for internet of things environment: challenges and solutions. IEEE Internet Things J. **6**(3), 4897–4909 (2018)
28. Kajwadkar, S., Jain, V.K.: A novel algorithm for DoS and DDoS attack detection in internet of things. In: 2018 Conference on Information and Communication Technology (CICT), pp. 1–4. IEEE (2018)
29. Bhardwaj, I., Kumar, A., Bansal, M.: A review on lightweight cryptography algorithms for data security and authentication in IoTs. In: 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), pp. 504–509. IEEE (2017)

30. Fotovvat, A., Rahman, G.M., Vedaei, S.S., Wahid, K.A.: Comparative performance analysis of lightweight cryptography algorithms for IoT sensor nodes. IEEE Internet Things J. **8**, 8279–8290 (2020)
31. Mthunzi, S.N., Benkhelifa, E., Bosakowski, T., Hariri, S.: A bio-inspired approach to cyber security. In: Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices, p. 75. CRC Press, Boca Raton (2019)
32. Saleem, K., Alabduljabbar, G.M., Alrowais, N., Al-Muhtadi, J., Imran, M., Rodrigues, J.J.: Bio-inspired network security for 5G-enabled IoT applications. IEEE Access **8**, 229152–229160 (2020)
33. Elmasry, W., Akbulut, A., Zaim, A.H.: Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic. Comput. Netw. **168**, 107042 (2020)
34. Dwivedi, S., Vardhan, M., Tripathi, S.: Defense against distributed DoS attack detection by using intelligent evolutionary algorithm. Int. J. Comput. Appl. 1–11 (2020)
35. Suhaimi, H., et al.: Network intrusion detection system using immune-genetic algorithm (IGA). Indon. J. Electr. Eng. Comput. Sci. **17**(2), 1059–1065 (2020)
36. Mazini, M., Shirazi, B., Mahdavi, I.: Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. J. King Saud Univ.-Comput. Inf. Sci. **31**(4), 541–553 (2019)
37. Deng, L., Li, D., Yao, X., Cox, D., Wang, H.: Mobile network intrusion detection for IoT system based on transfer learning algorithm. Clust. Comput. **22**(4), 9889–9904 (2019)
38. Sakr, M.M., Tawfeeq, M.A., El-Sisi, A.B.: Network intrusion detection system based PSO-SVM for cloud computing. Int. J. Comput. Netw. Inf. Secur. **10**(3), 22 (2019)
39. Ogundokun, R.O., Awotunde, J.B., Misra, S., Abikoye, O.C., Folarin, O.: Application of machine learning for ransomware detection in IoT devices. In: Misra, S., Kumar Tyagi, A. (eds.) Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities. SCI, vol. 972, pp. 393–420. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-72236-4_16
40. Gill, S.S., et al.: Transformative effects of IoT, blockchain and artificial intelligence on cloud computing: evolution, vision, trends and open challenges. Internet Things **8**, 100118 (2019)
41. Azeez, N.A., Salaudeen, B.B., Misra, S., Damaševičius, R., Maskeliūnas, R.: Identifying phishing attacks in communication networks using URL consistency features. Int. J. Electron. Secur. Digit. Forensics **12**(2), 200–213 (2020)
42. Odusami, M., Misra, S., Abayomi-Alli, O., Abayomi-Alli, A., Fernandez-Sanz, L.: A survey and meta-analysis of application-layer distributed denial-of-service attack. Int. J. Commun. Syst. **33**(18), e4603 (2020)
43. Salas-Fernández, A., Crawford, B., Soto, R., Misra, S.: Metaheuristic techniques in attack and defense strategies for cybersecurity: a systematic review. In: Misra, S., Kumar Tyagi, A. (eds.) Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities. SCI, vol. 972, pp. 449–467. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-72236-4_18
44. Misra, S.: A step by step guide for choosing project topics and writing research papers in ICT related disciplines. In: ICTA 2020. CCIS, vol. 1350, pp. 727–744. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-69143-1_55

Machine Learning for Recognition and Classification of Visual Art Architecture: A Survey

Amita Sharma(✉) and R. S. Jadon

Madhav Institute of Technology & Science, Gwalior, Madhya Pradesh, India
safalta.amita@gmail.com

Abstract. Advancement in the field of computational algorithms diverted the focus of researchers to use these algorithms in the preservation of Visual Art Architecture. There are few research literature works available in this field, but these become the base for further future research work in the better advancements in the preservation of architecture. These few related works are listed in the paper. The paper focuses on the main outcomes of the available literature and findings for future possibilities in the field. The research works of these researchers were classified, described, analyzed, and compared in the different sections of the paper. The research was classified into three proposed classes based on similarities and dissimilarities among the research works, which are further classified into sub-class based on some special parameter. The comparison of these research works was done based on parameters proposed class, Algorithm used in the research, common evaluation matrix Classification Accuracy.

Keywords: Classification · Visual arts architecture · Machine learning

1 Introduction

Visual architectures are one of the treasures of the past, which our ancestors gifted to us. There maintenance and conservation are necessary to pass it to our successor generations. But as now the world is moving in digitized phase and advanced algorithms with powerful machines are available, it is necessary to digitize this work of these arts to remain in their existence in future decades and hand it over to the next generations. Some researchers start working in the direction to digitize these works. The research works related to the visual art architectures are analyzed in this research. The number of such available research works is few in numbers. The number of research works is nine. These nine are [1–8], and [9]. These all nine-research works are considered for the study in this paper. The paper is divided into four sections. In the first section, the considered papers are classified into classes and sub-classes. These classes and sub-classes are proposed based on the similarities and dissimilarities among the

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 68–78, 2023.
https://doi.org/10.1007/978-3-031-13150-9_6

methodology mentioned in the research paper. The next section lists detailed descriptions of all the research works. The description covers the aim of the research work, their main outcomes, dataset, used methodologies, their results with evaluation matrices, and future work is available in the paper. In the second last section, an analysis of results is done. In the last section, conclusions are drawn while comparing the considered works. The comparison is done based on different parameters. These parameters include the proposed class, authors of the research work, the dataset used for the research, used methodology, and common evaluation parameter classification accuracy.

2 Related Work

Literature on recognition and detection of Visual Art Architecture is few. The number of these pieces of literature that are available for the study is nine. These nine can be classified into three categories (shown in Fig. 1)), based on some common parameters. These categories are as follows:-

1. Classification of monuments
2. Detection of monuments
3. Analysis of sentiments related to monuments

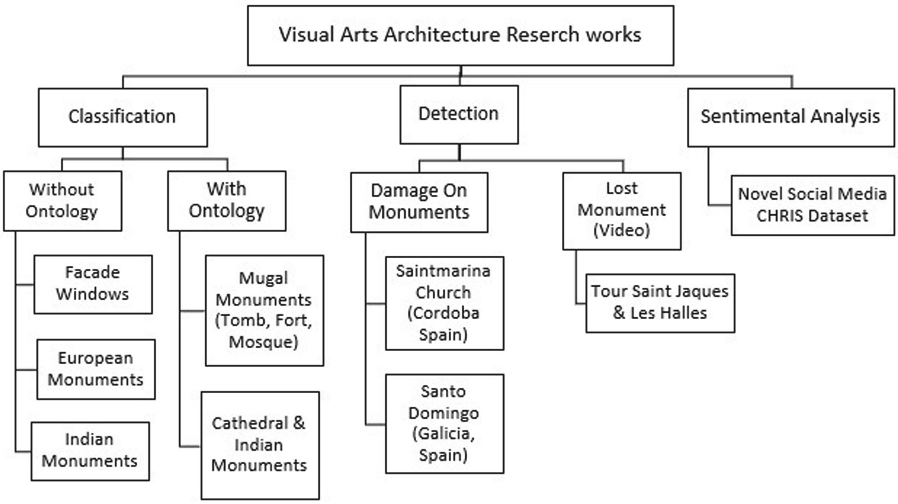


Fig. 1. Classification of research works.

2.1 Classification of Monuments

The research works that deal with the classification of monuments fall under this category. The classification of monuments can be done using ontology or without ontology. Three research works [3,8,9] propose the classification using without an ontology and two with ontology [4,6]. Without ontology, work is done by considering facade windows, European monuments, and Indian monuments. While with ontology, work is done by considering Mughal monuments (such as a tomb, fort, and mosque), cathedrals, and Indian monuments.

2.2 Detection of Monuments

The work that tries to find the damage on the structure of monuments and lost monuments are listed under this category. Out of nine studies, three fall under this category. In the first subcategories, the occurrence of damage on the monuments due to external factors such as environmental and human-related are detected. For this detection, two research works are considered [2,5]. In both the studies, Spain churches are taken as a sample. These two churches are Saint Marina Church (Cordoba, Spain) and Santo Domingo (Galicia, Spain). In the second subcategory, lost monuments that were the part of past are detected using available videos of that period [1]. The two buildings that are found in the research study are Tour Saint Jacques & Les Halles.

2.3 Analysis of Sentiments Related to Monuments

In this category, the research works that find the sentiments of tourists who visited the monuments are listed. In this list, only one research is classified [7]. This research is done by using not a specific monument but on all the world's monuments images that are shared on social media by the tourist. The collected social media images are named as novel social media CHRIS datasets.

3 Description and Comparative Study of Research Works

1. In 2011, Shalunts et al. [9] proposed a classification method to classify the building architectural styles from windows available on the facade of architecture. Architectural styles constructed in the historical period developed one after another follows similar or some modifications in the elements like windows of the facades. In the study, three types of window facades are considered. These are Romanesque windows, Gothic-style windows, and Baroque-style windows. These windows have some characteristic features like Romanesque windows have a round arch in one, two, or three in number, Gothic-style windows have an arch with points or rose shape, and Baroque style windows have Pediments in triangular or segmental shape. These characteristics help in virtual tourism, fast searching, and indexing of buildings. The author claims that before this study there exists no automatic system that can classify architectural styles by using building facade images. For the study 400 images were collected, of which 531 were collected by authors and 49 were collected from the Flickr website. Images resolution varies from 138*93 to 4320*3240 pixels. The training set used for the experiment contains

90 images. The experimental process used in this study is described in Fig. 2. In the process, firstly, local features of images were extracted using SIFT algorithm then image features were clustered using the k means clustering algorithm. After that, a bag of words algorithm was applied to the clusters. Then, histograms were created by the results of previous algorithm results. Lastly, using a histogram as an input of the classifier, classes were obtained. The outcomes of the study were as follows: -

– Due to the high complexity in architectural styles, the rate of false classification is very high.
– For this type of classification, there is a lack of visual information.
– This study is limited to only one component.

In the future, this classification can be done by considering other elements like towers, domes, columns, etc. And other architecture styles.

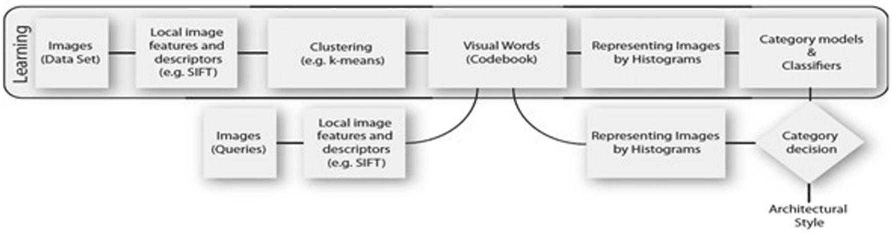


Fig. 2. Used Methodology

2. In 2012, Goel et al. [3] proposed a method for identification of the European architectural scenes' characteristic elements automatically. These characteristics elements play the role of low-level features. These low-level features can be mined to attain the categorical details of architecture styles. There exist some challenges that occurred during the mining of characteristics features. These challenges are first, characteristic features are measured by using different scales; second, image capturing done using different viewpoints; third, some visual characteristics appearance vary across monuments. To solve this problem, the author performs two experiments. For the experiment, high-resolution images were taken from the internet. For testing and training, different images of different monuments are considered. For the first experiment, the authors collected twenty-five different same architecture styles of European monuments, collected from flicker and Google images. Filtering of images was done manually. The images that contain the front view were selected and the rest were rejected from the collection. The final data set for the first experiment contains 6713 images having resolution 640 by 480 pixels. Features like shape color and appearance were used as a characterization of images. For color, color descriptors with visible words were used. For shape, HOG descriptors were used. And for appearance, SIFT descriptor was used. They perform a second experiment to compare their work with existing work.

For this purpose, they have used 423 images data set. The data set contains 111 Gothic images, 156 Korean images, 81 Islamic images, and 75 Georgian images. In both the experiments, classification was done on data sets using word mining and a combination of word mining with SVM algorithms. The results were collected using the classification accuracy parameter. The classification accuracy was 32.64% for World mining, 46.22% for SVM, and 48.25% for word mining with SVM. The classification accuracy was low because of two reasons. First, training and testing use different monument images. Second, the data set nature was challenging. This study reserve special context by using local features combination which was lost when the experiment was done only with the bag of words algorithms. Several characteristics that are difficult to capture like the plan of the building, internal features, or the monument height were not considered in the study. No future work is defined by the author in the paper.

3. In 2015, Gupta & Chaudhury [4] proposed a method to classify the fort, tomb, and mosque images using a combination of CNN and ontology. Ontology was used to define abstract classes of images having a lack of clear visual connection. Expected classes were obtained by applying certain rules. The motivation behind this study was that meta data and image tags are used by search engines to retrieve images. And the other studies were done in this field to classify use only on the knowledge domain of facade windows. According to the author, ontology provides better assistance for the classified learning phase and improves image retrieval. For performing the experiment, Taj Mahal, Humayun tomb, and Akbar tomb images were selected. Images of the Akbar tomb and Taj Mahal were used for training the classifier whereas the testing was done on Humayun tomb images. The training set also contains images of Red fort, Agra Fort, and Charminar to improve the learning. Images were labeled 1 if it is belonging to Tomb otherwise zero. The data set used in the study contains 1500 images. All images used in the study were downloaded from the internet. The authors used 7-layer CNN as shown in Fig. 3. Out of seven layers, five were convolution and two were fully connected. 4096 feature factors were obtained from the last year were used to find the class of the test image. The classification accuracy of the classifier was 75.59%. This approach can be applied in the future to the problems having hundreds category.
4. In 2021, Ninawe et al. [6] proposed a classification model to classify Indian Mughal and cathedral monuments. Their work was similar to (Gupta & Chaudhury, 2015). Their data set contains 5000 images of Indian Mughal monuments and cathedral monuments having different resolutions are used. For the experiment, python 2.7 with TensorFlow, intel R core TM i5 processor with 4GB RAM were used. They used a similar 7 layers CNN model that is used by paper Gupta & Chaudhury [4]. The only difference in their CNN model was in the fully connected layer. The first fully connected layer has 2048 features which reduce to 224 features in the second fully connected layer. The CNN model used in the study is shown in Fig. 4. This model performance was calculated by classification accuracy. The classification accuracy of the classifier was 80. In this study, results were compared with the results

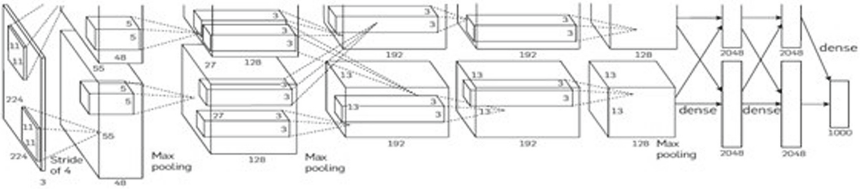


Fig. 3. The Architecture of 7-layer CNN

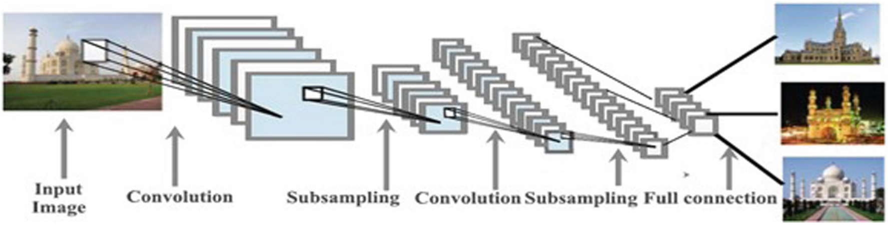


Fig. 4. The Architecture of 7-layer CNN

Table 1. Comparison of classification accuracy.

Method	Classifier	Best accuracy (%)
Gupta et al.	Logistic	54.6
	Objective 1	63.5
	Objective 2	71.4
Proposed method	CNN	80.0

of previous work as shown in Table 1. The limitation of the study was that the compared results were obtained by using different data sets while using a similar CNN model.

5. In 2017, Saini et al. [8] proposed a CNN model to recognize Indian monuments. This recognition helps in the promotion of the culture of India on the mobile application. The author claims that in this direction of image classification still less work has been done previously. Images of different orientations of monuments can help in their recognition. Two issues were addressed by the authors in the existing studies. First, less accuracy due to the presence of noise in the images. The noise consists of an animal, trees, people, decorations, etc. Second, for a single monument classification, too many images with different orientations were needed. The authors solved the first problem by cropping the images manually. For the study, data was collected from the internet. The data set contains 5000 images. For classification, data were divided into a 70:30 ratio. The training set and the testing set contain 35 and 15 images for each monument class. 100 classes of public monuments were used for classification. On the data set, HOG + SVM, HOG + Random for-

est, HOG + KNN, LBP + SVM, LBP + random forest, LBP+KNN, GIST + SVM, GIST+ Random forest, GIST + KNN, CNN FC6 CNN FC7 and CNN FC6 +FC7 were used. Classification accuracy was used to evaluate the models are listed in Table 2. From the table, it is concluded that CNN FC6 gives the best results. For CNN FC 6, classification accuracy was 92.7%. The CNN model used is shown in Fig. 5. In the future, this work can be extended by increasing the data set size and including more architectural styles.

Table 2. Compared results.

Technique	Accuracy (%)
HOG+SVM	1.47
HOG+Random Forest	1
HOG+KNN	1
LBP+SVM	7.23
LBP+Random Forest	14.27
LBP+KNN	20.09
GIST+SVM	1
GIST+Random Forest	1
GIST+KNN	1
CNN fc6	92.7
CNN fc7	90.60
CNN fc6+fc7	91.82

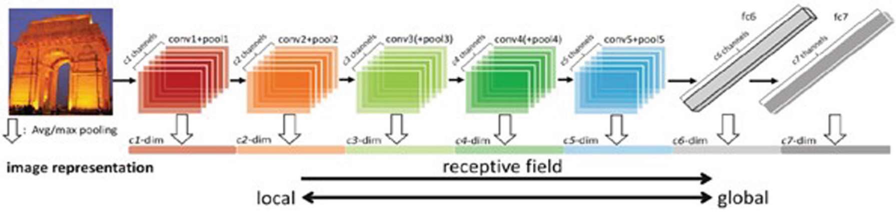


Fig. 5. Representation of CNN proposed architecture

6. In 2015, Meroño et al. [5] evaluate an object-oriented classification application for historical buildings. It includes: first, detect damage on stone; second, a position; third, measure and map concrete surface pathology; fourth, restoration and quantification. For the study, Santa Marina Church (Cordoba, Spain) was chosen because it was built in the 13th century and it is necessary to monitor it for conservation. For monitoring, different equipment was used. These equipment were Lica HDS 6600 laser scanner, fuji film IS-pro digital single-lens reflex camera, and ENVI Zoom 4.7 software. Lica HDS 6600 laser scanner was used to create a 3D virtual realistic monument model. Fuji film IS-pro digital single-lens reflex camera was used to identify the materials used during construction and identification of material affecting the pathologies.

Software ENVI Zoom 4.7 software was used to extract features of monuments for image restore. Previous studies done in this fieldwork were based on remote sensing where response levels on the electromagnetic spectrum of each photographic pixel were recorded while ignoring the image spatial structure. The issues of traditional studies were focused on in the study by using new object-oriented classification methods. These methods focus on the texture, shape, and spectral information of the image by dividing the image into a variety of objects. A list of these objects helps in the analysis of images and interprets some fruitful outcomes. The classes of classification include plaster and cement; patinas and alveolar erosion; upper vegetation; lichens; mosses and biocalcarenites. For classification, the k nearest neighbor algorithm model was used. Model performance was measured with the help of Kappa statistics and classification accuracy. The value of Kappa statistic and classification accuracy is 85.70% and 92% respectively. The outcomes of the study were as follows. First, each pathology effect on the church part was easily identified. Second, reduces the cost of restoration. And Third, accurate results for provided for damage detection.

7. In 2006, Crespo et al. [2] proposed unsupervised classification techniques to detect damages to historical buildings. Detection and documentation of these damages work are time-consuming and expensive. To address this issue, classification can be used. For classification, intensity data of terrestrial laser scanning and color was used. The data was collected using terrestrial laser scanner system Nikon D200 camera and Riscon Pro software. A terrestrial laser scanner was used to capture the intensity. Nikon D200 camera was used to capture the images that provide color information. Riscon Pro software was used to process the data. Images of Santo Domingo ruins (Galica, Spain) were used to create data set. The material of the building was granite. The classes used in the classification were lime/more remains and high moisture level ashlars. In the experiment, the Iso-data algorithm proposed by Tou in 1974, the k-means algorithm proposed by Tou in 1974, and the fuzzy k-means algorithm proposed by Bezdeke in 1973 were used. The Algorithm's performances were measured based on classification accuracy. The classification accuracy obtained from Iso-data, k-means, and fuzzy k-means was 62.14%, 74.21%, and 78.95% respectively. Based on the accuracy, it was concluded that the fuzzy k-means algorithm performs better to classify damages of the lime mortar. The results were also verified by the expert. The advantage of this study was that one cannot need any prior knowledge about the area.
8. In 2019, Paolanti et al. [7] proposed a method to analyze the sentiments of social media users about the monuments. The motivation behind the research was, if the sentiment is positive then it will increase the value of monument images. According to the author, before this study, there exists no research that relates social media users with cultural heritages. For experimental purposes, a new data set named novel social media CHRIS was used. The records were collected manually. It contains more than 17500 images. After selecting, only 8472 pictures were considered for the study. Out of 8472 pictures, 2960 picture shows positive sentiments, 2891 picture shows neutral

sentiments and 2626 picture shows negative sentiments. For this data set, 3 versions of different pixels were created. These versions were 224 by 224, 299 by 299, and 331 by 331 pixels. For classification, the used data sets were split into 80:20 ratio. VGG16 and inception algorithms were used for classification. The result of the classification was measured using accuracy, precision, support, and confusion Matrix. Best results were obtained with ResNet. For ResNet, all the measuring values parameter was 0.70. This research concluded that sentiment helps in finalizing the distribution of needs and better conservation planning of cultural heritages.

9. In 2020, Condorelli et al. [1] proposed a neural network-based approach for detecting lost heritages from historical videos. The motivation was that multimedia can help in documenting the details of lost heritages that were once part of the city and no organized data is available about them. To experiment, the author chooses two buildings. These two were Tour Saint Jacques and Les Halles. Data were collected using web crawling, Adhoc-photographic survey of the location, and historical archives of Paris consultation. The experimental process used in the study is shown in Fig. 6. The process consists of three phases. These phases were detection of the object using AI, SFM pipeline, and assessment of metric quality. Each phase has three steps. The first phase contains collection and labeling of data set as the first step, training, and testing as the second step, and peak organization of objects and extraction of frames as the last step. The second phase contains detection and extraction of features; matching features and verification of geometry; and structure and reconstruction of motions. The last phase contains the comparison of benchmark, comparison of cloud-to-cloud distance, and comparison of feature points. The process results were measured using accuracy, sensitivity, discovery rate (DR), time save ratio (TSR) and the time save efficiently (TSE). In the future, this research will become the source of interest in this field to create more efficient and accurate systems.

Fig. 6. The Architecture of 7-layer CNN

4 Result Analysis

The results of the study are given in Fig. 7. The results are drawn based on the common evaluation parameter of all the different considered literature discussed in the previous section. The common evaluation parameter is classification accuracy. Classification accuracy is obtained in the discussed literature by applying

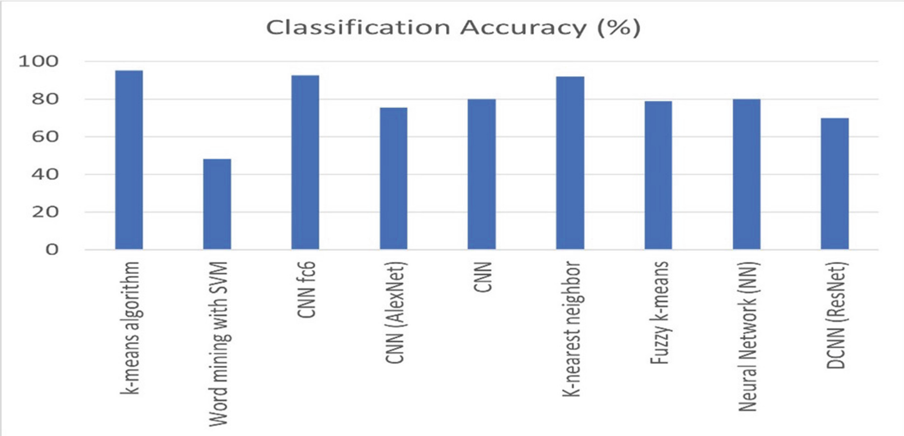


Fig. 7. Classification accuracy

different proposed algorithms. These algorithms are k-means [9], word mining with SVM [3], CNN fc6 [8], CNN(AlexNet) [4], CNN [6], K-nearest neighbor [5], Fuzzy k-means [2], Neural Network (NN) [1] and DCNN(ResNet) [7].

Table 3. Comparative study of research works.

Class	Authors	Monument types	#Dataset	Machine learning algorithm	Classification accuracy (%)
Without Ontology	Shalunts et al. [9]	Façade windows	400	k-means algorithm	95.16
	Goel et al., 2012 [3]	European monuments	6713	Word mining with SVM	48.25
	Saini et al. [8]	Indian monuments	5000	CNN fc6	92.70
With ontology	Gupta & Chaudhury [4]	Mughal monuments	5000	CNN (AlexNet)	75.59
	Ninawe et al. [6]	Cathedral & Indian monuments	800	CNN	80
Monuments damage detection	Meroño et al. [5]	Saint Marina Church	1000	K-nearest neighbor	92
	Crespo et al. [2]	Santo Do Mingo		Fuzzy k-means	78.95
Lost Monument detection	Condorelli et al. [1]	Tour Saint & les Halles	320	Neural Network (NN)	80
Sentimental analysis	Paolanti et al. [7]	Novel social medial CHRIS dataset	8472	DCNN (ResNet)	70

5 Conclusion and Future Work

Table 3 shows the comparison of all the research works considered for this study. From the table, it is interpreted that most of the research works are done on monuments of Europe and India. Out of 9, 5 research works use neural networks versions. The overall best accuracy of 95.16% is obtained for k-means clustering algorithms and the lowest 48.25% is obtained for World mining with SVM. This study shows that the documentation of visual arts can be done for existing as well as lost monuments by using machine learning algorithms. This will be an emerging area of research in the future because of the availability of powerful equipment that captures more data with high clarity and advanced algorithms.

References

1. Condorelli, F., Rinaudo, F., Salvadore, F., Tagliaventi, S.: A neural networks approach to detecting lost heritage in historical video. ISPRS Int. J. Geo-Inf. **9**(5), 297 (2020). https://doi.org/10.3390/ijgi9050297
2. Crespo, C., Armesto, J., González-Aguilera, D., Arias, P.: Damage detection on historical buildings using unsupervised classification techniques. Int. Arch. Photogrammetry **4**(20), 182–182 (2006). https://doi.org/10.1111/j.1477-9730.1962.tb00343.x
3. Goel, A., Juneja, M., Jawahar, C.V.: Are buildings only instances? Exploration in architectural style categories. In: ACM International Conference Proceeding Series (2012). https://doi.org/10.1145/2425333.2425334
4. Gupta, U., Chaudhury, S.: Deep transfer learning with ontology for image classification. In: 2015 Fifth National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG), pp. 1-4 (2015)
5. Meroño, J.E., Perea, A.J., Aguilera, M.J., Laguna, A.M.: Recognition of materials and damage on historical buildings using digital image classification. South Afr. J. Sci. **111**, 1–2 (2015). https://doi.org/10.17159/sajs.2015/20140001
6. Ninawe, A., Mallick, A.K., Yadav, V., Ahmad, H., Sah, D.K., Barna, C.: Cathedral and Indian Mughal monument recognition using tensorflow. Adv. Intell. Syst. Comput. **1221**AISC, 186–196 (2021). https://doi.org/10.1007/978-3-030-51992-6_16
7. Paolanti, M., et al.: Deep convolutional neural networks for sentiment analysis of cultural heritage. Int. Arch. Photogrammetry, Remote Sens. Spat. Inf. Sci. - ISPRS Arch. **42**(2/W15), 871-878 (2019). https://doi.org/10.5194/isprs-archives-XLII-2-W15-871-2019
8. Saini, A., Gupta, T., Kumar, R., Gupta, A.K., Panwar, M., Mittal, A.: Image based Indian monument recognition using convoluted neural networks. In: 2017 International Conference on Big Data, IoT and Data Science (BID), pp. 138-142 (2017)
9. Shalunts, G., Haxhimusa, Y., Sablatnig, R.: Architectural style classification of building facade windows. In: Bebis, G., et al. (eds.) ISVC 2011. LNCS, vol. 6939, pp. 280–289. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-24031-7_28

Technology Aspects of Artificial Intelligence: Industry 5.0 for Organization Decision Making

Aditi Chandel[1] and Bhisham Sharma[2](✉)

[1] School of Business Studies, Chitkara University, Solan, Himachal Pradesh, India
aditi.chandel@chitkarauniversity.edu.in

[2] Department of Computer Science & Engineering, Chitkara University School of Engineering and Technology, Chitkara University, Solan 174103, Himachal Pradesh, India
bhisham.pec@gmail.com

Abstract. In today's time, with the digital revolution and the advent of technologies both customers and organizations are getting exposed to a larger amount of information than ever before, making organizational decision making challenging. Industrial Revolution 4.0 led to the emergence of smart factories with the development of technologies such as Internet of Things (IoT), Sensors, Industrial Internet of Things (IIoT), Cyber-Physical Systems, Cloud Computing, Big Data, and Artificial Intelligence (AI). Their prime focus was to increase productivity and mass production through automation and somewhere superseded humans over technology-enabled machines. With the uprising of Industry 5.0, the vision for this industrial revolution is perceived as supporting not superseding humans. Humans and AI may have multiple roles to play in an organization, but organizations in which both humans and AI act as decision agents need to emphasize managing the impact of technological involvement on human performance and vice-versa, to work in collaboration. This study aims to understand the role of human and AI-enabled machines in organizational decision-making. Different strategies related to human-machine collaboration existing in research are also discussed to enable the organizations, as well as the researchers, to identify the most suitable strategy for organizational decision making in industry 5.0, where human-machine collaboration is the primary goal.

Keywords: Artificial Intelligence · Industry 5.0 · Industry 4.0 · Decision making · Human-machine collaboration · Organization

1 Introduction

Since early times organizations are on a continuous voyage of utilizing the information, they are bombarded with on a daily basis. Artificial Intelligence (AI) has the potential to drive valued outcomes for organizations; as a result organizations are rapidly adopting AI into their various organizational processes. The integration of technologies in the organization has become a default mechanism because of the several limitations of humans working in it. One of the major limitations is the limited brain capacity of humans to

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 79–90, 2023.
https://doi.org/10.1007/978-3-031-13150-9_7

analyze the huge influx of data the organizations are having. Therefore, with a perspective of overcoming the limitations of humans and machines, organizations are entering into the landscape of human and intelligent machine collaboration [1]. AI systems now no longer passively receive human inputs [2, 3] but are developing the capability of learning, adapting, and collaborating with human interaction [4] in organizations. Existing literature mainly discusses the application of AI in organizational functions such as assembly lines, job tasks, and customer interactions [2, 5, 6]. Further, Fig. 1 shows that convergence of various technologies including AI can provide a transition to society 5.0 by including evergetics that involve heterogeneous actors for the regulatory processes of problem situations [7]. Therefore, researchers, organizations have felt the need to shift their focus from considering AI just as an application to a collaborator.

It has been witnessed that organizations even on the adoption of AI are not able to experience the anticipated benefits, resulting in adoption failure [8]. Trend [9] reported that around 50% of senior managers found it difficult to integrate AI with the people working in the organizations. Few of the major challenges faced by humans in delegating tasks to AI, raise questions about joint human-machine managerial decision making:

1. Working of algorithm-based AI- How algorithm takes decisions [10].
2. Rationality behind AI-enabled decision software.
3. Organizational environment is uncertain and is available with asymmetric information [11]
4. Algorithm aversion [12]
5. Breaching of ethical, moral and basic fundamental human rights [13]

Researcher [14] explored empirically the difference in manager's perception concerning AI and humans as decision delegates. The results depicted that managers did not establish much emotional relationship with AI and felt insecure about delegating strategic decisions to AI. Various reasons for not delegating work to AI were also observed such as overconfidence in human capabilities, lack of trust in AI, and desire to remain in control. Further, it was revealed that human managers are ready to accept machines into the decision-making process provided machines have less control than humans [15]. In support of the above finding, researcher [16] depicted those managers experiencing loss aversion towards machines when the role of machines is just restricted to being advisory. The results of their study depicted that except for a small-scale class of managers all managers opposed the partnership with the machine having full control in managerial decisions. Therefore, it becomes clear that managers do not react in the same manner at various levels of human-machine involvement. Also, the role of humans (managers) as users and developers of AI-enabled decision solutions need to be distinguished.

Thus, the above discussion emphasizes the need to understand whether humans are comfortable having machines as a co-worker. An effort has been made in this study to identify the different roles performed by AI in organizational decision-making along with the critical issues associated with it that affect humans working in the organization. The understanding of this aspect is vital to understand how the integration of AI with a human in organizations is possible, thereby affecting the adoption rates of AI in organizations. Industry 4.0 is representative of technology-enabled machines and the future Industry 5.0 is of the vision to collaborate human and intelligent machines. Therefore, practitioners and researchers have realized that for the effective intervention of technology in the organization it is important that the humans working in the organization must interact, embrace and integrate their behavior with technology-enabled systems [17].

In the next section related work on Industry 5.0, role of both AI and humans in organizational decision making is discussed. Following sections discuss the human-machine collaboration, the role of explainable artificial intelligence in decision making and challenges. Finally, a conclusion has been made.

2 Related Work

2.1 Industry 5.0

Industry 4.0 was all about adding value to the manufacturing systems by creating cyber-physical production systems that involved networking of all the systems leading to autonomous decision-making processes in real-time. With rapid industrial revolutions and recent technological advancement, the 5th revolution is on its way. Industry 5.0 aims to create value in Industries by associating the robotic, automated, and digital advances with the creativity or intuitive side of humans through IoT and other automotive technologies such as AI. While Industry 4.0 was about automation, Industry 5.0 is about collaboration between humans and machines. Machines or robots are well attributed in achieving standardization in a high production volume but customization or personalization of products is a challenge for machines or robots as here they require guidance, making human intervention vital. Thus, in Industry 5.0 the focus will be on the return of human minds in the industries and covering the necessary core elements of personalization and mass customization of products for consumers by taking a step ahead of the core elements of Industry 4.0, that were mass production automation and digitization.

Sowa et al. [18] confirmed that productivity is enhanced due to human-AI collaboration. Their study focused on research modes of collaboration between humans and enterprise bots and suggested that AI in the future needs to focus on collaboration approaches rather than on full automation. Although practitioners and researchers have emphasized the augmenting and collaborative effect of AI with humans, an important context got highlighted by Haesevoets et al. [19]. They studied the extent to which human managers are willing to accept and cooperate with machines. Their study revealed that human managers are open to cooperative partnership with machines provided decisions are made mainly on their judgement and inputs. Few classes of managers exhibited complete resistance to the employment of machines taking managerial decisions. Thus, with Industry 5.0 upsurge, it becomes important to understand the different circumstances or organizational levels at which humans are ready for the cooperative partnership between humans and machines. The need is for a human touch revolution in Industry 5.0. The same is possible when the roles of both machines and humans are clearly defined to maintain a balance between both of them. Repetitive and labor-intensive work is meant to be kept for the machines [20] and creative and innovative work for humans. Thus, human intervention will be more on the intellectual side than physical. Table 1 highlights the technology enhancement from 4.0 to 5.0.

Table 1. Technology enhancement from 4.0 to 5.0

S. No	Subject area	Technology 4.0	Technology 5.0
1	Scalability of economy	Free from focus on efficiency	Target on problem-solving and value creation
2	Focus	Smart factories	Human-robot working together
3	Uniformness	Release from the repression of individuality	Focus on diversity where everyone can follow their abilities
4	Application	Free from discrepancy and imbalance	Focus on decentralization (Building a society where everyone gets opportunities anytime anywhere)
5	Fragility	Release from anxiety and uneasiness	To build a resilient society where everyone can follow challenges in a secure environment
6	Consumption of resources and impact on the environment	Removing the resources and environment constraints	Build a society where humans live in harmony with the environment. (Maintain and improve the resources and environment)

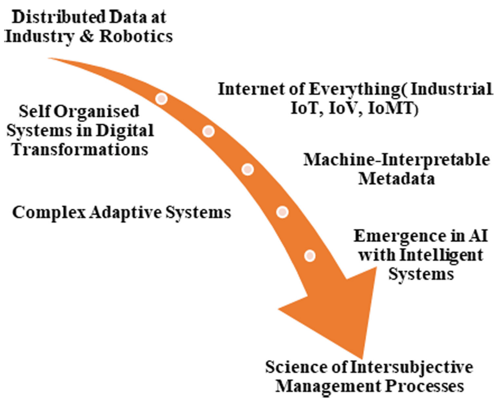


Fig. 1. Society 5.0-science and technology convergence

2.2 Decision Making

Organizations are perceived as a "network of decisions" that needs a holistic approach to arrive at the most suitable decision that attains the organizational goals in the best way.

Decision making in an organization becomes challenging because of the uncertain, complex and ambiguous environment prevailing at different organizational levels [21]. Thus, decision-making demands a decision-maker to have a holistic approach by being both rational and intuitive. Sadler-Smith and Shefy [22] stated that intuition and rationality are the "parallel systems of knowing". Understanding the nature of the organizational environment along with the role of human and technology (AI) in organizational decision making becomes necessary with the emergence of the fifth industrial revolution witnessing the synergy between humans and machines.

2.3 Human Role in Organizational Decision Making

For ages, the human role in decision-making has been recognized and accepted in organizations without any dilemma attached to it. However, with the increasing intervention of technologies in organizations, the contribution of the human role in decision-making is being questioned. Owing to the huge data influx and the available information in the real world, humans are facing the challenge of information processing because of their limited brain capacity or ability to process a large amount of information. This phenomenon has been explained as bounded rationality in past research [23]. Bounded rationality is based on the assumption that because of the human limitation of processing large information they are not fully capable of making optimal and rational decisions in complex environments. As a result, to make decisions in a complex environment, humans tend to use intuition which is a function of experiences and is associated with feelings and emotions [23, 24]. To consider intuition as the mode of decision- making is not embraced by all researchers because of the heuristics, biases, and irrational thoughts attached to it. According to Akinci and Sadler-Smith [25] the three forms of biases associated with it are availability- as it will consider only the information which will come easily to the human mind, representativeness- as it will be based on the similarities with prior situations and anchoring- refers to what comes first in the human mind. Lipshitz et al. [14] proposed the naturalistic decision-making framework which diverges from the biases discussed above. They highlighted the role of expert intuition as a necessary condition for using intuition as an impactful mode of decision-making [26]. In the situation of uncertainty, ambiguity, and when tasks are ill-structured in an organization, the role of expert intuition is considered as one of the effective modes of decision making in the domain of expertise [27, 28].

However, with the advent of new technologies and their unlimited capacity for information processing, efforts are made by organizations to make the rational or reasoning approach of new technologies run parallel with the intuition and rational approach of humans especially in complex decision-making environments [24]. AI is capable of imitating human reasoning more narrowly and powerfully. However, the rational processes related to new technologies are not considered appropriate in an ambiguous and uncertain environment as the intuition process is something that cannot be handled by AI. Weak AI such as ML follow rule-based decision making and cannot imitate or code the characteristics such as creativity, common sense, or imagination which are common characteristics of humans and play a vital role in decision making especially at managerial levels [29]. Humans using their advantageous capabilities and understanding of morals and ethics can mandate an AI-enabled machine to take a decision within a framework defined by them and prevent it from taking the decisions not acceptable by the society.

2.4 Technology Role in Organizational Decision Making

Extant literature is of the evidence that AI can be used for various organizational functions like an assembly line, job tasks, customer interactions [5, 6] but the research is still nascent concerning its relational aspect. The need for a new industrial revolution is to focus on AI as a collaborator rather than just as a technique or application. Many researchers are of the evidence that technology- enabled machines are active agents in improving decision making rather than just being the passive receivers of human inputs [2]. Till now industry has witnessed considerable adoption of AI in organizations because of its learning and prediction powers. In terms of organizational decision making the understanding of AI strengths and weaknesses is important both for the organization and its employees in order to enable higher-quality decision-making mechanisms [1].

In decision making, AI is expected to take decisions not only related to automation of routine tasks in operations but with recent advancements in new machine learning techniques, deep learning & neural networks allows the organizations to use AI-based decisions for managerial tasks [30], strategic decisions related to business models, pricing and competitive strategies and channels of communication [31].

In comparison to human decision-making, AI decision-making is made on algorithms. This algorithm-based AI is found to be functional in eliminating human cognitive bias based on emotions. The extensive automation in industrial revolution 4.0 led to the fear in the minds of employees that they will be replaced, but decision-making was one such context that was considered to be reserved only for humans. Continuously advancing technologies and their algorithms, especially AI and its sub- components like deep learning, machine learning are changing the scenarios by taking over many decision responsibilities. Human decision-making because of its biggest drawback of being biased and irrational is getting substituted by technology-enabled machine decision making which is autonomous, unbiased, and rational [29, 32]. There is evidence in the literature that supports that AI-enabled machines outperform humans in the majority of tasks such as medical diagnoses, recruiting new staff, employee performance and politicking [13, 33–36]. AI can learn, adapt and collaborate with employees but, it is less effective in an ill-structured and uncertain organizational environment. AI-enabled machines follow the rule of algorithms, as a result, their decision-making is considered to be rule-based decision making. Therefore, machines are meant to make decisions majorly dependent on the inputs they receive from humans, who are the developers or designers. They make the decisions and machines just reproduce them.

On the other side Burton et al. [37] highlighted that nowadays managers use AI-enabled software for both decision support and for delegating decision making. Therefore, the above discussion makes it evident that paradox prevails when it comes to AI as a decision-maker. Makarius et al. [4] suggested two social processes named sociotechnical systems theory and organizational socialization framework for understanding the effective integration of AI-enabled machines with humans. Dejoux and Léon [29] stated that when it comes to decision-making AI has three roles to play in an organization, as an assistant to the manager, as a decision-maker instead of a manager, and as a forecaster for the manager.

3 Human-Machine Collaboration

With the uprising of Industry 5.0, the fear in the mind of humans to get replaced is creating a thwarting effect on humans in the organizations. Therefore, it becomes important for organizations to find ways for AI-enabled machines and humans to work together and in cooperation. It is stated that AI and Humans complement each other in organizational decision-making by bringing in their respective strengths. AI contributes by extending human cognition when addressing complexity through their rational approach and Humans by using their intuitive approach in uncertain and equivocal environments [1]. In literature, emphasis is laid on the successful implementation of human-machine interaction by understanding the organizational aspect of an organization such as strategic planning and management. The "machine in the loop" approach supports this where machines play a supporting role and humans take full control [15]. Humans are ready for a partnership with machines only if in the partnership they have a major role in decision-making over machines. The prime focus of future AI is not full automation but collaborative approaches that tend to increase productivity. Industry 5.0 revolution will be about cobots, drones, and more advanced technologies. Cobots are collaborative robots that intend to interact and assist humans in their shared spaces mainly in manufacturing facilities [38]. Advanced technologies such as deep learning and natural language processing are continuously contributing by adding the element of emotions in the smart machines or robots which was the only aspect humans could express. This has led to the fear that smart machines will soon replace humans. Further, AI is considered as a threat of stealing of data and information of unsuspecting individual/consumers [39], creating trust issues not only among the organization but its consumers.

Huang and Rust [40] discussed that Human Intelligence (HI) and AI can effectively collaborate without imposing any threat, by identifying their respective strengths, by having lower-level AI augmenting higher-level HI and by moving HI to a higher intelligence level when AI automates the lower level. Therefore, the need is to have a more agile innovation organization [41]. Makarius et al. [4] explained the integration of employees and AI through sociotechnical systems theory and organizational socialization framework. Sociotechnical systems explain the link between the technological processes and social systems and emphasis on joint optimization of technology and the human within a given context and socialization transforms the organization outsiders into effective and participative insiders. They proposed that if a systematic and structured socialization process will be used to bring AI into the organizations then it will result in different levels of sociotechnical capital-competitive advantage.

AI's role in controlling human delegates was also studied by Kellogg et al. [42] who identified six mechanisms- restricting, recording, replacing, rewarding, recommending, and rating. Various studies in literature propose that there is a difference in the way human managers perceive AI and their fellow workers as potential human delegates [41, 43]. Along with managers, customers are also found to exhibit more negative responses in case of technology failure than for employee failure [13, 26, 39]. An empirical study conducted by Haesevoets et al. [19] comprising 1025 managers revealed that the acceptance rate of human managers for machines increased until the point where humans had 70% weight in managerial decisions. Therefore, the boundary between humans and machines in decision-making is shifting with every industrial revolution from the first industrial revolution to the fifth industrial revolution. Organizations must identify different ways to build a relationship between humans and technology or AI-enabled machines.

4 Role of Explainable Artificial Intelligence in Decision Making

AI is empowering humans by the use of its advanced technologies such as machine learning, deep neural networks and internet of things. Superhuman performances are being exhibited by machine learning as well as deep learning methods through increased model complexity, turning the systems into a "black box". The last hype of AI systems-expert systems and rule-based models were interpretable. But, new-generation AI systems such as deep neural networks entail opaque decision systems. Widespread adoption of the Black box is acceptable in case of recommendations where the cost of risk failure is less or was the case. However, the same is not true in the case of sensitive domains like healthcare, medicine, defense and self-driving cars where the cost of risk failure is high, making it vital to explain the what, how, and why of the decisions taken by the black box [44–46].

As a result, Explainable Artificial Intelligence (XAI), develops new methods that explain and interpret machine learning models or AI systems and make them understandable and trustable for humans [47]. Transparency and post-hoc explanations mainly describe XAI. Transparency is all about revealing the information about the internal structure of the model to identify in what manner the system reaches an output and post-hoc explanations provide information about the output cause [48]. Hepenstal and McNeish [49] are of the view that a 'one-size-fits-all approach to XAI is insufficient. They emphasized that the needs of both the developers and users need to be considered during the design process. Also, the explanation should be at the global level explaining the individual outputs as well as the process by which they have been reached. XAI methods enable to open the black box by assessing whether neural networks have learned their task or to analyze which input might have an adversarial attack.

To optimize assembly processes models Layer wise Relevance Propagation (LRP), the Gradient weighted Class Activation Mapping (Grad-CAM) method, and Local Interpretable Model Agnostic Explanations (LIME) are used [50]. In other words, for human-machine augmentation or collaboration, it's important that machine decision-making is open to human scrutiny and for that organizations need to adopt XAI which is the future of AI.

5 Challenge and Future Directions

- Human-Machine interaction, on its own, faces the biggest challenge of transparency and reliability. AI is not purely rational and free of bias. The reason being that AI is dependent on the quality of data used to train the algorithms which can be biased as well as can be subject to programmers' bias when developing the algorithm.

- The inability of humans to understand how machines make decisions, making technology driven machines a "black box". A decision made by machine learning algorithms that are multi-layered and based on combinations of multiple factors at every layer is difficult to explain and creates mystery and skepticism.
- AI-based decisions face the risk of omission errors that explains that AI during the process of decision-making rejects viable alternatives. As a result, the discarded alternatives never come across the human decision-makers, reproducing systemic and institutional biases that feed into human decisions [51]. Thus, AI's inability to take accountability for their decisions by providing desired explanations leads to a lack of trust in humans.
- Taking a view of the ethical consideration of AI, its extent to code the moral and ethical values is still a matter of concern [13, 39]. The practice of AI explainability in organizations will prove to be one of the major contributors in taking effective and ethical AI-driven decisions [51].
- The extended generation of advanced AI such as deep learning and neural networks can imitate human intelligence. They can make more accurate decisions based on AI information and be autonomous such as self-driving cars and autonomous robots. However, this kind of AI keeps humans out of the loop which is not the focus of Industrial revolution 5.0. The need is to revisit and rethink the role of AI in decision-making.

6 Conclusion

Organizations involve a network of decisions that are to be taken under a complex, uncertain, and ambiguous organizational environment. For effective decision making both AI and humans need to exploit their respective strengths. Industry 5.0 is seen as a revolution in which human-machines will be co-working and collaborating instead of replacing humans. Existing literature is found to have ignored the emergence of humans and machine interplay, especially in organizational decision making. Therefore, this paper makes an attempt to provide an insight into the role of AI and humans from the organizational decision-making perspective. Further, the study aims to develop a deeper understanding of different aspects that are contributory to the successful collaboration of human and machine decision- making in organizations. Human decision-makers are more capable of taking decisions in uncertain and ambiguous environments because of their intuitive ability and AI through its analytical approach helps to overcome complexity in organizations. Organizations need to clearly define the roles of the decision-makers both humans and technology driven machines, in the organization so that no one is thwarted. Also, understanding an organizational aspect of an organization at different maturity levels will make the collaboration successful. This research also contributes by highlighting the challenges involved in human-machine decision-making. One of the major barriers in collaborative decision-making is a lack of transparency and trust in the decision outcomes taken by AI-enabled machines. The responsibility of AI-based decision outcomes needs clarification within organizations and should be explainable. This research will contribute to ensuring the successful collaboration of humans and machines from a decision making perspective.

References

1. Jarrahi, M.H.: Artificial intelligence and the future of work: Ahuman-AI symbiosis in organizational decision making. Bus. Horiz. **61**(4), 577–586 (2018)
2. Davenport, T., Guha, A., Grewal, D., Bressgott, T.: How artificial intelligence will change the future of marketing. J. Acad. Mark. Sci. **48**(1), 24–42 (2019). https://doi.org/10.1007/s11747-019-00696-0
3. Murray, B.J., et al.: Explainable AI for the Choquet integral. IEEE Trans. Emerg. Top. Comput. Intell. **5**(4), 520–529 (2021)
4. Makarius, E.E., Mukherjee, D., Fox, J., Fox, A.K.: Rising with the machines: a sociotechnical framework for bringing artificial intelligence into the organization. J. Bus. Res. **120**, 262–273 (2020)
5. Barrett, M., Oborn, E., Orlikowski, W.J., Yates, J.: Reconfiguring boundary relations: robotic innovations in pharmacy work. Organ. Sci. **23**(5), 1448–1466 (2012)
6. Shrestha, A., Mahmood, A.: Review of deep learning algorithms and architectures. IEEE Access **7**, 53040–53065 (2019)
7. Vittikh, V.A.: Evergetics: science of intersubjective management processes in everyday life. Int. J. Manag. Concepts Philos. **9**(2), 63–72 (2016)
8. Fountaine, T., McCarthy, B., Saleh, T.: Building the AI-powered organization. Harv. Bus. Rev. **97**(4), 62–73 (2019)
9. Trends, D.G.H.C.: Rewriting the Rules for the Digital Age. Deloitte Development LLC (2017)
10. Samek, W., Montavon, G., Vedaldi, A., Hansen, L.K., Müller, K.-R.: Explainable AI: Interpreting, Explaining and Visualizing Deep Learning. Springer Nature (2019)
11. Chen, N., Mohanty, S., Jiao, J., Fan, X.: To err is human: tolerate humans instead of machines in service failure. J. Retail. Consum. Serv. **59**, 102363 (2021)
12. Dietvorst, B.J., Simmons, J.P., Massey, C.: Algorithm aversion: people erroneously avoid algorithms after seeing them err. J. Exp. Psychol. Gen. **144**(1), 114–126 (2015)
13. Wogu, I.A.P., Misra, S., Udoh, O.D., Agoha, B.C., Sholarin, M.A., Ahuja, R.: Artificial intelligence politicking and human rights violations in UK's democracy: a critical appraisal of the Brexit referendum. In: Singh, P.K., Singh, Y., Kolekar, M.H., Kar, A.K., Chhabra, J.K., Sen, A. (eds.) ICRIC 2020. LNEE, vol. 701, pp. 615–626. Springer, Singapore (2021). https://doi.org/10.1007/978-981-15-8297-4_49
14. Lipshitz, R., Klein, G., Orasanu, J., Salas, E.: Taking stock of naturalistic decision making. J. Behav. Decis. Mak. **14**(5), 331–352 (2001)
15. Cao, G., Duan, Y., Edwards, J.S., Dwivedi, Y.K.: Understanding managers' attitudes and behavioral intentions towards using artificial intelligence for organizational decision- making. Technovation **106**(102312), 102312 (2021)
16. Bigman, Y.E., Gray, K.: People are averse to machines making moral decisions. Cognition **181**, 21–34 (2018)
17. Glikson, E., Woolley, A.W.: Human trust in artificial intelligence: review of empirical research. Ann. R. Coll. Physicians Surg. Can. **14**(2), 627–660 (2020)
18. Sowa, K., Przegalinska, A., Ciechanowski, L.: Cobots in knowledge work: human–AI collaboration in managerial professions. J. Bus. Res. **125**, 135–142 (2021)
19. Haesevoets, T., De Cremer, D., Dierckx, K., Van Hiel, A.: Human-machine collaboration in managerial decision making. Comput. Hum. Behav. **119**, 106730 (2021)
20. Özkiziltan, D., Hassel, A.: Humans versus machines: an overview of research on the effects of automation of work. SSRN J., 1–13 (2020)
21. Snow, C.C., Fjeldstad, Ø.D., Langer, A.M.: Designing the digital organization. J. Organ. Des. **6**(1), 1–13 (2017)

22. Sadler-Smith, E., Shefy, E.: The intuitive executive: Understanding and applying 'gut feel' in decision-making. Acad. Manag. Perspect. **18**(4), 76–91 (2004)
23. Simon, H.A.: Models of Man. Economica **24**(96), 382 (1957). https://doi.org/10.2307/2550441
24. Kahneman, D.: A perspective on judgment and choice: mapping bounded rationality. Am. Psychol. **58**(9), 697–720 (2003)
25. Akinci, C., Sadler-Smith, E.: Assessing individual differences in experiential (intuitive) and rational (analytical) cognitive styles. Int. J. Sel. Assess. **21**(2), 211–221 (2013)
26. Dane, E., Rockmann, K.W., Pratt, M.G.: When should I trust my gut? Linking domain expertise to intuitive decision-making effectiveness. Organ. Behav. Hum. Decis. Process. **119**(2), 187–194 (2012)
27. Dane, E., Pratt, M.G.: Exploring intuition and its role in managerial decision making. AMRO **32**(1), 33–54 (2007)
28. Vincent, V.U.: Integrating intuition and artificial intelligence in organizational decision-making. Bus. Horiz. **64**(4), 425–438 (2021)
29. Dejoux, C., Léon, E.: Métamorphose des managers...: à l'ère du numérique et de l'intelligence artificielle. Pearson (2018)
30. Verma, K., et al.: Latest tools for data mining and machine learning. Int. J. Inno. Tech. Exp. Engi. **8**(9S), 24–28 (2019)
31. Stone, M., et al.: Artificial intelligence (AI) in strategic marketing decision-making: a research agenda. The Bottom Line **33**(2), 183–200 (2020)
32. Parry, K., Cohen, M., Bhattacharya, S.: Rise of the machines: a critical consideration of automated leadership decision making in organizations. Group Org. Manag. **41**(5), 571–594 (2016)
33. Grove, W.M., Zald, D.H., Lebow, B.S., Snitz, B.E., Nelson, C.: Clinical versus mechanical prediction: a meta-analysis. Psychol. Assess. **12**(1), 19–30 (2000)
34. Sharma, S., Nanda, M., Goel, R., Jain, A., Bhushan, M., Kumar, A.: Smart cities using internet of things: recent trends and techniques. Int. J. Inno. Tech. Exp. Engi. **8**(9S), 24–28 (2019)
35. Beck, A.H., et al.: Systematic analysis of breast cancer morphology uncovers stromal features associated with survival. Sci. Transl. Med. **3**(108), 108ra113 (2011)
36. Highhouse, S.: Stubborn reliance on intuition and subjectivity in employee selection. Ind. Organ. Psychol. **1**(3), 333–342 (2008)
37. Burton, J.W., Stein, M.-K., Jensen, T.B.: A systematic review of algorithm aversion in augmented decision making. J. Behav. Decis. Mak. **33**(2), 220–239 (2020)
38. Veloso, M., Biswas, J., Coltin, B., Rosenthal, S.: Cobots: Robust symbiotic autonomous mobile service robots. In: Twenty-Fourth International Joint Conference on Artificial Intelligence (2015)
39. Assibong, P.A., Wogu, I.A.P., Sholarin, M.A., Misra, S., Damasevičius, R., Sharma, N.: The politics of artificial intelligence behaviour and human rights violation issues in the 2016 US presidential elections: an appraisal. In: Data Management. Analytics and Innovation, pp. 295–309. Springer, Singapore (2020)
40. Huang, M.-H., Rust, R.T.: A strategic framework for artificial intelligence in marketing. J. Acad. Mark. Sci. **49**(1), 30–50 (2020). https://doi.org/10.1007/s11747-020-00749-9
41. Lodgaard, E., Dransfeld, S.: Organizational aspects for successful integration of human-machine interaction in the industry 4.0 era. Procedia CIRP **88**, 218–222 (2020)
42. Kellogg, K.C., Valentine, M.A., Christin, A.: Algorithms at work: the new contested terrain of control. Ann. R. Coll. Physicians Surg. Can. **14**(1), 366–410 (2020)
43. Leyer, M., Schneider, S.: Decision augmentation and automation with artificial intelligence: threat or opportunity for managers? Bus. Horiz. **64**(5), 711–724 (2021)
44. Reddy, S., Allan, S., Coghlan, S., Cooper, P.: A governance model for the application of AI in health care. J. Am. Med. Inform. Assoc. **27**(3), 491–497 (2020)

45. Taylor, T.: Artificial intelligence in defence. RUSI j. **164**(5–6), 72–81 (2019)
46. Rao, Q., Frtunikj, J.: Deep learning for self-driving cars: chances and challenges. In: Proceedings of the 1st International Workshop on Software Engineering for AI in Autonomous Systems, Gothenburg, Sweden, pp. 35–38 (2018)
47. Antoniadi, A.M., et al.: Current challenges and future opportunities for XAI in machine learning-based clinical decision support systems: a systematic review. NATO Adv. Sci. Inst. Ser. E Appl. Sci. **11**(11), 5088 (2021)
48. Tomsett, R., Braines, D., Harborne, D., Preece, A., Chakraborty, S.: Interpretable to Whom? A Role-based Model for Analyzing Interpretable Machine Learning Systems. arXiv [cs.AI] (2018)
49. Hepenstal, S., McNeish, D.: Explainable artificial intelligence: what do you need to know? In: International Conference on Human-Computer Interaction, pp. 266–275. Springer, Cham (2020)
50. Schönhof, R., Werner, A., Elstner, J., Zopcsak, B., Awad, R., Huber, M.: Feature visualization within an automated design assessment leveraging explainable artificial intelligence methods. Procedia CIRP **100**, 331–336 (2021)
51. Anderson, M., Anderson, S.L.: Machine ethics: creating an ethical intelligent agent. AI Magazine **28**(4), 15–26 (2007)

Dress Pattern Classification Using ResNet Based Convolutional Neural Networks

Manpinder Singh[1], Saiba Dalmia[1](✉), Ranjeet Kumar Ranjan[1], and Amit Singh[2]

[1] School of Computing, DIT University, Dehradun, India
saibadalmia2513@gmail.com
[2] Ministry of Electronics and Information Technology, New Delhi, India

Abstract. The fashion industry tries to adapt to changing fashion trends and is extremely versatile. Globally, the fashion industry is valued at three trillion dollars, and with the world GDP increasing by 400% by 2050, it would create a greater demand for clothing. E-commerce has become an integral tool in the fashion industry and users are looking for a better shopping experience and easier ways on online sites to find clothes according to their preferences. Many Machine Learning and Deep Learning approaches have helped a lot in many areas of the fashion industry. Convolutional neural networks (CNN) perform extremely well in tasks such as image classification. Inspired by this, a deep learning model is proposed based on the pre-trained ResNet which can detect the pattern of the cloth worn by a person with an accuracy of 82.13%. This dress classification approach will be beneficial in increasing the efficiency of the cloth-producing factories by automating their storage and the organizing process and when integrated with search engines of various websites, it can help in creating a recommendation system for the user.

Keywords: Computer vision · Deep learning · Dress pattern classification · Fashion · Machine learning · ResNet · Transfer learning

1 Introduction

For every individual, society, and its economy, Fashion matters. It represents who we are and what we aspire to be. Globally, the fashion industry is valued at three trillion dollars and is responsible for employing over 57M workers in developing countries out of which 80% of them are women [1]. Due to the fact, the middle-class population is growing across the globe, clothing production has doubled in the last 15 years, according to Ellen Mcarthur Foundation [1]. The world GDP will be increased by 400% by 2050 which would mean greater demand for clothing. The global economy will benefit by 192 billion dollars by 2030 if we start addressing the environmental and social problems created by the fashion industry [1]. The fashion industry tries to adapt to changing fashion trends and is extremely versatile. Since the product life cycle is becoming shorter and shorter with the rising middle-class population and their increasing income, the demand for fashion items is increasing very rapidly. Hence, the clothing production factories need

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 91–103, 2023.
https://doi.org/10.1007/978-3-031-13150-9_8

to be highly efficient while maintaining the same quality of clothing production to meet the demand of the fashion industry [2]. E-commerce has become an integral tool in the fashion industry. Fashion commerce generated $545 billion in revenue in 2019 and is projected to generate $713 billion by 2022 [3]. With the introduction of technology, the user experience is becoming smoother and more enjoyable for the customer. They are looking for easier ways on online sites to find clothes according to their preferences [3].

In recent years, classification tasks have been widely explored especially for image databases using deep learning. Convolutional neural networks (CNN) perform extremely well in tasks such as image classification. The three primary tasks of CNN are to classify the visual content, detect the objects from the image, and gather the recognized objects in the list. It consists of 2 main parts. The first is the feature extractor which consists of convolution and pooling layers that learn granular/universal features like boundaries and edges and gradually learn the complex high-level features and the second part is the classifiers which convert the image output into numerical prediction [4]. The downside of using CNN is that we require a large dataset to train it and the training process requires a lot of time [5]. These problems can be overcome by using transfer learning where the pre-trained state-of-the-art CNN architecture like Exception, GoogleNet, ResNet, etc. can be directly used in models and can dramatically reduce the data required and the training time [6]. Machine Learning and Deep Learning have helped in the task of dress pattern classification. Many authors have focused their work on classifying different types of clothing items like Coat, Shirt, Sandals, etc. One of the most popular dataset used is Fashion-MNIST which consists of 70,000 images belonging to 10 classes of clothing items [7]. But in our knowledge, the field which is very less explored by the authors is classifying between different patterns on a clothing item.

Inspired by this, a deep learning model is proposed based on the pre-trained ResNet which can detect the pattern of the cloth worn by a person. This dress classification approach will be beneficial in increasing the efficiency of the cloth-producing factories. Integrating the proposed model with a sensor will enable it to detect the pattern of the clothing items so that they can be arranged and packed accordingly in a more systematic manner. By automating the storage and the organizing process, it will help in increasing the production rate as well as decreasing the time required for the product to reach the customer once produced. Thus, saving a lot of time as earlier it used to be done manually. The proposed model can be integrated with search engines of various websites which will smoothen the customer's purchasing experience as it will allow the customer to upload a picture of their favorite clothing item and the website can detect the pattern of that clothing item and show clothes that match the taste of that customer. This will also help in creating a recommendation system based on the pattern of clothes preferred by the customer giving him/her a personalized experience on the website and thus improving the customer retention rate.

2 Related Work

In recent years, machine learning, the internet of things, and deep learning have played a vital role in various industries [8–10]. Machine learning and deep learning have helped in many areas of the fashion industry like fashion trend forecasting which helps in predicting the market patterns that impact the market and consumer needs [11]. A Machine Learning approach has been proposed to analyze fashion styles from large collections of online customer reviews. In [12], the authors have classified the images in the Fashion-MNIST dataset. They have used 3 convolution layers along with batch normalization to make the learning process efficient. Their model improved accuracy by 2% over the existing state of art models. On the same dataset, in [13], the authors have used a Long Short term memory network. The accuracy of their image classification model is 88.26%. They have used methods like network pruning and training pattern reduction to increase model performance. In [14], the author has used five different CNN architectures, that is, Vgg16, Vgg19, InceptionV3, Custom CNN, and Vgg-like respectively. The model is used for person detection, product detection, and gender classification. This will majorly help in e-commerce applications as it will differentiate the product and person and will classify the product category and gender. In [15], the study aimed to find whether a transfer learning model gets a better accuracy score within a short period and with limited computational power. They have used CIFAR-10 and Caltech Faces datasets and used Inception-v3 which was pre-trained on the ImageNet dataset. In [16], the authors have used the VGG-11 network to classify the Fashion-MNIST dataset. They have used a multilayer nonlinearity layer, batch normalization layer, and various other methods to get an accuracy of 91.5%. In [17], the author has applied machine learning models on two datasets Fashion-MNIST and CIFAR-10. He has also used feature extraction methods like Principal Component Analysis (PCA) and Autoencoder before applying the models.

In [7], the author has performed hyperparameter optimization and regularization methods with a deep learning model on the Fashion-MNIST dataset and got an accuracy of 93.99%.

3 Convolutional Neural Networks

Convolution Neural Network (CNN) is used for image detection and classification. Images are the 2D matrix on which CNN processes that image and helps the user to classify and detect that image. It is a basic neural network that deals with an image. In CNN, the weights are a small matrix-like 2×2 and 3×3 that is dot product with each pixel hence producing a new pixel and performing an image filter. The new image produced by these filters in a layer are then combined and become an input for another layer and this continues until the end of the network. There is one dense layer at the end of this convolution network to convert the image output into numerical prediction [18]. The three primary tasks of CNN are to classify the visual content, detect the objects from the image, and gather the recognized objects in the list. CNN Architecture consists of three-layer:

1. Convolutional Layer: Its main objective is to identify the features of the image from general to specific. A convolutional layer consists of an activation function. It is the extension of the Convolution Layer and helps to provide better feature extraction by removing the excessive fat of an image [18]. In this paper, ReLu (Rectified linear Unit Layer) is used as an activation function.

2. Pooling Layer: Its main purpose is to reduce the number of inputs by concentrating on the main part of the information that a user needs to do with that image. It reduces the dimensions of the feature maps which reduces the amount of computation performed in the network [19].
3. Fully connected layers: It uses a standard feed-forward network and backpropagation for learning [20]. It is like a simple artificial neural network and uses activation functions. In general, 'ReLu' is used as an activation function in hidden layers and 'Softmax' is used in the output layer in the case of multi-class classification.

4 ResNet152

Since every CNN architecture is becoming deeper and deeper to reduce the error rate, it introduces a problem in deep learning which is known as the Vanishing or Exploding gradient. Due to this, the gradient can become either too large or 0. To solve this issue, a concept called Residual Network was introduced [21]. This network introduces a technique that skips training from a few layers and connects directly to the output. This technique is called a skip connection or shortcut connection and is shown in Fig. 1.

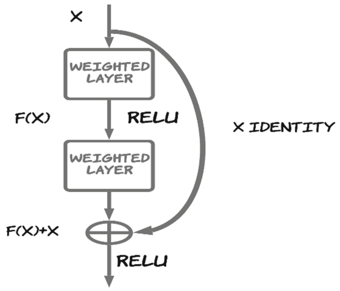


Fig. 1. Skip connection or shortcut connection used in ResNet152

It enables ResNet to have a very deep architecture of up to 152 layers since regularization skips any layer that hurts the performance of the network [21]. For the proposed model, ResNet152 (a ResNet version consisting of 152 layers deep CNN) is used which is pre-trained on millions of images from the ImageNet database. ImageNet is an extremely large visual dataset consisting of more than 14 million images and 21 thousand classes or labels intended for computer vision research [22]. ResNet instead of learning the signal representation directly learns the residual representation functions. Since the network goes very deep, the training time becomes high. To tackle this problem, a bottleneck pattern is used which reduces the complexity of the model. At the start and end of the network, 1×1 Conv layers are inserted which reduces the parameters of the network while not degrading the performance by much [23].

5 Dataset Pre-processing

For the proposed model, the dataset was collected from [24]. It consisted of four columns (unit id, category, category: confidence and image url) and 15,702 rows. Each image had a person wearing a dress of different patterns which was bounded by a red rectangle. For the pre-processing part, image names from the url's present in the 'image_url' column were extracted and a new column named 'image_name' was created. The target variable was the 'category' column which consisted of 17 different pattern labels. Since 5 pattern labels had very little data as compared to others, those labels ('chevron', 'letter_numb', 'houndstooth', 'stars', 'skull') were dropped. Therefore, the resultant dataset had 12 pattern labels. 'category: confidence' column told how sure it is that a particular image belonged to that category. All the rows having 'category: confidence' less than 0.5 were removed. Also, all the duplicate rows were removed from the dataset. After the above pre-processing 13813 images were left.

The data distribution was uneven for each label before and after pre-processing. For example, after pre-processing, the 'plain' label had 8079 data values whereas the 'geometry' label had 215 data values and the 'cartoon' label had 168 data values. This uneven data distribution resulted in a class imbalance problem.

This creates a problem where we cannot declare the performance of a model to be good even if it is having a high accuracy because in such situations the model ignores the minority class, and the majority class completely dominates and overwhelms the minority class [25–29]. Figure 2 depicts the class imbalance in the dataset (data values for each class were after pre-processing).

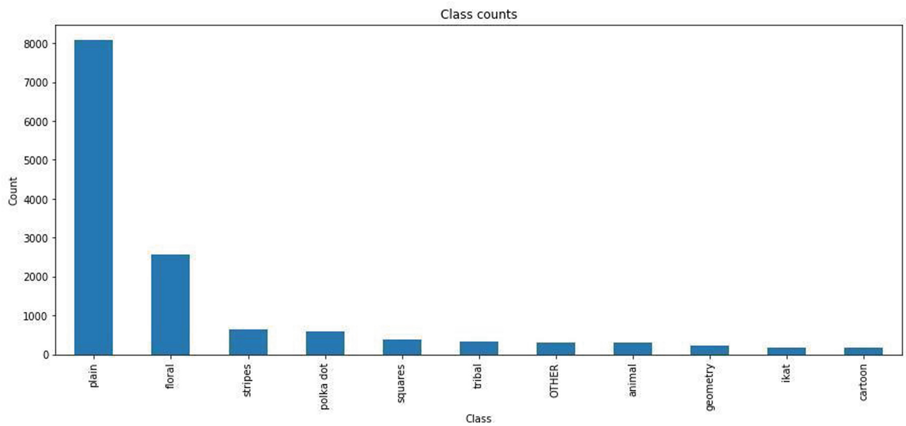
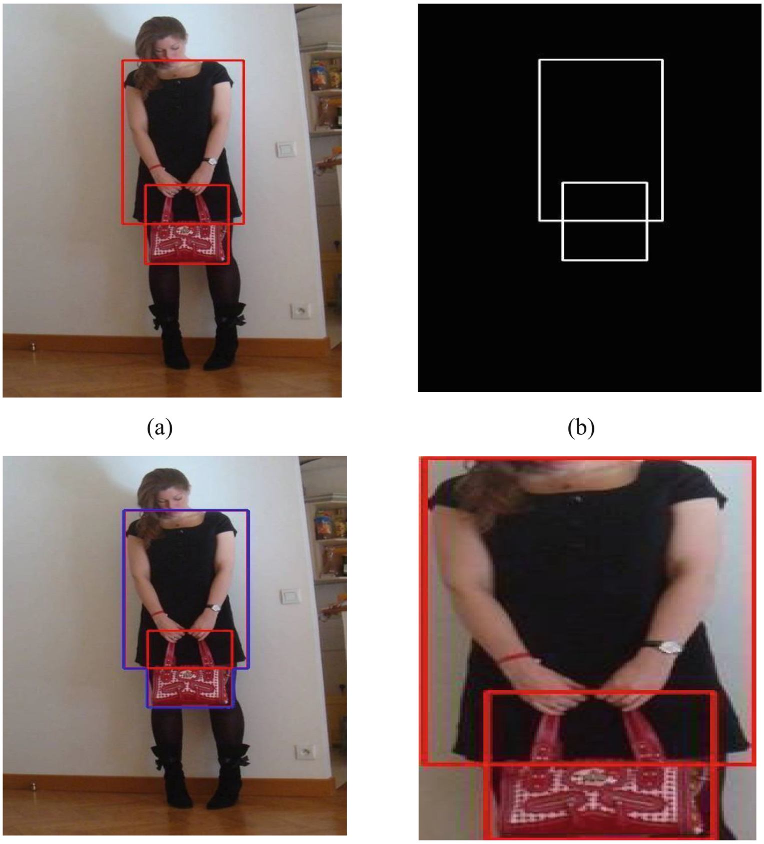


Fig. 2. Class imbalance in the dataset (data values for each class were after pre-processing)

Various techniques were applied to handle class imbalance problem like assigning higher weights to the class having fewer samples and vice versa, doing data augmentations to create synthetic examples of the minority class, etc. but none of them gave promising results. Hence, none of the techniques was chosen. Images were cropped to the red bounding box in which the dress containing the pattern is visible. Figure 3 depicts the process used to extract the desired area of the image.

Since the dataset also contained some black and white pictures having black bounding boxes like in Fig. 4, the same procedure was followed for them as well. Through this, the dimensions of the images were reduced thus removing the redundant pixel values.



(a) (b)

(c) (d)

Fig. 3. (a) Original image (b) a basic threshold operation was performed where all the red pixels in the image were converted to white while the rest of the pixels became black. (c) Contours were found in this binary image. Since there was more than one contour present and they were overlapping as well, the largest contour was selected to make sure the dress portion of the image was covered. (d) Rectangles were found that covered that contour and the one having the minimum area was chosen to keep unimportant pixels to a minimum and it was extracted.

This made the model learn only the important features from the image which resulted in lower training time and an increase in the accuracy of the model. The algorithm failed on a few of the images where all the sides of the bounding rectangle were not clearly defined like in Fig. 5. Therefore, these images were discarded. All the crop images were resized into 100×100 dimensions.

6 Model Description

The dataset was randomly divided into two independent datasets, that is, 90% for training and 10% for testing. The training dataset was split into 2 independent datasets, training

Fig. 4. Black and white image

Fig. 5. Sample images that are incompatible with the algorithm

and validation in the ratio of 9:1. In the proposed model, transfer learning was used where the output of a ResNet152 model, which was already trained on the ImageNet database, was fed into a convolutional layer. The output of this convolutional layer was flattened to convert it into a 1D vector which could be fed into fully connected layers. The benefits of transfer learning are that it results in improving the performance of our new classifier without requiring a lot of data and it saves a lot of computational time [6, 30]. The input shape was 100, 100, 3, and include_top was set to False to not include the fully connected layer on the top of the network [31]. Where include_top is the parameter that is used to select the fully connected layers of the pre-trained CNN model based on the value assigned as true or false.

6.1 Model Training

- Dense Layer – ReLu.was used as activation function

- Dropout – through this layer, randomly selected neurons are ignored during the training of the model. In the proposed model, the dropout rate was set to 0.5 [32].
- Output Layer – a dense layer was used as an output layer where its dimensionality of the output space was 12 and the activation function used was 'softmax'.

Functional API was used in this model.

6.2 Model Compilation

While compiling the proposed model, 'categorical_crossentropy' and 'accuracy' were chosen as loss function and metrics respectively while the optimizer used was 'Rectified Adam' with a lookahead mechanism [33]. The learning rate chosen for this optimizer was 0.001.

6.3 Model Fitting

Following four callbacks from Keras library was used:

- Model Checkpoint – verbose and save_best_only were set to 1 and True respectively. The rest of the parameters were set to default [34].
- ReduceLRonPlateau – factor, patience, min_lr was set to 0.80, 1, 0.00001 respectively. Rest of the parameters were set to default [35].
- EarlyStopping – verbose and patience was set to 1 and 10 respectively. The rest of the parameters were set to default [36].
- CSVLogger – append was set to True while all the other parameters were set to default [37].

While fitting the model, steps per epoch were calculated for both training and validation by dividing the total number of samples by the batch size (Batch size = 64) [38]. The number of epochs was set to 50 and verbose to 1.

7 Evaluation Metrics

Constructive feedback is extremely important while building machine learning models [39]. Performance metrics enable us to check the robustness of our model and discriminate among model results [40]. Various performance metrics used to evaluate the performance of the proposed model are described in Table 1.

In Table 1, TP is true positive, FP is false positive, TN is the negative and FN is false negative samples, N samples belong to M Classes, y_{ij} represents whether sample i belongs to class j or not, p_{ij} is the probability of sample i belonging to class j.

Table 1. Various performance metrics used to evaluate the performance of the proposed model.

Performance measure	Description	Mathematical formula
ROC AUC score	ROC (**Receiver Operating Characteristics**) is a probability curve and AUC (Area Under Curve) represents the measure of separability [41]	NA
Classification accuracy	It is defined as the number of correct predictions divided by the number of samples [42]	$Accuracy = \frac{TP+TN}{TP+TN+FP+FN}$
Cross-entropy loss	Also known as Logarithmic Loss or Log Loss works well for multi-class classification by penalizing the false classifications [43]	$CEL = \frac{-1}{N}\sum_{i=1}^{N}\sum_{j=1}^{M} loglog\left(p_{ij}\right) * y_{ij}$
Precision	It is defined as the ratio of true positive and the total predicted positive. It determines out of total predicted positive; how many are actually positive [44]	$Precision = \frac{TP}{TP+FP}$
Recall	It is defined as the ratio of true positive and the total actual positive. It determines out of total actual positive; how many are labeled positive by the model contagious [44]	$Recall = \frac{TP}{TP+FN}$
F1-Score	It is defined as the harmonic mean of precision and recall [35]. It is a suitable measure if we require a balance between the two and there is an uneven class distribution (a large number of True Negatives) [44]	$F1 - Score = 2 * \left(\frac{Precision*Recall}{Precision+Recall}\right)$

8 Experimental Setup and Results

Python Programming Language was used to train the proposed Deep Learning model. All experiments were performed on Google Colaboratory with GPU enabled and 12GB of RAM. Python libraries used were CV2 (4.1.2), Numpy (1.19.5), Matplotlib (3.2.2), Keras (2.5.0), Pandas (1.1.5), Sklearn (0.22.2.Post1), Tensorflow (2.5.0), Tqdm (4.41.1), OS and Google.Colab.

8.1 Experimental Results

We have used accuracy, precision, recall, f1-score, roc_auc score, and cross-entropy loss as performance metrics for the deep learning model. Table 2 depicts the performance stats of the model. Figure 6 depicts the Weighted Multiclass ROC Curve of our model.

Table 2. Performance metrics of our model

Model	Performance metrics					
	Test accuracy	Weighted precision	Weighted recall	Weighted f1-score	ROC-AUC score	Cross entropy loss
Proposed model	82.13%	0.81	0.82	0.81	0.9520	1.4589

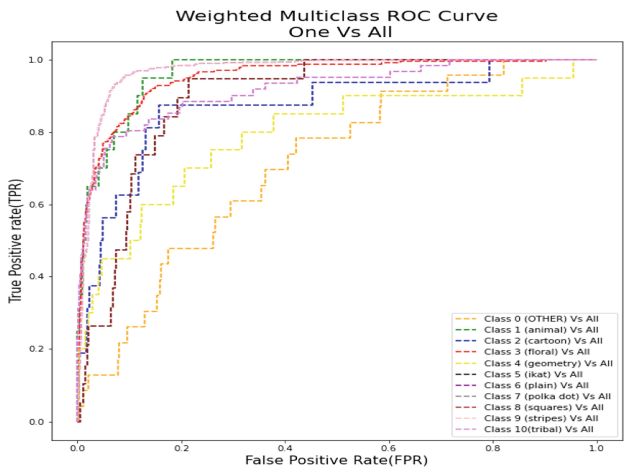


Fig. 6. Weighted multiclass ROC curve of dress pattern classification model

Table 3 depicts the performance of different models on various fashion datasets. Much work has been done on the Fashion-MNIST dataset, but very little has been done on the Dress Pattern dataset. By using a Resnet152 based CNN architecture a decent accuracy of 82.13% and roc_auc score of 95.20% were achieved. The weighted precision, recall, F1-Score, and Cross-entropy loss were 81%, 82%, 81%, and 1.4589. All these metrics can be improved by tackling the class imbalance problem in the dataset which is added in the future work of the model.

Table 3. Performance of different models on various fashion datasets

Authors	Dataset	Learning model	Accuracy
Shen [13]	Fashion-MNIST dataset	Long Short-Term Memory Networks (LSTMs)	88.26%
Duan et. al [16]	Fashion-MNIST dataset	VGG-11	91.5%
Hoang [17]	Fashion-MNIST dataset	SVM	91.16%
Greeshma and Sreekumar [7]	Fashion-MNIST dataset	CNN4 + HPO + Reg	93.99%
Proposed model	Dress Pattern dataset	ResNet152	82.13%

9 Conclusion

Globally, the fashion industry is valued at three trillion dollars and is responsible for employing over 57M workers in developing countries out of which 80% of them are women. With the rising middle-class population and their increasing income along with the life cycle of products becoming shorter, the demand for fashion items is increasing very rapidly. Since many authors have focused their work on classifying different types of clothing items like Coat, Shirt, Sandals, etc. and the field which is very less explored by the authors is classifying between different patterns on a clothing item. In this paper, a deep learning model is proposed which can detect the pattern of the cloth worn by a person. The dataset for the proposed model consisted of 15,702 images. After various pre-processing, 13813 images were left. Transfer learning was used in the proposed deep learning model where the output of a pre-trained ResNet152 model was passed to the rest of the CNN architecture. The accuracy of the proposed model was 82.13%. Since there are so many cultures and traditions across the world, each has its unique style and pattern of clothes. Therefore, the proposed model can be extended and trained on different parameters and much bigger datasets having images with various lighting conditions and containing more diverse patterns of clothes. A new technique or algorithm can be invented to tackle the class imbalance problem in the dataset. Integrating the proposed model with a sensor will enable it to detect the pattern of the clothing items so that they can be arranged and packed accordingly in a more systematic manner.

References

1. Corner, P.F.: Why Fashion Matters. https://artsandculture.google.com/story/_QKS0J-OeT7HIA. Accessed 03 Sep 2021
2. Research and Markets: Global Clothing Market Demand and Forecast to 2020 – Detailed Analysis of Asia and Australasia Market. https://www.businesswire.com/news/home/20160111005845/en/Research-Markets-Global-Clothing-Market-Demand-Forecast (2016). Accessed 03 Sep 2021
3. Smales, C.: The Importance of eCommerce to the Fashion and Apparel Industry. https://www.datafeedwatch.com/blog/ecommerce-and-the-fashion-industry. Accessed 03 Sep 2021

4. Khoshdeli, M., Cong, R., Parvin, B.: Detection of nuclei in H&E stained sections using convolutional neural networks. In: 2017 IEEE EMBS International Conference on Biomedical and Health Informatics (BHI), pp. 105–108 (2017)
5. Gupta, A.: Difference between ANN, CNN and RNN. https://www.geeksforgeeks.org/difference-between-ann-cnn-and-rnn/ (2020). Accessed 03 Sep 2021
6. Brownlee, J.: Transfer Learning in Keras with Computer Vision Models. https://machinelearningmastery.com/how-to-use-transfer-learning-when-developing-convolutional-neural-network-models/ (2019). Accessed 03 Sep 2021
7. Greeshma, K.V., Sreekumar, K.: Hyperparameter optimization and regularization on Fashion-MNIST classification. Int. J. Recent Technol. Eng. **8**(2), 3713–3719 (2019)
8. Sharma, S., Nanda, M., Goel, R., Jain, A., Bhushan, M., Kumar, A.: Smart cities using internet of things: recent trends and techniques. Int. J. Inno. Tech. Exp. Eng. **8**(9), 24–28 (2019). https://doi.org/10.35940/ijitee.I1004.0789S19
9. Verma, K., et al.: Latest tools for data mining and machine learning. Int. J. Inno. Tech. Exp. Engi. **8**(9S), 24–28 (2019). https://doi.org/10.35940/ijitee.I1003.0789S19
10. Mangla, M., Kumar, A., Mehta, V., Bhushan, M., Mohanty, S.: Real-Life Applications of the Internet of Things: Challenges, Applications, and Advances. CRC Press, Taylor & Francis Group, (2022). Available: www.appleacademicpress.com
11. Chang, A.A., et al.: Fashion Trend Forecasting Using Machine Learning Techniques: A Review
12. Hananto, V.R., Kim, S., Kovacs, M., Serdült, U., Kryssanov, V.: A machine learning approach to analyze fashion styles from large collections of online customer reviews. In: 2021 6th International Conference on Business and Industrial Research (ICBIR), pp. 153–158 (2021)
13. Shen, S.: Image classification of Fashion-MNIST dataset using long short-term memory networks. Res. Sch. Comput. Sci
14. Schindler, A., Lidy, T., Karner, S., Hecker, M.: Fashion and apparel classification using convolutional neural networks. arXiv Prepr. arXiv1811.04374 (2018)
15. Hussain, M., Bird, J.J., Faria, D.R.: A study on cnn transfer learning for image classification. In: Lotfi, A., Bouchachia, H., Gegov, A., Langensiepen, C., McGinnity, M. (eds.) UKCI. AISC, vol. 840, pp. 191–202. Springer, Cham (2019). https://doi.org/10.1007/978-3-319-97982-3_16
16. Duan, C., Yin, P., Zhi, Y., Li, X.: Image classification of fashion-MNIST data set based on VGG network. In: Proceedings of 2019 2nd International Conference on Information Science and Electronic Technology (ISET 2019). International Informatization and Engineering Associations: Computer Science and Electronic Technology International Society, vol. 19 (2019)
17. Hoang, K.: Image Classification with Fashion-MNIST and CIFAR10. Calif. State Univ. (2018)
18. Khandelwal, R.: Convolutional Neural Network (CNN) Simplified. https://medium.datadriveninvestor.com/convolutional-neural-network-cnn-simplified-ecafd4ee52c5 (2018). Accessed 03 Sep 2021
19. Khosla, S.: CNN|Introduction to Pooling Layer. https://www.geeksforgeeks.org/cnn-introduction-to-pooling-layer/ (2021). Accessed 03 Sep 2021
20. Bushkovskyi, O.: Business Applications Of Convolutional Neural Networks. https://theappsolutions.com/blog/development/convolutional-neural-networks/. Accessed 03 Sep 2021
21. Saxena, P.: Residual Networks (ResNet) – Deep Learning. https://www.geeksforgeeks.org/residual-networks-resnet-deep-learning/ (2020). Accessed 03 Sep 2021
22. Brownlee, J.: A Gentle Introduction to the ImageNet Challenge (ILSVRC). https://machinelearningmastery.com/introduction-to-the-imagenet-large-scale-visual-recognition-challenge-ilsvrc/ (2019). Accessed 03 Sep 2021

23. Tsang, S.-H.: Review: ResNet – Winner of ILSVRC 2015 (Image Classification, Localization, Detection). https://towardsdatascience.com/review-resnet-winner-of-ilsvrc-2015-image-classification-localization-detection-e39402bfa5d8 (2018). Accessed 03 Sep 2021
24. Crowdflower: Categorization Dress Patterns. https://data.world/crowdflower/categorization-dress-patterns (2016). Accessed 03 Sep 2021
25. Singh, A., Ranjan, R.K., Tiwari, A.: Credit card fraud detection under extreme imbalanced data: a comparative study of data-level algorithms. J. Exp. Theor. Artif. Intell. 1–28 (2021)
26. Johnson, J.M., Khoshgoftaar, T.M.: Survey on deep learning with class imbalance. J. Big Data **6**(1), 1–54 (2019). https://doi.org/10.1186/s40537-019-0192-5
27. Buda, M., Maki, A., Mazurowski, M.A.: A systematic study of the class imbalance problem in convolutional neural networks. Neural Netw. **106**, 249–259 (2018)
28. Luque, A., Carrasco, A., Martin, A., de las Heras, A.: The impact of class imbalance in classification performance metrics based on the binary confusion matrix. Pattern Recognit. **91**, 216–231 (2019)
29. Ali, A., Shamsuddin, S.M., Ralescu, A.L.: Classification with class imbalance problem. Int. J. Adv. Soft Comput. Appl. **5**(3) (2013)
30. Singh, D., Singh, S.: Realising transfer learning through convolutional neural network and support vector machine for mental task classification. Electron. Lett. **56**(25), 1375–1378 (2020)
31. Keras, DenseNet. https://keras.io/api/applications/densenet/. Accessed 25 May 2021
32. Brownlee, J.: A Gentle Introduction to Dropout for Regularizing Deep Neural Networks. https://machinelearningmastery.com/dropout-for-regularizing-deep-neural-networks/ (2018). Accessed 25 May 2021
33. Tensorflow, tfa.optimizers.Lookahead. https://www.tensorflow.org/addons/api_docs/python/tfa/optimizers/Lookahead. Accessed 25 May 2021
34. Keras, ModelCheckpoint. https://keras.io/api/callbacks/model_checkpoint/. Accessed 03 Sep 2021
35. Keras, ReduceLROnPlateau. https://keras.io/api/callbacks/reduce_lr_on_plateau/. Accessed 03 Sep 2021
36. Keras, EarlyStopping. https://keras.io/api/callbacks/early_stopping/. Accessed 03 Sep 2021
37. Keras, CSVLogger. https://keras.io/api/callbacks/csv_logger/. Accessed 03 Sep 2021
38. MRINALWALIA, keras.fit() and keras.fit_generator(), https://www.geeksforgeeks.org/keras-fit-and-keras-fit_generator/ (2020). Accessed 03 Sep 2021
39. Singh, M., Dalmia, S.: Prediction of number of fatalities due to Covid-19 using machine learning. In: 2020 IEEE 17th India Council International Conference (INDICON), pp. 1–6 (2020)
40. Srivastava, T.: 11 Important Model Evaluation Metrics for Machine Learning Everyone Should Know. https://www.analyticsvidhya.com/blog/2019/08/11-important-model-evaluation-error-metrics/ (2019). Accessed 25 May 2021
41. Narkhede, S.: Understanding AUC–ROC Curve. https://towardsdatascience.com/understanding-auc-roc-curve-68b2303cc9c5 (2018). Accessed 25 May 2021
42. DeepAI, Accuracy (error rate). https://deepai.org/machine-learning-glossary-and-terms/accuracy-error-rate. Accessed 25 May 2021
43. Mishra, A.: Metrics to Evaluate your Machine Learning Algorithm. https://towardsdatascience.com/metrics-to-evaluate-your-machine-learning-algorithm-f10ba6e38234 (2018). Accessed 25 May 2021
44. Shung, K.P.: Accuracy, Precision, Recall or F1? https://towardsdatascience.com/accuracy-precision-recall-or-f1-331fb37c5cb9 (2018). Accessed 25 May 2021

An Efficient MR Images Based Analysis to Predict Alzheimer's Dementia Stage Using Random Forest Classifier

Venkatesh Gauri Shankar[1,2](✉), Dilip Singh Sisodia[1], and Preeti Chandrakar[1]

[1] Department of Computer Science and Engineering, National Institute of Technology Raipur, Raipur, Chhattisgarh, India
vgshankar.phd2018.cse@nitrr.ac.in

[2] Department of Information Technology, Manipal University Jaipur, Jaipur, Rajasthan, India

Abstract. Alzheimer's Dementia is a collection of symptoms that impair the brain's everyday functioning. It is primarily defined by impairments in two brain processes: memory and judgment. Dementia is a broad term that encompasses many medical diseases, including Alzheimer's Disease. Symptoms of Dementia include poor memory, limited social skills, and worsening thinking abilities. No doctor can promise whether it can be cured or not, but Medications and Therapies might help improve the condition. Alzheimer's disease is a progressive condition that kills brain cells, resulting in memory loss and impairment of other brain processes. When someone is afflicted, their intellectual, behavioral, and social abilities deteriorate continuously. Alzheimer's disease is thought to be primarily caused by incorrect protein building in brain cells. Amyloid is a protein that, in this situation, forms plaques surrounding brain cells. On the other hand, Tau is a protein that binds to brain cells and produces tangles. Alzheimer's disease is often diagnosed around the mid-1960s. This paper presents a Random Forest-based model for stage-specific Alzheimer's disease classification. Our suggested network learns from a short dataset and performs better in diagnosing Alzheimer's disease. The Methodologies that we have adopted here are fundamental and necessary for study. Feature selection and data cleaning are the essential steps for our model. Reducing Training Time, reducing overfitting, and improving the model's accuracy through various algorithms is the next step for our model. We use Random Forest Algorithm for building our model and get the highest accuracy as 91.6% respectively. We also use Confusion Matrix, which considers many parameters for the model's accuracy. We then plot various graphs to understand better and better visualize our model.

Keywords: Alzheimer's dementia · Machine learning · Feature extraction · Random forest classifier · MR images · Discriminant features

1 Introduction

Alzheimer's Dementia is a collection of disorders—like cardiovascular disease—that encompasses a wide variety of different medical problems, including Alzheimer's Disease. Unusual changes in the brain cause illnesses referred to collectively as "dementia."

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 104–119, 2023.
https://doi.org/10.1007/978-3-031-13150-9_9

These alterations result in a deterioration of mental abilities severe enough to affect everyday living and self-care [1–3]. Additionally, they influence one's behavior, emotions, and relationships. Most instances are due to Alzheimer's disease. Vascular Dementia is the second most prevalent cause of dementia. It is caused by bleeding and obstruction of blood arteries in the brain. Other disorders that might mimic the symptoms of dementia, some of which are curable, include vitamin deficiency, thyroid dysfunction, and. Alzheimer's disease, a progressive neurological brain illness, is incurable [2, 19].

When diagnosed early, it is possible to help avoid brain tissue damage with correct therapy. It begins with the part of the brain responsible for speech and memory. Therefore, memory loss occurs, and trouble speaking, reading, and writing [8, 10, 12]. They often lose track of their lives and may not identify family members. They have difficulty doing basic tasks like brushing their teeth or combing their hair. All these factors contribute to the anxiety and aggression of AD patients. AD eventually damages the part of the brain responsible for breathing and heart function, resulting in death [20]. Alzheimer's disease is classified into very mild, mild, and moderate stages. Alzheimer's disease diagnosis is still imprecise until a patient reaches the moderate AD stage. Research has used several Machine Learning Models for diagnosing Alzheimer's Disease [12, 16]. MRI is the standard practice for diagnosing AD in clinical research. The existing image variants are given in Table 1, with pros and cons [1–4, 8, 10, 19, 20].

A classifier looks at the training data to figure out how input variables are linked to the class they belong to. There must be training data from people who have the brain disorder and people who don't. [16, 20] When the classifier is trained correctly, it can look for people with a specific brain disorder. The things you want to learn about also need to be known [8, 19].

Table 1. Alzheimer's image variant with pros and cons

Existing image variants	Pros	Cons
CT imaging of the head	Helpful in ruling out other causes of the symptoms	Not accurate
PET of the head	Helpful in determining the severity of the disease	Uses radioactive material
MRI of the head	Can detect abnormalities associated with mild cognitive impairment	In the early stages of the Disease, MRI could be normal
Medical examination (family medical history, blood test, neurological exam)	Successful diagnosis to a good extent	Expensive and time taking

2 Motivation

As stats say, more than four million people in India are diagnosed with Alzheimer's and other forms of Dementia. India stands as the third-highest country with cases of

Alzheimer's in the whole world, after China and the US. It is forecasted that by the end of 2030, India will reach almost 7.5 million disease cases [4, 5, 19].

According to the 2017 India Ageing Report, the senior population, rising at a quicker pace of 3%, may bear the brunt of Alzheimer's disease in India since the disease typically affects individuals over the age of 60. As a result, building an automated Alzheimer's disease (AD) detection system is commercially attractive for disease detection. Early detection of disease during the process is critical since it enables:

- Higher possibility of improving the quality of life.
- The opportunity to receive support services.
- A good time to express and decide wishes related to future care and living arrangements.
- To make financial plans on time.

3 Key Contribution

The key contributions of our work are as follows:

- We present a classification-based strategy for diagnosing and classifying Alzheimer's Disease.
- Our suggested network learns from a tiny dataset and performs much better at diagnosing AD.
- We train our machine learning model on a dataset that is skewed.
- We have evaluated model performance with assessment metrics and the AUROC curve.
- We have extracted discriminative brain features for model performance enhancement.

4 Material and Method

a. **Image Acquisition**

The dementia prediction and classification dataset are a labeled image comprising grey scaled images of size 178 x 208 pixels. These images are MRI scans of patients with Alzheimer's Disease ranging from level zero to level three. When working with MRI images, skull stripping is critical for the dataset. However, the images still needed to be processed before extracting features apart from skull stripping. Image processing involved grey scaling, blurring the image to make feature detection possible for the system, and determining the region of interest [21]. The dataset was gathered from the Alzheimer's ADNI database (adni.loni.usc.edu) [1–3]. The ADNI is a multi-focus study assessing neuroimaging for diagnosis and monitoring. The ADNI was propelled in 2003. Its essential goal is to evaluate Alzheimer's disease progression and mild cognitive impairment through natural markers such as MRI, PET, clinical and neuropsychological assessment [11–14].

b. **Feature Extraction**
The Alzheimer's disease dataset from ADNI was classified into four categories, namely, (1) non-Demented, (2) Very Mild Demented, (3) Mild Demented, and (4) Moderate Demented. This data consisted of 510 non-Demented,330 Very Mild, 328 Mild, and 52 Moderately affected brain MRI scanned images, making 1210 images. The next crucial step involved identifying the essential and extractable features from the images using image processing techniques. The contour's shape, size, time, standard deviation, area, and other parts were extracted from the cerebrum region of the brain for detection of AD. Some of the extracted essential features are discussed in detail:

c. **Number of Contours as a Feature**
A **contour** is a closed curve that joins all the boundaries of a particular shape in an image. It can be of different shapes and sizes. Contours can be an essential feature when detecting Dementia from a brain MRI image. Contour detection is a primary aspect of computer vision. It is used widely for object detection and classification in the real world. In the case of Alzheimer's Disease, the neurodegenerative condition impairs memory and cognitive function and gradually leads to Dementia, brain cells start to disintegrate physically, and hollow patches are filled with synovial fluid, termed contours, begin to appear.

Here, we first apply Mean shift filtering to smoothen the input image. The mean shift establishes a window around each data point and computes the data point's mean. After then shifts the window's center to the mean and continues the procedure until it converges. Next, we convert the input image to a greyscale image and apply binary thresholding. Thresholding is a technique that transforms a pixel to either pure white or black depending upon the threshold limit. It makes it easy to detect the contours in the image. Finally, the **number of contours** is calculated in Fig. 1 using the cv2.findContours(), Python's inbuilt function, which returns the list of contours found in the image.

d. **Area of Corpus Callosum as a Feature**
The corpus callosum is a large fiber bundle that links the brain's left and right cerebral hemispheres. It is a location that has been thoroughly investigated for signs of Alzheimer's Disease. A recessive genetic disease may cause problems with the corpus callosum. Almost all prior research on the corpus callosum in Alzheimer's Disease has focused on its size, namely its mid-sagittal cross-sectional area. We utilize the corpus callosum's size as a characteristic in this article because its size may be more deeply impacted than its shape in early Alzheimer's Disease. Here, we cycle over the collected corpus callosum and determine their size using the Python method cv2.contourArea(), while also saving the corpus callosum's maximum size [6, 7].

e. **Gray and White matter as a Feature**
Grey matter in the inner cerebrum, which contains a system of nerve cells engaged with handling signals from various senses, has all the earmarks of being progressively helpless to early maturing, which can prompt Alzheimer's Disease. A volumetric investigation on the Gray matter demonstrated a significant negative relationship

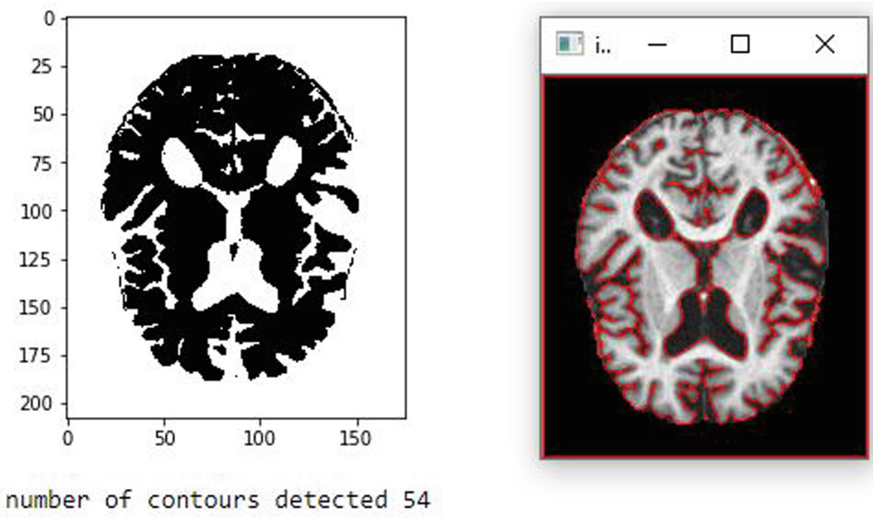


Fig. 1. Highlighting the detected contours

between the seriousness of intellectual changes and Gray matter volume. The deterioration of white matter in the biggest and deepest part of your patient's brain may be attributed to various factors, including age. This tissue includes millions of nerve fibers, or axons, linking multiple sections of the brain and spinal cord and communicating with your nerves. Myelin, a fatty substance, preserves the fibers and provides white matter color. Damage to the white matter plays a critical part in how the disease manifests and develops. The significant job of vascular illness in the advancement of white tissue harm ought to be underlined. White tissue will, in general, be dispersed in mind regions with moderately low perfusion levels, especially in periventricular white matter. The thickness of vessels in these regions diminishes both with typical maturing and in AD. The images were threshed hold and pixels converted to black (voxel value = 0) and white (voxel value = 255) to preserve the actual amount of Gray and white matter from the original data and smoothened using pyMeanShiftFiltering. The next step was to calculate the gray and white matter area, which was done using the cv.contourArea() function. The function calculates the number of pixels that make up the black and white portion of the image and multiples it with 0.264 mm, the standard pixel size [8–10].

f. **Structural Similarity Index (SSIM) & Mean Square Error (MSE)**

There are two prevalent and simple ways to check how similar, or dissimilar an image is from another: mean square error (MSE) and structural similarity index (SSIM). We used these two techniques to find out the similarity in left and right halves of the brain, as it is known that Demented brains tend to have more dissimilarity in their brain's right and left halves compared to non-demented brains. We know that AD is a neurodegenerative disease which means there is a loss of neurons from the brain tissue. However, these losses are not symmetric and instead follow no specific fixed pattern, resulting in the loss of neurons from the left and right half of the brain, resulting in an increased dissimilarity between the two hemispheres. Thus, we harvested this as a critical feature and applied SSIM and MSE combined to get better and firm results [15, 16].

g. **Mean & Standard Deviation**

The mean of an image is calculated by adding all the pixel values divided by the total number of pixels in an image. This will give us the average pixel value for each image, which can help analyze the different classes of Alzheimer's Disease. Calculating the mean of the image is significant as it provides us with a value whose range will differ for different stages of AD because, with increased severity of AD, the brain's overall structure starts to change or degrade. So, we take the mean of each image and store its value which will later help us classify the images into different categories.

The standard deviation is the focal moment depicting the probability distribution of a set of observed data points and can serve as a proportion of inhomogeneity. A higher worth shows a better intensity level and increased differentiation of edges in a picture. It is the most generally utilized proportion of inconstancy or diversity used in statistics. In terms of image processing demonstrates the degree of deviation or "scattering" from the standard (mean or anticipated average). A modest standard deviation shows that the data are skewed towards the mean. In contrast, an exclusive standard deviation suggests that the data span an extensive range of potential values.

h. **Entropy**

Entropy is determined to portray the arbitrariness of the textural image. Entropy is the amount of uncertain data about an event associated with a given probability distribution. The dataset images with low entropy are more homogenous. They can be categorized into one group compared to an image with high entropy. Certain textures might have specific entropy values, so that more entropy could mean more textures and variations in an image. Hence, entropy helps classify the image into four categories: moderate demented, non-demented, very mild, and mild.

i. **Skewness**

Skewness is a measure of equilibrium or the lack thereof. In image processing, darker and glossier surfaces will often have a more skewed appearance than lighter and matte surfaces. Henceforth, we will make judgments concerning brain surface based on skewness. Skewness is calculated as follows: ' N' denotes the number of data points, 'Xj' indicates the observation point, and 'X bar' is the mean divided by standard deviation. This is accomplished simply via Python's built-in function **skew ().**

j. **Feature Selection**

After all the pre-processing of images to remove noisy data, we extracted 13 features from about 1220 images and stored them into a CSV file. Data cleaning and selection is the next crucial step required to ensure smooth and unbiased machine learning model training. The extracted data might contain noisy and redundant data. Consequently, it is required to minimize noisy or redundant data and define the dataset using fewer optimum subset characteristics to increase performance and decrease computation time costs. We employed the concept of principal component analysis to determine the effect of all biomarker indicators on the detection of AD and MCI. [17, 18].

Here, we use PCA for dimensionality reduction of the 13 features we extracted (Fig. 2). We first import PCA from sci-kit learn. We then use the **plot_importance function** from the **boost** library to plot a graph representing the relative importance of each of the extracted features. Finally, we can use only the critical desired features and prevent overfitting or underfitting the machine learning model. We use PCA for dimensionality reduction and reduce the redundant features.

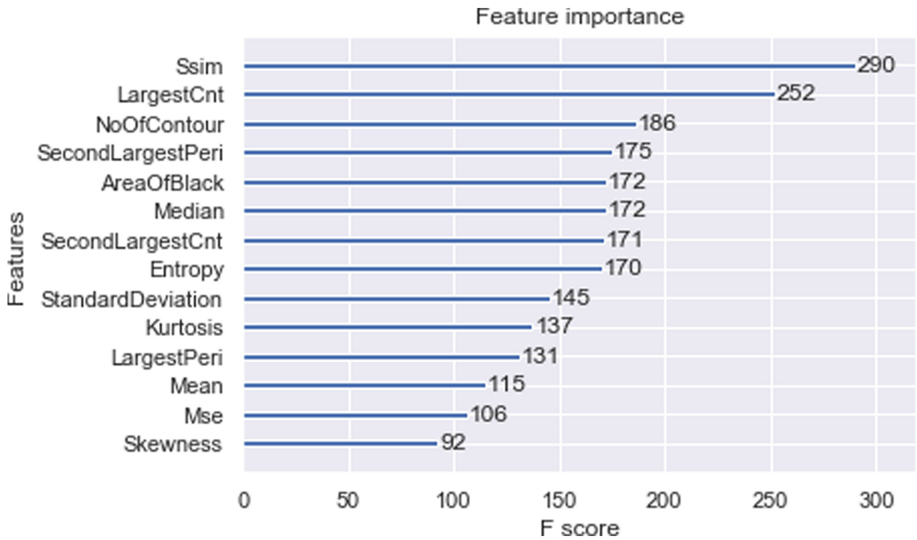


Fig. 2. Relative importance of each extracted feature

k. **Model Creation**

We used a random forest classifier, an ensemble learning algorithm, to create the classification model. Bagging, also known as bootstrap aggregation, is an assembled learning method in which smaller bootstrap datasets are formed, which are created by randomly selecting samples from the original dataset with replacement. A classification algorithm is fitted to each bootstrap dataset for training; then, a test tuple is provided to each classifier, and a prediction is made. The class with majority votes becomes the output of the master model, which is created by aggregating all the base classifiers(models). Random forest classifier follows the same bootstrap aggregation method, where each classifier in the base model is a decision tree. These decision trees are formed as they are least correlated for the best accuracy.

We first split the features and target data into train and test for implementing the random forest classifier. For this, we used the **train_test_split ()** method of sklearn.model_selection library. We divided the data into a 90:10 ratio, i.e., 90% data for training and 10% data for testing. Finally, the random forest classifier method is imported from the ensemble library of sklearn, and this classifier is fitted on our dataset for training. After training, the holdout validation method is used, and **accuracy of approximately 81%** was achieved on test data.

The overall process workflow is shown below in Fig. 3.

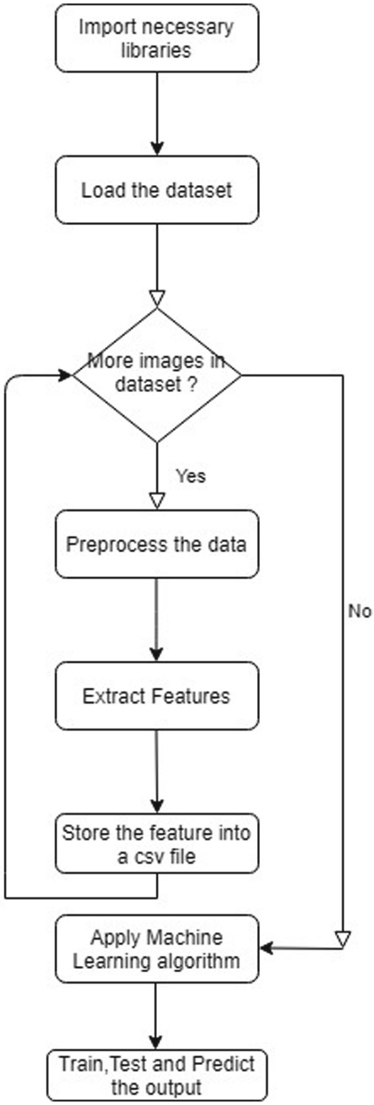


Fig. 3. Workflow followed during the model development

5 Results and Discussion

As for result concern, we will first show the bar chart, including everyone's classification of stages. Here we have used a bar graph to represent the count of each category/class present in our dataset in a graphical format which illustrates in Fig. 4:

- Non-Demented Cases
- Very Mild Demented Cases
- Mild Demented Cases
- Moderate Demented Cases

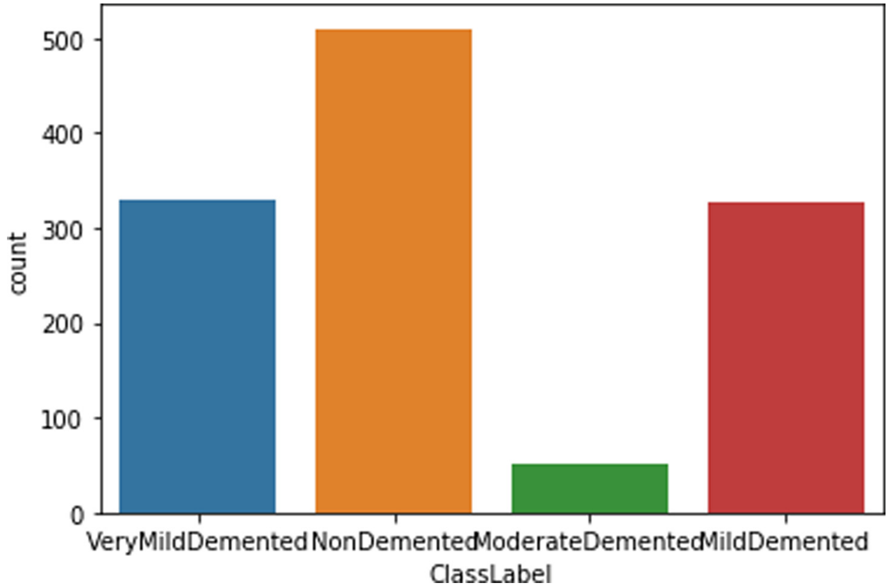


Fig. 4. Bar graph that gives us clear picture of the counts of each stage

Box Plots [13] are mainly designed to compare data distribution. Here we have used Box Plot to compare the features of the cases, which are Non-Demented, Very Mild Demented, Mild Demented, and Moderate Demented, with their values. The features that we have selected for our model are as follows:

- Area of Black
- Area of White
- MSE-Mean Square Error is used to find the similarity of an image to another.
- SSIM-Structural Similarity Index was used to quantify image quality.
- Kurtosis- Talks about the sharpness of the peak of a frequency distribution curve.
- Entropy-Used to extract features.
- Median

- Skewness
- Standard Deviation
- Mean
- LargestPeri
- SecondLargestPeri
- SecondLargestCnt

The Box Plot of extracted features is shown in Fig. 5.

We have also found the discriminative power of features between gray matter (on the x-axis) and Area of White matter (on the y-axis) using a Joint plot. A joint Plot is a plot for displaying a relationship between 1D profiles and between two variables. In our dataset, we plotted the Joint Plot between two features: Area of Gray matter (on the x-axis) and Area of White matter (on the y-axis) in Fig. 6.

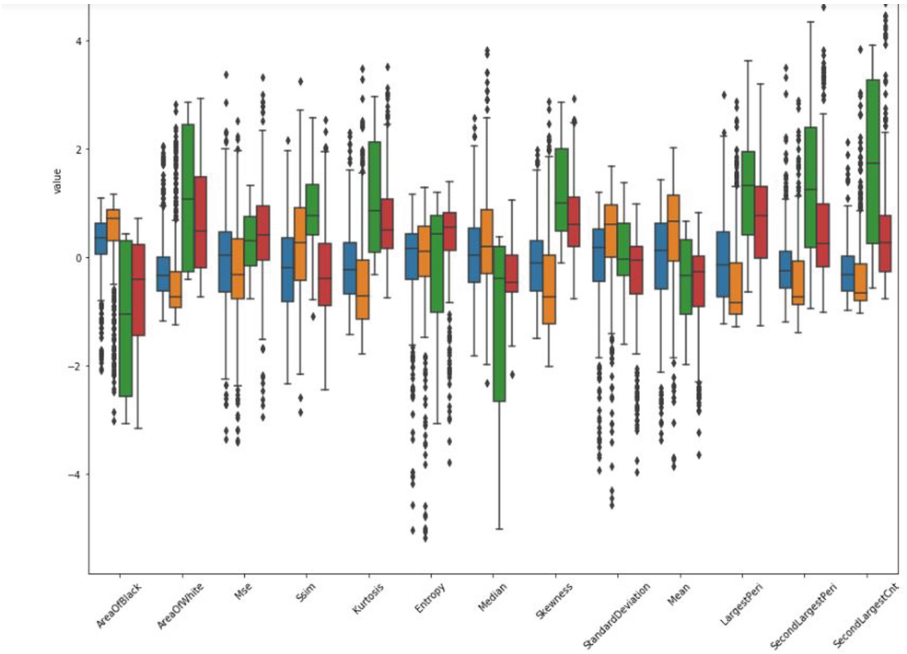


Fig. 5. Box Plot of the data extracted as features

As for the overall discriminative features presentation [9, 13]. A heat map shows which areas of the dataset get the most attention or have the most records. This helps in easy visualization of the dataset, and from a heat map, it is easy to read the dataset with clarity of information.

We have used a heat map for our model after dropping all the unimportant columns and considering only the relevant features. This gives us a clear vision of our features in Fig. 7.

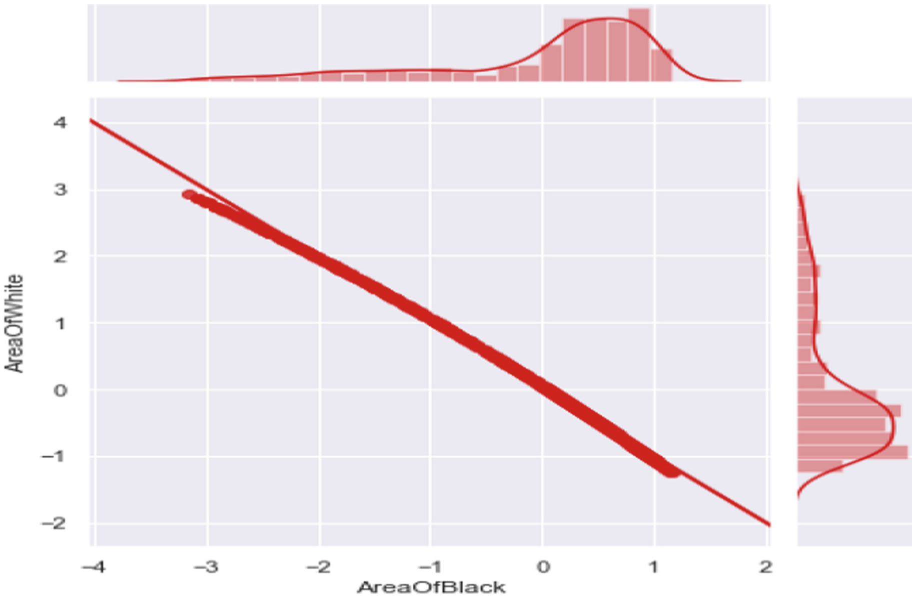


Fig. 6. Joint plot for Grey matter vs. White matter

Model Evaluation: ROC Curve and P-R Curve
The curve indicates how well the probabilities from the positive class are separate from the negative classes. The area under the ROC curve is known as AUC. Features of the curve are:

- It measures the performance of the model.
- The curve talks about how good the model is.
- A probability curve is referred to as a ROC (Receiver Operating Characteristics).
- The ROC curve is displayed using TPR (True Positive Rate) (y-axis) versus the FPR (False Positive Rate) (x-axis) (x-axis)

Precision-recall curves are helpful when there is a class imbalance, as in our case, precision represents the probability of the relevancy of an item, whereas recall is the measure of completeness.

Formula for precision is true positives/ (false positive + true positive),

Formula for recall is true positive/ (false negative + true positive) (Fig. 8).

Model Evaluation: Confusion Matrix
A confusion matrix [9] forms the basis of model evaluation. It consists of true positive, false negative, true negative, and false-positive instances that give us insight into how many test samples are correctly classified for each class label. The confusion matrix for our model is presented in Fig. 9.

Model Evaluation: Classification Report
The classification report gives us an overview of the different class labels' precision,

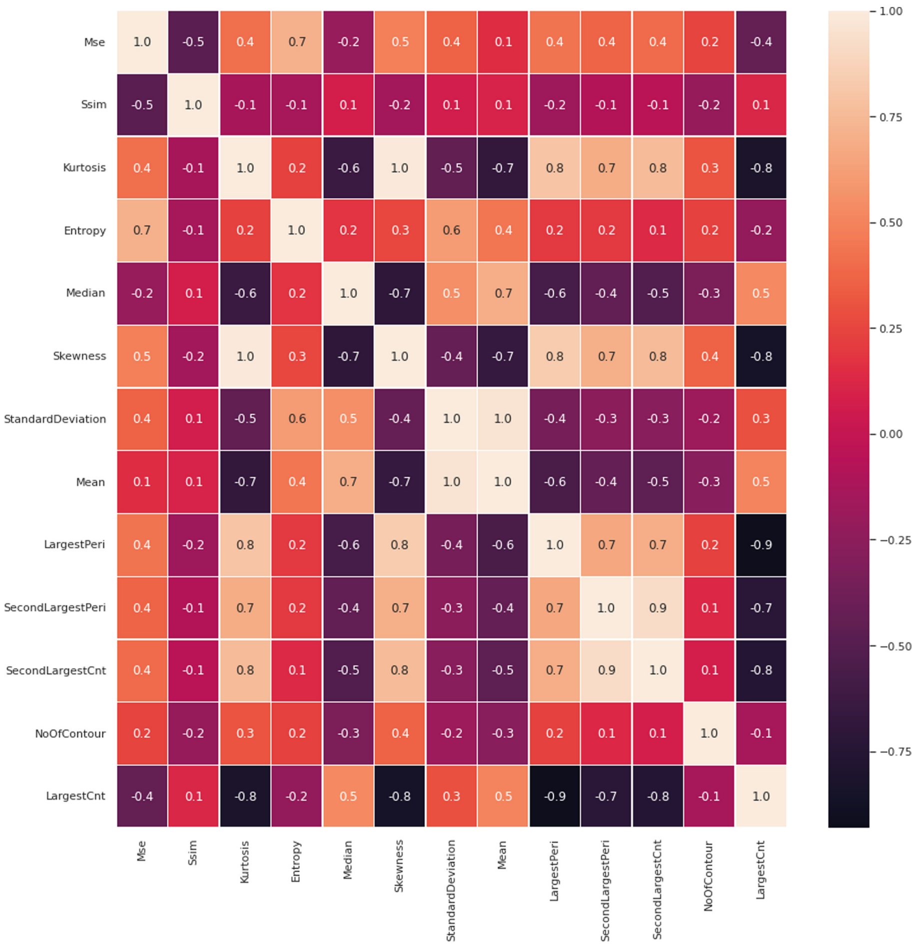


Fig. 7. Heat Map for feature discrimination and correlation

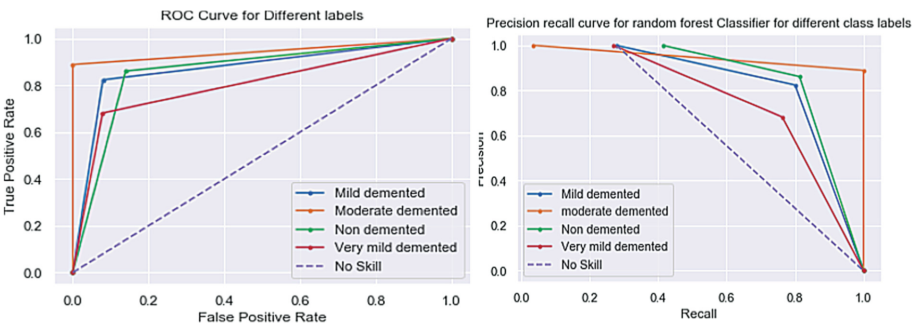


Fig. 8. Model evaluation: ROC curve and P-R curve

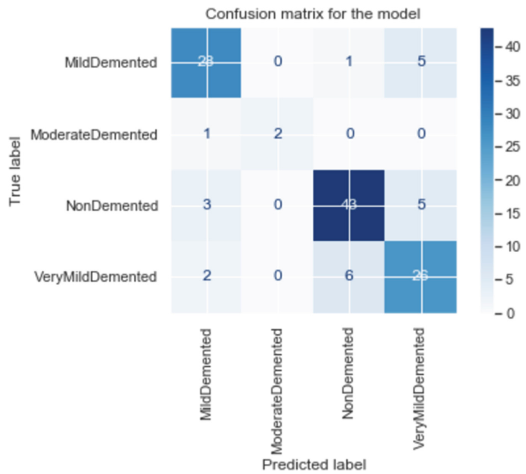


Fig. 9. Model Evaluation: Confusion matrix

recall, and f1-score and tells us about the model's accuracy. Below is Table 2 of the classification report for our model.

Table 2. Proposed work evaluation metrics

	precision	recall	f1-score	support
MildDemented	0.82	0.82	0.82	34
ModerateDemented	1.00	0.67	0.80	3
NonDemented	0.86	0.84	0.85	51
VeryMildDemented	0.72	0.76	0.74	34
accuracy			0.81	122
macro avg	0.85	0.77	0.80	122
weighted avg	0.81	0.81	0.81	122

We have implemented stratified k-fold cross-validation for our model, for **52 splits**, the maximum splits possible for our dataset. We got a **mean accuracy of 75.09%,** while **the highest accuracy achieved was 91.6%**, and the **lowest accuracy was 52%.** A comparative study of our proposed model with existing literature is given in Table 3.

Table 3. Comparative study with existing literature

Author	Data Set	Accuracy (Average)	Features
R. Chaves et al. 2013 [12]	ADNI	91.33–92%	Redundant
Anandh et al. 2016 [10]	ADNI	91–93%	Redundant
K.R. Kruthika et al. 2018 [8]	ADNI	85–88%	Redundant
F. Segovia et al. 2015 [16]	ADNI	85–91%	Redundant
Our proposed work	*ADNI*	*72–91.6%*	*Discriminant*

6 Conclusion

We establish an efficient strategy for AD diagnosis using brain MRI data processing. While most of the research has been on binary classification, our technique considerably improves multi-class categorization. Our suggested network may be precious for diagnosing early-stage AD. The manual identification of the presence and extent of Alzheimer's Disease by a pathologist is tedious and critical for patients at some stages. Therefore, this project will lead to better cross-validation of images which can be life-saving in some situations. The project will focus on a significant time reduction in the prediction of Alzheimer's in an image from a matter of hours to a matter of seconds. There are numerous novel techniques for the location of Alzheimer's. However, a significant fraction of them demands subject-matter knowledge or are prohibitively expensive. Developing a simple procedure that requires little talent in this fashion is necessary. One of the prerequisites should be early recognition of AD since it is a fatal disease. The suggested strategy is economically feasible and needs little skill.

Currently, our model can predict the stage of deadly AD, but it is still in the development phase. The model's accuracy needs to be increased to ensure it is safe to use in the medical industry. Also, it requires a user-friendly graphical user interface where a user can upload the MRI scanned image and get output within a fraction of seconds. This will need an online website built using the Django framework because a website can be easily accessible anytime, anywhere by common people.

Acknowledgments. My sincere gratitude to the National Institute of Technology Raipur and CIDCR Lab, Manipal University Jaipur for providing research resources and assistance. We appreciate the Alzheimer's Disease Neuroimaging Initiative for sharing the dataset.

References

1. LONI-ADNI: Alzheimer's Disease Neuroimaging Initiative (ADNI). http://adni.loni.usc.edu/data-samples/access-data/). Online Last Accessed 18 May 2021
2. Aisen, P.S., et al.: Alzheimer's Disease Neuroimaging Initiative 2 Clinical Core: Progress and plans. Alzheimer's & dementia: the journal of the Alzheimer's Association **11**(7), 734–9 (2015). https://doi.org/10.1016/j.jalz.2015.05.005

3. Petersen, R.C., et al.: Alzheimer's disease neuroimaging initiative (ADNI): clinical characterization. Neurology **74**(3), 2019 (2010). https://doi.org/10.1212/WNL.0b013e3181cb3e25
4. Bondi, M.W., et al.: Alzheimer's Disease: Past, Present, and Future. J. Int. Neuropsychol. Soc. JINS **23**(9–10), 818–831 (2017). https://doi.org/10.1017/S135561771700100X
5. Allsop, D.: Introduction to Alzheimer's disease. Methods Mol Med. **32**, 1–21 (2000). https://doi.org/10.1385/1-59259-195-7:1
6. Beheshtia, I., Demirelb, H., Matsudaa, H.: For the Alzheimer's Disease Neuroimaging Initiative, "Computers in Biology and Medicine," Classification of Alzheimer's Disease and prediction of mild cognitive impairment-to-Alzheimer's conversion from structural magnetic resource imaging using feature ranking and a genetic algorithm. Computers in Biology and Medicine **83**, 1–11 (2017)
7. Sa, B.K., Sa, A.S., Lala, K., Antonya, A., Kurupa, A.M.: Alzheimer's detection based on segmentation of MRI image. In: 7th International Conference on Advances in Computing & Communications, ICACC-2017, 22–24 August 2017, pp. 1–8. Cochin, India
8. Kruthika, K.R., Rajeswari, H.D.M.: Alzheimer's Disease Neuroimaging Initiative, "Informatics in Medicine Unlocked," Multistage classifier-based approach for Alzheimer's disease prediction and retrieval, pp 1–9 (2018)
9. Goel, V., Jangir, V., Shankar, V.G.: DataCan: Robust Approach for Genome Cancer Data Analysis. In: Sharma, N., Chakrabarti, A., Balas, V.E. (eds.) Data Management, Analytics and Innovation. AISC, vol. 1016, pp. 153–166. Springer, Singapore (2020). https://doi.org/10.1007/978-981-13-9364-8_12
10. Ramaniharana, A.K., Manoharanb, S.C., Swaminathana, R.: Expert systems with applications. Laplace Beltrami eigen value-based classification of normal and Alzheimer MR images using parametric and non-parametric classifiers, pp. 1–9 (23 April 2016)
11. Munteanu, C.R., et al.: Expert Systems with Applications, Classification of mild cognitive impairment and Alzheimer's Disease with machine-learning techniques using 1 H Magnetic Resonance Spectroscopy data, pp. 1–10 (30 March 2015)
12. Chaves, R., Ramírez, J., Górriz, J.M.: For the Alzheimer's Disease Neuroimaging Initiative, "Expert Systems with Applications," Integrating discretization and association rule-based classification for Alzheimer's disease diagnosis. Expert Systems with Applications **40**, 1–8 (2013)
13. Shankar, V.G., Devi, B., Bhatnagar, A., Sharma, A.K., Srivastava, D.K.: Indian Air Quality Health Index Analysis Using Exploratory Data Analysis. In: Sharma, D.K., Son, L.H., Sharma, R., Cengiz, K. (eds.) Micro-Electronics and Telecommunication Engineering. LNNS, vol. 179, pp. 545–554. Springer, Singapore (2021). https://doi.org/10.1007/978-981-33-4687-1_51
14. Sun, Yan., Tang, Y., Ding, S., Lv, S., Cu, Y.: Expert Systems with Applications, Diagnose the mild cognitive impairment by constructing Bayesian network with missing data. Expert Systems with Applications **38**, 1–8 (2011)
15. Shankar, V.G., Sisodia, D.S., Chandrakar, P.: DataAutism: An Early Detection Framework of Autism in Infants using Data Science. In: Sharma, N., Chakrabarti, A., Balas, V.E. (eds.) Data Management, Analytics and Innovation. AISC, vol. 1016, pp. 167–178. Springer, Singapore (2020). https://doi.org/10.1007/978-981-13-9364-8_13
16. Segovia, F., Górriz, J.M., Ramírez, J., Salas-González, D., Álvarez, I.: Expert Systems with Applications, Early diagnosis of Alzheimer's disease based on Partial Least Squares and Support Vector Machine. Expert Systems with Applications **40**, 1–7 (2013)
17. Ha, D., Tomotoshi, Y., Senda, M., Watanabe, H., Katagiri, S., Ohsaki, M.: A Practical method based on bayes boundary-ness for optimal classifier parameter status selection. Journal of Signal Processing Systems **92**(2), 135–151 (2019). https://doi.org/10.1007/s11265-019-01451-y

18. Garg, M., Dhiman, G.: A novel content-based image retrieval approach for classification using GLCM features and texture fused LBP variants. Neural Comput. Appl. **33**(4), 1311–1328 (2020). https://doi.org/10.1007/s00521-020-05017-z
19. Shankar, V.G., Sisodia, D.S., Chandrakar, P.: A novel discriminant feature selection–based mutual information extraction from MR brain images for Alzheimer's stages detection and prediction. Int. J. Imag. Sys. Technol. 1–20 (2021). https://doi.org/10.1002/ima.22685
20. Devi, B., Srivastava, S., Verma, V.K.: Predictive Analysis of Alzheimer's Disease Based on Wrapper Approach Using SVM and KNN. In: Senjyu, T., Mahalle, P.N., Perumal, T., Joshi, A. (eds.) ICTIS 2020. SIST, vol. 196, pp. 707–715. Springer, Singapore (2021). https://doi.org/10.1007/978-981-15-7062-9_71
21. Shankar, V.G., Devi, B., Sachdeva, U., Harsola, H.: Real-Time Human Body Tracking System for Posture and Movement Using Skeleton-Based Segmentation. In: Sharma, D.K., Son, L.H., Sharma, R., Cengiz, K. (eds.) Micro-Electronics and Telecommunication Engineering. LNNS, vol. 179, pp. 499–510. Springer, Singapore (2021). https://doi.org/10.1007/978-981-33-4687-1_48

EMG Pattern Recognition: A Systematic Review

Sushama Dhumal[1](✉) and Prashant Sharma[2]

[1] PAHER University, Udaipur, Rajasthan, India
sushama.dhumal@gmail.com
[2] CSE, Pacific University, Udaipur, Rajasthan, India
prashant.sharma@pacific-it.ac.in

Abstract. EMG (electromyography), which records the electrical activity of our muscles, is a common test for muscle movement. This test helps determine whether there is a nerve injury or a muscle disease present, allowing the best course of treatment to be determined. EMG (electrical muscle activity) signals are used in a wide range of biomedical and neurological applications. It's a quick overview of pattern recognition using EMG signals, explaining the various models and techniques available. EMG signals can be collected using needle electrodes or wearable devices like the Myo Armband for hand gesture recognition. For the purposes of this study, both cases were considered and analyzed. The electromyographic sensors found in the Myo armband can be used to create cost-effective and easy-to-use prototype models for a variety of applications. Traditional algorithms are characterized by complex computational methods and a high level of variability. Electromyographic signals, on the other hand, can now be analyzed thanks to advances in digital signal processing and mathematical models.

Keywords: EMG · Pattern recognition · Gesture

1 Introduction

EMG (electromyography) is a common test that measures how our muscles function these days. It is based on the fact that when a muscle contracts, it produces a burst of electric activity that passes through adjacent tissues and bones as well as being recorded from adjoining skin areas. This test can help determine whether a damage or muscle problem exists, as well as the appropriate course of treatment. Although MRI and X-ray images can disclose information about the spine's anatomy, EMG testing provides details about how the muscles and nerves function.

Basic Principle
The following is the fundamental principle underlying the generation of the EMG signal. Motor nerve cells in the cerebral cortex are responsible for the generation of electrical pulses under the supervision of the central nervous system [20]. When these brain impulses pass through axons and into muscle fibers, they induce pulse sequences that drive the muscle fibers to contract and produce muscular tension. The human body generates a current, which results in transmembrane potential, while all of this is happening.

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 120–130, 2023.
https://doi.org/10.1007/978-3-031-13150-9_10

In muscle cell membranes, the transmembrane potential is defined as the difference between the internal and exterior potentials of the cell membrane [31]. According to [29], when muscle cells are relaxed, the cell membrane potential is polarized. When a cell is stimulated, it depolarizes, and the depolarization pattern spreads throughout the body [32]. An electromyography signal correlates to the action potential that is linked with it. The nerve and muscle system's EMG signal generation process is depicted in Fig. 1.

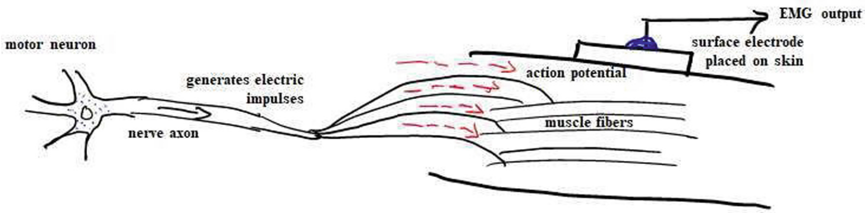


Fig. 1. Natural process of generation of EMG signals

When the human body performs a specific movement, a group of muscles is activated. The number of muscles that are activated is determined by the type of activity that the body is engaging in at the time. Taking the example of lifting a little stone, the muscles required are noticeably smaller than those necessary to move a 6-kilo bag. In order to generate more force, the Central Nervous System's excitation is increased, more motor units are activated, and the firing rate of all motor units is in- creased, resulting in increased EMG signal amplitudes [33].

Herein, we have published a survey on Pattern Recognition utilizing Electromyographic Signals (EMG signals). In the following part, you will find an introduction to electromyographic signals, which is followed by three sections. Throughout the Second Section, you will gain a general understanding of the EMG pattern recognition process. In the Third Section, a review of pattern recognition utilizing EMG signals has been carried out, and a comparison of the results has been shown in the comparison table. Section Four discusses the advantages and disadvantages of the strategies that have been studied. Finally, Section Five provides an explanation of the topic's conclusion as well as its future study.

2 EMG Pattern Recognition Process

When EMG data is collected in its raw form, it is frequently noisy and cannot be categorized effectively. As a result, a number of processing stages must be completed as a result of this. Overall, the pattern recognition approach consists of four stages: data collection, signal pre-processing, feature extraction (including dimension reduction), classification (including categorization), and classification (including categorization) [17]. The technique of EMG pattern recognition is depicted in Fig. 2.

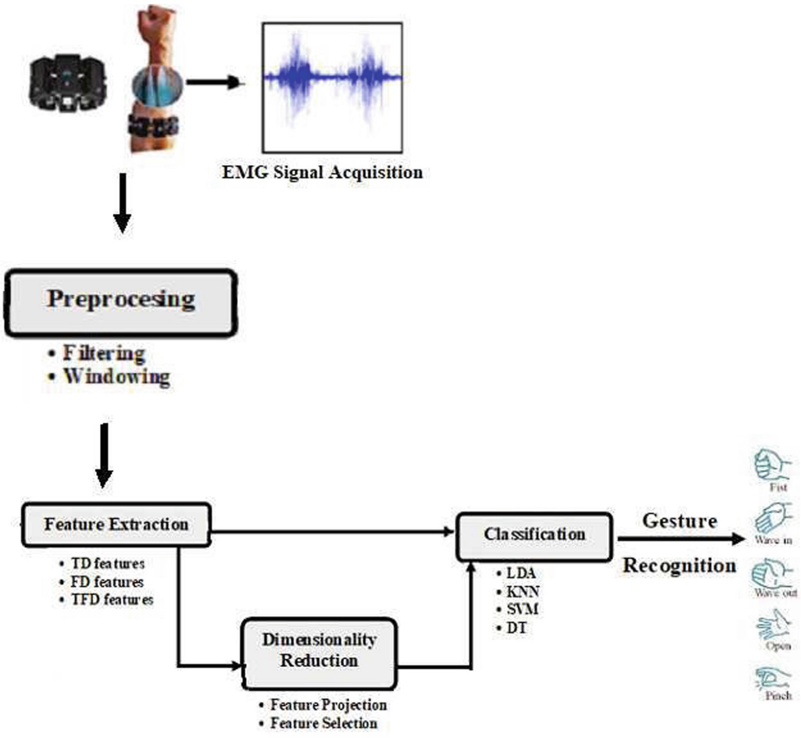


Fig. 2. EMG pattern recognition process

In addition to intramuscular EMG and surface EMG, there are several electromyography signal acquisition methodologies. Filtering and windowing are processes that are used to reduce the amount of noise in raw data and separate EMG signals from one another. After a signal has been pre-processed, the noise level can be lowered, and window segments can be generated from the signal. When extracting features from window sequences, feature extraction approaches such as time-domain features, frequency domain features, and autoregressive features are used, among them being time-domain features. Dimensionality reduction techniques are used to ascertain the characteristics of the object. The extraction of features is followed by the application of classification methods to divide the extracted feature vectors into discrete categories [30].

Traditional classification approaches such as linear discriminant analysis (LDA), support vector machines (SVM), k nearest neighbour (KNN), Bayesian analysis, fuzzy logic (FL), and hidden Markov models are examples of traditional classification approaches [21]. Modern classification approaches such as artificial neural networks (ANN) and convolutional neural networks (CNN) are examples of modern classification approaches. The typical heuristic optimization strategy particle swarm optimization (PSO) paired with SVM is the most effective way to categorize more characteristics than any other method. Technological advancements are enabling the development of novel methods for the extraction and categorization of EMG data features.

3 Related Work

The EMG data collected with and without the Myo Armband were used in a review of the literature on pattern recognition using EMG signals, which included both positive and negative results. Wearable gesture and motion control device developed by Thalmic Labs, the Myo armband detects movements and gestures using electromyographic sensors in conjunction with gyroscopes, accelerometers, and magnetometers to provide accurate motion control. It is a low-cost device and can recognize up to five hand motions by default, which is sufficient for most users. EMG electrodes, are used to detect muscle activity in the human body and are the most widely used and professionally utilized technology for doing so [12]. Surface electrodes (also known as skin electrodes) and inserted electrodes are the two most common types of EMG electrodes. In addition, there are two types of inserted electrodes: needle electrodes and fine-wire electrodes [9]. Figure 3 depicts different types of electrodes that could be used for EMG signal acquisition. The top row shows skin electrodes, whereas the bottom row shows the inserted type of electrodes.

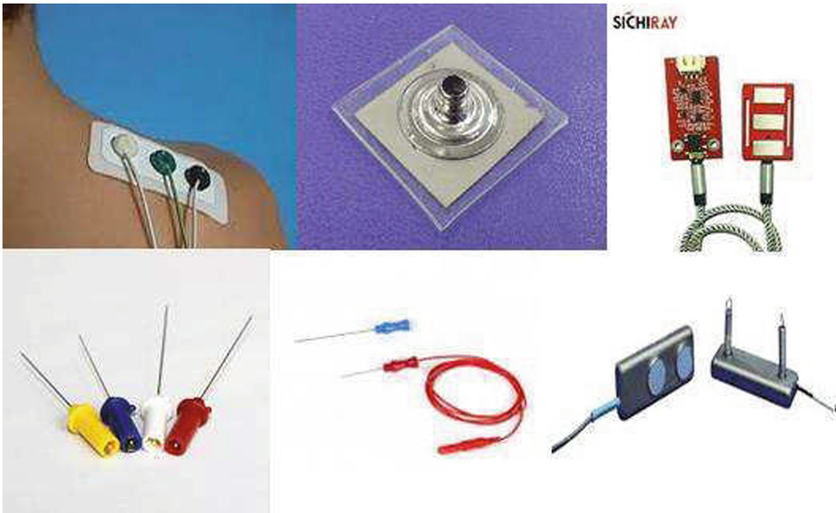


Fig. 3. Different types of electrodes for EMG signal acquisition

Benalcázar and colleagues (2017) have developed a real-time hand gesture identification model that detects five movements based on forearm EMG recordings taken with the Myo armband. The model was based on k-nearest neighbor and dynamic time warping algorithms [22].

A BP neural network classification technique based on five eigenvalues in the time domain collected from upper limb forearm sEMG data was proposed by (S. He et al. 2017) for recognizing six gestures [4]. Researchers (Z. Arief et al. 2015) analyzed five feature extractions from eight-channel electromyography (EMG) signals collected from a Myo Armband positioned on the forearm muscles in order to detect statistically significant differences during hand movements [25].

Researchers (Yansheng Wu et al. 2018) investigated a time-domain gesture detection system based on the envelope signal characteristic of a single-channel sEMG [18]. An improved KNN algorithm and a soft margin SVM algorithm were used to complete the classification of five different types of gestures. (Phinyomark et al. 2018) discuss the latest developments in existing shareable EMG data sets, as well as a review of recent research and development in EMG pattern identification methodologies and their applications to big data analytics. A discussion of future research aspects of EMG signal pattern recognition is included in this literature. In accordance with this paper, a number of factors have contributed to the growth of EMG signals data resources, including the availability of individual EMG data sets for research purposes, benchmark EMG databases, a large amount of high-density surface EMG image data, and multi-modality sensor systems that can generate a large volume of data via EMG signals [15].

Four deep learning models were used to classify various movements and gestures from multichannel noisy sources, including a 1-D Convolutional neural network (1-D CNN), a Recurrent neural network (RNN) with Long Short-Term Memory (LSTM), a basic hybrid model containing one convolutional layer and one recurrent layer (C-RNN) [27], and an advanced hybrid model containing three convolutional layers and three recurrent layers were proposed for hand medical monitoring system based on a feature selection method based on hand movement prediction and a support vector machine (SVM) classifier, which was subsequently implemented [19].

A feed-forward artificial neural network-based real-time hand gesture identification model based on surface electromyography was developed and tested [7]. Because the model's response time is only one-third of the total time required for the gesture, pattern identification occurs before the gesture is completed. A new convolutional neural network structure for hand gesture classification is proposed to process raw EMG signals directly. A large window is used to demonstrate how classification accuracy can be improved when using a large window. There is no feature extraction required for this model. For this experiment, two publicly available datasets were used [15].

Al Khazzar and colleagues (2020) used a Myo armband in conjunction with a Multi-Layer Perceptron Neural Network (MLPNN) to distinguish fourteen different gestures. Adaptive Neuro Fuzzy Inference System (ANFIS) for gesture recognition, for example, can be considered an alternative to MLPNN because it is susceptible to local minima and high computational costs [7]. An ANOVA and neural network-based technique for optimizing sEMG features and measurements positions were proposed by (Wu C. et al. 2020) for gesture recognition using surface electromyography (sEMG) measurements and features. Based on the notion of achieving high recognition accuracy in the BPNN with minimal input information the optimization is carried out in two stages [3].

Hand gestures recognized using Naive Bayes and Neural networks on Myo armband dataset can be used to control mobile robots. The Naive Bayes algorithm, according to a study, is both faster and produces better results [26].

(Le Cao et al. 2021) describe a proposed method for sEMG gesture detection that incorporates feature extraction, a genetic algorithm (GA), and a support vector machine (SVM) model. For the purpose of optimizing SVM parameters, a novel adaptive mutation particle swarm optimization approach is used (AMPSO). For the purpose of training this AMPSO-SVM model, the MYO bracelet dataset was used. The model was then tested on four different gesture classifications to see how well it performed. It is discovered that when AMPSO-SVM is compared to PSO-SVM, GS-SVM, and BP algorithms for low-frequency sEMG signal gesture identification, it performs significantly better [4].

(Li, Qi, et al. 2021) provided a total of 12 different feature selection and classification combinations. The feature selection approaches include no feature selection (NFS), sequential forward search (SFS), and particle swarm optimization (PSO). The classification algorithms include the nonadaptive support vector machine (N-SVM), the incremental support vector machine (I-SVM), the support vector machine based on TrAdaBoost (T-SVM), and the incremental support vector machine (I-SVM). The TI-SVM combined with the SFS approach outperformed accuracy and provided a good real-time performance on a small EMG dataset, despite the small size of the dataset [5]. The study (Vasanthi SM, et al. 2020) is concerned with the use of pattern recognition networks in conjunction with EMG signals and time-domain information to classify individual finger motions of a single hand. The discrete wavelet transform is used as an EMG denoising technique, and it can be used to compute variables such as variance, root mean square, integrated EMG, mean absolute value, simple square integral, mobility, skewness, and kurtosis, among others. In order to recognize hand gestures, a variety of classifiers have been used, including SVM and various feed forward neural networks [6].

Yongyu Jiang et al. (2020) investigated the effects of motion speed, individual variability, the EMG recording device, and a number of EMG datasets on the accuracy of shoulder motion pattern recognition accuracy using sEMG signals from the shoulder and upper limb muscles in the shoulder and upper limb. Feasibility of machine learning algorithms in the recognition of shoulder motion patterns using sEMG signals from the shoulder and upper limb muscles was also examined. According to the researchers, CNN was used to interpret EMG information from 12 muscles in order to identify patterns of upper arm motions [9].

Table 1 below summarizes the algorithms used in several articles to recognize EMG signal patterns.

Table 1. Algorithms used in various papers for hand gesture recognition

Paper Ref.	Model	Number of Subjects/ inputs	Proprietary System used as Source
22	k-nearest neighbor and the dynamic time warping algorithms	10	Myo armband
23	BP-NN classification algorithm	40	Myo armband
2	MLPNN	3	Myo armband
4	AMPSO-SVM	36	Myo armband
26	Naïve Bayes and NN	1	Myo armband
7	feedforward artificial neural network (FFANN)	12	Myo armband
8	Convolutional neural network (CNN)	40 18	NinaPro-DB2 CapgMyo-Dba
11	Convolutional neural network (CNN)	17	Myo Dataset
12	recurrent neural network (RNN)	13	Myo armband
18	Convolutional neural network (CNN)	7	Myo armband
28	Deep learning –Recurrent neural networks (RNNs) with LSTM+GRU along with bidirectional versions.	18	CapMyo dataset – Part A
27	Advanced hybrid model with 3 convolutional layers and 3 recurrent layers (3+3 C-RNN)	30	HAR dataset from UCI repository
16	PCA dimensionality reduction, improved KNN and soft margin SVM	4	AgCl electrodes
19	SVM with LDA,BPNN,KNN	27	NinaPro-DB1 dataset

4 Discussion

When the RMS values in the time domain are used in the Naive Bayes and NN algorithms, it has been discovered that these values can be used to detect patterns in the subject's hand positions. Although Neural Networks are better at recognizing hand movements, the Naive Bayes algorithm has the advantage of being more responsive and faster [5]. When the number of characteristics or measurement positions is in- creased, the accuracy of recognition suffers as a result. When using a Neural Net- work, increasing the input dimension can help to improve the overall accuracy of the recognition process [3].

It is possible that traditional parameter optimization approaches, such as grid search and gradient descent (GSGD), BPNN, and MLPNN, will reach local optimality during the optimization process, resulting in high processing costs and significant errors when the parameters are manually adjusted [7]. The adaptive particle swarm optimization

(AMPSO) approach was used to determine the optimal parameters for improving model classification accuracy and anti-interference capabilities [4]. PSO combined with SVM is one of the best combinations for gesture recognition because of its high recognition rate. It is possible that the weight-optimized KNN algorithm is more accurate than the classic KNN algorithm. According to the researchers, using KNN with appropriate feature selection and on a standard database such as DB1 results in higher accuracy [19]. In order to stabilize the ANN classifier during training and testing, the minimum mean square error (MSE) is used as a benchmark. The SVM classifier outperforms ANN classifiers in terms of accuracy [6].

Misclassification will occur if the classification threshold for activation time is set to a value that is either too small or too large. If the threshold is set to a lower value, the classifier will complete its task in less time; therefore, the threshold must be set appropriately. Using the categorized EMG signal, it is possible to develop a human-computer interface that can assist people who have physical or mental disabilities [8].

Comparing different mixed CNN models, a simple CNN model trained on EMG datasets of a defined motion was found to have the highest accuracy for various speeds of motion pattern recognition [9]. Aside from these advantages, CNN has higher accuracy and a lower classification error rate (CE) when compared to LDA, making it more robust and computationally efficient. When parameter selection is optimized, these deep learning algorithms can produce superior results, and they are also influenced by the network architecture.

A standard RNN recognizes 8 gestures with 78% accuracy, which is a good result. The use of an RNN model in conjunction with bi-LSTM and GRU for hand gesture recognition, on the other hand, resulted in improved performance and accuracy, even when more participants were used. Additionally, using Bidirectional LSTM and GRU, it is possible to associate past and future events, and output can be generated based on the most recent available data. In this way, it is more realistic and precise than alternative approaches. Table 2 provides a more in-depth analysis of the same studies, with accuracy and gestures identified.

When the number of hidden layers, the number of nodes in hidden layers, and the error rate in neural networks are changed, the recognition rate and optimization rate can both increase. In deep learning systems, the accumulation of large amounts of data, the use of a high sampling rate, and the lack of sufficient information cause ac- curacy to deteriorate.

Table 2. Precision review of hand gesture recognition

Paper Ref.	Recognition Accuracy	No. Of Gestures
22	89.5%	5
23	93.43%	6
2	90.5%	14
4	97.5%	4
26	90.61% (with Naïve Bayes) 93.07% (with NN)	5
7	98.7%	5
8	73.5% (with NinaPro-DB2) 78.5% (with CapgMyo-Dba)	50 9
11	98.81%	7
12	89.6%	21
18	97.60 ± 1.99 (CNN), 98.12 ± 1.07 (SSAE-f)	7
28	98.57% (Bi-LSTM)	8
27	90.29% (DB1-HAR dataset from UCI repository) 83.61% (DB2- Ninapro database) 63.74% (DB3- Ninapro database)	17
16	75.8 (with Improved KNN), 79.4% (with Soft-margin SVM)	5
19	99.23% (with KNN on DB1 Ninapro database)	52

5 Conclusion

This systematic literature review examines state-of-the-art real-time hand gesture detection algorithms using electromyography (EMG) data and machine learning techniques, most of which are based on EMG data collected by the Myo Armband and presented in this paper. When developing a pattern recognition model, it is important to consider the principles of different types of models, data collection, segmentation, pre-processing, feature extraction, classification, post-processing, real-time processing, different types of gestures, and evaluation metrics, among other things.

The development of a low-cost implementation model that takes into account the advantages and disadvantages of the aforementioned algorithms will be the primary focus of future research. Similarly, the number of gestures to be recognized using Myo armband will be the next important step, irrespective of the percentage accuracy achieved by the model, The occurrence of new issues will be caused by a variety of factors, including signal instability, mechanical design, encoder accuracy, data collection, and motor torque, among other things. Using the electro-myographic sensors in the Myo armband, it is possible to develop a low-cost, simple-to-use prototype model that can recognize and translate Indian sign language hand gestures into something that can be understood by differently-abled individuals.

References

1. Farina, D., Stegeman, D.F., Merletti, R.: Biophysics of the generation of EMG signals. In: Surface Electromyography: Physiology, Engineering and Applications, pp. 1–24. Wiley, Hoboken, New Jersey (2016)
2. Al-Khazzar, A., Raheema, M., Hussein, J.: Recognition of new gestures using myo armband for myoelectric prosthetic applications. Int. J. Electr. Comput. Eng. (IJECE) **10**(6), 5694–5702 (2020)
3. Wu, C., et al.: sEMG measurement position and feature optimization strategy for gesture recognition based on ANOVA and neural networks. IEEE Access **8**, 56290–56299 (2020)
4. Cao, L., Zhang, W., Kan, X., Yao, W.: A novel adaptive mutation PSO optimized SVM algorithm for sEMG-based gesture recognition. Sci. Program. **2021**, 1–13 (2021). https://doi.org/10.1155/2021/9988823
5. Li, Q., Zhang, A., Li, Z., Yan, W.: Improvement of EMG pattern recognition model performance in repeated uses by combining feature selection and incremental transfer learning. Front. Neurorobotics **15**, 87 (2021). https://doi.org/10.3389/fnbot.2021.699174
6. Vasanthi, S.M., Jayasree, T.: Performance evaluation of pattern recognition networks using electromyography signal and time-domain features for the classification of hand gestures. Proc. Inst. Mech. Eng. H. **234**(6), 639–648 (2020). https://doi.org/10.1177/0954411920912119. Epub 2020 Mar 23 PMID: 32202473
7. Zhang, Z., et al.: Real-time surface EMG pattern recognition for hand gestures based on an artificial neural network. Sensors **19**(14), 3170 (2019). https://doi.org/10.3390/s19143170
8. Yang, W., Yang, D., Liu, Y., Liu, H.: EMG pattern recognition using convolutional neural network with different scale signal/spectra input. Int. J. Humanoid Rob. **16**(04), 1950013 (2019)
9. Jiang, Y., et al.: Shoulder muscle activation pattern recognition based on sEMG and machine learning algorithms. Comput. Meth. Programs Biomed. **197**, 105721 (2020)
10. Zhou, Y., Chen, C., Ni, J., Ni, G., Li, M., Xu, G., et al.: EMG signal processing for hand motion pattern recognition using machine learning algorithms. Arch. Orthop. **1**(1), 17–26 (2020)
11. Chen, L., Fu, J., Wu, Y., Li, H., Zheng, B.: Hand gesture recognition using compact CNN via surface electromyography signals. Sensors **20**(3), 672 (2020)
12. Zhang, Z., He, C., Yang, K.: A novel surface electromyographic signal-based hand gesture prediction using a recurrent neural network. Sensors **20**(14), 3994 (2020)
13. Jaramillo-Yánez, A., Benalcázar, M.E., Mena-Maldonado, E.: Real-time hand gesture recognition using surface electromyography and machine learning: a systematic literature review. Sensors **20**(9), 2467 (2020)
14. Christodoulou, C.I., Pattichis, C.S.: Unsupervised pattern recognition for the classification of EMG signals. IEEE Trans. Biomed. Eng. **46**(2), 169–178 (1999)
15. Phinyomark, A., Scheme, E.: EMG pattern recognition in the era of big data and deep learning. Big Data Cogn. Comput. **2**(3), 21 (2018). https://doi.org/10.3390/bdcc2030021
16. Wu, Y., Liang, S., Zhang, L., Chai, Z., Cao, C., Wang, S.: Gesture recognition method based on a single-channel sEMG envelope signal Wu et al. EURASIP J. Wirel. Commun. Netw. **2018,** 35 (2018). https://doi.org/10.1186/s13638-018-1046-0
17. Li, W., Shi, P., Yu, H.: Gesture recognition using surface electromyography and deep learning for prostheses hand: state-of-the-art, challenges, and future. Front. Neurosci. **15**, 621885 (2021)
18. Zia Ur Rehman, M., et al.: Multiday EMG-based classification of hand motions with deep learning techniques. Sensors, **18**(8), 2497 (2018)

19. Yu, M., Li, G., Jiang, D., Guozhang, J., Bo, T., Chen, D.: Hand medical monitoring system based on machine learning and optimal EMG feature set. Pers. Ubiquit. Comput. 1–17 (2019).https://doi.org/10.1007/s00779-019-01285-2
20. Kaur, A., Panag, N.: Different techniques for the segmentation of the EMG signal - a review. Int. J. Eng. Manage. Res. **5**(6), 15–19 (2015)
21. Karlık, B.: Machine learning algorithms for characterization of EMG signals. Int. J. Inf. Electron. Eng. **4**(3), 189 (2014)
22. Benalcázar, M.E., et al.: Real-time hand gesture recognition using the Myo armband and muscle activity detection. In: 2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM), pp. 1–6 (2017)
23. He, S., Yang, C., Wang, M., Cheng, L., Hu, Z.: Hand gesturerecognition using MYO armband, pp. 4850–4855 (2017). https://doi.org/10.1109/CAC.2017.8243637
24. Benalcázar, M.E., Jaramillo, A.G., Jonathan, A., Zea, A., Páez, A., Andaluz, V.H.: Hand gesture recognition using machine learning and the Myo armband. In: 25th European Signal Processing Conference (EUSIPCO), pp. 1040–1044 (2017)
25. Arief, Z., Sulistijono, I.A., Ardiansyah, R.A.: Comparison of five time series EMG features extractions using Myo Armband. In: 2015 International Electronics Symposium (IES), pp. 11–14 (2015)
26. Pamungkas, D.S., Simatupang, I.: Comparison EMG pattern recognition using bayes and NN methods. In: 2020 3rd International Conference on Mechanical, Electronics, Computer, and Industrial Technology (MECnIT), pp. 1–4 (2020)
27. Xie, B., Li, B., Harland, A.: Movement and gesture recognition using deep learning and wearable-sensor technology. In: Proceedings of the 2018 International Conference on Artificial Intelligence and Pattern Recognition (AIPR 2018). Association for Computing Machinery, NewYork, USA, pp. 26–31 (2018)
28. Xiong, D., Zhang, D., Zhao, X., Zhao, Y.: Hand gesture recognition using instant high-density EMG graph via deep learning method. In: 2020 Chinese Automation Congress (CAC), pp. 5143–5148, (2020)
29. Azim, M.R., Haque, S.A., Amin, M.S., Latif, T.: Analysis of EEG and EMG signals for detection of sleep disordered breathing events. In: ICECE 2010 - 6th International Conference on Electrical and Computer Engineering, December, pp. 646–649 (2010)
30. Mahmood, N.T., Al-Muifraje, M.H., Saeed, T.R., Kaittan, A.H.: Upper prosthetic design based on EMG: a systematic review. In: IOP Conference Series: Materials Science and Engineering, vol. 978, no. 1 (2020)
31. Fang, C., He, B., Wang, Y., Cao, J., Gao, S.: EMG-centered multisensory based technologies for pattern recognition in rehabilitation: state of the art and challenges. Biosensors **10**(8), 85 (2020)
32. Ibrahim, A.F.T., Gannapathy, V.R., Chong, L.W., Isa, I.S.M.: Analysis of electromyography (EMG) signal for human arm muscle: a review. In: Sulaiman, H.A., Othman, M.A., Othman, M.F.I., Rahim, Y.A., Pee, N.C. (eds.) Advanced Computer and Communication Engineering Technology, pp. 567–575. Springer International Publishing, Cham (2016). https://doi.org/10.1007/978-3-319-24584-3_49
33. Jamal, M.Z.: Signal acquisition using surface EMG and circuit design considerations for robotic prosthesis, computational intelligence in electromyography analysis - a perspective on current applications and future challenges. In: Naik, G.R. (eds.) IntechOpen, 17 October 2012. https://doi.org/10.5772/52556

Image Generation Using GPT-2

Rushikesh Pupale(✉), Adarsh Shrivastava, and Pradeep Singh

National Institute of Technology, Raipur, India
pupalerushikesh@gmail.com, psingh.cs@nitrr.ac.in

Abstract. Recently, Unsupervised Representational Learning Approaches like BERT and GPT-2 have outperformed the state of art supervised models in the field of Natural Language Processing. These approaches work on the principle of pre-training the models to arrive at a decent initialization point that is task-independent and aims to learn the general representation and distribution of the dataset. In this paper, we try to exploit a similar approach for the task of Image Generation. GPT-2 as our base model is used for developing of image owing to its state of art performance in various NLP tasks. The novel idea presented in this paper is to experiment with the usage of Cross-Domain Transfer Learning i.e. using a Pretrained GPT-2 model (trained only on textual data) to generate images of handwritten text. The developed GPT-2 based model achieved an FID score of 10.63, with minimal training on a fraction of the MNIST Dataset. The results we obtained are very close to the state of art results that were obtained by training on the complete dataset.

Keywords: Image generation · GPT · Image GPT

1 Introduction

Unsupervised Representation learning has pushed the start of art results forward in the domain of Natural Language Processing. The use of Word Vectors [1], Glove Vectors [2], BERT [3] have shown a significant hike in the model performances in the field of NLP. This class of algorithms aims to find a suitable representation of input data in the latent vector space, and these vectorized representations can further be used on a variety of tasks as initialization points. These models aim to learn a data distribution P(X) which can be further leveraged to perform tasks of supervised nature like P(X|Y). However, unlike textual data, images are high dimensional, have redundant modality and are more prone to noise. Therefore, it becomes difficult to perform generative pretraining on images. Moreover, improvements in initialization strategies, activation functions and regularization strategies suggested that pre-trained might be unnecessary in the modern scenario. Le Paine et al. [4] in their research have even demonstrated degradation in performance using pre-training for images. Thus, it is of utmost importance to use a suitable pre-training method and a proper representation of Data to leverage the principle of generative pre-training when applied to images.

This paper tries to leverage the idea of generative pretraining on the task of Image Generation on the MNIST Dataset. The novel idea developed in this paper is that it

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 131–141, 2023.
https://doi.org/10.1007/978-3-031-13150-9_11

tries to apply the Transfer Learning Principle across different domains (i.e. from text to Image). In this paper GPT-2 is used as the base model which is trained on textual data. This model is then fine-tuned on the image dataset. The key point to note here is that the base model was never trained on any kind of image data and had no prior training on any kind of 2-D data. Even then it was able to pick-up long-term dependencies across dimensions and produce results comparable to the state of art results in the domain and that too with minimal training on a fraction of Dataset. Another point to be noted here is that since we are not using any kind of encoding or convolution steps on the images this method requires substantially high compute as compared to other methods. This is the reason that only a fraction of the dataset was used to produce the results with minimal training. But this also highlights the point that the feature extraction step can be eliminated and compensated with enough computing power. This paper uses Fréchet Inception Distance (FID) [5] as a metric for quantifying the results of the experiment.

The primary objective of the project is to experiment the image modelling capabilities of the GPT-2 model and to check whether it can be used for image generation tasks. This paper provides a systematic study of all the steps used in the process. The paper introduces a novel image generation technique using GPT-2. The importance of this project lies in the fact that it demonstrates that GPT-2 can be used for image modelling and other image related tasks as well. Further this also opens up new possibilities of experimenting with the GPT-2 model in other domains.

2 Literature Review

Image generation is a fairly studied topic and with the recent popularity of Generative Adversarial Networks (GAN) [6] there have been quite a few remarkable results in this field. Owing to its generator discriminator architecture, GANs are good data generators and estimators. GANs have been fairly successful in generating realistic natural images [7, 8] and it has achieved remarkable results in fields of image enhancement [9], artistic style transfer [10] image-to-image translation [11] etc. But GANs suffer from training instability [12] and are often susceptible to non-convergence, mode collapse issues [13].

MNIST [14] is a dataset of handwritten 28×28 pixel images. Due to their relatively smaller dimensions these images are a good starting point for image generation with limited computing resources. There have been quite a few GAN variations that have shown remarkable results on image generation with MNIST such as Prescribed GAN [15], Hyperbolic GAN [16], DCGAN [17], PACGAN [18], VEEGAN [19].

GPT2 [20] is a large transformer based model with 1.5 billion parameters trained on 8 million web pages. GPT, GPT2 and now GPT3 are trained to predict the next word in a text sequence and are state of the art language models. These models have been extensively used in a wide variety of language generation tasks such as generating theatre play scripts [21, 22], text summarization tasks such as [23], dialog modelling tasks such as [24]. Recently there have been some attempts to test the performance of GPT on cross domain tasks such as image classification [25, 26].

Evaluation of generated images is an important aspect of the image generation problem. The Inception score (IS) [12] is a very popular method to quantify the quality of generated images. Most of the methods to quantify image generation results return a single score value representing the quality of images while some of the evaluation techniques such as GAM [27] and NRDS [28] perform relative comparison between models. This paper uses the Fréchet Inception Distance (FID) [5] score as it is more consistent with the human perception and is more robust to noise than IS.

3 Proposed Method

3.1 Dataset

The dataset used for the image generation in this paper is a collection of handwritten digit images popularly known as MNIST dataset. It is a collection of 60,000, 28 $\times$ 28 grayscale images of the 10 digits, along with a test set of 10,000 images. This dataset has been fairly studied for image generation tasks with various GAN variations and hence various image generation benchmarks are available for this dataset. Considering that our method is a computationally intensive method the lower dimensions of MNIST images and availability of benchmarks to compare makes it a suitable choice for this experiment.

3.2 Workflow

This paper follows a general workflow for generation tasks in GPT-2 in which the first step is loading the pre-trained model of GPT-2 which is then fine-tuned on the corpus in consideration. The step that's important for this experiment is the encoding of the dataset to the appropriate format before fine-tuning and decoding the generated output inorder to get the generated images. The flowchart in Fig. 1 describes all the steps involved in the process in a concise way.

3.3 Procedure

Step 1: Load the MNIST Dataset and encode the dataset using the procedure described above.
Step 2: Load the Pre-trained GPT Model and finetune it on the encode image dataset.
Step 3: Use the finetuned GPT model to generate new samples.
Step 4: Decode the Generated samples using the procedure described above and convert them to raw images.
Step 5: Generate the FID score using decoded generated images and real images.

3.4 Encoding/Decoding the Images

Since the GPT-2 is a text-based generative model, thus it can't take two-dimensional image input out of the box. Thus, it is essential to encode the image in a proper format that is compatible with the GPT model and at the same time preserve all the required characteristics of the images. GPT-2 expects the input to be a sequence of tokens where each token represents an individual word. To represent an image in a similar fashion each pixel (value between 0–255) was treated as an individual token. Also, delimiters

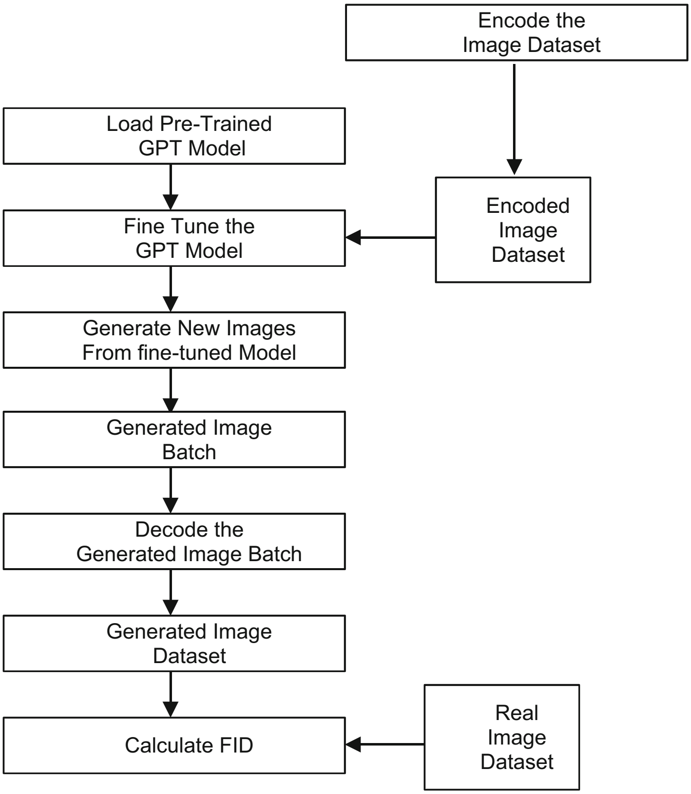


Fig. 1. Workflow of proposed system

were provided to mark the end of each row say, ‘|’. Also, <start > and <end> tokens were used to mark the start and end of a given sample.

Consider a 3 * 3 image,

Original image =

[[1, 2, 3],

[4, 5, 6],

[7, 8, 9]]

After using the above-described method the image becomes:

Encoded Image = “ <start> 1 2 3 | 4 5 6 | 7 8 9 | <end>”.

Thus ‘single space’ was used to separate individual pixels in same row, ‘|’ are used to separate rows, and <start> and <end> separates individual samples.

The decoding procedure is just the reverse procedure of Encoding. For a generated sample first the <start> and <end> token is stripped off, then the resulting string is split with delimiter ‘|’. Each section of resulting strings now represents individual rows of the image. Each row is further split with delimiter ‘ ‘, which gives individual pixel value.

Also, it was observed that sometimes the generated images have some inconsistencies in the dimensions, so to eradicate the noise extra pixels were stripped off the row and if there were insufficient pixels, they were padded with 0's.

Ex: generated image = " <start> 1 2 3 4 | 5 6 | 7 8 9 | <end>".

Decoded Image =

[[1, 2, 3],

[5, 6, 0],

[7, 8, 9]]

3.5 GPT

GPT stands for Generative Pre-Training, it is a high-performance model for generative language modelling tasks. Traditional methods mostly use a supervised approach towards target specific tasks like POS tagging, named entity recognition, classification etc. But such models can't be transferred to a new task. Moreover, such models tend to learn the correlation of input text to the target labels and not the basic organization of language. Also, there is significant scarcity of labeled data as compared to the unlabeled data. Thus, it is of utmost importance to develop methods that can draw significant conclusions from the unlabeled data in its raw form. This is why unsupervised models like word vectors and glove vectors came into picture. These models work in an unsupervised way to generate word level statistics from image corpora. GPT uses the Hybrid of these two approaches. It can be considered a semi-supervised learning model that works in two phases: the first step involves training a model on a large text corpus to capture the basic organization of text and the next step is supervised fine tuning on the target task to capture the finer details. GPT uses a transformer model with self-attention [29] mechanism at its core (Fig. 2).

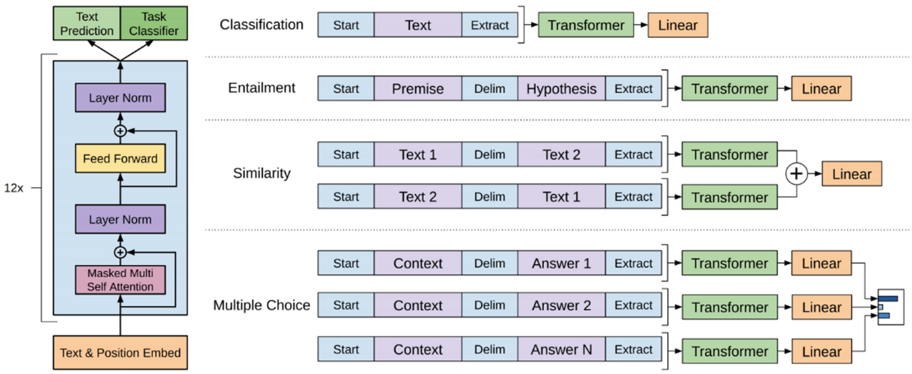


Fig. 2. The architecture of Model used in GPT-2 [29]

This model is capable of learning very long-term dependency in the text. The stages involved in training a GPT model are:

Unsupervised Pre-training

This step involves unsupervised training of the transformer model to capture the word level relations and statistics. The goal in this step is to maximize the following likelihood using standard modeling objectives.

$$L_1(U) = \sum \log P\left(u_i \mid u_{i-k} \ldots u_{i-1}; \theta\right) \quad (1)$$

where U is the corpora of tokenized text, U = {u_1, u_2, u_3…}

k describes the context window size

P is the conditional probability of u_i appearing in the context window

θ are the trainable parameters of neural network.

GPT uses a high-performance variant of transformer, multi-layered Transformer Decoder as the base model for language modeling tasks. It also uses a self-attention mechanism which is capable of emphasizing critical details of the text.

$$h_0 = UW_e + W_p \quad (2)$$

$$h_i = transformer\_block(h_{i-1}) \forall \text{ i} \in [1,\ \text{n}] \quad (3)$$

$$P(u) = softmax\left(h_n W_e^T\right) \quad (4)$$

W_e is the token embedding matrix

W_p is the position embedding matrix.

h_i is the output of transformer at layer l.

Supervised Fine Tuning

This step is used to capture the finer details of the text pertaining to a specific target task. In this step the model requires a labeled dataset and uses classic supervised learning to perform the target task. This step uses the trained model from the previous step as an initialization point, adds one more linear layer with parameters W_y and tries to predict the output label y:

$$P\left(y \mid x_1, \ldots x_m\right) = softmax\left(h_1^m W_y\right) \quad (5)$$

where P is the conditional probability of label y give the feature x_1, x_2, $x_{3,\ldots,}x_m$

h_l = output of final layer of transformer network.

W_y = parameters of final linear layer.

The following objective is maximized in this step:

$$L_2(C) = \sum \log P\left(y \mid x_1, \ldots x_m\right) \quad (6)$$

Combining Eq. 1 and Eq. 2, the final learning objective becomes:

$$L_3(C) = L_2(C) + \lambda * L_1(C) \quad (7)$$

λ is the weight associated with L1

3.6 Evaluation Metric: FID (Fréchet Inception Distance)

FID or Fréchet inception distance [5] is one of the most popular metrics to quantitatively analyze performance of GAN's or any generative model in general. FID takes into account the comparison of the distribution of both the real and generated images unlike the inception distance that evaluates only statistics of generated images. FID uses Inception V3 [30] to generate embeddings of the images, then a multivariate normal distribution is fitted on these embeddings, and finally the Fréchet distance is calculated for these multivariate normal distributions by using the formula:

$$FID = |\mu - \mu_w|^2 + tr\left(\sum + \sum_w - 2\left(\sum \sum_w\right)^{1/2}\right) \tag{8}$$

where μ and μ_w are the mean of real and fake image embeddings
$\sum$ and $\sum_w$ are the covariance matrices of real and fake image embeddings
T_r represents the trace of matrix

Limitations of FID
Since FID is based on the Inception V3 model, it might not be able to capture all details in every dataset. Also, this metric only takes mean and covariance into account and completely disregards other properties like skewness, which might not be ideal for every dataset. Another major limitation of FID is that it is dependent on the sample size used, larger sample size results in smaller FID for the same model. It is also comparatively more computationally intensive and hence slower in operation.

4 Results and Discussion

This section represents the results for the image generation using GPT-2 on MNIST. For this experiment gpt-2-simple library [30] was used for fine-tuning the gpt-2 model. The FID calculations were done using the pytorch-fid library [31].

4.1 Variation of FID Score with Training Data Size

Figure 3 shows the FID score vs training sample size variation. From the Fig. 3 it is clear that with just a fraction of total images GPT-2 is able to overperform most of the GAN networks in terms of FID score.

4.2 Comparison of FID scores

The results shown in Table 1 clearly demonstrates that the GPT-2 based model outperforms all the GAN results and is comparable to the benchmarks on this dataset. The FID scores show that the GPT-2 is capable of generating images and the model is capable of learning image representations. This result also shows the representational capabilities of transformers and reciprocate the findings of Image GPT [25] regarding image representation using GPT.

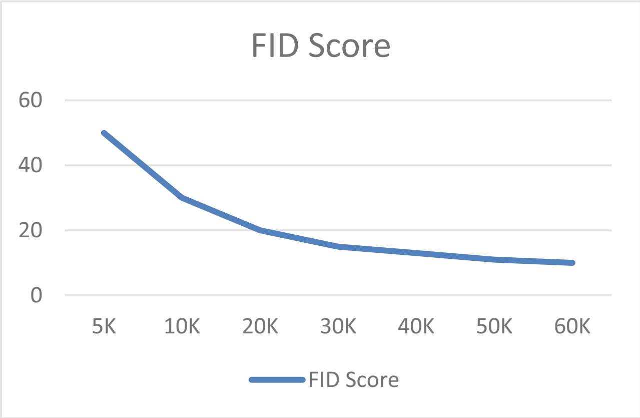


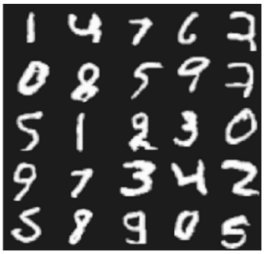
Fig. 3. FID score vs Training sample size

Table 1. Comparison of FID Scores for different methods.

Model	FID score
GAN models	
DCGAN [17]	113.12
VEEGAN [19]	68.74
PACGAN [18]	58.53
PresGAN [15]	42.02
HYPGAN [16]	12.88
Proposed GPT-2 based approach	10.63

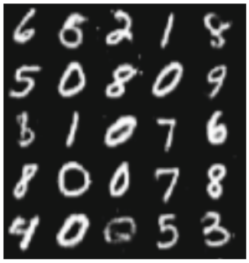
Figure 4 shows some of the generated images using GPT-2. Images of GAN, HGAN, CGAN, HCGAN, HWGAN are part of generated images represented in the HGAN [16].

The results demonstrate the capabilities of GPT-2 model to learn image representations. This shows that the model is capable of image modelling and understanding the image representations owing to its ability to preserve long-range dependencies and finding the correlation between the tokens owing to its attention mechanism.

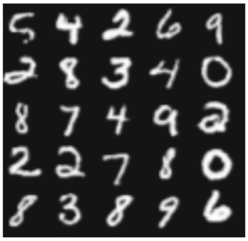


(a) This Paper

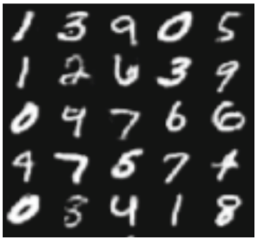
(b) GAN



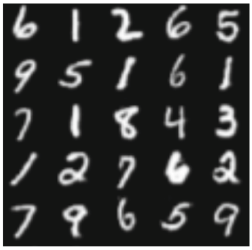
(c) HCGAN



(d) CGAN



(e) HCGAN



(f) HWGAN

Fig. 4. Sample digits produced using different methods

5 Conclusion and Future Work

This paper introduces a novel method of generating images. Images generated with this model are comparable to the popular GAN models using the GPT-2 model. This demonstrates the capabilities of GPT-2 model to learn image representations. This excellent image representation capabilities can be attributed to the ability of GPT-2 model to preserve long-range dependencies. The results achieved by the proposed model is better than GAN models for image generation of MNIST data and we believe that GPT models have great image modelling capabilities, and it could be used in a wide variety of image tasks as well. The results also highlight the exceptional learning capabilities of the GPT-2 model.

Instead of using the simple encoder and decoder described in the paper some better performing encoders and decoders can be used with GPT-2 to generate images. From this paper it was evident that GPT-2 can learn image representations, thus its application can be extended to other image tasks as well. Not only this, but similar procedure can also be used for data generation in other domains as well such as audio and video.

References

1. Mikolov, T., Chen, K., Corrado, G., Dean, J.: Efficient estimation of word representations in vector space (2013)

2. Pennington, J., Socher, R., Manning, C.D.: Glove: Global Vectors for Word Representation, pp. 1532–1543 (2014). https://doi.org/10.3115/V1/D14-1162
3. Devlin, J., Chang, M.W., Lee, K., Toutanova, K.: BERT: Pre-training of deep bidirectional transformers for language understanding (2019)
4. Paine, T.L., Khorrami, P., Han, W., Huang, T.S.: An analysis of unsupervised pre-training in light of recent advances (2015)
5. Heusel, M., Ramsauer, H., Unterthiner, T., Nessler, B., Hochreiter, S.: GANs trained by a two time-scale update rule converge to a local Nash equilibrium. In: Advances in Neural Information Processing Systems, pp. 6629–6640 (2017)
6. Goodfellow, I., et al.: Generative adversarial nets (NIPS version). In: Advance Neural Information Processing System 27 (2014)
7. Brock, A., Donahuey, J., Simonyany, K.: Large scale GAN training for high fidelity natural image synthesis, arXiv (2018)
8. Gong, X., Chang, S., Jiang, Y., Wang, Z.: AutoGAN: neural architecture search for generative adversarial networks (2019). https://doi.org/10.1109/ICCV.2019.00332
9. Rakotonirina, N.C., Rasoanaivo, A.: ESRGAN+ : further improving enhanced super-resolution generative adversarial network (2020). https://doi.org/10.1109/ICASSP40776.2020.9054071
10. Yang, S., Wang, Z., Liu, J.: Shape-matching GAN++: scale controllable dynamic artistic text style transfer. IEEE Trans. Pattern Anal. Mach. Intell. (2021). https://doi.org/10.1109/TPAMI.2021.3055211
11. Li, Y., Tang, S., Zhang, R., Zhang, Y., Li, J., Yan, S.: Asymmetric GAN for unpaired image-to-image translation, arXiv (2019)
12. Salimans, T., Goodfellow, I., Zaremba, W., Cheung, V., Radford, A., Chen, X.: Improved techniques for training GANs. In: Advances in Neural Information Processing Systems, pp. 2234–2242 (2016)
13. Bau, D., et al.: Seeing what a GAN cannot generate (2019). https://doi.org/10.1109/ICCV.2019.00460
14. LeCun, Y., Bottou, L., Bengio, Y., Haffner, P.: Gradient-based learning applied to document recognition. Proc. IEEE **86**(11), 2278–2324 (1998). https://doi.org/10.1109/5.726791
15. Dieng, A.B., Ruiz, F.J.R., Blei, D.M., Titsias, M.K.: Prescribed generative adversarial networks, arXiv (2019)
16. Lazcano, D., Fredes, N., Creixell, W.: Hyperbolic Generative Adversarial Network, arXiv (2021)
17. Radford, A., Metz, L., Chintala, S.: Unsupervised representation learning with deep convolutional generative adversarial networks. In: 4th International Conference Learning Represent. ICLR 2016 - Conference Track Proceeding, pp. 1–16 (2016)
18. Lin, Z., Fanti, G., Khetan, A., Oh, S.: PacGan: the power of two samples in generative adversarial networks. In: Advances in Neural Information Processing Systems, vol. 2018-Decem, pp. 1498–1507 (2018). https://doi.org/10.1109/jsait.2020.2983071
19. Srivastava, A., Valkov, L., Russell, C., Gutmann, M.U., Sutton, C.: VEEGAN: Reducing mode collapse in GANs using implicit variational learning. In: Advances in Neural Information Processing Systems, vol. 2017-Decem, pp. 3309–3319 (2017)
20. Radfort, A., Narasimhan, K., Salimans, T., Sutskever, I.: Improving language understanding by generative pre-training. In: OpenAI (2018)
21. Rosa, R., et al.: THEaiTRE: Artificial Intelligence to Write a Theatre Play, arXiv (2020)
22. Liao, Y., Wang, Y., Liu, Q., Jiang, X.: GPT-based generation for classical Chinese poetry, arXiv (2019)
23. Tan, B., Kieuvongngam, V., Niu, Y.: Automatic text summarization of COVID-19 medical research articles using BERT and GPT-2, arXiv (2020)

24. Yang, Y., Li, Y., Quan, X.: UBAR: towards fully end-to-end task-oriented dialog systems with GPT-2, arXiv (2020)
25. Chen, M., et al.: Image GPT. In: Icml (2020)
26. Tsai, T.J., Ji, K.: Composer style classification of piano sheet music images using language model pretraining, arXiv (2020)
27. Im, D.J., Kim, C.D., Jiang, H., Memisevic, R.: Generating images with recurrent adversarial networks, arXiv (2016)
28. Zhang, Z., Song, Y., Qi, H.: Decoupled learning for conditional adversarial networks (2018). https://doi.org/10.1109/WACV.2018.00082
29. Vaswani, A., et al.: Attention is all you need, arXiv (2017)
30. GitHub - minimaxir/gpt-2-simple: Python package to easily retrain OpenAI's GPT-2 text-generating model on new texts
31. Seitzer, M.: pytorch-fid: FID Score for PyTorch (2020)

LightMobileNetV2: A Lightweight Model for the Classification of COVID-19 Using Chest X-Ray Images

Shankey Garg(✉) and Pradeep Singh

Department of Computer Science and Engineering, National Institute of Technology, Raipur, Chhattisgarh, India
sgarg.phd2019.cse@nitrr.ac.in

Abstract. Deep Learning is most widely used in the area of medical imaging. Due to its success, many works of literature use deep learning methodsto classify COVID-19 related cases. Currently, the world is facing the second and third waves of this deadly disease. Therefore, the need of the hour is to develop some user-friendly lightweight model that could easily detect the disease with little effort. It is found that early diagnosis is the only way to defeat this deadly virus. This paper tried to classify the chest X-ray(CXR) images into different categories, such as normal lung opacity, viral pneumonia, and COVID-19 positive using a transfer learning mechanism. For this classification task, we have removed eight blocks of the pre-trained MobileNetV2model, and then it is fed to the classifier consisting of a dropout and linear layers. The proposed model is approximately 9times lighter than the original MobileNetV2 and performing almost with the same accuracy. Experimental evaluation proves that the proposed model gives satisfactory results compared with the original and other recent works.

Keywords: Deep learning · Transfer learning · COVID-19 · Lightweight models

1 Introduction

An unidentified virus officially named Coronavirus Disease-2019 (COVID-19) by World Health Organization (WHO) was first diagnosed in late December 2019 from Wuhan, China, and outbreaks in many cities of China, further expanded globally, including our country. It is a positive single-strand RNA virus belonging to the Orthocoronavirinae subfamily having crown-like spikes on its surfaces. COVID-19 is a severe infection that occurs in the respiratory tract for which various differential diagnoses related to common viral pneumonia could be considered [1]. Our country is currently facing the second wave of this global pandemic. Approximately twenty-one million active cases and more than two and a half million deaths have been recorded worldwide in March 2021. COVID-19 diagnosis is made by performing Reverse Transcription Polymerase Chain Reaction (RT-PCR), which usually shows low accuracy, delay, and sensitivity.Nevertheless, it is seen that early diagnosis may increase the chance of correct treatment of infected patients, thereby reducing the community spread [2]. Various machine learning-based prediction

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 142–150, 2023.
https://doi.org/10.1007/978-3-031-13150-9_13

models were used for predicting the rate of infections and the chances of the second and third waves across the world. Due to the high transmissibility of COVID-19, the smash on the health care system is also high; thereby, the number of patients requiring ICU and mechanical ventilators for longhours increases. In this situation, early detection is critical for the correct line of treatment so that the pressure in the health care unit may get reduced. In this regard, automated systems can supply a cost-effective&efficient diagnosis for COVID-19. The primary diagnostic test for COVID-19 is CXR& computed tomography (CT) [3, 4]. In this paper,we will identify various kinds of infections using CXRs only. Also, due to the recent pandemic the world faces, the main aim is to classify the COVID-19 condition, among other types of infection and normal lungs.The main contribution involves developing a lightweight model to classify the diseases effectively and compared the proposed model with the base model and other recent literature. Due to the limited availability of the x-rays samples, a transfer learning paradigm is followed in this work.

1.1 Background

Researchers are always inclined towards machine learning and deep learning-based algorithms for solving complex computer vision-based classification tasks. As it is seen that the COVID-19 has become a threat to the world, it is high time to find some practical solution to mitigate this deadly disease. A lot of research is already being conducted in this field using the chest X-rays samples of the patients. Authors of Paper [5] have applieddifferent transfer learning-based approaches for classifying COVID-19 using CXRsand found that ResNet-50 outperforms the other pre-trained models.Furthermore, a robust model following generative adversarial network for synthetic data generation and proposing lightweight architectures is given by [6] and found that the model is more powerful& reliable in classifying COVID-19 than the baseline ResNet8. Finally, the deep learning-based COVID-19 detection method is developed by [7] using ResNeXt, Inception V3, and Xception. A novel deep learning-based COVID detection model named CoroDet for automated detection of COVID using CXR and CT scans presented in the paper [8]. A novel classification and segmentation study by enhancing images concerning different parameters is proposed in [2] along with the largest publicly available CXRdataset for COVID-19 detection.COVID-Net, an open-source model for detecting COVID-19 using CXR images, is presented in paper [4],and authors have made it open to the public. Internet of things (IoT) enabled depthwise separable convolution neural network (DWS-CNN) with support vector machine (SVM)is developed for detecting and classifying COVID-19 [9]. This model satisfactorily organizes both the binary and multiple classes of COVID-19.

2 Methodology

Here, we will discuss the proposed transfer learning-based architecture for classifying COVID-19. The objective of developing the proposed model is to classify COVID-19 from Chest X-rays. However, training the model from scratch will not be efficient due to the shortage of data and may cause a bias vs. variance trade-off. So, to overcome this issue, we have opted transfer learning paradigm [10]. A lightweight pre-trained MobileNetV2 is modified to act as a base model for the classification task. Using a lightweight model is to have a reduced number of parameters and small model size, thereby reducing the overall execution time of the model and allowing them to be installed in the embedded devices [11]. These experiments have been implemented using the pytorch [12] deep learning library on the Google Colab platform with the following configurations: NVIDIA-SMI 495.44, CUDA Version 11.2, Tesla K80, and 12.69 GB RAM.

2.1 Deep Learning Model: MobileNetV2

MobileNetV2 architecture is developed to run on mobile devices that have less computational power [13]. The model was given by Google and used depth-wise separable convolutions to decrease the number of parameters in the model. Depth-wise separable convolution splits the kernel into two smaller ones as depth-wise convolution and pointwise convolutions to significantly reduce computational costs [14, 15].

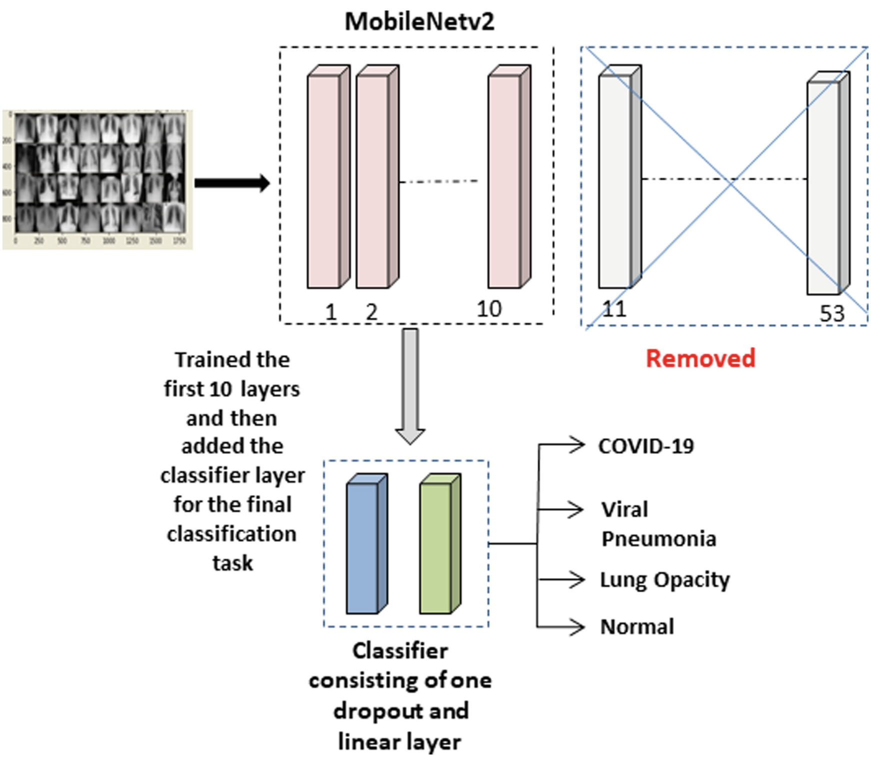


Fig. 1. Proposed LightMobileNetV2 model for COVID-19 classification

2.2 Dataset Used

The proposed model usesa CXRdataset taken from the publicly available repository and given by [2]. As shown in Table1, the dataset used.

The four classes have 3616 COVID-19 positive cases, 10,192 Normal, 6012 lung opacity, and 1345 viral pneumonia images. This dataset is prepared by researchers from Qatar University and the University of Dhaka with collaborators from Pakistan and Malaysia. Inhis dataset, the images are of PNG format with a size 256X256. Some samples of CXR are depicted in Fig. 2.

Table 1. Dataset distribution

Class	Count
COVID-19 positive	3,616
Lung opacity	6,012
Viral pneumonia	1,345
Normal	10,192
Total	21,165

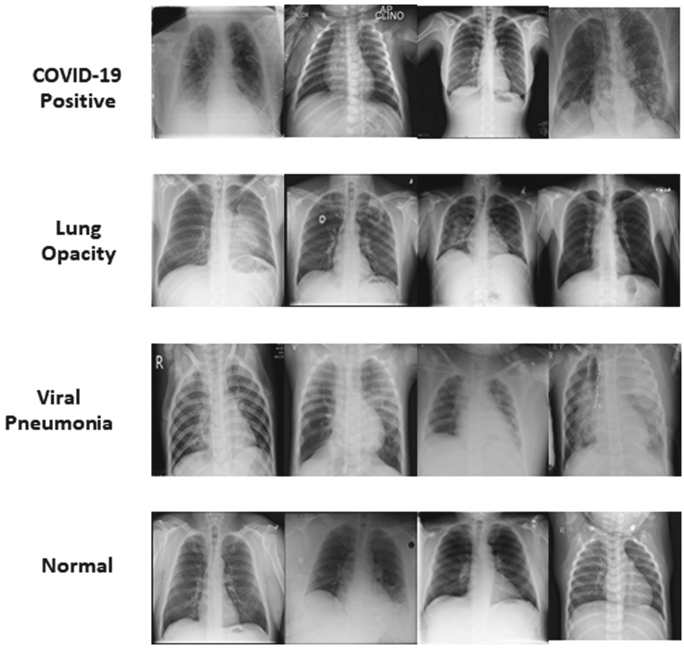


Fig. 2. Sample images from the dataset used for this study

2.3 Proposed Model

Base model selection is an essential task while performing any classification task. While selecting the base model, many parameters need to be considered, such as the model size, complexity, execution time, and detection speed. MobileNetV2 consisting of 18 blocks pre-trained on the ImageNet dataset, is regarded as the base model for this experiment. Instead of fine-tuning each layer of the base model, the proposed work removed 8 layers of the base model. It used the first ten layers for training, reducing the model's size by approximately 9times the base model. A dropout layer with a value of 0.2 and the linear layer is used for the final classification task. Figure 1 shows the schematic view of the proposed LightMobileNetV2 model. The idea behind eliminating some final layers is that the initial layers could effectively extract the valuable knowledge containing low-level features that are helpful in the training process, thereby giving better test results.

2.4 Experimental Settings

The dataset is pre-processed to resize the X-ray images into the pixel value 112*112. Also, we have normalized the data so that our LightMobileNetV2 model could learn faster and better. For this we have used default normalization of ImageNet models having value [0.485, 0.456, 0.406] and a standard deviation of [0.229, 0.224, 0.225]. For the proposed classification task, 70% (14815) of the Chest X-ray images were used for training, and 30% (6350) of the images were used for testing. The training uses a batch size of 32 images, a learning rate of 0.001 for 15 epochs using an Adams optimizer. We have taken cross-entropy loss for calculating the training & validation loss of our model. The accuracy of 15 epochs is calculated at the end of the execution phase.

Table 2. Comparing performance with the recent literature that uses the same dataset

Model	Overall accuracy	Weighted precision	Weighted recall	Weighted F1-measure
ResNet18 [2]	93.43	93.43	93.43	93.42
ResNet50 [2]	93.01	93.12	93.02	93.04
ResNet101 [2]	93.01	93.04	93.01	93.00
ChexNet [2]	93.21	93.28	93.21	93.20
DenseNet201 [2]	92.70	92.78	92.7	92.72
Inception V3 [2]	93.46	93.49	93.47	93.47
Proposed	**95.67**	**95.66**	**95.34**	**95.89**

3 Results

This section describes the efficiency of the proposed model for classifying COVID-19 patients. Table2 shows the comparative evaluation of the given model with the other state-of-the-art models using the same dataset. From the Table2, it can be observed that the proposed model is performing better than different variants of ResNet(18,50,101), DenseNet201, InceptionV3, and ChexNet.We can easily compare the proposed work in terms of accuracy, f1 measure, precision, and recall from the table. Still, the compared paper has not mentioned the size of the model, the number of parameters, and execution time. Although the base model of the compared work is complex, it requires significant memory and a higher execution time(each having more than 11M parameters). Figure 3 represents the heatmapfor the proposed work, and Fig. 4 depicts the testing accuracy graph of the proposed LightMobileNetV2 model. It is found that out of 1067 tested samples, 1053 samples are correctly classified as COVID-19 positive; for the lung opacity, 1808 samples were tested. Our models correctly classify 1690 samples. Our model correctly classifies 390 samples of viral pneumonia out of 392 samples, and 2942 samples belonging to the normal class are correctly classified out of the 3083 testing samples.We can observe that our model works well with this high imbalance dataset without any balancing technique from the analysis. As the data is an imbalance, we also check for the f1 score of the model along with the accuracy. From Table2 it is clear that the weighted f1 score of this multiclass problem is higher than the compared work.

Further, it is also noted that the proposed model is lightweight. It has a significantly fewer sample than other recent models, and it is known that the lightweight model takes less time for execution. Our model takes 2 h 19 min and 9 s, for the completion of these classification tasks. Table3 depicted below gives the general information of the various parameter comparison of the proposed model with the base model.The table shows that the proposed model has around 9times less number of parameters, ten times smaller concerning the model size, and execution time is also less than the base model. While the performance is approximately the same as that of the base model, that means we got a lighter model without any performance loss.

Table 3. Comparison of the proposed model with the base model

Model	No. of parameters	Model size	Execution time	Accuracy
MobileNetV2 (Base)	2.2 M	8.916 MB	2h 24min 55 s	95.91
LightMobileNetV2 (Proposed)	203 K	0.812 MB	2 hr19 min9 s	95.67

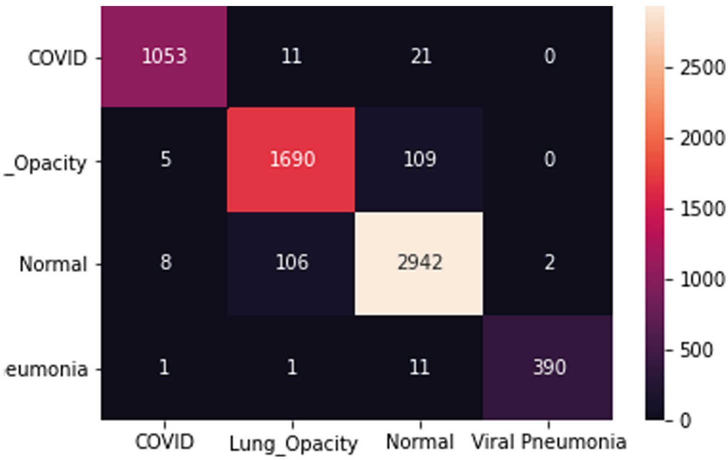


Fig. 3. Heatmap of the obtained results

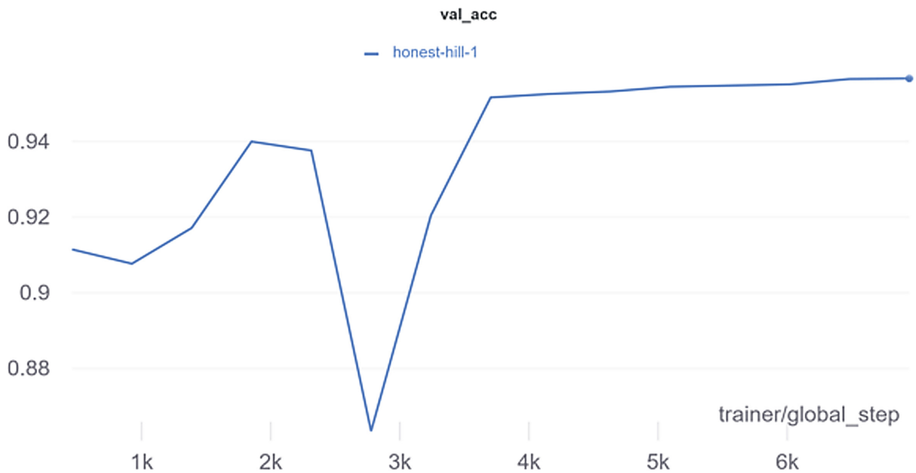


Fig. 4. Testing accuracy of the proposed LightMobileNetV2 model

4 Conclusion

COVID-19 has adversely affected the day-to-day lives of human beings. Arguably, the research community is putting a lot of effort in this direction. This work is a user-friendly and straightforward approach for the diagnosis of COVID-19 using a CXR. The proposed model could detectCOVID-19 using a simple, lightweight model achieving high performance and accuracy. This work haseliminated 8 blocks of thepre-trained MobileNetV2 and uses the CXR dataset to classify the images into four categories. As a result, the model gives a satisfactory performance with an accuracy of 95.67%.As this is a multiclass classification task, we could not rely on the accuracy alone to analyze the proposed model's performance. Hence, other parameters like weighted precision, recall, and f1 measure were also considered here, and it is found that the proposed model is also performing better in these metrics. In future work we will apply some data balancing techniques to improve the performance before giving input to the train the model.

References

1. Wu, Y.C., Chen, C.S., Chan, Y.J.: The outbreak of COVID-19: an overview. J. Chin. Med. Assoc. **83**, 217–220 (2020). https://doi.org/10.1097/JCMA.0000000000000270
2. Rahman, T., et al.: Exploring the effect of image enhancement techniques on COVID-19 detection using chest X-rays images. arXiv. 132, 104319 (2020). https://doi.org/10.1016/j.compbiomed.2021.104319
3. Pereira, R.M., Bertolini, D., Teixeira, L.O., Silla, C.N., Costa, Y.M.G.: COVID-19 identification in chest X-ray images on flat and hierarchical classification scenarios. Comput. Methods Programs Biomed. **194**, 105532 (2020). https://doi.org/10.1016/j.cmpb.2020.105532
4. Wang, L., Lin, Z.Q., Wong, A.: COVID-Net: a tailored deep convolutional neural network design for detection of COVID-19 cases from chest X-ray images. Sci. Rep. **10**, 1–12 (2020). https://doi.org/10.1038/s41598-020-76550-z
5. Ismael, A.M., Şengür, A.: Deep learning approaches for COVID-19 detection based on chest X-ray images. Expert Syst. Appl. **164**, 114054 (2021). https://doi.org/10.1016/j.eswa.2020.114054
6. Karakanis, S., Leontidis, G.: Lightweight deep learning models for detecting COVID-19 from chest X-ray images. Comput. Biol. Med. **130**, 104181 (2021). https://doi.org/10.1016/j.compbiomed.2020.104181
7. Hasan Jahid, M., Alom Shahin, M., Ali Shikhar, M.: Deep learning based detection and segmentation of COVID-19 Pneumonia on chest X-ray image. In: 2021 International Conference Information Communication Technology Sustainable Development ICICT4SD 2021 – Proceedings, pp. 210–214 (2021). https://doi.org/10.1109/ICICT4SD50815.2021.9396878
8. Hussain, E., Hasan, M., Rahman, M.A., Lee, I., Tamanna, T., Parvez, M.Z.: CoroDet: a deep learning based classification for COVID-19 detection using chest X-ray images. Chaos, Solitons Fractals **142**, 110495 (2021). https://doi.org/10.1016/j.chaos.2020.110495
9. Le, D.-N., Parvathy, V.S., Gupta, D., Khanna, A., Rodrigues, J.J.P.C., Shankar, K.: IoT enabled depthwise separable convolution neural network with deep support vector machine for COVID-19 diagnosis and classification. Int. J. Mach. Learn. Cybern. **12**(11), 3235–3248 (2021). https://doi.org/10.1007/s13042-020-01248-7
10. Sufian, A., Ghosh, A., Sadiq, A.S., Smarandache, F.: A Survey on Deep Transfer Learning and Edge Computing for Mitigating the COVID-19 Pandemic. J. Syst. Archit. **108**, 101830 (2020). https://doi.org/10.1016/j.sysarc.2020.101830
11. Zhou, Y., Chen, S., Wang, Y., Huan, W.: Review of research on lightweight convolutional neural networks. In: Proceedings 2020 IEEE 5th Information Technology Mechatronics Engineering Conference ITOEC 2020, pp. 1713–1720 (2020). https://doi.org/10.1109/ITOEC49072.2020.9141847
12. Paszke, A., et al.: Automatic differentiation in PyTorch. paszke2017automatic **5**, 1–4 (2017). https://doi.org/10.1145/3434309
13. Deng, B.L., Li, G., Han, S., Shi, L., Xie, Y.: Model compression and hardware acceleration for neural networks: a comprehensive survey. Proc. IEEE. **108**, 485–532 (2020). https://doi.org/10.1109/JPROC.2020.2976475

14. Sandler, M., Howard, A., Zhu, M., Zhmoginov, A., Chen, L.C.: MobileNetV2: inverted residuals and linear bottlenecks. In: Proceedings IEEE Computer Society Conference Computer Vision Pattern Recognition, pp. 4510–4520 (2018). https://doi.org/10.1109/CVPR.2018.00474
15. Howard, A.G., et al.: MobileNets: efficient convolutional neural networks for mobile vision applications. arXiv (2017)

Intention to Adopt E-Grocery Shopping Service in Vietnam During Covid-19 Pandemic

Cuong Quoc Nguyen[1(✉)], Hang Thuy Truong[1], and Anh Minh Tu Nguyen[2(✉)]

[1] Faculty of Business Administration, Industrial University of Ho Chi Minh City, Ho Chi Minh City, Vietnam
nguyenquoccuong@iuh.edu.vn

[2] Office of Science Management and International Affairs, Industrial University of Ho Chi Minh City, Ho Chi Minh City, Vietnam
nguyenminhtuanh@iuh.edu.vn

Abstract. The purpose of this study is to determine the factors that influence the intention to adopt e-grocery shopping service of Vietnamese consumers during Covid-19 Pandemic. The sample size includes 235 responses collected from e-grocery shoppers in Vietnam. The research methodology includes Cronbach's Alpha analysis, EFA analysis and multiple regression analysis. Data is analysed in SPSS 20 software. The results have identified four factors that directly affect the intention to adopt e-grocery shopping service which are social influence, perceived ease of use, brand image and perceived usefulness. Social influence is the most significant factor that impacting the intention to adopt e-grocery shopping service among consumers during Covid-19 Pandemic in Vietnam.

Keywords: Intention to adopt · E-grocery shopping · Social Influence · Covid-19 pademic

1 Introduction

The rapid development of the Internet has greatly influenced consumer behavior. Mondern consumers demand their daily problems solved more quickly and easier. It is the increasing demand for convenience that simplify life by digital solutions. Goga et al. (2019) point out that online platforms and electronic commerce (e-commerce) have transformed retail experience and expanded the opportunities for businesses to reach a wider range of customers. E-grocery shopping is an innovative service in Vietnam but is has not been popular among consumers. However, the emergence of the COVID-19 pandemic has prompted consumers to make rapid changes. Especially, consumers start using purchasing service on demand and home delivery services. According to the Department of E-commerce and Digital Economy (2021), Vietnamese e-commerce will experience impressive growth in 2020, with an increase of 18%, a market size of 11.8 billion USD, estimated to account for 5.5% of total sales goods and sesrvices used nationwide. According to the Vietnam E-commerce White Paper (2020), 42% of the population participates in online shopping, the growth rate reaches 25%. The average

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 151–162, 2023.
https://doi.org/10.1007/978-3-031-13150-9_14

number of customers accessing e-commerce stores is 3.5 million per day, an increase of more than 150% over the previous period. Covid-19 Pandemic creates many businesses that have never sold online are now selling online, many people who have never shopped online are now buying online. Vietnamese consumers are struggling to adjust to life during the Covid-19 pandemic because of government regulations on epidemic prevention and social distancing. Therefore, the demand for e-grocery shopping has been booming during Covid-19 pandemic. The main objective of this research is to identify the factors that influence the intention to adopt e-grocery shopping among Vietnamese consumers during Covid-19 pandemic.

2 Development

2.1 E-Grocery Shopping as Electronic Service

Rust and Kannan (2002) argue that e-services can be understood as the provision of services over electronic networks such as the Internet. Zeithaml and Bitner (2003) state that electronic service is a set of activities that take place under mutual influence between a supplier and a customer through an electronic channel. Järvinen and Lehtinen (2004) defined an electronic service as an object that provides the benefits of a transaction that can be described as an intangible process by which at least part of it is produced, marketed and consumed in a simultaneous interaction through electronic networks. Rowley (2006) defines e-service as an attempt to deliver goods through the intermediation of information technology (including the Internet, public kiosks, and mobile devices). The Internet is the main intermediation channel for e-services, while other traditional channels (such as telephones, public kiosks, television) are also considered. Jeong (2007) confirm that electronic services are online services available on the Internet where a valid purchase and sale can be made online, as opposed to traditional websites where only a description is available and no online transactions are possible. Online purchasing on request and home delivery service are done online through a website or mobile application. The shopping staff of the company providing the service selects products from stores and supermarkets based on customer's orders. The goods are delivered directly to the customer's location by delivery staff. These companies are not online retailers, but only offer an e-grocery shopping service. Handayani et al. (2020) suggest that consumers have the intention to switch from offline to online shopping because of perceived channel risk, perceived price-search intentions, mobility, and perceived difference in delivery time.

2.2 Theory of Planned Behavior and the Technology Acceptance Model

The Theory of Planned Behavior (TPB) was developed by Ajzen (1991) based on the Theory of Reasoned Action (TRA) by Fishbein and Ajzen (1975) by adding the element of perceived behavioral control in TRA. According to TPB, consumers' behavioral intentions are influenced by attitudes, subjective norms and perceived behavioral control. Intention is a factor used to evaluate the probability of performing a behavior in the future. According to Ajzen (1991), intention is a motivating factor that leads a person to perform a behavior and it is directly influenced by attitude, subjective norm and perceived behavioral control. Attitude is the evaluation of the results that a person obtains by performing a behavior. Subjective norms can be described as an individual's perception of social pressure to perform or not perform a behavior. Perceived behavioral control reflects the ease or difficulty of performing a behavior, which depends on the availability of resources and opportunities to perform the behavior (Ajzen 1991). The Technology Acceptance Model (TAM) was proposed by Davis (1989) based on the Theory of Reasoned Action (TRA) by Fishbien and Ajzen (1975) and the Theory of Planned Behavior (TPB). TAM has shown the influence of two main factors, perceived ease of use and perceived usefulness, on consumers' attitudes towards technology use, which lead to behavioral intentions and eventually to actual technology use. According to Davis (1989), perceived usefulness is the extent to which a person believes that using the system will improve his or her job performance. Perceived ease of use describes the extent to which an individual believes that using the system will be effortless and effortless. The model assumes that the two factors of perceived usefulness and perceived ease of use are fundamental to users' acceptance of the system (Chuttur 2009).

Venkatesh et al. (2003) proposed the Unified Theory of Acceptance and Use of Technology (UTAUT) as a unified model from previous theories of technology acceptance. The UTAUT showed that performance expectations, effort expectations, and social influence are factors that influence behavioral intention to use technology, while behavioral intention and convenience determine the use of technology use. Key concepts in the model include: Performance Expectancy is the extent to which an individual believes that using technology will bring efficiency to his or her operations; Effort Expectancy is the ease with which technology is used by consumers; Social Influence is the extent to which consumers perceive that they should use technology; Facilitating Conditions is a consumer's perception of the resources and support available to perform a behavior; behavioral intention is the user's intention to use technology in the future (Venkatesh et al. 2012). Bauer (1967) argues that information technology product consumption behavior is associated with perceived risk, which includes two factors: perceived risk associated with the product or service and perceived risk associated with online transactions. Perceived risk associated with a product or service represents the customer's concern about loss of functionality, financial loss, loss of time, and loss of opportunity when using information technology products or services. Perceived risks associated with online transactions include risks that may occur when consumers conduct transactions electronically, such as confidentiality, security, and overall transaction risk. Shukla and Sharma (2018) concluded that consumers are well adapted to use of mobile apps for general shopping but influence of mobile app as a tool was found limited in grocery sector in consistence to previous studies.

2.3 Hypotheses Developement

Perceived Risk and Intention to Use E-Grocery Shopping Service

In Vietnam, one of the reasons that discourages consumers from using electronic services is concern about the potential risks of buying, selling, or conducting transactions through electronic channels. Common risks include product quality is not guaranteed, payment methods are not secure, personal information is exposed, delivery is not guaranteed.

Chen et al. (2010) state that the risk of losing money or not receiving the goods negatively affects the intention to store online. According to Nguyen (2019), perceived risk negatively affects consumers' intention to adopt e-grocery shopping services. Concern about product quality, actual quality not meeting expectations. All these limit consumers' intention to buy online. Kian et al. (2018) confirm that perceived risk influences consumer purchase intention on online grocery shopping. Van Droogenbroeck and Van Hove (2021) confirm that perceived risk negatively impact the intention to adopt or continue to use e-grocery services. Hence, the first hypothesis is stated as follow:

H1: Perceived Risk negatively impact the intention to use E-grocery shopping services.

Perceived Ease of Use and Intention to Use E-Grocery Shopping Service
Davis (1989) used the Technology Acceptance Modeladoption to show the influence of the two factors perceived usefulness and perceived ease of use on consumers' attitude towards using technology. According to Nguyen et al. (2019), online shopping intention in Vietnam is strongly influenced by perceived consumer usefulness. Wang et al. (2018) also confirmed that perceived usefulness is the most important factor influencing consumer intention to purchase online. Nguyen (2019) said that perceived ease of use has a positive influence on online purchase intention, namely ease of use, simple and fast interface in information search, payment and it positively influence customers' purchase intention. Many studies show that perceived usefulness has a positive influence on consumers' online purchase intention (Kian et al. 2018; Elango et al. 2018; Do et al. 2019). Therefore, the second hypothesis is stated as follow:

H2: Perceived Ease of Use positively impact the intention to use E-grocery shopping services.

Perceived Usefulness and Intention to Use E-Grocery Shopping Service
Elango et al. (2018) confirm that Perceived Usefulness has positive influence of the intention to use on-demand food delivery applications. Kian et al. (2018) suggest that perceived usefulness positively influences consumer purchase intention on online grocery shopping. Van Droogenbroeck and Van Hove (2021) support that perceived in-store shopping enjoyment is significant to explain the intention to adopt or continue to use e-grocery services. However, Hooi et al. (2021) confirm that perceived usefulness were found insignificant to predict the intention to use online food delivery. Hence, the third hypothesis is stated as follow:

H3: Perceived Usefulness positively impact the intention to use E-grocery shopping services.

Social Influence and Intention to Use E-Grocery Shopping Service
According to Ajzen (1991), behavioral intentions are directly influenced by attitudes, subjective norms, and perceived behavioral control. Subjective norm can be understood

as an individual's perception of societal pressure to perform or not perform a behavior. The UTAUT model (Venkatesh et al. 2003) also shows the impact of social influence on consumers' intention to adopt technology. E-grocery shopping appeared in a short time, so it is still a new type of service for many consumers. Before deciding to buy a product or use a service, especially when they are new products and services or when they are bought and used for the first time, consumers often consult reference groups such as family, friends, colleagues, the community. Kian et al. (2018) confirm that social influence is identified as the most important factor which influences consumer purchase intention on online grocery shopping. Van Droogenbroeck and Van Hove (2020) insist that social influence is the trigger in the decision to use online grocery services for the first time. Gatta et al. (2020) confirm that peer influence positively impact on the purchasing habit of e-grocery consumers. Hence, the fourth hypothesis is described as follow:

H4: Social Influence positively impact the intention to use E-grocery shopping services.

Brand Image and Intention to Use E-Grocery Shopping Service

Huang et al. (2004) found that brand name or brand image is essential for online purchase decisions and lack of it can lead to mental risk. Degeratu et al. (2000) suggest that brand image is essential for certain types of products for customers to purchase online. Aghekyan-Simonian et al. (2012) argue that since there is no actual product testing prior to online purchase, the two most important factors that reduce customers' perceived risk are: (1) the brand image of the product and (2) the image of the online store. Lee (2012) concluded that consumers will always reach for brands with a better image than brands with a lower brand image. A successful brand image increases the likelihood of a consumer's purchase intention towards a brand and helps consumers to fulfill their needs and satisfaction (Hsieh et al. 2004). Fornari et al. (2018) report that brand image should be considered in e-grocery to reach proportionate sales levels. Besides, Ali and Naushad (2021) report that brand image is positively associated with online grocery shopping. Therefore, the proposed research hypothesis is as follows:

H5: Brand Image positively impact the intention to use E-grocery shopping services.

The proposed research model are illustrated in Fig. 1.

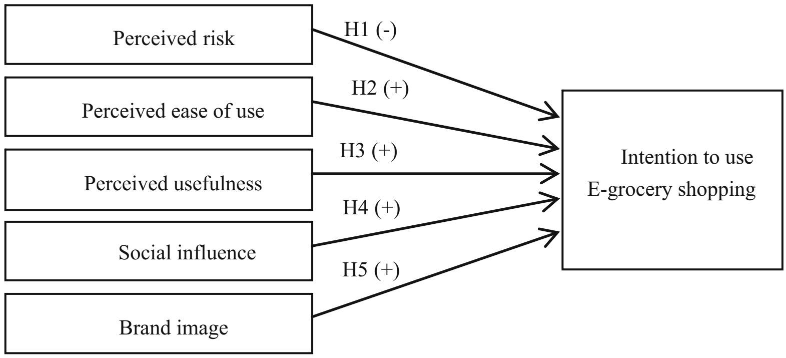


Fig. 1. The proposed research model

3 Research Method

The research was conducted in two steps: qualitative research and quantitative research. Qualitative research is conducted through two methods: Expert interview and group discussion. The participants in the group discussion are people aged 18 years or older and have experience of E-grocery shopping services. Qualitative research aims to determine the scale that will be used as the basis for creating a questionnaire in the quantitative research phase. In quantitative research, questionnaire survey method is used. Data collection was done through face-to-face interview (paper questionnaire) and online survey (sending a Google form link via email, social network). The questionnaire used a 5-point Likert scale ranging from "strongly disagree" to "strongly agree". Random sampling method was used for the study. The sample size is 300. The respondents are consumers in Vietnam, who are 18 years old or older and have experience with E-grocery shopping services. The collected data will be filtered using SPSS 20 software and analyzed using the following methods: descriptive statistics, reliability test using Cronbach's alpha, Exploratory Factor Analysis (EFA), correlation analysis, correlation and linear regression for the principal components and their relationships in the model.

4 Results

4.1 Descriptive Analysis

Respondents are individuals 18 years of age or older at Vietnam, who have experience of E-grocery shopping service. The result was 277 votes, of which 42 were invalid (because respondents had not typed all the questions and were typing at random). The remaining result is 235 valid questionnaires that were included in the analysis. The respondents has the following characteristics (Table 1):

Table 1. Respondent's profile

		Frequency	Percent (%)
Sex	Male	61	26
	Female	174	74
Age	From 18–25	85	36.2
	From 26–33	103	43.8
	From 34–41	28	11.9
	From 42–49	15	6.4
	Upper 50	4	1.7
Education	High School	7	3
	Undergraduate	185	78.7
	Graduate	41	17.4
	Other	2	0.9
Job	Students	59	25.1
	Office staff	70	29.8
	Freelancers	24	10.2
	Officals	60	25.5
	Entrepreneurs	15	6.4
	Other	7	3
Income	Under 10 million dong	84	35.7
	From 10–20 million dong	107	45.5
	From 20–30 million dong	40	17
	Upper 30 million dong	4	1.7
Daily Internet usage	Under 2 h	5	2.1
	From 2–4 h	48	20.4
	From 4–6 h	87	37
	Upper 6 h	95	40.4
Online shopping frequency	Never	11	4.7
	Sometimes	74	31.5
	One times/week	72	30.6
	One times/month	56	23.8
	Everyday/usually	22	9.4

Table 2. Evaluate the reliability of the scale using Cronbach's Alpha

Factors	Amount of variables	Cronbach's alpha coefficient
Perceived risk	5	0.908
Perceived ease of use	5	0.891
Perceived usefulness	5	0.904
Social influence	4	0.868
Brand image	4	0.861
Intention to use E-grocery	5	0.895

4.2 Reliability Analysis

From the results of testing the reliability of the scale, the Cronbach's alpha coefficient is consistently above 0.7 and the correlation coefficient of the total variables is above 0.5, which shows that the concept scale meets the reliability requirements (Table 2).

4.3 Exploratory Factor Analysis

Factor analysis for 5 independent variables yielded the following results: KMO coefficient = 0.933 (satisfies the condition $0.5 \leq \text{KMO} \leq 1$), from which the conclusion of the factor analysis is reasonable (William et al. 2010). The sig coefficient of Bartlett's test, sig = 0.000 (<0.05), reveals that the observed variables are correlated with each other in total. Eigenvalues of the factor $= 1.115 > 1$, the extracted factor has a good summary of the information. The total extracted variance reached $72.964\% > 50\%$, which means that the 5 extracted factors explain 72.964% of the variation in the observed data. Factor loading of the observed variables > 0.5, so the observed variables among the factors are important, they have practical significance. Factor 1 includes 5 observed variables RR1, RR2, RR3, RR4, RR5, which belong to the group of factors Perceived risk (RR). Factor 2 comprises 5 observed variables SD1, SD2, SD3, SD4, SD5, which belong to the group of factors Perceived ease of use (SD). Factor 3 includes 5 observed variables HI1, HI2, HI3, HI4, HI5 belonging to the group of factors Perceived usefulness (HI). Factor 4 comprises 4 observed variables XH1, XH2, XH3, XH4 belonging to the group of factors social influence (XH). Factor 5 includes 4 observed variables TH1, TH2, TH3, TH4, which belong to the group of factors brand image (TH). EFA for the dependent variable yields the following results: KMO coefficient = 0.866 ($0.5 \leq \text{KMO} \leq 1$), which shows that the factor analysis is appropriate (Hair et al. 2007). Bartlett's test has sig = 0.000 and Eigenvalues $= 3.523 > 1$. Total variance extracted $= 70.454\% > 50\%$, which explains 70.454% of the variation of observed data. All observed variables have Factor Loading coefficient > 0.5 satisfactory.

4.4 Correlation Analysis and Multivariate Regression

PEARSon's Correlation Analysis

Table 3. Pearson's correlation coefficient matrix

	RR	SD	HI	XH	TH	YD
RR	1					
SD	0.459	1				
HI	0.423	0.700	1			
XH	0.451	0.592	0.586	1		
TH	0.430	0.585	0.615	0.567	1	
YD	0.490	0.616	0.584	0.633	0.595	1

Note: Sig. (2-tailed) < 0.01; N $= 235$

The results of Pearson correlation analysis showed that the significance level of all independent variables (RR, SD, HI, XH, TH) with the dependent variable (YD) were $0.000 < 0.01$. Thus, there is a linear relationship between the 5 independent variables and the dependent variable. The correlation coefficients between the independent and dependent variables are both positive. The factor that correlates most strongly with the dependent variable is the "social influence" factor with a correlation coefficient of 0.633, and the factor with the weakest correlation with the dependent variable is the perceptive risk factor with a correlation coefficient of 0.490 (Table 3).

Multivariate Regression Analysis

Multivariable regression analysis showed that the VIF coefficients of the independent variables were all less than 2, thus, there is no multicollinearity. The adjusted value of $R^2 = 0.535$ is smaller than the value of $R^2 = 0.545$, which means that the independent variables included in the regression explain 53.5% of the change in the dependent variable (the intention to use E-grocery shopping services). Durbin-Watson coefficient = 1.970, ranging from 1.5 to 2.5, so there is no multicolinearity. Sig test F is equal to $0.000 < 0.05$, so the multiple linear regression model fits the data set and can be used. All of 4 independent variables are accepted and significant explanatory significance for the dependent variable. The beta coefficient of the 4 independent variables Perceived Ease of Use, Perceived Usefulness, Social Influence and Brand image > 0 shows that these independent variables have a positive influence on the dependent variable. Moreover, the sig coefficient of the perception risk variable > 0.05 should be excluded. The multivariate regression equation is (Table 4):

$$\mathbf{YD = 0.764 + 0.196SD + 0.089HI + 0.275XH + 0.187TH}.$$

Table 4. Multivariate regression analysis

Model	B	Beta	t	Sig.	VIF
Constant	0.764		3.364	0.000	
RR	0.128	0.146	2.789	0.153	1.388
SD	0.196	0.200	2.956	0.003	1.316
HI	0.089	0.096	1.413	0.006	1.347
XH	0.275	0.280	4.593	0.000	1.871
TH	0.187	0.197	3.203	0.002	1.898
R	0.739				
R^2	0.545				
R^2 correlation	0.535				
Durbin-Watson	1.970				
F (54.951)	Sig. = 0.000				

5 Conclusion

5.1 Discussion

The regression coefficients of the 4 independent variables Perceived ease of use, Perceived usefulness, Social influence and Brand image are all greater than 0, coefficient bearing (+), indicating that these four independent variables all have a positive influence on intention to use E-grocery shopping services, at a confidence level of 95% (sig $<$ 0.05). Thus, hypotheses H2, H3, H4 and H5 are accepted. The independent variable risk perception has sig $>$ 0.05, so it should be excluded, that is, the perceived risk factor does not affect the intention to use the service of consumers. Therefore, hypothesis H1 is rejected. This finding is contradictory with many previous study which confirm perceived risk is negatively related to intention to use e-grocery shopping service (Chen et al. 2010; Kian et al. 2018; Nguyen 2019; Van Droogenbroeck and Van Hove 2021). Remarkably, social influence is the factor that has the strongest impact on the intention to use E-grocery shopping services. This finding is consistent with many previous studies (Venkatesh et al. 2003; Kian et al. 2018; Van Droogenbroeck and Van Hove 2020; Gatta et al. 2020) Moreover, consumers' intention to adopt the service is slightly influenced by the perceived usefulness of the service.

5.2 Magerial Implications

This study identified the factors that influence consumers' intention to adopt e-grocery shopping service during Covid-19 pandemic in Vietnam. While assessing the extent of the influence of these factors. From this, some managerial implications are suggested to help businesses better serve their customers and develop their business activities during social distancing because of Covid-19 pandemic.The research findings show that the social influence factor has a great impact on consumers' intention to adopt e-grocery shopping service. Therefore, businesses need to focus on this factor if they want to attract customers, especially new customers who have never used the service before the pandemic's conditions. The e-grocery shopping companies should increase their promotional activities to increase the brand awareness among the target customers. To make it easy and convenient for customers to adopt the e-grocery shopping service, businesses need to invest in designing websites and mobile applications that provide users with comprehensive information about products and services, as well as instructions. Descriptions should be clear and easy to understand in highly visible places during access, and the user interface should be attractive and easy to use. In addition, the speed of transmission is also an important aspect. Businesses need to invest in increasing Internet bandwidth to ensure the speed of login and online transactions, and minimize the waiting time for customers. Since product quality cannot be verified before purchase, companies need to maintain their reputation in the market, or in other words, building a good brand image is crucial to reduce customers' fear of defective products. This should be done over a long period of time. When customers have doubts about the quality of the product they will receive, a reputable brand helps customers overcome their doubts and use the service. During Covid-19 pandemic, the more customers know about the company's brand and services, the more they will be encouraged to use the service. In addition to the results obtained, the study also has some limitations. In the context of using electronic services, quality of service and cost to the customer are also factors that may influence consumers' intention to adopt the service. However, this study did not investigate these factors. Therefore, in the future, it is necessary to investigate the influence of other factors on consumers' intention to adopt e-grocery shopping service.

References

Aghekyan-Simonian, M., Forsythe, S., Kwon, W.S., Chattaraman, V.: The role of product brand image and online store image on perceived risks and online purchase intentions for apparel. J. Retail. Consum. Serv. **19**(3), 325–331 (2012)

Ajzen, I.: The theory of planned behavior. Organ. Behav. Hum. Decis. Process. **50**(2), 179–211 (1991)

Alagoz, S.M., Hekimoglu, H.: A study on TAM: analysis of customer attitudes in online food. Procedia. Soc. Behav. Sci. **62**, 1138–1143 (2012)

Ali, I., Naushad, M.: Determinants of customer satisfaction in online grocery shopping. Int. J. Data Netw. Sci. **5**(3), 383–390 (2021)

Brown, S.A., Venkatesh, V.: Model of adoption of technology in the household: a baseline model test and ext, Incorporating household life cycle. MIS Q. **29**(4), 399–426 (2005)

Chen, X., Kim, K., Yao, T., Yu, T.: On the predictability of Chinese stock returns. Pac. Basin Financ. J. **18**(4), 403–425 (2010)

Chuttur, M.Y.: Overview of the technology acceptance model: origins, developments and future directions. In: Sprouts: Working Papers on Information Systems, vol. 9, issue 37 (2009)

Davis, F.D.: Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Q. **13**(3), 319–340 (1989)

Degeratu, A., Rangaswamy, A., Wu, J.: Consumer choice behavior in online and traditional supermarkets: the effects of brand name, price, and other search attributes. Int. J. Res. Mark. **17**(1), 55–78 (2000)

Do, T., Nguyen, T., Nguyen, C.: Online shopping in an emerging market. J. Econ. Manag. Sci. **2**(2), 1 (2019)

Dodds, W.B., Monroe, K.B., Grewal, D.: Effects of price, brand and store information for buyers. J. Mark. Res. **28**(3), 307–319 (1991)

Elango, D., Dowpiset, K., and Chantawaranurak, J.: A Study on Factors Impacting Consumers' Intention to Use On-demand Food Delivery Applications in Bangkok, Thailand (2018)

Fornari, E., Grandi, S., Fornari, D.: Retailing 4.0: the new era of E-commerce in fast moving consumer goods. Symphonya. Emerg. Issues Manag. **2**, 77–90 (2018)

Gatta, V., Marcucci, E., Le Pira, M., Inturri, G., Ignaccolo, M., Pluchino, A.: E-groceries and urban freight: Investigating purchasing habits, peer influence and behaviour change via a discrete choice/agent-based modelling approach. Transport. Res. Procedia **46**, 133–140 (2020)

Goga, S., Paelo, A., Nyamwena, J.: Online retailing in South Africa: an overview (2019)

Hair, J.F.: Research methods for business. Education + Training **49**(4), 336–337 (2007). https://doi.org/10.1108/et.2007.49.4.336.2

Handayani, P.W., Nurahmawati, R.A., Pinem, A.A., Azzahro, F.: Switching intention from traditional to online groceries using the moderating effect of gender in Indonesia. J. Food Prod. Mark. **26**(6), 425–439 (2020)

Hooi, R., Leong, T.K., Yee, L.H.: Intention to use online food delivery service in Malaysia among university students. In: CoMBInES-Conference on Management, Business, Innovation, Education and Social Sciences, vol. 1, no. 1, pp. 60–73 (2021)

Hsieh, M.-H., Pan, S.-L., Setiono, R.: Product-, corporate-, and country-image dimensions and purchase behavior: a multicountry analysis. J. Acad. Mark. Sci. **32**(3), 251–270 (2004)

Huang, W.-Y., Schrank, H., Dubinsky, A.: Effect of brand name on consumers' risk perceptions of online shopping. J. Consum. Behav. **4**(1), 40–50 (2004)

Järvinen, R., Lehtinen, U.: Services, e-services and e-service innovations - Combination of theoretical and practical knowledge. Front. e-Bus. Res. 84 (2004)

Jeong, C.H.: Fundamental of Development Administration. Scholar Press, Selangor (2007)

Lee, K.Y.: Consumer processing of virtual experience in e-commerce: a test of an integrated framework. Comput. Hum. Behav. **28**(6), 2134–2142 (2012)

Nguyen, C., Do, T.: Factors affecting the decision to shop online via e-commerce platforms in Vietnam. J. Sci. Technol. **37** (2019)

Rowley, J.: An analysis of the e-service literature: towards a research agenda. Internet Res. **16**(3), 339–359 (2006)

Rust, T., Kannan, P.K.: e-Service: New Direction in Theory and Practice. M.E. Sharpe, Armonk, New York (2002)

Shukla, A., Sharma, S.K.: Evaluating consumers' adoption of mobile technology for grocery shopping: an application of technology acceptance model. Vision **22**(2), 185–198 (2018)

Van Droogenbroeck, E., Van Hove, L.: Triggered or evaluated? a qualitative inquiry into the decision to start using e-grocery services. Int. Rev. Retail., Distrib. Consum. Res. **30**(2), 103–122 (2020)

Venkatesh, V., Morris, M.G., Davis, G.B., Davis, F.D.: User acceptance of information technology: toward a unified view. MIS Q. **27**(3), 425–478 (2003)

Venkatesh, V., Thong, J.Y., Xu, X.: Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. MIS Q. **36**(1), 157–178 (2012)

Williams, B., Onsman, A., Brown, T.: Exploratory factor analysis: a five-step guide for novices. Australas. J. Paramedicine **8**(3), 1–13 (2010)

Zeithaml, V., Bitner, M.J.: Services Marketing. Integrating Customer Focus across the Firm, 3rd edn. McGraw-Hill, New York (2003)

Optimizing the Compressive Strength of Concrete with Altered Compositions Using Hybrid PSO-ANN

Raunaq Singh Suri[1], Vikrant Dubey[2], Nishant Raj Kapoor[3,4], Aman Kumar[3,4(✉)], and Megha Bhushan[5]

[1] School of Planning and Architecture, Bhopal 462016, Madhya Pradesh, India
[2] Rabindranath Tagore University, Bhopal 462045, Madhya Pradesh, India
[3] CSIR-Central Building Research Institute, Roorkee 247667, Uttarakhand, India
[4] AcSIR-Academy of Scientific and Innovative Research, Ghaziabad 201002, Uttar Pradesh, India
aman.civil16@outlook.com
[5] School of Computing, DIT University, Dehradun 248009, Uttarakhand, India

Abstract. The characteristics of concrete change as the composition changes. It is critical to understand mechanical characteristics for safety concerns. In the case of concrete, the compressive strength is the most significant mechanical property to explore. It has been critical to anticipate the compressive strength of concrete using artificial intelligence. The main focus of this study is to present an "optimized model", which is capable to accurately predict the CS of concrete with varied ingredient levels at different ages ranging from 1 to 365 days by using ANN technique optimized with particle Swarm Optimization. A total of 1030 data sets were extracted from the UC Irvine ML repository, with eight input parameters. Age (in days), fine aggregate, coarse aggregate, superplasticizer, water, fly ash, blast furnace slag, and cement have been used to estimate the compressive strength of concrete as an output. The experimental data is then validated using R, R^2, MSE, RMSE and MAPE. In comparison, the optimized PSO-ANN method has a high R value of 0.96, whereas the R value for the ANN algorithm is 0.94. With more precise compressive strength data, this prediction model helps to decrease laboratory experimental effort, as well as time and expense.

Keywords: Particle Swarm Optimization · Artificial Neural Network · Mechanical property · Concrete · Compressive strength of concrete

1 Introduction

As it is well known, the globe is full of human creations, but concrete is one of the most essential and widely used materials on the planet, second only to water.

R. S. Suri, V. Dubey, N. R. Kapoor, A. Kumar and M. Bhushan—These authors contributed equally to this work.

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 163–173, 2023.
https://doi.org/10.1007/978-3-031-13150-9_15

As a growing country, India has a burgeoning building sector. As the building sector expands, it will create a considerable amount of construction waste, which will have a substantial environmental impact [1]. Concrete is widely utilized as a building material all over the world due to its numerous advantages, including economy, integrity, modularity, and durability. Fine aggregate (FA), Coarse Aggregate (CA), Ordinary Portland Cement (OPC), and water are commonly used constituents in Normal Concrete (NC). Other various types of advanced concretes are Polymer cement concrete, self-consolidated concrete, glass concrete, and high-performance concrete. Compressive Strength (CS) is one of the most fundamental mechanical characteristics of concrete that is utilized in the design of concrete structures, and it is subject to change over time [2]. As we know that, concrete is a brittle material with good CS and minimal tensile strength. The main properties of concrete such as compressive, tensile, flexural strength, and durability studies accounted by the structural engineers. The various available guidelines for the concrete mix design over worldwide such as IS 10262:2019 (India) [3], ACI 211.1-91 (USA) [4], EN 206-1 (Europe) [5] and JGJ 55-2011 (China) [6].

Among all the physical properties of concrete compressive strength is an essential quality in which designers are primarily concerned, and relevant findings are obtained via laboratory testing [7]. Real-time experimental testing is expensive, time-demanding, as well as harmful to the environment (generate a lot of wastage). Empirical and statistical models have been extensively used, these models need a huge amount of laboratory information and still delivers inaccurate results. Sometimes these models are unable to predict the properties of concrete due to complexity in the concrete mix design and curing conditions [8]. To conquer such kinds of issues artificial intelligence models have been introduced as another approach for forecasting the CS and other properties of concrete.

Machine learning approaches [9,10], on the other hand, are now being extensively researched in the estimation of concrete CS. Among these are Artificial Neural Networks (ANN), Support Vector Machines (SVM), decision trees, and linear regression [11]. These algorithms can help estimate concrete CS more rapidly and at a lesser cost. In this research article, ANNs and optimized-ANNs are used to build prediction models for predicting CS of concrete mixes. CS is influenced by factors like the water-to-cement (w/c) ratio, the amount of CA and FA. Ordinary Portland cement (OPC) has traditionally been the principal binder in concrete mixes. In addition to that, other additional cementitious binders and waste materials, like Blast Furnace Slag (BFS) as well as Fly Ash (Fa), have been widely employed to improve the CS of concrete mixtures in recent decades. In this work, ANNs and Particle Swarm Optimization (PSO)-ANN were trained and tested using data points acquired from the literature as mentioned in Sect. 2. In past studies, ANNs and PSO-ANNs were used to forecast a variety of important concrete characteristics using a variety of input factors. There are numerous prediction models accessible in the literature that employ ANN [12–15], however only a few models with optimal approaches are available.

2 Data Description

The data set needed to predict the CS of concrete using altered composition was attained from the "University of California Irvine (UC Irvine) Machine Learning Repository's" area of concrete's CS [16]. A total of 1030 data sets

Table 1. Details of input and output variables

Parameters	Units	Min.	Max.	Std.
Input variables				
C	(kg/m^3)	102	540	104.51
W	(kg/m^3)	122	247	21.36
BFS	(kg/m^3)	0	359	86.28
Fa	(kg/m^3)	0	200	63.99
S	(kg/m^3)	0	32	5.97
CA	(kg/m^3)	801	1145	77.75
FA	(kg/m^3)	594	993	80.18
A	(Days)	1	365	63.17
Output variables				
f_{ck}	(MPa)	2.33	82.60	16.71

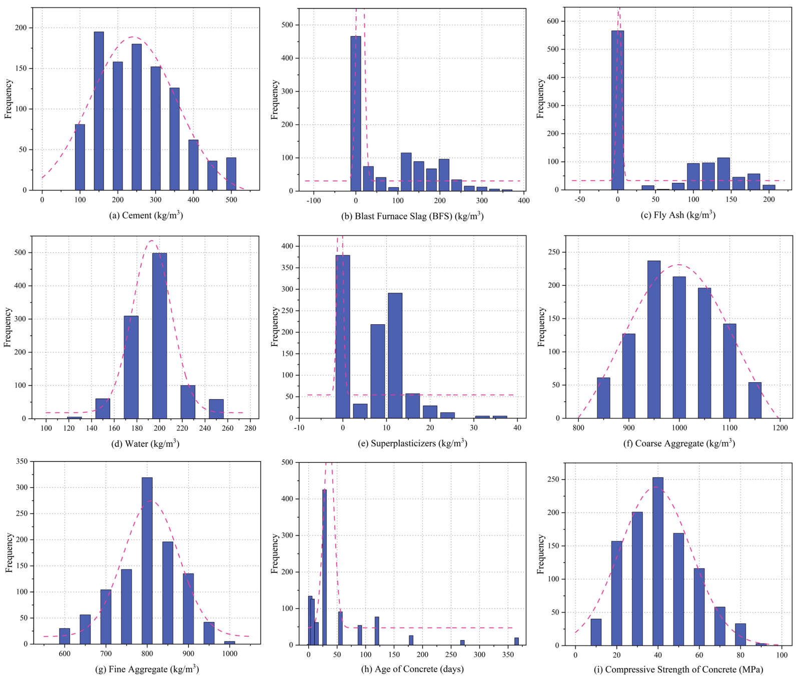


Fig. 1. Normal distribution on histogram of input and output parameters

were extracted with no missing values. The data set consists of nine parameters, with the CS of concrete (in MPa) as the predicted output parameter. The other eight input parameters are age of concrete (in days), fine aggregate (FA), coarse aggregate (CA), superplasticizer, water, Fa, BFS, and cement (all in kg/m^3). Figure 1 facilitates statistical analysis by graphing the database, as seen below. Figure 1 also demonstrates the link between inputs by displaying the relative frequency distribution along with the normal distribution curve drawn over the data histogram. The input and output variables are tabulated in Table 1.

2.1 Data Preparation

Prior to training the network, data standardization was performed to decrease undesirable feature scaling effects and increase computational stability. For the modelling, all parameters were transformed linearly between 0 and 1 in accordance with Eq. 1 [17]. The following is a quantitative representation of the normalizing process.

$$x^*_{normalized} = \frac{(E - E_{\min})}{E_{\max} - E_{\min}} \tag{1}$$

where, $x^*_{normalized}$ = normalizing value, E = original value, E_{max} = upper value in the selected data set, and E_{min} = lower value in the selected data set.

2.2 Performance Evaluation

The Correlation Coefficient (R), Mean Absolute Error (MAE), Root Mean Squared Error (RMSE), and Mean Square Error (MSE), Coefficient of Determination (R^2), Mean Absolute Percentage Error (MAPE) [12] are five widely used indices that are used to assess the effectiveness of compressive strength prediction model. These indices are expressed in Eqs. 2–6.

$$R^2 = 1 - \left(\frac{\sum_{i=1}^{N} (M_i - P_i)^2}{\sum_{i=1}^{N} P_i^2} \right) \tag{2}$$

$$RMSE = \sqrt{\frac{1}{N} \sum_{i=1}^{N} (M_i - P_i)^2} \tag{3}$$

$$MAE = \frac{\sum_{i=1}^{N} |M_i - P_i|}{N} \tag{4}$$

$$MSE = \frac{1}{N} \sum_{i=1}^{N} (M_i - P_i)^2 \tag{5}$$

$$MAPE = \frac{1}{N} \frac{\sum_{i=1}^{N} |M_i - P_i|}{\sum_{i=1}^{N} |M_i|} \tag{6}$$

where, N is the number of points in the data set, and M and P sets are the experimental and predicted output sets, respectively.

3 Methodology

Several sectors are now using nature-inspired AI methods to anticipate and understand the behaviour of materials. This work provides an AI-based techniques comprising of an ANN improved using PSO are utilised to predict the CS of concrete. Both these methods were chosen because of their robustness, easy-to-use, and popularity in predicting findings in peer studies, as well as their reputation as the finest data optimization techniques.

3.1 Artificial Neural Network

ANN has been investigated for last five decades to attain human-like aptitude in many sectors such as image and recognition of speech. "ANN are inspired by the architecture of the human central nervous system which consists in a large number of cells (neurons) working in parallel in order to facilitate decision-making in the most rapid way" [18]. Internally, an electrical stimulation known as a synapse connects these basic components. Similarly, this synaptic activity connects the ANN-model to each other through numeric values (matrix weight), which are upgrade by the human-like process of learning [19]. The main benefit of the ANN model is that in which, there is no need to program the model, this ANN model chooses the initial values by itself with a least prediction errors. The learning algorithm is used to execute the learning process, which is also able to do the modifications in the weight matrix. In neurons, input data are processed across several consecutive layers. In ANN, the input and output layers are always taken into account. The layer between the input and output layers is known as the "hidden layer." In most cases, one hidden layer is adequate, however two hidden layers are also employed to improve the accuracy and performance of ANN. Figure 2 depicts the ANN model's approach [20].

The hidden layers were established on the basis of training and learning stages. A fifteen trials were carried out to reach the quantity of neurons in the hidden layer with uppermost value of R with respect to target datasets. The ANN model is similar for all the conditions only changes in the hidden layers. With the trials, it has been found that this L1, L2,... and L10 give the best and better performance with a high degree of accuracy. The input data in the ANN model defined the matrix weights w as well as the bias b. After that, an activation function is used to produce the neuron's output. In this model, initial weights were chosen randomly. Then initial input weights are processed in the hidden layers for some time to check the possibilities of error. This technique was continued until the weights were adjusted. In order to achieve the correctness of the ANN algorithms, data was constantly processed multiple times until the corrected weights were continuously experienced, and scatter was computed every 25 iterations.

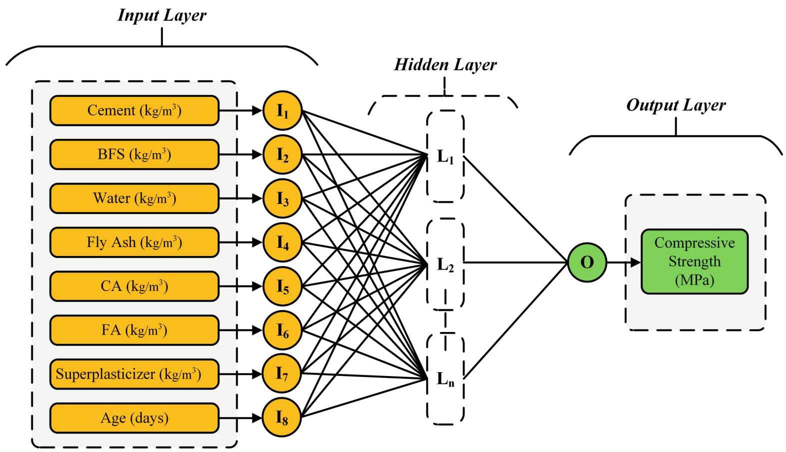


Fig. 2. Architecture of Artificial Neural Network process

3.2 Particle Swarm Optimization-Artificial Neural Network

ANN training results in a minimization issue that may be addressed using traditional or metaheuristic methods. In a hybrid ANN-PSO model, PSO is used to reduce the ANN's mistakes by identifying the best values for the model's weights and biases. As a result, the weights and biases are variables in this issue, and the problem's feasible space is determined by the interval at which these variables fluctuate. The i_{th} particle's cost function (fitness function) can be described as follows in terms of RMSE [21].

$$f\left(W_i\right) = \frac{1}{n}\sum_{k=1}^{n}\left[\sum_{l=1}^{O}\left\{M_{kl} - P_{kl}\left(W_i\right)\right\}^2\right] \tag{7}$$

where f is the fitted value, n is the no. of samples in the training set, M_{kl} is the measured target value, P_{kl} is the predicted target, W_i is the weight matrix, and O is the number of output neurons.

Create a NN with initial weights and biases based on the number of neurons in the hidden layer. Reform the weights as well as biases such that they may reflect a particle's position in the problem's D-dimensional space, where D is the total number of weights and biases. We can estimate output values for each particle in each iteration and then use Eq. 7 to compute the value of the given cost function. Particles' locations are updated using the PSO algorithm for a certain number of populations and iterations until the goal is reached (i.e., the cost function is minimized).

4 Results and Discussions

The normalized data were split into two groups named training and testing with a percentage of 80% and 20% respectively. The ANN model was trained from 3 neurons to 15 neurons and 10 neurons show the best-fitted neuron on the basis of R, MSE, and MSPE (%). The basic hit and trial method was adopted and performance of the each neuron was ranked highest to lowest for R and lowest to highest for MSE and MAPE (%). The accuracy of the ANN model was reached only up to the value of R is 0.9473 as mentioned in Table 2. To increase the accuracy of the ANN model optimized PSO algorithms with swarm particles from 30 to 1000 were used. The best prediction results were obtained with 300 swarm particles. The achieved value of R with the optimized ANN model is 0.9630. The prediction results of ANN and PSO-ANN models are presented in Fig. 3 (a) and (b). The ratio of anticipated to experimental results vs influencing factors, which indicates the predictability of compressive strength, is illustrated in Fig. 3 (e) and (f). Tables 1 list the influencing parameters, which were standardized in the [0, 1] domain due to their significant variance. The fluctuation of data around the horizontal line starting at 1 (the bold line in red colour) indicates parameter stability, and the closer the data is to this line, the greater parameter stability. The variation of no. of specimens with compressive strength is presented in Fig. 3 (c) and (d) The absolute error value of the ANN model is 95.83% accurate for 10 MPa compressive strength and for the PSO-ANN model it is 97.57% for the same compressive strength as shown in Fig. 4.

Table 2. Statistical analysis of analyzed models

Method	Statistical Parameters for f_{ck}						Std.
	R	R^2	MSE	RMSE	MAE	MAPE (%)	
ANN	0.9473	0.8975	28.63	5.35	4.15	13.47	15.82
PSO-ANN	0.9630	0.9274	20.27	4.50	3.40	12.56	16.02

The prediction equation to calculate the compressive strength of concrete is expressed in Eq. 8.

$$f_{ck} = \text{purlin}\left(OW_2 Z_i + OB_2\right) = OW_2 Z_i + OB_2 \tag{8}$$

where, OW_2 and OB_2 are the weight and bias between the hidden layer to the output layer, mentioned in Eq. 12 and 13 respectively. The value of Z_i is calculated using Eq. 9.

$$Z_i = \tanh\left(IW_1 X_{i,\text{ norm}} + IB_1\right) \tag{9}$$

where, IW_1 and IB_1 are the weight and bias between the input layer to hidden layer, mentioned in Eq. 10 and Eq. 11 respectively and '$tanh$' is the activation function.

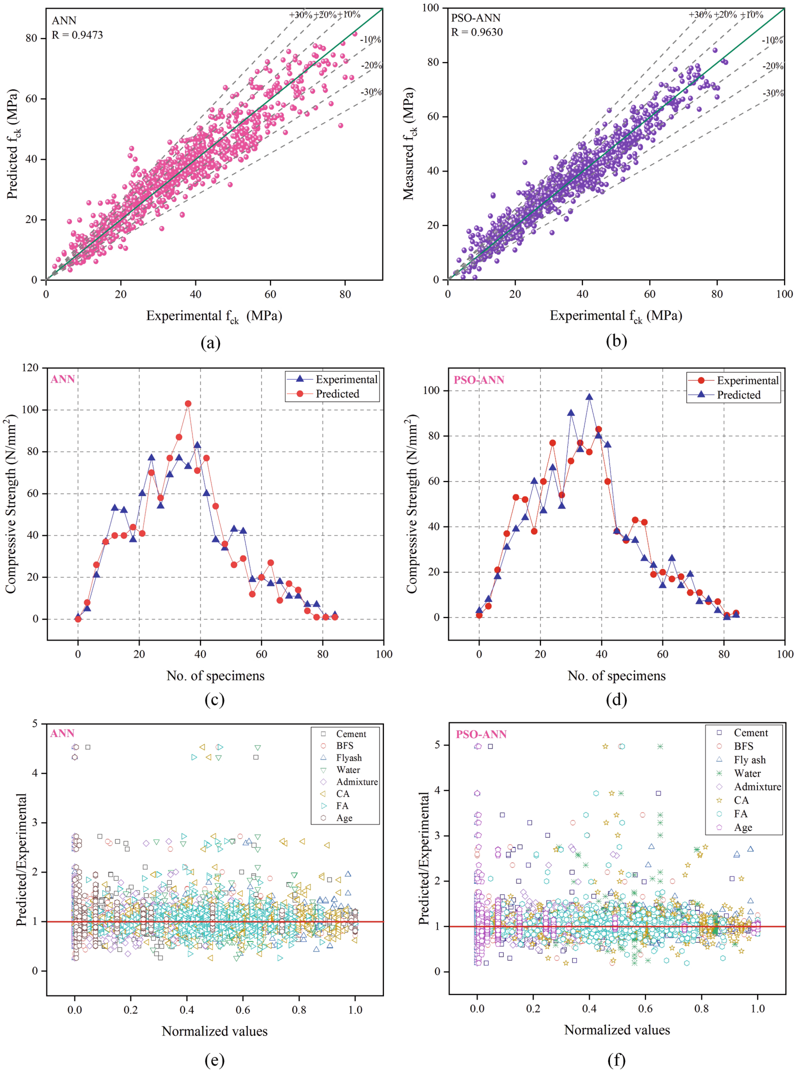
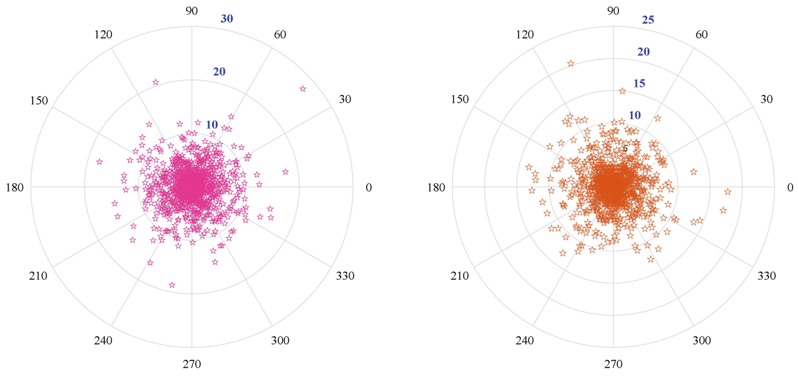


Fig. 3. (a) Experimental and predicted results by ANN model (b) PSO-ANN model results (c) stability of compressive strength for input variables using ANN model (d) PSO-ANN model (e) comparison of experimental and predicted results with respect to and no. of samples by ANN model and (f) PSO-ANN model



(a) ANN

(b) PSO-ANN

Fig. 4. Absolute error of ANN and PSO-ANN model (MPa)

$$IW_1 = \begin{bmatrix} -0.88 & -1.33 & -0.90 & -0.37 & -0.67 & -1.59 & -0.83 & -0.06 \\ -0.31 & -0.52 & -0.50 & 2.71 & 1.82 & 0.01 & -2.41 & -0.46 \\ -0.39 & -0.56 & -0.20 & 0.06 & 0.03 & -0.20 & -0.30 & 4.60 \\ 0.01 & 0.09 & 0.02 & -1.81 & 0.86 & 0.01 & 1.40 & 0.36 \\ 0.91 & 1.16 & 0.55 & -0.08 & 0.79 & 0.21 & -0.15 & -0.04 \\ -1.56 & -0.94 & -0.36 & -1.47 & 1.18 & 0.01 & 2.85 & -0.28 \\ -0.80 & -0.50 & -0.68 & 0.50 & 0.26 & -1.53 & -1.40 & 0.09 \\ -1.24 & -1.63 & 0.76 & 0.61 & -0.70 & -0.12 & 0.06 & 1.33 \\ 0.02 & 0.31 & 0.16 & 0.45 & -0.01 & -0.83 & -0.95 & -0.02 \\ 0.33 & 0.67 & 0.35 & -0.28 & 0.36 & -0.77 & -0.83 & -0.02 \end{bmatrix} \quad (10)$$

$$IB_1 = \left(-1.99\ -0.41\ 4.94\ 0.14\ 1.44\ -1.62\ -1.01\ 2.69\ -0.06\ 0.48\right) \quad (11)$$

$$OW_2 = \left(1.01\ 1.15\ 2.39\ 2.31\ 2.21\ -0.25\ -1.35\ -0.86\ -2.97\right) \quad (12)$$

$$OB_2 = (-1.438812) \quad (13)$$

5 Conclusion

In this work, a hybrid method called PSO-ANN was used to forecast and quantify the uncertainty of the final CS of concrete in a stochastic environment, with the goal of more accurate and reliable predictions. The use of an ANN model reinforced with PSO optimization to estimate the compressive strength of concrete having different constituent compositions is responsible for both accuracy and simplicity. This can be beneficial in terms of saving time, energy, and money. The data extracted from the UC Irvine ML repository containing 1030 data sets with eight input parameters and compressive strength of concrete as desired output shows PSO competence with ANN. The findings demonstrate that the presented PSO-ANN model excels at predicting the precise CS value. The optimized PSO-ANN method has a high coefficient correlation (R^2) value of 0.96, whilst the ANN algorithm's R^2 value is 0.94. In both the training and testing stages, the ANN optimized by PSO can effectively represent the complicated nonlinear connection between the eight input parameters and the eventual CS of concrete with an accuracy of more than 90%. The model may also be used as a starting point for developing multi-output models that forecast many concrete qualities at once, such as slumps, strength, durability, chloride penetration, corrosion, depth of cracks, and so on. As a result, the model may be used to optimize the mix percentage for the given slump, strength, durability, and chloride penetration constraints, i.e., to design new concrete mix proportions with improved characteristics. In the near future, these elements will be investigated based on the work provided in this research article.

References

1. Luangcharoenrat, C., Intrachooto, S., Peansupap, V., Sutthinarakorn, W.: Factors influencing construction waste generation in building construction: Thailand's perspective. Sustainability **11**(13), 3638 (2019). https://doi.org/10.3390/su11133638
2. Bae, B.-I., Choi, H.-K., Lee, B.-S., Bang, C.-H.: Compressive behavior and mechanical characteristics and their application to stress-strain relationship of steel fiber-reinforced reactive powder concrete. Adv. Mater. Sci. Eng. **2016** (2016). https://doi.org/10.1155/2016/6465218
3. IS 10262:2019: Concrete mix proportioning—Guidelines (second revision). https://www.services.bis.gov.in:8071/php/BIS/bisconnect/pow/is_details?IDS=MTA4Mw
4. ACI PRC-211.1-91: Standard practice for selecting proportions for normal, heavyweight, and mass concrete (reapproved 2009). https://www.concrete.org/store/productdetail.aspx?ItemID=211191&Language=English&Units=US_Units
5. EN 206-1:2000: Concrete - part 1: Specification, performance, production and conformity; German version. https://www.techstreet.com/standards/din-en-206-1?product_id=924895
6. JGJ 55-2011: Specification for mix proportion design of ordinary concrete (English version). https://www.codeofchina.com/standard/JGJ55-2011.html
7. Ambroziak, A., Ziolkowski, P.: Concrete compressive strength under changing environmental conditions during placement processes. Materials **13**(20), 4577 (2020). https://doi.org/10.3390/ma13204577
8. Chong, B.W., et al.: Design of experiment on concrete mechanical properties prediction: a critical review. Materials **14**(8), 1866 (2021). https://doi.org/10.3390/ma14081866
9. Verma, K., et al.: Latest tools for data mining and machine learning (2019). https://doi.org/10.35940/ijitee.I1003.0789S19
10. Mangla, M., Mehta, V., Bhushan, M., Kumar, A., Mohanty, S.N.: Applications of the internet of things: challenges, applications, and advances (2022)
11. Güçlüer, K., Özbeyaz, A., Göymen, S., Günaydın, O.: A comparative investigation using machine learning methods for concrete compressive strength estimation. Mater. Today Commun. **27**, 102278 (2021). https://doi.org/10.1016/j.mtcomm.2021.102278
12. Mohamed, O., Kewalramani, M., Ati, M., Al Hawat, W.: Application of ANN for prediction of chloride penetration resistance and concrete compressive strength. Materialia **17**, 101123 (2021). https://doi.org/10.1016/j.mtla.2021.101123

13. Hammoudi, A., Moussaceb, K., Belebchouche, C., Dahmoune, F.: Comparison of artificial neural network (ANN) and response surface methodology (RSM) prediction in compressive strength of recycled concrete aggregates. Constr. Build. Mater. **209**, 425–436 (2019)
14. Eskandari-Naddaf, H., Kazemi, R.: ANN prediction of cement mortar compressive strength, influence of cement strength class. Constr. Build. Mater. **138**, 1–11 (2017)
15. Prasad, B.R., Eskandari, H., Reddy, B.V.: Prediction of compressive 12 optimizing the compressive strength of concrete strength of SCC and HPC with high volume fly ash using ANN. Constr. Build. Mater. **23**(1), 117–128 (2009)
16. UCI: Concrete compressive strength data set. https://archive.ics.uci.edu/ml/datasets/Concrete+Compressive+Strength
17. Gavali, P., Banu, J.: Deep convolutional neural network for image classification on CUDA platform (chap. 6). In: Sangaiah, A.K. (ed.) Deep Learning and Parallel Computing Environment for Bioengineering Systems, pp. 99–122 (2019). https://doi.org/10.1016/B978-0-12-816718-2.00013-0
18. Cascardi, A., Micelli, F., Aiello, M.A.: An artificial neural networks model for the prediction of the compressive strength of FRP-confined concrete circular columns. Eng. Struct. **140**, 199–208 (2017). https://doi.org/10.1016/j.engstruct.2017.02.047
19. Kumar, A., Mor, N.: An approach-driven: use of artificial intelligence and its applications in civil engineering. In: Manoharan, K.G., Nehru, J.A., Balasubramanian, S. (eds.) Artificial Intelligence and IoT. SBD, vol. 85, pp. 201–221. Springer, Singapore (2021). https://doi.org/10.1007/978-981-33-6400-4_10
20. Kumar, A., Mor, N.: Prediction of accuracy of high-strength concrete using data mining technique: a review. In: Dutta, M., Krishna, C., Kumar, R., Kalra, M. (eds.) Proceedings of International Conference on IoT Inclusive Life (ICIIL 2019), NITTTR Chandigarh, India. LNNS, vol. 116, pp. 259–267. Springer, Singapore (2020). https://doi.org/10.1007/978-981-15-3020-3_24
21. Chau, K.W.: Application of a PSO-based neural network in analysis of outcomes of construction claims. Autom. Constr. **16**(5), 642–646 (2007). https://doi.org/10.1016/j.autcon.2006.11.008

Adaptive Strategies for Multicriteria Auctions: An Empirical Study

Imène Brigui[1(✉)], Philippe Caillou[2], and Suzanne Pinson[3]

[1] Emlyon Business School, 23 Avenue Guy de Collongue, 69130 Écully, France
brigui-chtioui@em-lyon.com
[2] Université Paris Sud, LRI, INRIA, TAO Team, Bat 490, Paris, France
caillou@lri.fr
[3] Place du Maréchal de Lattre de Tassigny, Université Paris-Dauphine - PSL, Lamsade, 75775 Paris, France
Suzanne.pinson@dauphine.fr

Abstract. In this paper, we propose bidding strategies for conducting automated reverse auctions based on a non-compensatory multicriteria model. We conduct an empirical multiagent study in order to appreciate the relevance of the proposed strategies. In this type of auction and in order to ensure ascending process evolution, the design of such automated systems often uses a fixed bid increment representing the minimum amount by which a bidder must improve on the current best bid. This article suggests adjusting the bid increment as the auction process goes on. To this end, we propose buyer counterproposal which ensures an acceptable solution at any given time. To this end, we refer to the auction context based on the number of remaining suppliers or the remaining time at each process step. We also present and demonstrate some interesting properties of the proposed algorithm. Finally, we provide an empirical study that compares a fixed-increment strategy to our proposed strategies on the basis of a variation of different auction settings.

Keywords: Decision models · Automated auctions · Multiagent systems · Bidding strategies

1 Introduction

Due to their wide popularity, auctions represent an interesting research field of study with regard to both the theory and the practice. Auctions have attracted tremendous interest due to the rigorous environment that they provide, and the clear rules on which they are based. Design of auction systems is a complex and challenging task because of the many economic and computational levels that need to be considered. Many research fields focus on auctions such as artificial intelligence, operational research, and theoretical computer science [9]. In this work, we focus on reverse auctions, which involve one buyer negotiating with multiple suppliers or bidders. This type of auctions gained popularity as a result of the maturity of Internet-based auction systems and the growth

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 174–184, 2023.
https://doi.org/10.1007/978-3-031-13150-9_16

of transaction security tools. Consumers face a huge number of offers and suffer from the complexity of making a choice. Reverse auctions propose solutions to assist human buyers or organizations in their decision-making process. Reverse-auction design often considers adopting a bid increment representing the minimum amount by which a bidder must improve on the current best bid. Generally, the bid increment is fixed before the beginning of the process and kept the same throughout without any consideration of the auction process context. To address this drawback, we propose a counterproposal definition based on an evolutive increment. To this end, we have chosen an exponential smoothing method to adjust the increment at each round of the auction process. This method uses the remaining time or the number of remaining suppliers as key information in determining the variable increment at a given round [6]. To summarize, our research question is: How should buyer counterproposal strategies be constructed to implement an auction mechanism that ensures an acceptable solution at any given time and that considers auction context evolution?

After discussing the literature on multicriteria auctions in the first section, we provide in Sect. 2 an overview of our multicriteria auction mechanism. In Sect. 3, we present buyer counterproposal evolutive strategies and we outline the properties of our algorithm. Section 4 provides the results of our empirical study comparing a fixed-increment strategy to our proposed strategies based on a variation of different auction settings. We show that the proposed strategies provide good results as quickly as the fast-fix strategy in the case of a request for an early solution. We also observe that when the auction is not interrupted, the final solution is as good as the best fixed-increment strategy, but is reached much faster. Finally, we present a conclusion and an overview of our planned future work.

2 Related Works

Multiple research works focus on multicriteria negotiation [3, 7, 8] and especially on multicriteria English auctions [4, 5, 9]. Multicriteria auctions can be considered as a logical extension of classical auction theory [8]. Their aim is to include all product attributes (not only the price) in the negotiation process. By "multicriteria auction", we mean several distinctly different approaches, some with and others without an explicit scoring function. Teich et al. [12] proposed the first type, which consists of a leap-frog method in which a bidder must improve on the previous bid on at least one criterion, while being no worse on any other criterion. The second type of multicriteria auction is based on a scoring function and an aggregation multicriteria model that recognizes the overall utility of a bid [2]. Thus, during the auction process, all attribute values of the product can evolve.

In iterative auction mechanisms, the process is based on multiple, time-discrete rounds of bidding. The auctioneer provides counterproposals to bidders to help them decide how they can improve their bids. Whereas, in price auctions, only price could be improved by the supplier (a win–lose situation), multicriteria auctions allow the overall bid value to be increased, considering all negotiable attributes (an efficient alternative being to vote in parallel on all the possible attribute bundles [11]) by applying an increment on the current best bid at each round. Most of the multicriteria reverse-auction models proposed in the literature use a fixed increment that operates on the current best utility to guarantee ascending evolution of the auction. Another alternative is to leave bidders free to fix the amount they improve on the current best utility [5] which can make the process too long because of too small increments. We consider that these counter-proposal strategies have one main drawback: The negotiation process does not consider the current auction context, which means that the auctioneer's behavior does not change as the process goes on.

Despite this expanding literature, no study has yet – to the best of our knowledge –focused on adaptive strategies based on evolutive increment definition. In this paper, we focus on the formulation of the buyer counterproposal by proposing an adaptive reverse auction process.

3 Auction Model

Our auction model is based on a reverse-English-auction protocol and a multicriteria reference-point auction model introduced in [4]. Our protocol is based on classical auction mechanism requiring that the rules are explicit, complete, and fixed for the duration of the process. Before presenting the preference and aggregation models, we start by proposing some preliminary useful notations:

Let p be the number of attributes.

$D = D_1 \times ... \times D_p$ is the decision space where D_j is the domain of values for attribute j ($j = 1,\dots, p$);

$C = C_1 \times ... \times C_p$ is the criterion space; v_j is the value function defined from D_j to $C_j = [0; v_{max}]$ that corresponds to attribute j; let $x = (x_1 \times ... \times x_p) \in D$ denote a bid, $b = (b_1 \times ... \times b_p) \in C$ where $b_j = v_j(x_j)$ denotes the bid evaluated on all criteria, and $j = 1, ..., p$ - $\hat{t}$, the auction deadline.

3.1 Preference Model

The preference model is based on two reference points:

- The aspiration point, denoted by $a = (a_1 \times ... \times a_p)$, whose coordinates $a_j = v_j(dv_j)$ are aspiration levels, where $dv_j \in D_j$ is the desired value of the buyer on criterion j. The aspiration point is kept private during the auction process, which means that the buyer does not communicate it to the participating suppliers.
- The reservation point, denoted by $r = (r_1 \times ... \times r_p)$, whose coordinates $r_j = v_j(mv_j)$ are reservation levels, where $mv_j \in D_j$ is the minimum value required on criterion j. The reservation point can be partially defined (over only some criteria) and is public to all participating suppliers.

3.2 Aggregation Model

The aggregation model determines the overall utility associated with a supplier bid. It is calculated by the deviation from the buyer aspiration point. The model measures the differences between the aspiration values and the bid values on each criterion and retains the closest one. The max function is chosen to ensure that a bad score on a criterion cannot be compensated by good scores on other criteria. The Eq. (1) gives the utility of a supplier bid *b*.

$$U_a(b) = \max_{j=1,\ldots,p} \left(a_j - b_j\right) \tag{1}$$

The preference relationship based on the utility presented above is given by Eq. (2).

$$b \succ b' \Leftrightarrow U_a(b) < U_a\left(b'\right) \tag{2}$$

According to this preference relationship, the buyer agent tries to minimize the deviation from the aspiration point. A bid *b* is preferred to a bid *b'* if its utility is less than that of *b'*.[1]

4 The Auction System

In all the auction models based on an absolute fixed increment, the constraint at $t + 1$ is given by the following relationship:

$$\forall t,\ U_a\left(b^{t+1}\right) \leq U_a\left(best^t\right) - \varepsilon \tag{3}$$

$best^t$ denotes the current best supplier bid at round t. ε denotes the increment defined over the utility of the current best bid $best^t$.

r^t represents buyer reservation point at round t. After evaluation of supplier bids received at t, the buyer selects bid b_3 as the current best bid. The new reservation point r^{t+1} is computed using b_3 and ε.

We propose a counterproposal algorithm that ensures the increment evolution and that satisfies the "beat-the-quote" constraint introduced in [13], which assigns the following constraint:

$$\forall t,\ U_a\left(b^{t+1}\right) < U_a\left(best^t\right) \tag{4}$$

Our proposed approach stems from the exponential smoothing method that we use by observing at a given time t: the number of remaining supplier agents $|B^t|$ and the remaining time $(\hat{t} - t)$. According to these observations, we formulate two propositions for the increment ε^t adjustment [6].

Definition 1. *Using the exponential smoothing method over the number of remaining suppliers* $|B^t|$, *the increment* ε^t *is calculated as follows*:

$$\varepsilon^t = (\alpha \times \varepsilon^{t-1}) + ((1 - \alpha) \times v_j(\left|B^t\right|)) \tag{5}$$

v_j: the normalization function; $\alpha \in [0, 1]$: the smoothing factor.

[1] This measure could be called "disutility," since the buyer aims to minimize it.

The auction constraint at t is given by:

$$\forall t, U_a\left(b^{t+1}\right) \leq U_a\left(best^t\right) - \left(\alpha \times \varepsilon^{t-1}\right) + \left((1-\alpha) \times v\left(\left|B^t\right|\right)\right) \tag{6}$$

Definition 2 We propose a new adjusted bid-increment technique based on the remaining time as follows:

$$\varepsilon^t = (\alpha \times \varepsilon^{t-1}) + ((1-\alpha) \times v_j(\hat{t} - t)) \tag{7}$$

4.1 Properties

To evaluate the algorithm performance, we establish:

$$\xi(best) > \xi(Disagreement), \forall\ best \in B \tag{9}$$

Following [12], we summarize two properties that the proposed algorithm satisfies:

Property 1 ***Measurable performance***. *We propose to measure the algorithm performance using the utility of the winning bid*. The final agreement defines the expected performance ξ. We suppose, in line with [8], that disagreement is the worst outcome.

Proof *Considering two agreements* g^1 *and* g^2, *and* $best^1$ *and* $best^2$ (*the corresponding winner propositions*), *we establish that*:

$$\xi(g^1) > \xi(g^2) if\, U_a(best^1) < U_a(best^2) \tag{10}$$

Property 2 ***Monotonicity***. *According to this property, the quality of the result is a non-decreasing function of time and increment.*

Proof $\forall t, U_a\left(best^{t+1}\right) \leq U_a\left(best^t\right) - \left(\left(\alpha \times \varepsilon^{t-1}\right) + \left((1-\alpha) \times v\left(\hat{t} - t\right)\right)\right)$ *A sufficient condition for monotonicity is to demonstrate that* $\left(\left(\alpha \times \varepsilon^{t-1}\right) + \left((1-\alpha) \times v\left(\hat{t} - t\right)\right)\right) > \ = 0$, *equivalent to* $\alpha \times \varepsilon^{t-1} \geq 0 and \left((1-\alpha) \times v\left(\hat{t} - t\right)\right) \geq 0$, *which can easily be deduced from* $0 < \alpha < 1 and v\left(\hat{t} - t\right) \geq 0$.[2]

In this section, we present our empirical study which aims to analyse different counterproposal buyer strategies. Our auction process was implemented using the GAMA Framework [1]. Human agents were represented by autonomous intelligent agents able to analyse negotiation context and to conduct auctions on behalf of their objectives, preferences and local constraints.

[2] The proof is the same using the number of remaining suppliers.

5 Experimental Settings

5.1 Interaction Protocol and Global Parameters

For each simulated market, an auction is conducted by considering one buyer agent and *NbBidders* supplier agents interacting during at most *MaxSteps* steps.

The interaction protocol follows the steps described in the previous sections:

1. At the beginning of the auction process, the buyer agent sends the reservation point to every supplier agent. The supplier agents return their first bids.
2. At each step *t*, the buyer selects the best bid *BestOffer(t)*. The minimum bid for step *t* + *1* will be *ReservationUtility(t* + *1)* = *BestOffer(t)* + *Epsilon(t)*.
3. The auction process ends when there are no more remaining suppliers at time *t* or the maximum number of steps *MaxSteps* is reached. The winner is the supplier who proposed *BestOffer(t* − *1)*.

5.2 Buyer Agent

We compare six buyer strategies: four fixed strategies and the two adaptive strategies described in the previous section.

- ***FixU/N, Fix3U/N, Fix6U/N, Fix9U/N***: *Epsilon(t)* is fixed and depends only on the aspiration point of the buyer (*UMax*) and the maximum number of time steps (*MaxSteps*). The obvious strategy considering a fixed epsilon and a fixed time limit is *Epsilon* = *UMax/MaxSteps*. This strategy would progressively increase the minimum bid to the maximum utility during the whole time-allowed window. We compare our adaptative strategies to three other quicker strategies: Fix3U/N, with *Epsilon* = *3*UMax/MaxSteps*; Fix6U/N, with *Epsilon* = *6*UMax/MaxSteps*; Fix9U/N, with *Epsilon* = *9*UMax/MaxSteps*

  The drawback of higher *Epsilon* values is the possibility of missing interesting bids when the last *ReservationUtility* is set too high.
- ***VarN*** uses the number of remaining bidders to adapt its *Reservation Utility* – see Eq. (5).
- ***VarT*** uses the number of remaining time steps to adapt its *Reservation Utility* – see Eq. (6).

Both *VarN* and *VarT* strategies use an alpha parameter for their adaptation speed.

5.3 Supplier Agents

We consider that each supplier agent has a fixed number of *NbProposals* possible bids. For each proposal *Pi*, a random couple $\{US(\mathrm{i}); UB(\mathrm{i})\}$ is generated, corresponding respectively to the supplier's and to the buyer's utility for this proposal. If a proposal is dominated, another couple is randomly generated. A proposal is dominated when: $\exists j \neq i \quad / \quad US(j) > US(i) \ and \ UB(j) > UB(i)$.

Each supplier *s* has a maximum buyer utility it can offer *BidderMax(s)*.

BidderMax(s) is generated using a uniform distribution:
BidderMax(s): *U[0; UMaxBidders*UMax].*

The random values are generated using uniform distribution: *US*(i): U[0;1]; *UB*(i): U[0; *BidderMax*(s)].

At each step, when a supplier agent receives the *ReservationUtility(t)* value from the buyer, it selects the first proposition such as *UB*(i) $\geq$ *ReservationUtility(t)* and returns it to the buyer. If none exists, the supplier returns Ø.

For a more precise comparison of buyer strategies, the supplier's random proposals are kept identical for the different buyer strategies. Our aim is to study the efficiency of the protocol from the buyer perspective. Thus, we focus our analysis on the utility of the best bid for the buyer compared to that of the best-acceptable bid, considering all the suppliers in the simulation.

5.4 Parameter Settings

For our experiments, we consider a standard setting with average parameter values. This standard setting will be used to study the impact of each parameter on the auction results.The standard setting parameters are: *NbBidder* = 100; *MaxSteps* = 100; *Alpha* = 0.5; *UMax* = 10; *UMaxBidders* = 0.9; *NbProposals* = 1000.

The high number of proposals by supplier is due to the fact that some criteria may be continuous, allowing a high number of possible bids for each supplier.

Figures 1 and 2 illustrate the results of different buyer strategies during otherwise-identical auctions. In Fig. 1, *UtilityProportion* is represented, i.e. the proportion of the maximum reachable buyer utility during this auction process, for each step. For example, if the negotiation is interrupted at *t* = *5*, the winning-bid utility value is only 7% of the maximum utility if the buyer chooses the *FixU/N* strategy. For the other strategies, it would be 19%, 36%, 40%, 46%, and (for the best) 53%, respectively for fthe *Fix3U/N*, *Fix6U/N*, *VarN*, *VarT* and *Fix9U/N* strategies.

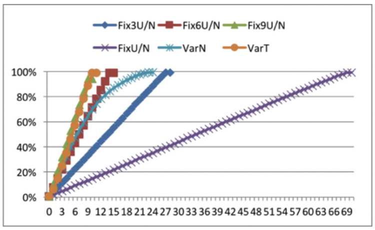


Fig. 1. Evolution of Utility Proportion for each strategy

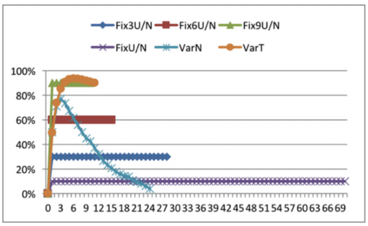


Fig. 2. Evolution of the increment value at each round

The advantage of the adaptive strategies (*VarN* and *VarT*) is visible in Fig. 1: At the beginning of the negotiation, the *BestBid* utility increases quickly – almost as fast as the *Fix9U/N* strategy. In the case of early auction termination, the utility is already high. Then, the utility steps decrease to improve precision and achieve a very high final bid.

The final situation (where the auction continues until no supplier remains in the auction) illustrates the drawback of the fast-fix strategies: the risk of missing good opportunities. As illustrated in Fig. 1, *Fix9U/N* is the only strategy not to reach 100% for the winning bid, even if it is the fastest to terminate (the winning bid being selected in ten steps, but being only 94% of the maximum). *VarT* is the fastest to terminate and find the maximum bid (11 steps), followed by *Fix6U/N, VarN, Fix3U/N,* and *FixU/N*.

We can check the expected behaviors of the strategies: the *Fix* strategies increase the minimum requested utility linearly. The different variants of this strategy change the slope of the line. *VarN* and *VarT* strategies adapt the evolution to the number of remaining suppliers/remaining time, smoothing the utility curve. This is confirmed in Fig. 2, representing the corresponding increment values (increase in the *Reservation Utility* requested by the buyer).These results are confirmed by a more complete analysis of the quality of the final situation and of the time to reach it. Table 1 gives the average and variance values for the *UtilityProportion* of the winning bid and for the final step over 20 simulations with similar parameters. Whereas *Fix9U/N* is clearly faster to terminate (ten steps), with the lowest quality (93% on average), *VarT* is almost as quick and gives a much better result (96%). At the opposite end of the spectrum, *VarN* gives results as good as the best fix strategy (*FixU/N*), with 98.3% versus 98.2%, but with a much quicker result (26 steps versus 68). These results confirm that these strategies are both useful for early and late termination of the auction.

Table 1. For each strategy, average and variance for the UtilityProportion of the winning bid and for the number of steps to reach this bid with standard settings (for 20 simulations)

Strategy	Winning bid *UtilityProportion* average	Wining bid *UtilityProportion* variance	Final step average	Final step variance
FixU/N	98.2%	1.08%	68.3	1.19
Fix3U/N	97.3%	1.58%	27.1	0.46
Fix6U/N	97.1%	2.49%	14.6	0.49
Fix9U/N	93.4%	0.40%	10.0	-
VarN	98.3%	1.19%	25.6	3.97
VarT	96.2%	4.29%	10.5	0.50

5.5 Parameter Analysis

We notice that a higher number of bidders increases the number of solutions and also the "continuity" of the problem. Thus, the auction evolution observed with *NbBidders* = 1000 and *MaxPropositions* = 10,000 (Figs. 3 and 4) are very similar to that observed with standard parameters (Fig. 1). *VarN* gets a very good final utility with a quick start. *VarT* also gives very good early results, but the drawback is that the factor supposed to slow down the negotiation stays low: The number of remaining steps stays high due to a fast termination of the auction.

With a lower number of steps (Fig. 5 with 50 steps), the slowdown is more effective for *VarT*, as illustrated by the increment evolution (Fig. 6) and the number of steps before the winning bid is selected (11 steps versus five for *Fix9U/N* and eight for *Fix6U/N*). However, the quality of the results stays low compared to *VarN*, and even to *Fix6U/N* and *Fix3U/N*. *VarN* seems a much more stable and effective strategy for the buyer.

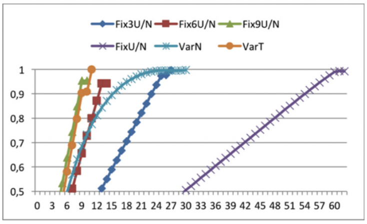


Fig. 3. Evolution of the Utility Proportion value at each round – NbSuppliers = 1000 (20 runs)

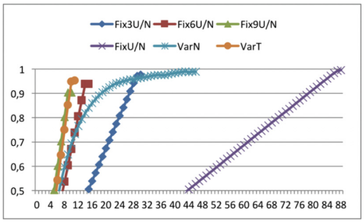


Fig. 4. For each strategy, evolution of the Utility Proportion value at each round – NbProposals = 10,000 (20 runs)

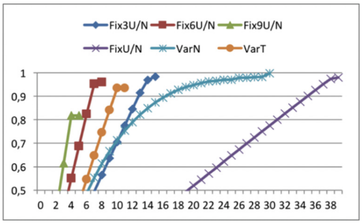


Fig. 5. For each strategy, evolution of the Utility Proportion value at each round with standard settings except MaxSteps = 50 (20 runs)

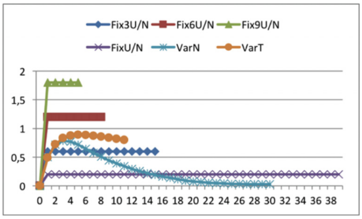


Fig. 6. For each strategy, evolution of the increment value (increase of the Reservation Utility requested by the buyer) at each round with standard settings except MaxSteps = 50 (20 runs)

To refine the analysis of the strategy, we studied the auction results for different values of the alpha parameter (for strategy *VarN*). The *UtilityProportion* graphs are represented in Fig. 7 and the *Epsilon* values in Fig. 8. High values of alpha give more prudent strategies, with a slower increase of the bids at the beginning, whereas low values provide a very quick adaptation to the number of remaining bidders.

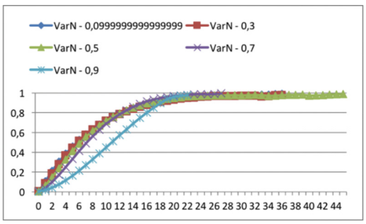


Fig. 7. For the VarN buyer strategy, evolution of the UtilityProportion value at each round with standard settings except alpha between 0.1 and 0.9 (20 runs)

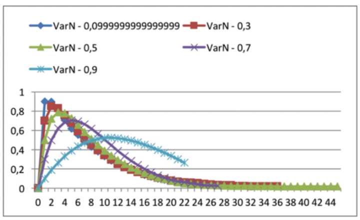


Fig. 8. For the VarN buyer strategy, evolution of the Epsilon value at each step of the negotiation with standard settings except alpha between 0.1 and 0.9 (20 runs)

6 Conclusion

We place our research in the field of reverse auctions that involve one buyer or auctioneer negotiating with multiple bidders or suppliers. Reverse auctions gained popularity as a result of the emergence of Internet-based auction tools. They aim to assist the human buyer in choosing a product.

In this paper, we have presented adaptive counterproposal strategies (that adapt the bid increment during the auction process), as opposed to classical auction models (where the bid increment is fixed before the process begins and is kept the same during the process). We have conducted an empirical study to validate the presented strategies. We argue that a variable increment, depending on the remaining time or the number of remaining buyers, should speed the auction process and give better results.

We also showed that a variable increment based on exponential smoothing decreases the auction-process duration compared to a classical approach with a fixed increment. Furthermore, a variable increment enables a solution to be found where the winning-bid utility is closer to the buyer aspiration point.

More research has to be done in several directions: (1) extending the model to other multicriteria models; (2) generalizing our results to other types of ascending as well as descending auctions; and (3) taking into account different buyer behaviours such as optimism, risk aversion, tolerance of ambiguity, cognitive complexity, and other cognitive scores.

References

1. Amouroux, E., Chu, T.-Q., Boucher, A., Drogoul, A.: Gama: an environment for implementing and running spatially explicit multi-agent simulations. In: PRIMA, pp. 359–371 (2007)
2. Asker, J., Cantillon, E.: Properties of scoring auctions. RAND Journal of Economics **39**(1), 69–85 (2008)
3. Bellantuono, N., Ettorre, D., Kersten, G.E., Pontrandolfo, P.: Multi-attribute auction and negotiation for e-Procurement of logistics. Group Decision and Negotiation **23**(3), 421–441 (2014)
4. Bellosta, M.J., Brigui-Chtioui, I., Kornman, S., Vanderpooten, D.: A multicriteria model for electronic auctions. In: 19th ACM Symposium on Applied Computing (SAC'04), pp. 759–765. Nicosia, Cyprus (2004)
5. Bichler, M.: An experimental analysis of multi-attribute auctions. Decision Support Systems **29**, 249–268 (2001)
6. Brigui-Chtioui, I., Pinson, S.: Progress in Artificial economics, Chapter, Chapter: 'A Variable Bid Increment Algorithm for Reverse English auction'. Lecture Notes in Economics and Mathematical Systems, vol. 645, Part 2, pp. 41–51. Springer (2010)
7. Kersten, G.: Seller-determined two-attribute reverse auctions: the case of linear utilities. In: 49th Hawaii International Conference on System Sciences (HICSS), pp. 406–413 (2016)
8. McAfee, R.P., McMillan, J.: Auctions and bidding. Journal of Economic Literature **25**, 699–738 (1987)
9. Pham, L., Teich, J., Wallenius, H., Wallenius, J.: Multi-attribute online reverse auctions: recent research trends. European Journal of Operational Research **242**, 1–9 (2015)
10. Qian, C., Anderson, E.: Buyer's optimal information revelation strategy in procurement auctions. European Journal of Operational Research **283**(3), 1011–1025 (2020)

11. Strecker, S.: Information revelation in multiattribute English auctions: A laboratory study. Decision Support Systems **49**(3), 272–280 (2010)
12. Teich, J., Wallenius, H., Wallenius, J.: Multiple-issue auction and market algorithms for the world wide web. Decision Support Systems **26**, 49–66 (1999)
13. Wurman, P.R., Wellman, M.P., Walsh, W.E.: Specifying rules for electronic auctions. AI Magazine **23**(3), 15–23 (2002)

Crowd Management System Based on Hybrid Combination of LSTM and CNN

Neeraj Kumar Sharma(✉), G. V. Arun Krishna, V. Bharath Kumar, T. Sai Praveen Kumar, C. H. Rakesh, and Ram Chandra Reddy

Department of Computer Science and Engineering, SRM University, Amaravati, AP, India
neeraj16ks@gmail.com, {ganugapati_venkata,vajinepalli_bharath, praveenkumar_s,chunchu_rakesh}@srmap.edu.in

Abstract. Automatic recognition of violence and nonviolence activities in the crowd management system is a broad area of interest in today's scenario. In this paper, we propose a hybrid combination of the Convolution Neural Networks (CNNs), and Long Short-Term Memory (LSTM) model to recognize violence/nonviolence activities in a crowded area. In the proposed approach a stream of video is applied to a pretrained Darknet-19 network, then a CNN with LSTM network is used to extract spatial and temporal features from the video. In the end, these spatial features are applied to a fully connected layer to identify the violence/nonviolence condition. The experimental results show that 98.1% accuracy was achieved in the case of video, and 97.8% accuracy was achieved in the case of the image frame by our proposed violence/nonviolence detection model.

Keywords: Convolutional Neural Network (CNN) · Long Short-Term Memory (LSTM) · Spatial-temporal features · Crowd behavior · Malicious activity · Optical flow · Darknet-19

1 Introduction

In today's scenario, security is a major concern in a crowded area, there are so many harmful activities such as pickpocketing, fighting, kidnapping, etc. we experience in our day-to-day life. To recognize such types of activities by human effort is not possible in a crowded area. Therefore, to ensure public safety there is a need to design and develop an automated system that identifies the violence/nonviolence activities with good accuracy. The proposed system identifies various suspicious activities that happen in a crowded place. Crowd gathering can be categorized into different categories such as protest, entertainment, marriage, and so on. Therefore, the crowd behavior prediction techniques are important for observing and tracking the emergency that occurs in crowded places, which includes sports stadiums, open-air concerts, roadways, and pilgrimages.

The key challenges to analyzing the normal and abnormal scenes from the video data set of the crowded area are dealing with uncertainties and crowd density [1]. A maximum number of crowd management techniques use low-level visual features for the analysis and modeling of crowd behavior [2]. But in the real condition, the crowd

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 185–194, 2023.
https://doi.org/10.1007/978-3-031-13150-9_17

behavior is a very complex task and, it depends on highly ambiguous features at the semantic level. Thus, the low-level features are not sufficient to define the high-level diverse behaviors. Therefore, detecting crowd behavior in addition to visual clues, by identifying personality traits is also very helpful in bridging the linguistic gap between high-level and low-level crowd behaviors [3]. Hence, in our proposed work, we are bridging this gap by classifying crowd behavior based on personality traits.

Fortunately, currently raised deep learning techniques can detect anomalies automatically [4]. These anomaly detection techniques are faster and can be used as preprocessing to filter out normal surveillance videos. Further, these anomaly video sets analyze the movements of the crowded people by other highly accurate algorithms. The key motivation to use the combination of the CNN-LSTM model is to detect the uploaded video in a better way, and by the hybrid combination of these two deep learning models, we can easily extract the required part from the video. Further, violence/nonviolence detection in a video is related to the spatiotemporal features classification problem. Once a model can recognize the spatiotemporal features in the video correctly it will be easy to classify the violence/nonviolence activity. In short, the overall idea of the proposed work in this paper is to detect the violence in the given videos. First of all, the input video is converted into the frames, and then a stream of frames is applied to the pretrained Darknet-19 network then a CNN with LSTM networks is used to extract the spatial-temporal features from the video. In the end, these spatial features are applied to a fully connected layer to identify the violence/nonviolence condition. A hybrid combination of CNN and LSTM algorithms is applied to classify the video in violence or nonviolence categories. In our proposed method two CNNs are used, one is for the temporal feature extraction and another one which learns from the optical flow vectors of multiple frames. Since only one node is used as output, it gives True or False.

The remaining sections of the research paper are organized as follows. Section 2 describes a literature review of the related research work. The proposed hybrid combination of the CNN + LSTM network is described in Sect. 3. Experimental setup and analysis of results are discussed in Sect. 4. Section 5 highlights the conclusion and future works of malicious activity detection in crowded areas using deep learning.

2 Related Work

Abnormal activities can be categorized into several types such as one to one person violence, family violence, violence with guns, crowd violence, sports violence, and many more. The related work w.r.t. crowd management, violence/nonviolence activity detection is described as follows.

D. Jackson et al. [5], proposed an LSTM based real-time violence detection system for the football match. In their proposed work author implemented a Bidirectional LSTM network for violence detection. The 94.5% accuracy was achieved by the author using Bidirectional LSTM for crowd analysis. The key limitation of the proposed work is that a Bidirectional LSTM requires a lot of computational time to train the model.

Ding et al. [6] built a Support Vector Machine (SVM) based violence detection system. In their proposed violence detection model author used four different types of features. It includes audio features, attribute features, trajectory-based motion features, and spatial-temporal interest points (STIP). The Spatial-Temporal Interest Points algorithm has been used to present the interest points in temporal and spatial dimensions. The audio from each of the video datasets has been taken as one of the features. Classification is done completely using the Support Vector Machine (SVM). 68.2% accuracy achieved by the proposed model. The key limitation of the proposed model is that the classification accuracy achieved by the model is very low.

Table 1. Summarization of the existing work

Sr. No	Author	Proposed work	Limitations /Merits
1	Ullah et al. [7]	By comparative analysis and final prediction made, the sliding window performs better as compared to SVM. OPENVINO toolkit is used to optimize the model and to increase the performance of the system	The accuracy of the proposed work was low 80.2%
2	Sudhakaran et al. [8]	A network trained to model changes in frames performs better than a network trained using frames as inputs and comparative study between the traditional fully connected LSTM and Conv LSTM	The author performed a comparative study between fully connected LSTM and Conv LSTM
3	Khaleghi et al. [9]	The proposed methodology consists of three main components to detect normal and abnormal incidents. The first component is pre-processing which is used to estimate and remove the background that eliminates computing cost and time. The second component is the feature extraction and learning component	To evaluate the system, the famous UCSD dataset is used for anomaly detection

To adopt features and multi-classifier combinations. This model applied its models on two public video datasets and obtained a great result. They figured out that, a great accuracy was obtained by applying ViF and OViF together which rates 94.84 percentage. Table 1 summarizes the existing work on the crowed analysis. On other hand, some researchers [15] focused on abnormal behavior detection, which is not well studied, as only action recognition usually focuses on detecting simpler actions. Thoroughly, they used a well-known framework, which is a bag of words and two action descriptors, they used STIP and MoSIFT in their model. They also made a big video dataset which consists of 1,000 video datasets of two categories, violence, and non-violence. By applying this model, they obtain 90% accuracy.

3 Proposed Work

Since the proposed violence/nonviolence detection system is based on the hybrid combination of CNN and LSTM deep neural networks. Therefore, before going to describe the proposed architecture of violence/nonviolence detection in the crowded area, the basics of the CNN and LSTM network are described as follows:

(A) Convolutional Neural Networks (CNN): Figure 1 shows the architecture of a CNN [14]. A CNN deals with higher dimensional unstructured data such as image/video datasets. It is useful in different applications such as image recognition and video recognition etc. CNN is specially designed to process the pixel data. The first layer in the CNN is the convolution layer which is the primary building block of CNN. It extracts the high-level features from the input signal. The next following layer is the pooling layer which is used for dimensionality reduction and to select the most significant features. The pooling operations are fixed according to their applications. There are different types of pooling that can be possible such as max-pooling, min-pooling, and the average pooling. Further, after extracting the features from the pooling layer, these features are fed to the completely connected layer which consists of an activation function.

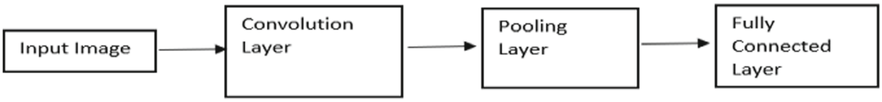


Fig. 1. The architecture of Convolution Neural Network.

(B) Bi-directional Long Short-Term Memory (LSTM): Figure 2 shows the Bi-directional LSTM [10] which is designed to recognize the pattern in a sequence of data. The Bi-directional LSTM consists of two layers of LSTM. In the first LSTM, the input data is applied from the left to right direction, and in the second LSTM, the sequential data is applied from right to left. Hence, by this way the predicted out by a layer of the LSTM depends on all the words in the sequential data. Bi-directional LSTM gives more accuracy as compared to the normal LSTM because two layers of LSTM consider all complete sentences. The Bi-directional LSTM is useful to solve a wide variety of problems such as predicting sales to find the patterns in the stock market, from understanding movie plots to recognizing the way of speech, from the translations to predicting our next word on your phone keyboard. Long Short-Term has an edge over conventional feed-forward neural networks and RNN in many ways. Such that, this is for their property of selective remembering patterns for some duration of time [13].

(C) Proposed CNN+LSTM Architecture: The architecture of proposed hybrid of CNN and LSTM algorithm is described in Fig. 3. In the proposed architecture our key

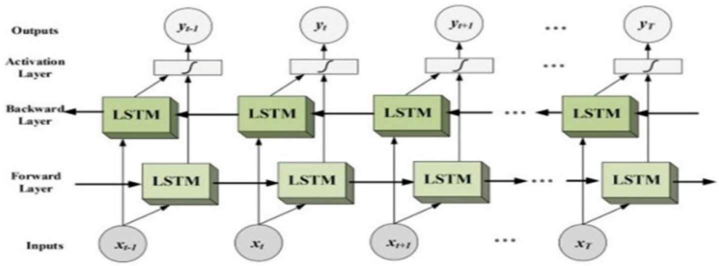


Fig. 2. Architecture of Bi-directional LSTM.

task is two identify or capture the temporal patterns of the violence/nonviolence conditions. Both the violence/nonviolence patterns occur at different resolutions by leveraging the visual patterns from different levels. First of all the input frames are applied to the CNN. The CNN consists of 3 convolution and 3 pooling operations in the overlapped manner. At the end of the last pooling operation, the output of the CNN is converted into a vector. Further, this vector is applied to a Bi-directional LSTM network. The Bidirectional LSTM network consists of two layers of LSTM. The output of a Bidirectional network is further applied to a fully connected layer, at the end the output layer classified the input frame into violence or nonviolence class. In addition to summing the (LSTM) which is supposed to show the global temporal features, after the Convolutional Neural Network (CNN), the temporal features (local) can be obtained from the optical flow. In the proposed model both the CNN and LSTM networks are combined to get a better result. In this work, the effect of the optical flow is supposed to be copied by taking two video frames as input. Then the taken input frames are processed by the pre-trained CNN. The frame outputs from the bottom layers from the pre-trained model are connected in the last channel into the additional CNN (shown by orange color in Fig. 2. Now the output from the additional CNN is then concatenated and passed to a fully connected layer and the LSTM cell to learn the global temporal features. Finally, the outputs of the LSTM cell are classified by a layer that contains two neurons to represent the two categories which are Violence and Non-violence respectively.

The network architecture of the proposed model is shown in Fig. 3. In Fig. 3 it is shown that in addition to adding the Long Short-Term Memory (which is supposed to extract the temporal features) after the CNN, the temporal features (local) that can be obtained from the optical flow is also important. Further, it has been reported that the virtue of optical flow is due to its invariance in appearance as well as they are accurate at the boundaries and at the small displacements. Therefore, in the proposed work, the effect of optical flow is supposed by taking two video frames as input. The input frames are processed by the pre-trained CNN.

The frame outputs from the lower layer of the pre-trained model are concatenated in the last channel and then fed into the additional CNN (labeled by orange color in Figure). Since the outputs from the lower layer are regarded as the low-level features, the additional CNN is supposed to learn the motion features as well as the appearance of invariant features by comparing the frame feature map. The frame output from the top layer of the pre-trained network is also merged and fed into the other additional

CNN to compare the high-level features of the frame. The output from the additional CNN is concatenated and passed to a completely connected layer and the LSTM cell to learn the global temporal features. Finally, the output of the LSTM cell is classified by a completely connected layer which contained two neurons that represent the two categories (Violence and Non-violence), respectively.

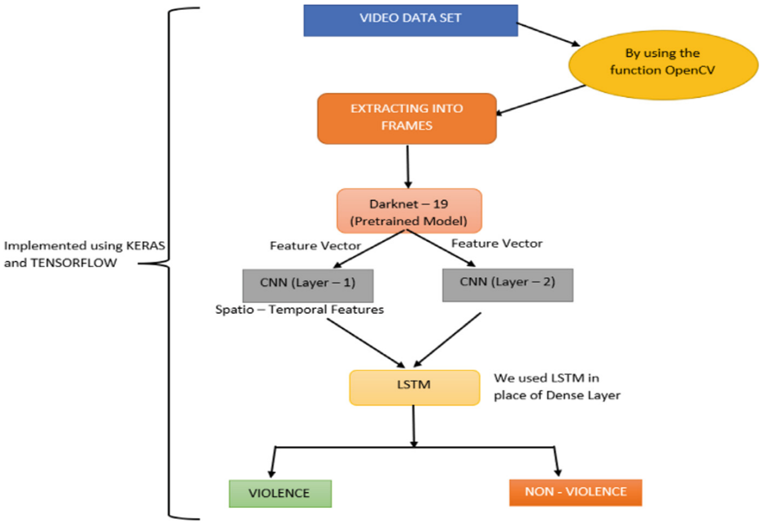


Fig. 3. The proposed network architecture.

The layers that labeled in orange color are pre-trained on the ImageNet dataset and are frozen during training. The layers that are labeled in orange color are trained for the video dataset. The pre-trained model is implemented by Darknet19 [1] due to its accuracy on ImageNet and the above real-time performance. Where the previous work that uses darknet-19 concludes that there are some localization errors, Darknet 19 struggles with small objects that appear in groups. It also struggles to generalize to objects in new or unusual aspect ratios or configurations. Our proposed model overcomes localization errors by using multi-scale training the model can learn to generalize and detect objects with different aspect ratios or configurations. Since the Darknet19 already contains 19 convolutional layers, to avoid the degradation problem, the additional CNN are implemented by the residual layers.

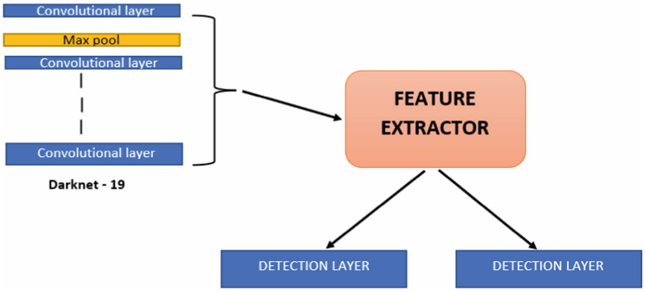


Fig.4. Architecture of Darknet – 19

As shown in Fig. 4 the output from the pretrained darknet – 19 model is feature vectors which will be given as input to the two CNN layers. In our proposed work we removed the output layer of the darknet 19, and a set of feature vectors generated by the darknet 19 is further applied to the two CNN.

(D) Performance Measurement: To check the performance of the proposed hybrid model for violence/nonviolence detection in the crowded area we calculate the accuracy of the proposed model. The accuracy of the proposed model is described in Eq. 1.

$$Accuracy\ (\%) = \left(\frac{T_P + T_N}{T_P + T_N + F_P + F}\right) \tag{1}$$

where True positive (T_P) represents violence action is classified as violence by the classifier; False negative (F_N) represents the violence action is classified as non-violence: False positive (F_P) corresponds to the classification of non-violence action as violence and True negative (T_N) represents the non-violence action classified as non-violence.

4 Experimental Setup and Result Analysis

(a) Experimental Setup: To check the performance of our proposed hybrid approach of LSTM and CNN, we used python 3.9. The key motivation to use the python 3.9 language is because python is simple and easy to implement the deep neural networks, and it also provides different useful libraries such as TensorFlow, Keras, Pytorch, Pandas to implement the deep learning models. Further, we used a video data set [11] which contains a total set of 300 videos which are separated by two categories that are violence and nonviolence both containing 150 each, all the 300 video clips we used to train and test the model. The training part consists of 80% and the testing part consists of 20% of the 300 videos. In our experimental work, we used different python libraries such as TensorFlow, Open cv, SK- video, Scikit-image, and Jupiter notebook as a python IDE. The experiment was performed on a system, which consist of 8 GB RAM, 440 GB hard disk with Windows operating system. The proposed work consists of two phases for the violence/nonviolence detection such as training and testing phases. In the training phase, we trained our proposed hybrid model by the training videos, and in the testing phase, we check the accuracy of the proposed model by applying testing videos. The detailed description of the training and testing phases are described as follows.

1. Downloaded the fight/non-fight dataset and separated into different directories.
2. Make the data catalogs which will tell the data manager where to load the videos and set the variables to fit your environment.
3. We used the network which is based on the pretrained Darknet19. The checkpoint of such model is converted from the Darknet format to the TensorFlow format using Dark flow.
4. Then by executing the Train.py file we are successfully trained the model.
5. By executing the Deploy.py file we will get the output. We need to give the input video path as an argument and as a result, we will get the output video frame with detection of violence if present.

(b) Performance Evaluation: The output of the proposed hybrid model describes whether either there is violence involved or not in the given input video. To check the superiority of the proposed CNN LSTM based hybrid model for violence/nonviolence detection we compared our model with other existing state-of-the-art violence/nonviolence detection models. Further, to check the frame-level result, we classified the video data sets into a particular category if and only if a number of constant signals of such particular category is greater than a certain threshold. That threshold can be derived by scanning the threshold from 0 to the length of the video and seeing which threshold yields the best accuracy in the validation set, as shown in Fig. 5. The small one will be chosen if there are multiple thresholds that can yield the same accuracy.

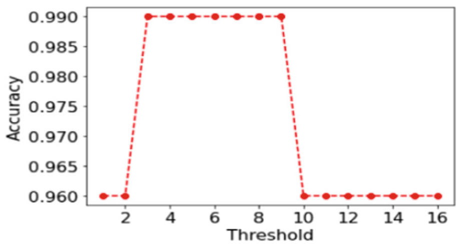


Fig.5. Threshold-accuracy

In the above diagram, the horizontal axis indicates the threshold of the number of continuous frames that has the positive signal, and the vertical axis indicates the accuracy at such threshold in the validation set. The thresholds start from 3 to 9 are all yield the best accuracy. The smallest threshold is chosen so that we can get continuous false positive in the test set could be reflected by this metric. We had chosen this threshold as in the previous paper [12] the smallest threshold (i.e. threshold = 3) is chosen so that the continuous false positive in the test set could be reflected by this metric. The Hockey dataset [11] planned by Bermejo has fighting clips and non-fighting clips from the hockey game, and we have a tendency to take a hundred video clips for the validation The results are shown within the Table 2. One will see that the planned technique during this work outperforms different progressive ways.

It has been reported that the single frame models already have a strong performance. This may be due to the fact that several categories in the video classification task can be recognized by the scene or the background in the videos. It is not necessary to learn the motion features of the moving objects for the network. However, to compare the present proposed model with the previous single-frame model, a simple single-frame network has also been proposed. The result of the comparison is shown in below Table 2. In Table 2 we can see that the frame accuracy and video accuracies are 97.81% and 98.50% respectively, which is high as compared to existing Darknet19 architecture.

Table 2. Single frame baseline comparison with the proposed model

Method	Threshold	Frame accuracy	Video accuracy
Darknet19 + 3FC	14	93.77%	96.00%
Darknet19 + CNN + LSTM (Our proposed)	3	97.81%	98.50%

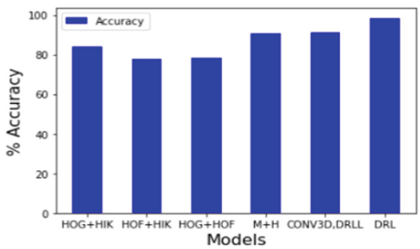


Fig. 6. Accuracy of different models.

Figure 6 shows the accuracy of the proposed hybrid model with other state-of-the art existing models such as HOG + HIK, HOF + HIK, HOG + HOF, M + H, CONV3D, and DRL. As we can see in Fig. 6 the highest amount of accuracy which is 98.5% achieved by our proposed hybrid model w.r.t. violence/nonviolence detection in the crowded dataset.

5 Conclusion and Future Work

In this paper, we design and develop a hybrid model using CNN and LSTM for violence/nonviolence detection in the crowded place. The proposed model is useful for detecting suspicious activities like violence, fights etc., it can be able to detect the nonviolence aspects from the given glimpse of some situation which is recorded in surveillance footage or by any other handy devices. The proposed hybrid model achieved 97.81% as a frame accuracy and 98.50% as a video accuracy in terms of violence detection. The future direction of the proposed work is to design and develop an IOT device using cloud/fog as a real time crowed management system.

References

1. Yogameena, B., Nagananthini, C.: Computer vision-based crowd disaster avoidance system: a survey. Int. J. Disaster Risk Redact. **22**, 95–129 (2017)
2. Dupont, C., Tobias, L., Luvison, B.: Crowd-11: a dataset for fine grained crowd behavior analysis. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, pp. 9–16 (2017)
3. Sultani, W., et al.: Real-world anomaly detection in surveillance videos. In: 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 6479–6488 (2018)
4. Aktı, Ş., Tataroğlu, G.A., Ekenel, H.K.: Vision-based fight detection from surveillance cameras. In: IEEE/EURASIP 9th International Conference on Image Processing Theory, Tools and Applications, Istanbul, Turkey, Vols. Volume - 1, pp. 150–169 (2019)
5. Fenil, E., Manogaran, G., Vivekananda, G.N., Thanjaivadivel, T., Jeeva, S., Ahilan, A.J.C.N.: Real time violence detection framework for football stadium comprising of big data analysis and deep learning through bidirectional LSTM. Comput. Netw. **151**, 191–200 (2019)
6. Ding, C., Fan, S., Zhu, M., Feng, W., Jia, B.: Violence detection in video by using 3D convolutional neural networks. In: Bebis, G., et al. (eds.) ISVC 2014. LNCS, vol. 8888, pp. 551–558. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-14364-4_53
7. Ullah, F.U.M., Ullah, A., Muhammad, K., Haq, I.U., Baik, S.W.: Violence detection using spatiotemporal features with 3d convolutional neural network. Sensors **19**, 2472 (2019). https://doi.org/10.3390/s19112472
8. Sudhakaran, S., Lanz, O.: Learning to detect violent videos using convolutional long short-term memory. In: 2017 14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), pp. 1–6 (2017)
9. Khaleghi, A., Moin, M.S.: Improved anomaly detection in surveillance videos based on a deep learning method. In: 2018 8th Conference of AI & Robotics and 10th RoboCup Iran open International Symposium (IRANOPEN), pp. 73–81 (2018)
10. Analytics Vidya- Link. https://medium.com/analytics-vidhya/what-does-it-mean-by-bidirectional-lstm-63d6838e34d9)
11. https://www.kaggle.com/yassershrief/hockey-fight-vidoes
12. http://joshua-p-r-pan.blogspot.com/2018/05/violence-detection-by-cnn-lstm.html
13. Zheng, H., Lin, F., Feng, X., Chen, Y.: A hybrid deep learning model with attention-based Conv-LSTM networks for short-term traffic flow prediction. IEEE Trans. Intell. Transp. Syst. **22**(11), 6910–6920 (2021)
14. Alotaibi, R., Alzahrani, B., Wang, R., Alafif, T., Barnawi, A., Hu, L.: Performance comparison and analysis for large-scale crowd counting based on convolutional neural networks. IEEE Access **8**, 204425–204432 (2020)
15. Vasavi, S., Priyadarshini, N.K., Harshavaradhan, K.: Invariant feature-based Darknet architecture for moving object classification. IEEE Sens. J. **21**(10), 11417–11426 (2021). https://doi.org/10.1109/JSEN.2020.3007883

Facial Liveness Detection in Biometrics: A Multivocal Literature Review

Kikelomo A. Omotoye[1], Sanjay Misra[2](✉), Manju Kaushik[3], Roseline Ogundokun[4], and Lalit Garg[5]

[1] Covenant University, Otta, Nigeria
kikelomo.omotoyepgs@stu.cu.edu.ng
[2] Ostfold University College, Halden, Norway
sanjay.misra@hiof.no
[3] Amity University, Rajasthan, India
mkaushik@jpr.amity.edu
[4] Kaunas University of Technology, Kaunas, Lithuania
[5] University of Malta, Msida, Malta

Abstract. The science and technology of monitoring and analyzing biological data is known as biometrics. Biometrics refers to technologies that measure and analyze human bodily characteristics for authentication purposes, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements. The discipline of biometric has grown tremendously. Biometrics is a technique for identifying persons based on their physical and behavioral characteristics. Biometric solutions have been increasingly popular in recent years as a way to mitigate the weaknesses in knowledge-based identity data. Vendors have built systems that recognize behavioral aspects, and have offered additional features such as liveness detection and the accompanying security processing, in addition to using physical biometrics such as fingerprints, faces, and palms. The aim of this study is to know what liveness facial detection is about, examine its importance, as well as the advantages and limitations of certain existing types of biometric using Multivocal Literature Review (MLR). In the context of healthcare, the integration of biometric and information systems has resulted in a novel strategy to reducing patient identity fraud, improving user experience, and improving patient medical care by using historical data. Finally, future work can focus on exploring the importance of liveness detection for voice biometrics on smart devices.

Keywords: Biometric · Liveness · Facial detection · Multivocal Literature Review

1 Introduction

Biometric comes from the Greek words “bios” (life) and “metrein” (measurement) (to measure). As the name implies, it deals with determining life-related factors—parameters that are unique to each individual, allowing them to be identified with certainty.[1] Biometric has become a well-known subject of study in the last ten years. Biometric-based solutions have made a niche for themselves in an era when customers want faultless

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 195–209, 2023.
https://doi.org/10.1007/978-3-031-13150-9_18

security measures that are simple, convenient and user friendly. Biometric systems are a collection of technologies and methods for detecting and identifying human documentation based on physiological and behavioral features. One of the most significant advantages of biometric technology is that the identities developed cannot be transferred or purchased, and they are extremely difficult to fabricate or copy. Biometric identifiers, unlike other access control methods, cannot be forgotten or stolen; for example, passwords are readily forgotten, and keys and cards may be simply lost or taken from us by force; however biometric features can easily and securely sustain our connectivity with internet of things (IoT). Biometric has the following benefits over traditional identifying techniques such as passwords or IDs: "cannot be transmitted", "cannot be stolen", "cannot be lost or forgotten", "cannot be cracked", and "cannot be guessed" [2]. Biometric solutions have been increasingly popular in recent years as a way to mitigate the weaknesses in knowledge-based identity data. Vendors have built systems that recognize behavioral attributes, and have offered additional features such as liveness detection and the accompanying security processing, in addition to using physical biometric such as fingerprints, faces, and palms [3]. A biometric system can function in either verification or identification mode as shown in Fig. 1, depending on the application context:

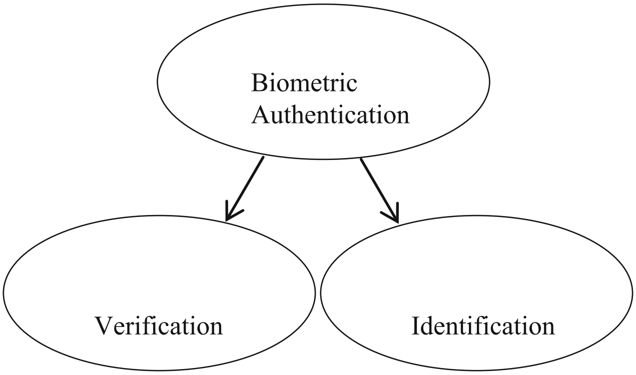


Fig. 1. Basic modes of a biometric system

Enrollment mode in Fig. 2, is common to verification and identification mode [4] where a biometric scanner captures a user's biometric information and stores it in a database template. To enable authentication, the user's identity is kept in the stored template.

The term "enrollment" refers to the first time a feature "sample" is entered into the database. The feature sample is referred to as the "template" for the individual to whom it refers once it has been entered into the database and maybe associated with an identity by external information (supplied by the enrollee or others). The pattern matching mechanism compares a supplied feature sample to a stored template and sends a quantitative measure of the comparison to the decision subsystem. The pattern matching procedure can be bypassed in this application [5].

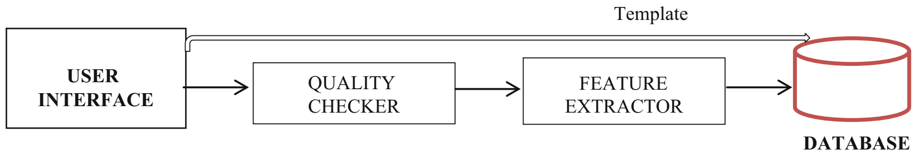


Fig. 2. Enrolment mode

Biometric verification (Fig. 3) is the process of automatically verifying a person's identity using biometric features derived from physiological and behavioral factors. Traditional methods that use a card or a password have less ability to consistently discriminate between an authorized person and an imposter than biometric verification systems. A person could be recognized in biometrics based on who he or she is rather than what they have (ID card) or what they know (password). Biometrics are being used in ATMs, computers, security systems, mobile phones, credit cards, health care, and social services [6]. Positive recognition is frequently used in the verification mode, "where the goal is to prevent numerous people from utilizing the same identity." Patients that visit hospitals present different forms of ID to doctors so their identity can be determined before they are being attended to. If a patient is brought to the hospital in an unconscious state, the doctor gives them a name pending the time their true identity is known. In this circumstance, having a biometric technology that can identify patients and allow medical personnel to identify the unconscious person more quickly would be beneficial [7].

Identity verification is used for positive recognition, with the goal of preventing numerous people from using the same identity [4]. While biometric data and authentication are being more widely used in all aspects of modern life, concerns about the safety and privacy of users/consumers who provide biometric inputs to corporations and governments, as well as the objectives for which they are used, have arisen.

A matching module in biometric verification systems generally measures the similarity (or dissimilarity) between the feature representation acquired from the 'live' biometric sample (the probing sample) and the template of a particular identity stored in the systems database [8].

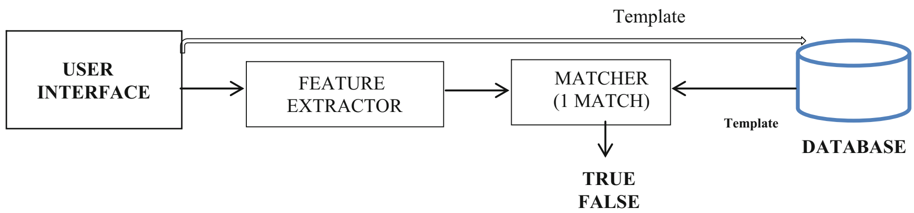


Fig. 3. Verification mode

In recent years, there has been a lot of discussion about using biometrics instead of passwords in authentication systems. Individuals are labeled and described using biometric identifiers, which are unique, measurable features [9]. The user's biometric information is acquired by the sensor in the identification mode (Fig. 4); however, unlike the verification mode, a one-to-many evaluation is performed with biometric templates from the database to establish the identity of an unknown user. A match is found during the evaluation if the system successfully identifies the person based on the biometric template in the database and the assessment falls within a previously established threshold [7, 10].

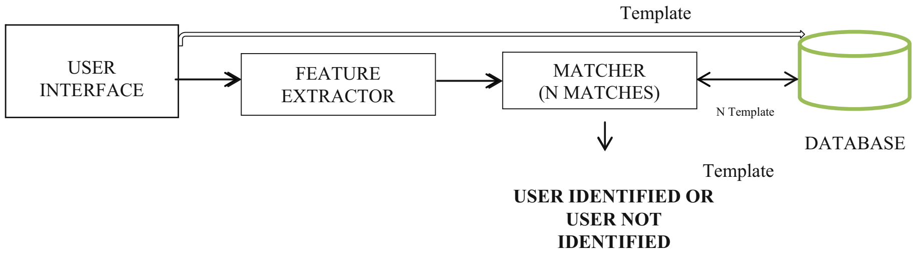


Fig. 4. Identification mode

2 Background

2.1 Biometric

The biometric recognition method was initially mentioned in the 14th century. Joao de Barros, a European explorer, was first to document the use of biometric recognition technologies. He witnessed Chinese shopkeepers taking children's fingerprints for identification using ink. Biometric recognition systems, such as fingerprinting, are a sort of biometric recognition system. Juan Vucetich began collecting fingerprints of convicts in Argentina in 1881 [11].Recently, the most often used system is fingerprint recognition. It has mostly supplanted traditional recognition mechanisms such as pins, passwords, and the like. However, facial recognition is rapidly catching up. Facial recognition technologies are projected to become more popular as artificial intelligence improves. The Artificial intelligence algorithms will soon aid in the advancement of facial recognition systems [12].

Many alternative presentation attack detection (PAD) approaches and strategies can be used to detect presentation attacks. Basically, these attacks are captured either through a whole-system monitoring method or through the addition of features to the data capture subsystem that is integrated into a biometric system. Liveness detection is one of the most commonly utilized PAD techniques. The purpose of liveness detection is to identify whether a biometric probe (for example, a fingerprint) belongs to a living person who is present at the time of biometric collection [13]. The usage of biometrics is becoming more diverse, in line with the development of cloud infrastructures and security regulations [14].

Types of Biometric Systems
Because each biometric system has its own set of advantages and disadvantages, choosing which biometric system to use for a certain authentication application is based on the application's requirements. A variety of biometric technologies have been proposed for authentication reasons. Traditionally, they are classified into two groups: physiological and behavioral characteristics (Fig. 5).

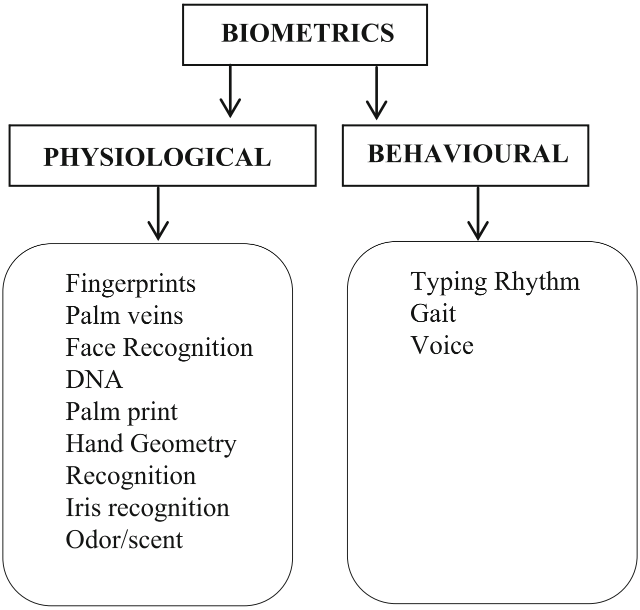


Fig. 5: Types of biometrics

Physiological Characteristics
Physiological characteristics refer to the qualities of a human body that do not alter with age [15]. The shape of the body influences physiological features. Fingerprints, palm veins, face recognition, DNA, palm print, hand geometry, recognition, iris recognition, and odor/scent; these are few of the many examples.

DNA
Deoxyribonucleic Acid, or DNA (Fig. 6), is a molecule that contains the biological instructions of living creatures. Nucleotides are chemical building units that make up DNA. A gene is a DNA sequence that carries information for creating a protein, whereas a genome is an organism's whole DNA instructions [16]. The use of this type of biometric has its limitation in healthcare and other field of use, they are: the information about a person's state of health to a certain disease can be retrieved from their DNA and such could lead to unequal treatment, it is very easy to collect a piece of the DNA without the person's awareness thereafter using it for dubious purposes, and the technology behind DNA matching requires rigorous chemical methods from an expert [4].

Fingerprint
Fingerprints (Fig. 5) are used for personal identification in humans and the matching accuracy has been seen to be very high. It is formed in the first seven month of a fetus and it is a pattern and ridges on the surface of a fingertip. It differs in two different people and cannot be the same [4]. Due to its originality, it is seen as one of the most trustworthy type of biometric for human recognition [16]. The disadvantage with its use is that it consumes lots of computational resources especially when used in identification mode [4].

Iris Recognition
Iris (Fig. 5) is a colorful ring that surrounds the pupil and is visible from the outside. It is stable throughout life; however, iris patterns are unique and not genetic, meaning that even parent and child iris patterns are expected to differ. The iris patterns of an individual's right and left eyes are different or non-matching. Around the pupil, there is a lot of irregularity in the iris patterns. In the NIR region, the pigmentation of the iris is undetectable at longer wavelengths. An individual's Iris pattern does not alter with age and has roughly 256 distinct traits [11].

Behavioral Characteristics
Identification methods based on behavior pay attention to a person's activities and allow the user to manage them. Biometrics based on these methods account for a large number of internal variables (mood, health condition), which is why they are only useful when used frequently [17]. These include typing rhythm, gait and voice etc.

Signature
Signatures are widely utilized in a variety of settings, including government and legal applications as well as commercial ones. Signature authentication might be static or dynamic in the past. Static signature authentication relies solely on the signatures' geometric features, whereas dynamic signature authentication incorporates not only those aspects but also additional data such as signature velocity, acceleration, pressure, and trajectory. A person has a distinguishing feature by the way the person signs his or her name. Signature changes over time and is influenced by a person's physical and mental states [4, 16].

Gait
Gait is all about the way a person walks and this behavioral characteristic changes due to increase in weight of a person over time. Gait-based systems are input intensive and computationally expensive since they employ video sequence footage of a walking human to measure numerous separate movements of each articulating joint [4].

Voice Recognition
Today, voice or speech recognition is a new biometric technology. It's been around for a while but has been gaining traction in recent years, particularly in applications that deal with financial transactions and call centers. Because no actual physiological or biological samples are collected or examined, it is also known as the 'Non-Biological Biometric.' Speaking and voice production is a crucial element of our lives that we take for granted, yet it is a very difficult process. Due to the generation of sounds, the actual voice sample produced from the user end originates at the level of the vocal chords [11].

Advantages of Biometric

Because biometric systems do not require users to remember passwords, they have several advantages over traditional authentication systems (password or PIN) [18]. This technology is its uniqueness, which is also the major feature that permits biometric technology to grow its importance in our lives. Because biometric technology is unique, each user's identification will be the single most effective identification for that user. In a biometric security technology system, the chance of two users having the same identification is not possible. The simplicity of having authentication mechanisms with a user is the best reason why biometric is becoming more popular and extensively utilized. We can't leave parts of our bodies at home alone, and we can't lease them out. We don't have to memorize fingerprints and change them every three months like we do with passwords. Until something is severed or damaged, biometric can last practically indefinitely [16, 19]. Biometric characteristics cannot be forgotten or lost (while password can). Its characteristics are harder to duplicate, share, and distribute (username and password can be announced on crackers' websites). Finally, they demand that the person who is being authenticated be present at the time and place of authentication [20].

Disadvantages of Biometric

Even though biometric security systems have a lot of advantages, they nonetheless have a lot of drawbacks. Every biometric application method contains flaws that can cause issues for consumers. For example, if the biometric security system employs fingerprints to identify its users and a user loses his or her finger as a result of an accident, the verification procedure may be hampered [16]. Misuse of information. Any identity registry, especially one that contains highly sensitive information, is vulnerable to abuse. Several examples of registry abuses may be found throughout history. Governing authorities have utilized identity registration to limit the mobility and liberty of sections of their populations even during times of peace. These dangers are enhanced when personal information is acquired and stored using electronic technologies (e.g., a database rather than a paper record) [21]. Software support for biometric hardware devices is another major difficulty in biometric implementation. However, this issue is progressively dissipating. Many individuals are still concerned about biometric technology in terms of security and adaptability to rate of change. Life changes, scalability, accuracy, privacy, and other factors are all factors to consider [19].

Another disadvantage is the high cost of implementation; it also necessitates more user expertise than simply utilizing the device. Biometrics will not work properly if they are exposed to the environment or if they are infected with a disease, because the higher the sensitivity, the greater the security, but it also implies that an authorized user may be refused incorrectly. Finally, biometrics is thought to be damaging to people's health due to the use of lasers, infrared, and other components in biometric technology [20].

Because of its speed, efficacy, and user friendliness, face recognition has progressively become a significant encryption and decryption method. Face recognition technology's security risks, on the other hand, are growing more significant. As a result, liveness detection has become a need, a crucial component of dependable authentication systems. Among the different biometric techniques, such as fingerprinting, iris scanning, and hand geometry, face recognition is the most efficient and commonly used. The rationale for this is that it is a natural, non-intrusive, and low-cost strategy. As a result, over the last decade, academics have created a number of recognition techniques. According to the face feature extraction approach, these strategies can be classified into two categories: methods that manually extract features based on classical machine learning and methods that automatically acquire face characteristics based on deep learning [22]. Differentiating the feature space into live and non-living is the act of liveness. Imposters will attempt to infiltrate the system using a huge quantity of forged biometrics. The performance of a biometric system improves with the help of liveness detection. It is a significant and difficult topic that determines the security of biometric systems against spoofing [23]. Another advantage of the passive method is that potential bad actors are unaware that a liveness check is taking place, making it difficult for them to figure out how to circumvent it. The current active solutions reveal the game's outcome. In a video replay assault or with deep fake screen images, it's all too easy to imitate blinking, smiling, and even moving your head from side to side.

3 Research Methodology

A Multivocal Literature Review (MLR) is a type of Systematic Literature Review (SLR) that incorporates both published (formal) and grey literature (e.g., blog posts, videos, and white papers, that is, journal and conference papers). MLRs are important for both researchers and practitioners since they summarize the state of the art and practice in a certain field. As more MLR studies are undertaken and reported, it is critical to have a set of rules in place to ensure that MLR methods and results are of high quality [24].

It will be good to ask research questions that would help in achieving the objectives of this review.

RQ$_1$: What is liveness biometric facial detection?
RQ$_2$: What are the methods used for facial detection?
RQ$_3$: What are the future trends?

Search Strategy and Data Source

This study's research methodology was built around a variety of search tactics, including sources, study selection, and selection execution. The essential data for the research was gathered via electronic libraries, specifically Google search and Google scholar [25]. Google and Google Scholar are the only search engines that provide results from the most popular academic publishers' predefined sources such as IEEE, Wiley, ACM, Springer, and Science Direct. The remaining data sets were gathered from grey literature, which included other databases, websites, catalogs, and Google provider reports.

The PRISMA flow chart, as shown in Fig. 6, depicts the systematic review process and the identification of relevant articles at various phases.

Search Term. Identifying search word(s) is the initial step in the search strategy. This was done by analyzing study questions and selecting broad keywords relating to the topic that is being reviewed. This will ensure that the majority of relevant works are included in the research. As a result, biometric, liveness, facial detection and facial recognition was the primary search words.

Search Process. This procedure is divided into four steps, each of which aids in the discovery of scientific primary research using a test-retest method. The scientific selection method enables primary research to be chosen from the scientific literature. The four steps are stated as follows:

Phase 1 (Initial Search): The search phrase was applied to each digital resource, with the purpose of finding all studies connected to the issue under consideration. Only the title, abstract, and keywords were searched.

Phase 2 (Removing duplicates): When duplicates of a paper are found, only the paper whose digital resource contains additional information about the paper, such as the abstract or full text of the paper were considered for the next stage of the selection process.

Phase 3 (First Selection Process): During this step, paper's title and abstract was scrutinized for inclusion and exclusion criteria. If a publication plainly fails to meet the inclusion and exclusion criteria, it will be categorized as a non-selected paper and will not be considered for the next stage of the selection process. If a publication meets the inclusion requirements but the information provided by the title and abstract is insufficient to make a decision, the publication will be classed as a possible selected paper and will be included in the next round of the review process.

Phase 4 (Second Selection Process): This phase was completed to ensure that the publication contains material that is relevant to the topic under consideration.

Search Criteria

The authors examined not only the relevancy of the studies when screening and selecting them, but also the contribution of the chosen study. The collection of papers that have been filtered using many criteria and concepts can be used to include and reject articles in any review. During the initial screening stage, authors simply read the titles and abstracts of candidate papers before deciding whether or not to include them in the review. If there is any dispute about the study's inclusion or exclusion, it is necessary to read the complete text of the publication. The technique for separating relevant items for the evaluation is made easier by establishing criteria for inclusion or exclusion from the start (Table 1). The primary criterion for study exclusion and inclusion was the degree to which the specified article was useful in answering the research questions. The articles were eliminated from the selection because they did not meet the eligibility requirements for inclusion [26].

To include and exclude publications, titles, abstracts, and keywords, as well as full-text reading were used as factors in achieving this. Titles, abstracts, and keywords were all subjected to inclusion and exclusion criteria by the writers. The following criteria were used to determine what to include and what to exclude:

- Studies are based on biometric
- Studies that look at liveness biometric facial detection
- Studies that highlight discussion on the features of facial detection
- Studies that emphasize the future trends of facial detection

When a study was ruled out, the following criteria were used:

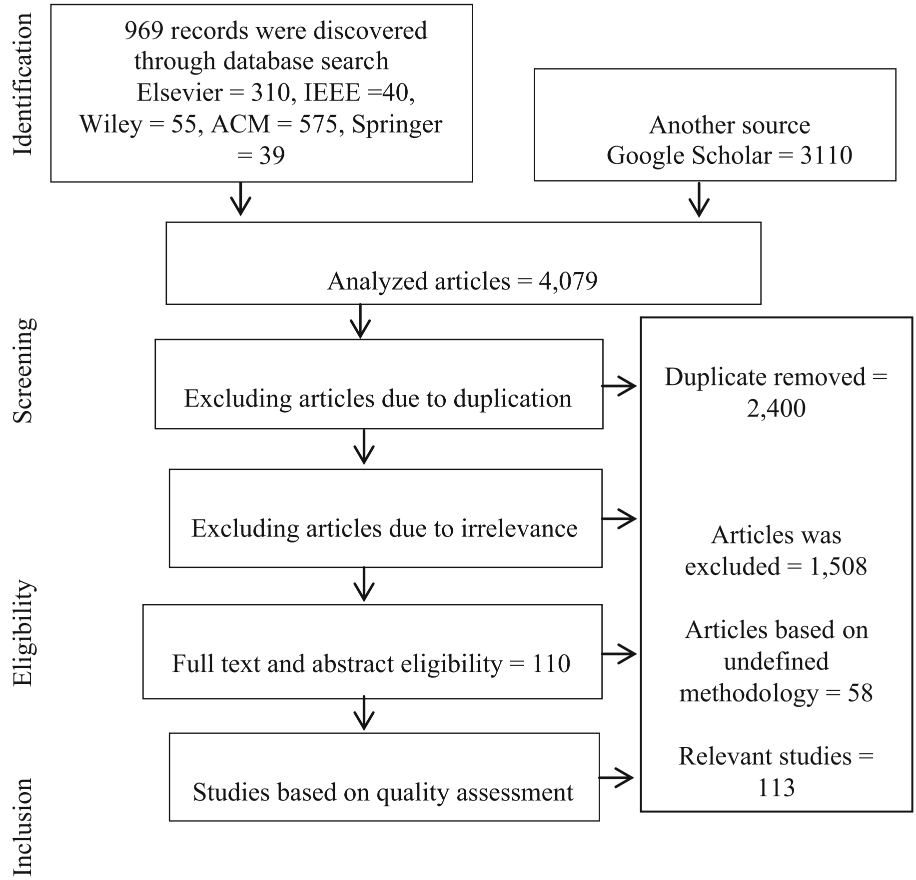


Fig. 6: PRISMA flow chart of study selection

- Studies provided in a language other than English
- Studies that isn't available in full text
- Literature or studies that are unrelated to the topic at hand
- Studies that have been done twice'

4 Result

The result of the MLR in relation to the research questions are provided below.

Facial Liveness Detection (**RQ**$_1$)

Human face detection means determining whether a given image or video contains face regions and, if so, determining the number, exact location, and size of all the faces. The accuracy and efficiency of face detection is critical to the performance of various face-based applications, ranging from traditional face recognition and verification to modern face clustering, tagging, and retrieval. Humans rely on their ability to detect

Table 1. Inclusion and exclusion criteria

Inclusion criteria	Exclusion criteria
Studies are based on biometric	Studies provided in a language other than English
Studies that look at liveness biometric facial detection	Studies that isn't available in full text
Studies that highlight discussion on the features of facial detection	Literature or studies that are unrelated to the topic at hand
Studies that emphasize the advantages of passive liveness facial detection	Studies that have been done twice

faces in a scene in their daily activities. As a result, automating this could be used in a variety of applications, including intelligent human-computer interfaces, content-based image retrieval, security, surveillance, gaze-based control, video conferencing, speech recognition assistance, video compression, and many others [27].

Face detection systems security is becoming increasingly critical as the technology gets more widely used. Fabricated faces, such as those found in fake images or video clips, can be used to fool face recognition software [28]. Face detection is the process of estimating the bounding-box of a face in a given image or video frame. If the images contain multiple faces, all of them are detected. Face detection should be resistant to differences in pose, illumination, and scale, and it should eliminate as much background as possible [29]. Attacks on the proper functioning of the biometric sensor in use are becoming more important due to the expanding use of biometric technology in numerous application scenarios ranging from border control to financial services [30]. Any attempt to tamper with a biometric system's intended function is referred to as a presentation-based attack. Spoofing is a presentation-based attack. Many alternative presentation attack detection (PAD) approaches and strategies can be used to detect presentation attacks. Basically, catching these attacks requires either a whole-system monitoring approach or the inclusion of new features to the data capture that is integrated into a biometric system [13]. There are various (facial detection) PAD approaches; some rely on hardware, while others do not; some still use photos, while others use video [31].

Liveness detection is one of the most commonly utilized PAD techniques. The goal of liveness detection is to determine whether a biometric probe (for example, a fingerprint) belongs to a living person who is present at the time of biometric collection. For example, liveness detection algorithms can be used to build a trustworthy recognition of dead fingers or photographed faces. As a result, the chances of a successful presentation attack are greatly lowered. As a result, in addition to routine biometric recognition, liveness detection is a crucial operation aimed at improving biometric system reliability. Passive detection techniques, in general, make use of biometric probes that have been recorded using a biometric sensor. Further contacts with the data subject are not required as a result of this [13].Liveness detection algorithms are frequently dependent on a prior known spoof manufacturing materials that are unrealistic. This restricts their use in the actual world, because the nature of attacks is unpredictably unexpected. As a result, researchers must create generic liveness detection methods that can identify a wide range of spoofing assaults that have never been seen before [32].

For mobile authentication, facial recognition is an excellent biometric option. It's simple to use and adaptable to a wide range of mobile devices, with camera integration in many commercial devices. It utilizes a well-known "selfie" stance. Facial biometric, on the other hand, are more vulnerable to spoofing due to the extensive availability of digitized facial photos via social media. As a result, robust liveness detection is crucial for mobile biometric authentication solutions that use facial recognition.

Methods Used for the Face Detection (**RQ**$_2$)
Objects are typically identified by their distinguishing characteristics. The human face has many distinguishing features that allow it to be distinguished from other objects. It detects faces by extracting structural features such as eyes, nose, and mouth and then using them to detect a face. Typically, a statistical classifier qualified then useful to distinguish between facial and non-facial regions. In the literature, numerous feature extraction methods have been proposed. The issue with these algorithms is that they are tainted by illumination, occlusion, and noise [33].

*Knowledge-Based Top-Down Method*s
Face detection methods are created using criteria obtained from the researcher's knowledge of human faces. Simple criteria for describing the features of a face and their relationships are easy to come up with. A face, for example, frequently appears in an image with two symmetrical eyes, a nose, and a mouth. The relative distances and positions of features can be used to depict their relationships. Face candidates are determined based on the specified rules after facial features in an input image are retrieved. To reduce false detections, a verification method is frequently used. This consists of three levels of rules. All viable face candidates are determined at the highest level by scanning a window over the input image and applying a set of rules to each spot. The higher-level rules are generic descriptions of what a face looks like, but the lower-level rules rely on specific facial traits [34].

Bottom-Up Feature-Based Methods
Bottom–up selection is linked to salience, which is determined by detecting areas with local visual attributes that differ considerably from the surrounding picture attributes along some dimension or combination of dimensions. This method goes back to the theory of features integration, claiming that in early stages of cortical visual processing such as color, edge orientation, brightness or motion direction a number of simple visual dimensions are represented. Even though salience is important in bottom–up selection, we also consider it bottom–up when other factors such as the emotional content of stimuli (e.g., angry faces) or previous experience drive selection against the observers' intentions [35].

MLeNet Methods
MLeNet is used to generate a detector that can determine whether a given fixed window has a masked face or not. Recently, two frameworks have been developed to generate these candidates. The first is followed by R-CNN, which generates selective search region proposals. The other is DPM, which generates candidates with masked faces using a sliding window. The first framework (R-CNN) can speed up object detection,

but the detector may fail if the generated proposals do not include masked faces. The other framework (DPM) generates masked face candidates by sliding window, which is simple and all-inclusive for generating masked face candidates, especially with our low-resolution training dataset. DPM does not directly address the multi-scale problem or the detection overlapping problem. To address the aforementioned issues, we use a pyramid matching scheme with non-maximal suppression based post-processing in a classic setting [36].

Future Trends (**RQ**$_3$)
Most of the approaches to facial liveness detection are software based, time consuming, expensive, loud and lighting sensitive. A facial vitality detection was recently proposed with flash against 2D spoofing. The hardware and software method is employed in this strategy. Flash has the key advantage of enhancing the separation between real users and false users and reducing the effects of external factors [37].

5 Conclusion and Future Work

The goal of this paper review is to know what liveness facial detection entails as well as its benefits over different existing types of biometrics and also to contribute to a deeper understanding of the title based on literature. Biometrics is the technology of determining an individual's identity based on their physical or behavioral characteristics. The requirement for large-scale identity management systems whose functionality depends on the accurate inference of an individual's identification in the context of multiple applications has increased the importance of biometrics in modern civilization. This review aims to identify the existing types of biometric, liveness of facial recognition and its importance over the existing types of biometric. The findings were majorly based on the state of art.

There are two questions that need to be asked about today's facial recognition technology. Is this the correct person that is being portrayed, and is it a real person? Facial recognition cannot tell whether or not a person is real. As a result, you must now verify that a person is a real person, especially in online situations hence passive liveness face detection. The focus has been on liveness facial detention but future work can focus on exploring the importance of liveness detection for voice biometrics on smart devices.

References

1. Saeed, K.: Biometrics principles and important concerns. In: Saeed, K., Nagashima, T. (eds.) Biometrics and Kansei Engineering, pp. 3–20. Springer, New York, (2012). https://doi.org/10.1007/978-1-4614-5608-7_1
2. Hamidi, H.: An approach to develop the smart health using Internet of Things and authentication based on biometric technology. Futur. Gener. Comput. Syst. **91**, 434–449 (2019). https://doi.org/10.1016/j.future.2018.09.024
3. Bhalla, A.: The latest evolution of biometrics. Biometric Technol. Today **2020**(8), 5–8 (2020). https://doi.org/10.1016/S0969-4765(20)30109-0
4. Jain, A.K., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Trans. Circuits Syst. Video Technol. **14**(1), 4–20 (2004). https://doi.org/10.1109/TCSVT.2003.818349

5. Wayman, J.L.: Fundamentals of biometric authentication technologies. Int. J. Image Grap. **1**(01), 93–113 (2001). https://doi.org/10.1142/S0219467801000086
6. Rubab, S., Mir, A.: Biometrics Verification: A Literature Survey, vol. 5, p. 67, Dec (2011)
7. Mason, J., Dave, R., Chatterjee, P., Graham-Allen, I., Esterline, A., Roy, K.: An investigation of biometric authentication in the healthcare environment. Array **8**, 100042 (2020). https://doi.org/10.1016/j.array.2020.100042
8. Štruc, V., Žganec-Gros, J., Vesnicer, B., Pavešić, N.: Beyond parametric score normalisation in biometric verification systems. IET Biom. **3**(2), 62–74 (2014). https://doi.org/10.1049/iet-bmt.2013.0076
9. Haghighat, M., Zonouz, S., Abdel-Mottaleb, M.: Identification using encrypted biometrics. In: Wilson, R., Hancock, E., Bors, A., Smith, W. (eds.) CAIP 2013. LNCS, vol. 8048, pp. 440–448. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40246-3_55
10. Balameenakshi, S., Sumathi, S.: Multi-biometric system for newborn recognition. Int. J. Eng. Res. **2**(5), 7 (2013)
11. Rai, V., Mehta, K., Jatin, J., Tiwari, D., Chaurasia, R.: Automated biometric personal identification-techniques and applications. In: 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, May 2020, pp. 1023–1030. https://doi.org/10.1109/ICICCS48265.2020.9120896
12. Prabhakar, S., Kittler, J., Maltoni, D., O'Gorman, L., Tan, T.: Introduction to the special issue on biometrics: progress and directions. IEEE Trans. Pattern Anal. Mach. Intell. **29**(4), 513–516 (2007). https://doi.org/10.1109/TPAMI.2007.1025
13. Krieg, M., Rogmann, N.: Liveness Detection in Biometrics, p. 8
14. Kanak, A.: Biometric ontology for semantic biometric-as-a-service (BaaS) applications: a border security use case. IET Biom. **7**(6), 510–518 (2018). https://doi.org/10.1049/iet-bmt.2018.5067
15. Alsaadi, I.M.: Physiological biometric authentication systems, advantages, disadvantages and future development: a review.Int. J. Sci. Technol. Res. **4**(12), 5 (2015)
16. Jhaveri, H., Jhaveri, H., Sanghavi, D.: Biometric Security System and its Applications in Healthcare. Int. J. Tech. Res. Appl. **2**(6), 6 (2014)
17. Shrivastava, S.: Biometric: Types and its Applications, p. 4 (2013)
18. Al-Ajlan, A.: Survey on fingerprint liveness detection. In: 2013 International Workshop on Biometrics and Forensics (IWBF), Lisbon, Apr 2013, pp. 1–5. https://doi.org/10.1109/IWBF.2013.6547309
19. Sukhai, N.B.: Access control & biometrics. In: Proceedings of the 1st Annual Conference on Information Security Curriculum Development – InfoSecCD '04, Kennesaw, Georgia, 2004, p. 124. https://doi.org/10.1145/1059524.1059552
20. Conejar, R.J., Jo, J., Bae, J., Kim, H.-K.: A study of different biometrics recognition technology and its application. In: 2015 8th International Conference on Bio-Science and Bio-Technology (BSBT), Jeju Island, South Korea, Nov 2015, pp. 12–15. https://doi.org/10.1109/BSBT.2015.14
21. Sepúlveda Carmona, M.: Biometric technology and beneficiary rights in social protection programmes. Int. Soc. Secur. Rev. **72**(4), 3–28 (2019). https://doi.org/10.1111/issr.12219
22. Liu, S., Song, Y., Zhang, M., Zhao, J., Yang, S., Hou, K.: An identity authentication method combining liveness detection and face recognition (2019). https://doi.org/10.3390/s19214733
23. Chakraborty, S., Das, D.: An overview of face liveness detection. IJIT **3**(2), 11–25 (2014). https://doi.org/10.5121/ijit.2014.3202
24. Garousi, V., Felderer, M., Mäntylä, M.V.: Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. Inf. Softw. Technol. **106**, 101–121 (2019). https://doi.org/10.1016/j.infsof.2018.09.006

25. Iqbal, A., Colomo-Palacios, R.: Key opportunities and challenges of data migration in cloud: results from a multivocal literature review. Proc. Comput. Sci. **164**, 48–55 (2019). https://doi.org/10.1016/j.procs.2019.12.153
26. Keirstead, J.: How to do a quantitative literature review in R (2011) [Online]. http://www.r-bloggers.com/how-to-do-a-quantitative-literature-review-in-r/. Accessed 17 Jun 2021
27. Mathias, M., Benenson, R., Pedersoli, M., Van Gool, L.: Face detection without bells and whistles. In: Fleet, D., Pajdla, T., Schiele, B., Tuytelaars, T. (eds.) ECCV 2014. LNCS, vol. 8692, pp. 720–735. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-10593-2_47
28. Gao, C., Li, X., Zhou, F., Mu, S.: Face liveness detection based on the improved CNN with context and texture information. Chin. J. Electron. **28**(6), 1092–1098 (2019). https://doi.org/10.1049/cje.2019.07.012
29. Otti, C.: The Past, Present and Future of Biometrics, p. 6
30. Herzog, T., Uhl, A.: Analysing a vein liveness detection scheme. In: 2020 8th International Workshop on Biometrics and Forensics (IWBF), Porto, Portugal, Apr 2020, pp. 1–6. https://doi.org/10.1109/IWBF49977.2020.9107960
31. Hofbauer, H., Debiasi, L., Kränkl, S., Uhl, A.: Exploring presentation attack vulnerability and usability of face recognition systems. IET Biom. **10**(2), 219–232 (2021). https://doi.org/10.1049/bme2.12015
32. Akhtar, Z., Micheloni, C., Foresti, G.L.: Biometric liveness detection: challenges and research opportunities. IEEE Secur. Privacy **13**(5), 63–72 (2015). https://doi.org/10.1109/MSP.2015.116
33. Hatem, H., Beiji, Z., Majeed, R.: A survey of feature base methods for human face detection. IJCA **8**(5), 61–78 (2015). https://doi.org/10.14257/ijca.2015.8.5.07
34. Chaudhari, M., Sondur, S., Vanjare, G.: A review on face detection methods. Int. J. Comput. Trends Technol. **25**(July), 54–61 (2015)
35. Theeuwes, J.: Top-down and bottom-up control of visual selection. Acta Physiol. (Oxf.) **135**, 77–99 (2010). https://doi.org/10.1016/j.actpsy.2010.02.006
36. Lin, S., Cai, L., Lin, X., Ji, R.: Masked face detection via a modified LeNet. Neurocomputing **218**, 197–202 (2016). https://doi.org/10.1016/j.neucom.2016.08.056
37. Daniel, N., Arulappan, A.: A study on recent trends in face spoofing detection techniques, Nov 2018, pp. 583–586. https://doi.org/10.1109/ICICT43934.2018.9034361

An Innovative User Authentication Method: Replacements of Text Based Passwords

Varun Shukla[1], Shivani Dixit[1], Ravi Kumar[2(✉)], and Manish Patidar[2]

[1] Department of Electronics and Communication Engineering, Pranveer Singh Institute of Technology, Kanpur, India
[2] Department of Electronics and Communication Engineering, Jaypee University of Engineering and Technology, Guna, India
ravi.kumar6@gmail.com

Abstract. Authentication is an important aspect for information security. Text based passwords have been the choice for authentication over the years, but many security threats and vulnerabilities are reported now. Researchers and academicians have suggested many alternatives with some advantages and limitations. It has been noted that few alternative methods are very promising but very complicated to implement hence they have not been adopted in real life applications. Keeping this in mind, a simple, innovative and easily implementable method for user authentication as an alternative of text-based passwords is proposed in this paper. User needs to upload an image of his choice as a sign-up process initially. This image is analysed by server and decomposed into many components. When the user wants to get access to the system next time, the server gives him a challenge to arrange all the image components in a sequence. These image components are randomly jumbled and server plays an intelligent role here. Based on the pattern and log in attempt by user, server can increase or decrease number of image components based on an algorithm and it enhances the randomness and security level of the authentication process. The server learns about variations gradually and in case of any suspicious activity, server can instruct the user to change the image which acts as a password. The test results and security analysis along with proposed method is discussed here in order to prove the feasibility and validity of the proposed method. It is believed that the proposed method has the strength to replace text-based passwords and the method can be incorporated with various machine learning based cryptographic procedures which will enhance the overall utility of the proposed work.

Keywords: Authentication · Data communication · Image components · Machine learning (ML) · Passwords · Security

1 Introduction and Literature Review

Data communication is an inseparable part of life in the modern world. Cryptography has the responsibility to provide secure and reliable data communication. Authentication as a cryptographic goal is of utmost importance along with other goals as shown in below Fig. 1 [1–3].

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 210–224, 2023.
https://doi.org/10.1007/978-3-031-13150-9_19

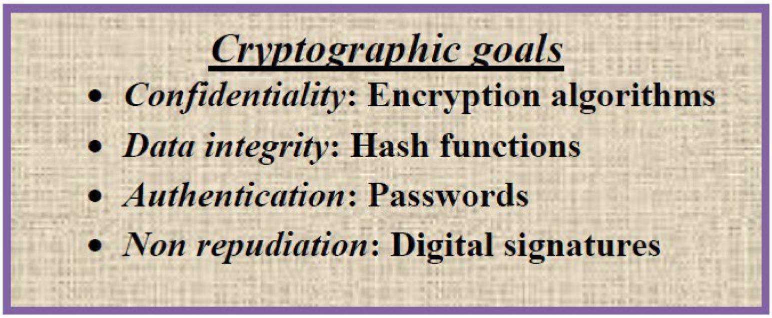


Fig. 1. Showing cryptographic goals with their corresponding methods

Text based passwords have dominated the authentication procedures over the years but now they suffer with many security flaws as intruders have founded many ways to crack user passwords [4, 5]. Many incidents of security breaches of passwords are reported and this is the right time to surprise intruders with alternative methods. These alternative methods must be robust, implementable and suitable for various real-life scenarios. If the alternative authentication methods are intelligent enough to take decisions, then they can be incorporated with Machine Learning (ML) based cryptographic systems for future endeavours [6]. So we want to discuss the work done in past decade i.e. 2012–2021 for the efforts made for the replacement of text based passwords so a clear roadmap can be set up for the readers of this paper. The inclusion of too many papers and previous methods can create various ambiguities so we have picked only few selected papers of past decade which can tell about the efforts done in this regard. In 2012, J. Bonneau et al. [7] have published an article with a very lucrative title "The quest to replace passwords." They have discussed the benefits of using passwords and the alternative methods too. They have mentioned those passwords are not resistive against physical observations because even if a user types it quickly then also it can be easily recovered from a high-quality video of the keyboard. The alternative methods include encrypted password managers, proxy-based schemes, graphical passwords and cognitive authentication schemes. Hardware tokens like RSA-Ids, biometric authentication methods and mobile phone-based methods are also in the list. The discussion made by authors was so fruitful and it has attracted the attention of research fraternity on replacing passwords. In 2013, J.L. Tsai et al. [8] have introduced an innovative method which is robust to password guessing attacks. They have discussed that earlier password schemes are prone to various attacks including offline guessing attack. So, in order to overcome the obstacles, the authors have presented a multi-server authentication scheme where the registration centre needs to transmit an alternative key to help the server so that a user can get access without using password. The values of these keys are made variable in each run. In order words, the registration server has the capability to authenticate user and server. The proposed scheme is said to have enough strength to replace smart cards also. In 2014, Y.W. Chow et al. [9] have presented a unique one-time password authentication method which uses cell phones and the method is an alternative of traditional passwords as they can be stolen very easily. The method is basically a challenge-response-visual mechanism and it sends a challenge over a public communication channel in order to obtain a session key keeping the long term secret key of user safe. The limitations of the proposed method include the usage of public channel and the mobile phone must be capable enough to perform the required task and the method also relies on human visual system. In 2015, S. Prabhu et al. [10] have discussed a new authentication scheme which replaces alphanumeric passwords by graphical passwords. They have merged text with images in session passwords in order to increase security. They have proposed two different approaches to achieve this. In the first approach, no additional registration is required and a session password is generated using a grid. In the second approach, ratings are assigned to colours and grid and then the session password is generated but these proposed approaches are not checked properly for applicability and efficiency and that is the limitation of proposed approaches. In 2016, A. Abdellaoui et al. [11] have discussed an alternative to alphanumeric password and it can be useful in cloud authentication scenarios. In their proposed method they have incorporated multifactor authentication, one time password and SHA1 (Secure Hash Algorithm) together. The proposed password generator system can be implemented on mobile phones as well but some common security aspects like data integrity and ease of implementation remains unaddressed. The proposed method is said to be resistive against replay attacks, Man in The Middle (MITM) attack and brute force attack etc. In 2017, M. Habid et al. [12] have discussed a password free authentication method. The scheme is based on hybrid vein keystroke approach. The authors have discussed that approximately 5 million passwords of Gmail accounts have been compromised in the year 2014 and after that research fraternity have started looking for alternative methods to alphanumeric passwords. The proposed method consists of two stages, one is static authentication using vein biometric and the second stage is continuous authentication using keystroke dynamics. Since vein patterns inputs require an additional hardware which uses near infrared light and a monochrome charge-coupled device camera, so this could be a limitation of the proposed method. In 2018, B. Bilgi et al. [13] have discussed a graphical password method which can replace text-based passwords. They have discussed that people are now using various communication methods in public places using shared communication channels and hence the attacks on text-based passwords are also increased. The theme of their proposed method relies on the fact that users remember visual objects more than texts. The proposed method uses hybrid images that provide two different impressions in proportion of the distance and it is said to be resistive against eavesdropping and various other attacks. In 2019, M. Yildirim et al. [14] have come up with a very interesting empirical study on text-based passwords. They have proposed new user-friendly guidelines for the creation of text passwords. They have suggested that users must have their own unique way to compose their passwords. In their empirical study, they have divided users into two groups. First group has a freedom to develop their own passwords based on their own rules and second group have to compose passwords based on the given traditional guidelines. The study has shown that the first group have performed better than the second group. The suggestions for improving passwords include mnemonic passwords, password chunking and password strength meters etc. In 2020, S. J. Alsunaidi et al. [15] have discussed brainwaves-based biometric authentication systems. They have mentioned that initially various biometrics such as thumb impression, face and retina detection etc were considered as replacement of text-based passwords, but they have suffered with various attacks including shoulder surfing by others. So, brainwaves as a biometric input have attracted the attention of researchers and the belief was that it could enhance the level of security and can replace text-based passwords. Now alternative methods of text-based passwords are getting useful for various applications like cloud environments, Electronic Health Records (EHR) etc and in this context, in 2021, C.H. Liu et al. [16] have discussed an authentication method which combines passwords with smart cards in order to get log in and access the user's health records. The daily health records of a user are stored in a cloud environment and in order to get access, a smart card is needed which stores all the parameters and an authentication scheme based on bilinear pairing is used as a verification process. The rest of this paper is organized as follows: In Sect. 2, proposed methods and test results are discussed. Security analysis and advantages are given in Sect. 3. Paper ends with conclusion and future scope in Sect. 4.

2 Proposed Method

In this method, the method to replace the usage of passwords for authentication has been discussed. Users create their passwords for authentication and they need to insert same password when they log in next time. These passwords can be stolen or cracked by intruders and vulnerability increases even more when users are not restricted to select strong passwords means they can choose a simple 4–6-digit password. In the proposed method, the user uploads the image on the server through the website during the credential's initialization time. This uploaded image is known to user only and acts as a password for authentication. Now server processes the image and performs segmentation using a specific method. The uploaded image is divided into various components and server can change number of components in every run in a random jumbled fashion. When user wants to log in next time, then he has to arrange all the components in order to create the original image. The image can be of any type. It can be an image of particular sequence as it enhances the level of difficulty for intruders. Here server plays an intelligent role. In the first login attempt, the number of components may be high (high difficulty level) but in next consecutive attempts, it can be reduced (low difficulty level). So based on the usage pattern, it can be altered at any point of time as it is flexible and depends on server. In case of any suspicious activity detected by the server, the number of components can be increased so that the difficulty level can be increased. The uploaded image can be changed by the user or server can instruct the user to change the image after a certain login attempts. This approach has the capability to replace the need of passwords along with the benefit that user need not to remember multiple passwords for various applications. The idea enhances security and it is easily implementable. Suppose user selects an image of $X \times Y$ size where X represents column and Y represents rows. Server needs to select random initialisation vectors $R_{initial}$ (for rows) and $C_{initial}$ (for columns) in order to create image components. These $R_{initial}$ and $C_{initial}$ decide the number of components of an image because the values of $R_{initial}$ *and* $C_{initial \propto \frac{1}{numberofcomponents}}$. These $R_{initial}$ and $C_{initial}$ are also known as the selected block size (selected by server as initial values). Then the corresponding block range vectors for $R_{initial}$ and $C_{initial}$ can be calculated as $R_{range} = \left[R_{initial} \times 1, remainder\left(\frac{Y}{R_{initial}}\right)\right]$ and $C_{range} = \left[C_{initial} \times 1, remainder\left(\frac{X}{C_{initial}}\right)\right]$ (These ranges are shown maximum to minimum). Now for rows, $Y = (P \times R_{initial}) + \alpha$ where P is the quotient and α is the remainder for rows and similarly for columns $X = (Q \times C_{initial}) + \beta$ where Q is the quotient and β is the remainder for columns. So the block vectors can be written as $R_{vector} = [R_{initial} apperasPtimes, \alpha]$ and $C_{vector} = [C_{initial} apperasQtimes, \beta]$ and $total\ number\ of\ components = (P + 1)(Q + 1)$.

- **Test results 1:** An image of size 1092×658 size has been selected that means $X = 1092$ and $Y = 658$ with $R_{initial} = 250$ and $C_{initial} = 200$. So, it is considered as $658 = 2 \times 250 + 158$ and similarly $1092 = 5 \times 200 + 92$ which means that $P = 2$ and $Q = 5$ and $\alpha = 158$ and $\beta = 92$. Further, $R_{range} = [250, 158]$ and $C_{range} = [200, 92]$ and it means $R_{vector} = [250, 250, 158]$ and $C_{vector} = [200, 200, 200, 200, 200, 92]$. So, total number of components are going to be $(P + 1)(Q + 1) = (2 + 1)(5 + 1) = 18$. Finally, the user needs to arrange total 18 randomly jumbled components of the uploaded image in order to authenticate him in the next login attempt. It is shown in the below Fig. 2 and 3:

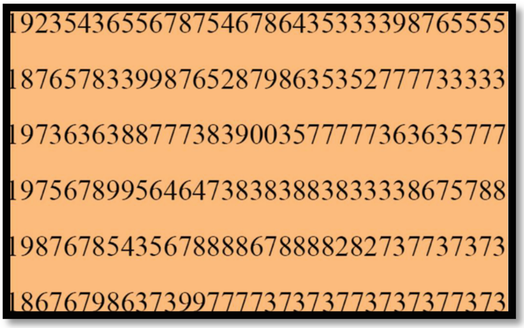


Fig. 2. Showing input image for test result 1

As it has been mentioned earlier also that if the values of $R_{initial}$ and $C_{initial}$ are changed by the server for the same image, then all the corresponding parameter and hence the number of image components will change. So, different values for the same image of size 1092×658 has been shown in the following Table 1 (1.1 to 1.5) and the relationship between $R_{initial}$ and $C_{initial}$ with number of components is shown in Fig. 4 through a graph.

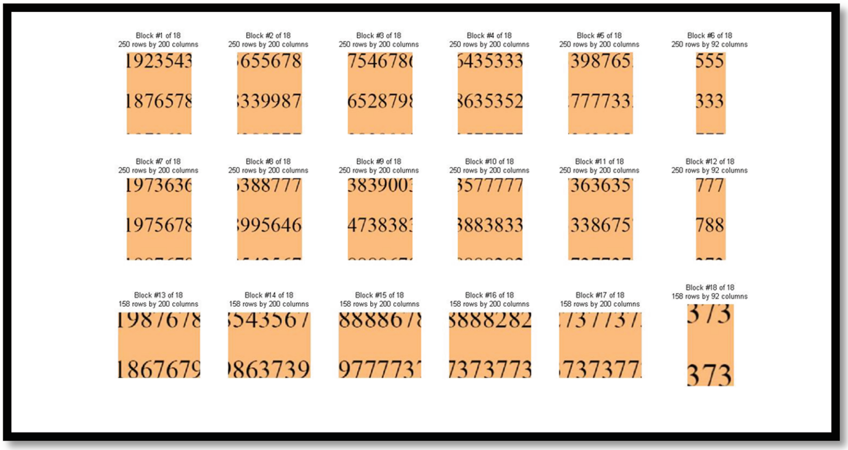


Fig. 3. Showing generated image components of test result 1

- **Test results 2:** An image of size 853×659 has been selected that means $X = 853$. And $Y = 659$. $R_{initial} = 250$ and $C_{initial} = 200$ has been selected. So, $659 = 2 \times 250 + 159$ can be written and similarly $853 = 4 \times 200 + 53$ which means that $P = 2$ and $Q = 4$ and $\alpha = 159$ and $\beta = 53$. Further, $R_{range} = [250, 159]$ and $C_{range} = [200, 53]$ and it means $R_{vector} = [250, 250, 159]$ and $C_{vector} = [200, 200, 200, 200, 53]$. So total number of components are going to be $(P + 1)(Q + 1) = (2 + 1)(4 + 1) = 15$. The user needs to arrange total 15 randomly jumbled components of the uploaded image in order to authenticate him in the next login attempt. It is shown in the below Fig. 5 and 6:

Table 1. **(1.1 to 1.5)**. Showing values of parameters for the image of size 1092 × 658

Table 1.1

S.N	Size	X	Y	$R_{initial}$	$C_{initial}$	P	Q	α	β	R_{range}	C_{range}
1	1092 × 658	1092	658	150	130	4	8	58	52	[150,58]	[130, 52]
		$R_{vector} = [150, 150, 150, 150, 58]$									
		$C_{vector} = [130, 130, 130, 130, 130, 130, 130, 130, 52]$									
		$Number\ of\ components = (4 + 1)(8 + 1) = 45$									

Table 1.2

S.N	Size	X	Y	$R_{initial}$	$C_{initial}$	P	Q	α	β	R_{range}	C_{range}
2	1092 × 658	1092	658	200	180	3	6	58	12	[200,58]	[180, 12]
		$R_{vector} = [200, 200, 200, 58]$									
		$C_{vector} = [180, 180, 180, 180, 180, 180, 12]$									
		$Number\ of\ components = (3 + 1)(6 + 1) = 28$									

Table 1.3

S.N	Size	X	Y	$R_{initial}$	$C_{initial}$	P	Q	α	β	R_{range}	C_{range}
3	1092 × 658	1092	658	250	230	2	4	158	172	[250,158]	[230, 172]
		$R_{vector} = [250, 250, 158]$									
		$C_{vector} = [230, 230, 230, 230, 172]$									
		$Number\ of\ components = (2 + 1)(4 + 1) = 15$									

Table 1.4

S.N	Size	X	Y	$R_{initial}$	$C_{initial}$	P	Q	α	β	R_{range}	C_{range}
4	1092 × 658	1092	658	310	280	2	3	38	252	[310,38]	[280, 252]
		$R_{vector} = [310, 310, 38]$									
		$C_{vector} = [280, 280, 280, 252]$									
		$Number\ of\ components = (2 + 1)(3 + 1) = 12$									

Table 1.5

S.N	Size	X	Y	$R_{initial}$	$C_{initial}$	P	Q	α	β	R_{range}	C_{range}
5	1092 × 658	1092	658	400	320	1	3	258	132	[400,258]	[320, 132]
		$R_{vector} = [400, 258]$									
		$C_{vector} = [320, 320, 320, 132]$									
		$Number\ of\ components = (1 + 1)(3 + 1) = 8$									

Similar to test results 1, if the values of $R_{initial}$ and $C_{initial}$ are changed by the server for the same image, then all the corresponding parameter and hence the number of image components will change. So, different values for the same image of size 853 × 659 have been shown in the following Table 2 (2.1 to 2.5) and the relationship between $R_{initial}$ and $C_{initial}$ with number of components is shown in Fig. 7 through a graph.

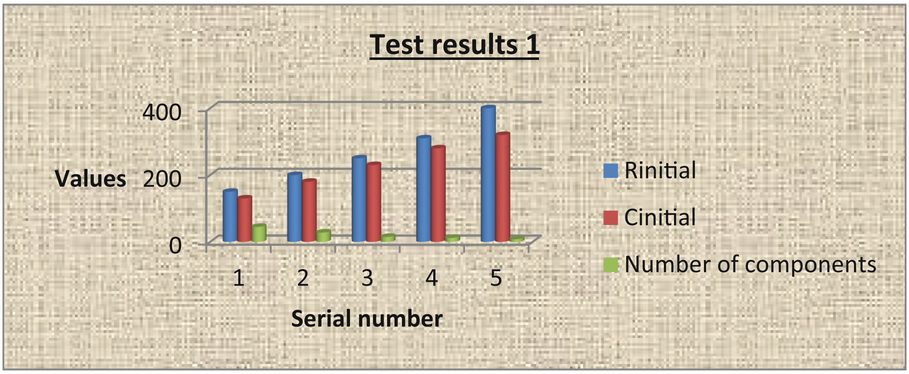


Fig. 4. Relation of $R_{initial}$. And $C_{initial}$. With number of components for test results 1

Fig. 5. Showing input image for test result 2

3 Security Analysis and Advantages

- **Replacements of passwords:** The proposed method provides complete replacements of passwords along with CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) also. It is well known that users need to insert CAPTCHA of various kinds in order to prove that they are not robots. Since in the proposed method, only users knows the image so there is no need to insert a separate CAPTCHA for getting the access. Passwords can be stolen or forgotten but humans memorize visuals better than numbers or texts so the proposed method will provide a better environment for user authentication at a better security level.
- **Password guessing attacks:** Passwords are vulnerable to various online and offline guessing attacks but these attacks are not applicable in proposed method. User can select any image of his choice which he or she can memorize better or that may be related to any event of his life. It can be a specific sequence of numbers or a sequence of family photographs etc. which is well known and in memory of user. So to guess

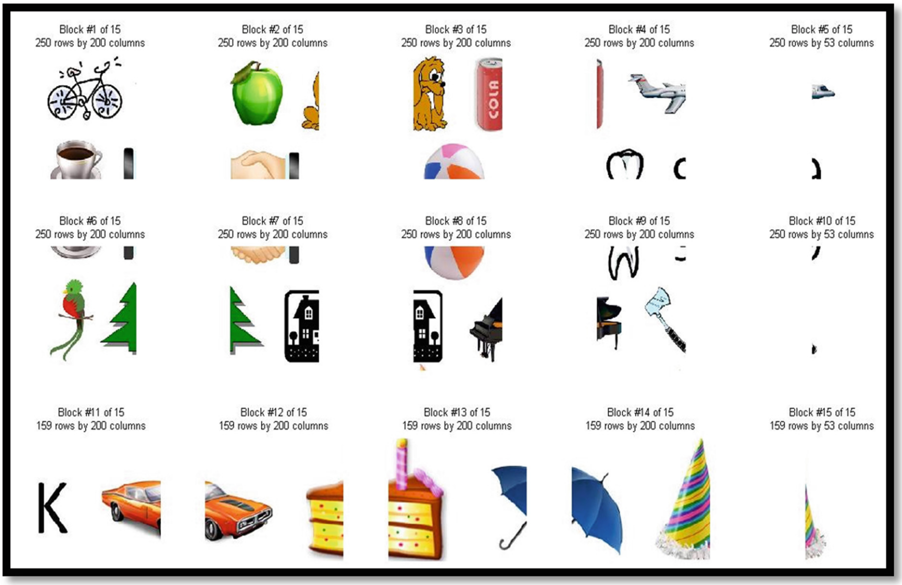


Fig. 6. Showing generated image components of test result 2

the correct sequence is not possible and the chances of forgetting the password by user also get null.

- **Role of user:** In password based authentication schemes users are bound to select their password based on rules like password should be minimum of eight characters with a combination of upper case and lower case letters etc. but these restrictions are not applicable in the proposed method. User can select image of his own choice and not bounded by any specific rule. User can change image at any point of time. It can be set on a predefined basis also like after n login attempts, the image must be changed
- **Role of server:** Server plays an intelligent role here. Since $R_{initial} and C_{initial} \propto \frac{1}{numberofcomponents}$ so based on the selected image by user, the server can decide $R_{initial}$. And $C_{initial}$ and it will give a challenge to user to arrange the jumbled sequence of images. On next consecutive attempts by same address, the server can increase the values of $R_{initial}$. And $C_{initial}$ in order to decrease the number of jumbled components. So it will act as intelligent user authentication scheme and in case of any suspicious activity observed by server, the values of $R_{initial}$ and $C_{initial}$ can be reduced significantly in order to increase the number of image components or server can also instruct the user to change the image. Needless to say that it will enhance the level of security along with the ease of implementation.
- **Can be run of any device:** The proposed authentication procure is simple enough that it can be run or implemented on any device like laptops, mobile phones or customized authentication devices. No complex procedure or extensive calculation is required and users need to simply upload an ima of their own choice which will be processed by server and consecutive tasks will be given to users on further attempts. User can

Table 2. **(2.1 to 2.5)**. Showing values of parameters for the image of size 853 × 659

Table 2.1

S.N	Size	X	Y	$R_{initial}$	$C_{initial}$	P	Q	α	β	R_{range}	C_{range}
1	853 × 659	853	659	150	130	4	6	59	73	[150,59]	[130, 73]
		$R_{vector} = [150, 150, 150, 150, 59]$									
		$C_{vector} = [130, 130, 130, 130, 130, 130, 73]$									
		$Number\ of\ components = (4+1)(6+1) = 35$									

Table 2.2

S.N	Size	X	Y	$R_{initial}$	$C_{initial}$	P	Q	α	β	R_{range}	C_{range}
2	853 × 659	853	659	200	180	3	4	59	133	[200,59]	[180, 133]
		$R_{vector} = [200, 200, 200, 59]$									
		$C_{vector} = [180, 180, 180, 180, 133]$									
		$Number\ of\ components = (3+1)(4+1) = 20$									

Table 2.3

S.N	Size	X	Y	$R_{initial}$	$C_{initial}$	P	Q	α	β	R_{range}	C_{range}
3	853 × 659	853	659	250	230	2	3	159	163	[250,159]	[230, 163]
		$R_{vector} = [250, 250, 159]$									
		$C_{vector} = [230, 230, 230, 163]$									
		$Number\ of\ components = (2+1)(3+1) = 12$									

Table 2.4

S.N	Size	X	Y	$R_{initial}$	$C_{initial}$	P	Q	α	β	R_{range}	C_{range}
4	853 × 659	853	659	310	280	2	3	39	13	[310,39]	[280, 13]
		$R_{vector} = [310, 310, 39]$									
		$C_{vector} = [280, 280, 280, 13]$									
		$Number\ of\ components = (2+1)(3+1) = 12$									

Table 2.5

S.N	Size	X	Y	$R_{initial}$	$C_{initial}$	P	Q	α	β	R_{range}	C_{range}
5	853 × 659	853	659	400	320	1	2	259	213	[400,259]	[320, 213]
		$R_{vector} = [400, 259]$									
		$C_{vector} = [320, 320, 213]$									
		$Number\ of\ components = (1+1)(2+1) = 6$									

instantly take pictures from their mobile camera and can upload on the server as a authentication password.

- **No involvement of third party:** There is no involvement of any third party in the proposed method. It has been observed that in some of the alternative methods suggested by researchers are dependent on third parties [8, 17]. The dependency on third parties increases the overall complexity of the authentication method and if the reliability of third party is compromised the entire system gets crashed. In the proposed method, the communication takes place directly between user and server so the above-mentioned difficulty is not applicable here.

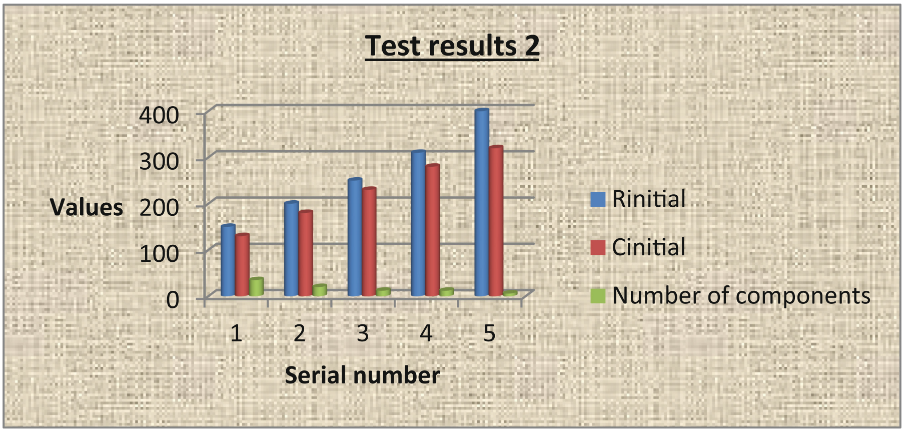


Fig. 7. Relation of $R_{initial}$ and $C_{initial}$ with number of components for test results 2

- **Session timer can be applied:** The concept of timer can also be applied in the proposed authentication system. That means users are supposed to arrange the randomly jumbled image components in a predefined time. This timer can be made variable in every run based on the usage pattern of user. For example, the timer is of 45 s in the first run but it could be reduced to 30 s in the next consecutive login attempt made by user (may be from the same address). In case of any suspicious activity observed by server, the timer can significantly reduce and the number of image components can be increased by server as an intelligent decision so that the security of the authentication process remains intact.
- **Multiple images can be uploaded:** The proposed authentication method can be used as a multi-level authentication where different images can be uploaded by user for different stages. If it is a two-level authentication, then user has to arrange sequences of first image (timer one is applied) as primary authentication level and on success, the user is supposed to arrange the sequences of second image (timer two is applied) as secondary authentication level. The server takes user to secondary authentication level only when first level is crossed successfully. So based on the required security level, the proposed method can be used as a multi-step-multi-timer authentication method as shown in below Fig. 8.
- **Separate CAPTCHA is not desired:** The proposed method is capable of differentiate between human and robots so a separate CAPTCHA is not required. Since the image is known to user only (which is subject to change also), a robot can't put correct sequence because number of image components are variable in each login attempt with a different timer value. It solves the CAPTCHA problem of authentication [18, 19] as it has been observed that authentication fails due to incorrect CAPTCHA even after the right password because user is not able to see the correct CAPTCHA properly because of noise inserted.

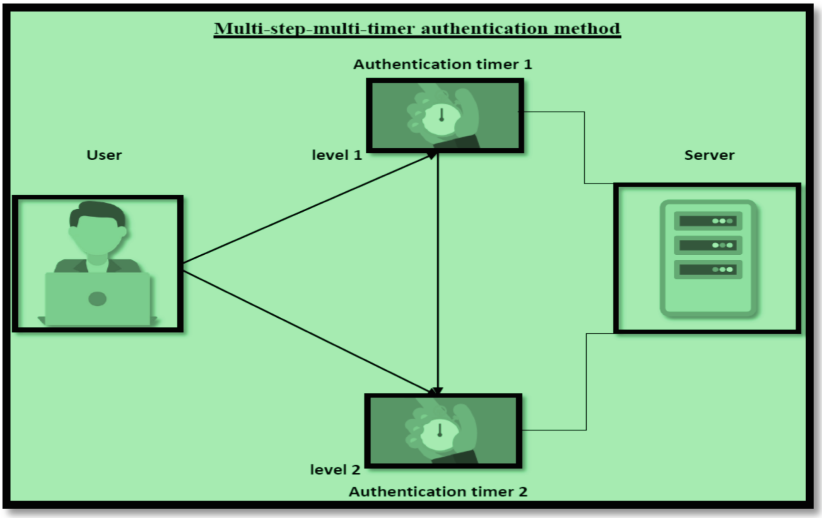


Fig. 8. Utility of the proposed method as multi-step-multi timer authentication process

- **Flexibility of algorithm:** The proposed authentication method is flexible enough to provide the challenge to user. The number of components and the associated timer value keeps on changing in each run depending upon the usage and login pattern of user. The image components can be increased with a reduced timer value in case of any suspicious activity observed by server. So this method provides flexibility in terms of efforts needed by user and makes sure that the security of the authentication system remains intact.
- **Resistive against dictionary attacks:** Text based passwords suffer with various online and offline dictionary attacks [20–22]. In the proposed authentication system, image acts as a password so dictionary attacks are not applicable. Users need not to store their passwords anywhere and it will further save the authentication procedure from exhaustive search attacks [23]. Any increment in number of image components or in case of change of image by user, the difficulty level will be enhanced for intruders. Inclusion of timer will further increase it.
- **Machine learning based authentication procedure:** As discussed earlier also, it's an intelligent authentication process where server as a machine learns the login and usage pattern of a particular user [24–26]. The image sequencing task of jumbled components is based on the login history and this ML based approach increases the overall efficiency of the authentication procedure. In case of any malicious activity observed by server, the user is bound to cross second level of authentication (with variable timer) as an additional security measurement.
- **Useful for various applications:** The proposed authentication process solves multiple problems together and hence suitable for various applications. It solves the associated vulnerability of text-based passwords and putting separate CAPTCHA. It can be used as a client-server authentication procedure in financial transactions, high security applications and device/process authentication applications etc. [27]. Further, the

method can be customized as multi-level authentication process for all the processes demanding high security at user authentication end. So, this compatibility, ease of implementation and simplicity makes the proposed authentication method very useful and convenient for various applications.

4 Conclusion and Future Scope

In this paper, a new authentication method as a replacement of text-based password is proposed. The user is supposed to upload the image of his choice. The server processes the image and gives the tasks to user to rearrange the randomly jumbled components in a given time on next subsequent attempts. The server plays an intelligent role here as it learns the login and usage pattern of user and based on this, the number of image components and associated timer value can be made variable. This flexibility provides ease of implementation and high security too and in case of any malicious activity observed by server, the level of toughness can be increased significantly. The proposed method is easily implementable on all devices and solves the additional requirement of CAPTCHA too. Test results with reading sets are shown to validate the feasibility of the proposed method. The proposed authentication method can be used as a multi-step-multi-timer method in variety of applications. The proposed method is resistive against password guessing attacks, dictionary attacks and exhaustive search attacks etc. The proposed method does not require any third-party involvement which was the problem with many earlier proposed methods. The method is a ML based authentication procedure and the future scope is also very rich. The method can be implemented as a Graphical User Interface (GUI) with many amendments also. The proposed method uses mathematical relations for deciding the number of image components but other analysing techniques can also be incorporated in order to compare the overall efficiency with proposed system. So, it can be said that a lot of further modifications and enhancements can be done in the proposed method which are subjected to implementation strategies, usage and applications keeping the overall complexity as minimum as possible.

Conflict of Interest. On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. Menezes, A.J., Oorschot, P.C.V., Vanstone, S.A.: Handbook of applied cryptography, 5th edn. CRC Press Inc., USA (2001)
2. Shukla, V., Chaturvedi, A., Srivastava, N.: A secure stop and wait communication protocol for disturbed networks. Wireless Pers. Commun. **110**, 861–872 (2019). https://doi.org/10.1007/s11277-019-06760-w
3. Shukla, V., Chaturvedi, A., Misra, M.K.: On authentication schemes using polynomials over non commutative rings. Wireless Pers. Commun. **118**(1), 185–193 (2021). https://doi.org/10.1007/s11277-020-08008-4

4. Chou, H.C., Lee, H.C., Yu, H.J., Lai, F.P., Huang, K.H., Hsueh, C.W.: Password cracking based on learned patterns from disclosed passwords. Int. J. Innovative Comput., Inform. Control **9**(2), 821–839 (2013). https://core.ac.uk/download/pdf/225229085.pdf
5. Yu, F., Huang, Y.: An overview of study of password cracking. In: International conference on computer science and mechanical automation, pp. 25–29 (2015). https://doi.org/10.1109/CSMA.2015.12
6. Alani, M.M.: Applications of machine learning in cryptography: a survey. In: Proceedings of the 3rd international conference on cryptography, security and privacy, pp. 23–27 (2019). https://doi.org/10.1145/3309074.3309092
7. Bonneau, J., Herley, C., Oorschot, P.C.V., Stajano, F.: The quest to replace passwords: a framework for comparative evaluation of web authentication schemes. In: IEEE Symposium on Security and Privacy, pp. 553–567 (2012). https://www.cl.cam.ac.uk/~fms27/papers/2012-BonneauHerOorSta-password--oakland.pdf
8. Tsai, J.L., Lo, N.W., Wu, T.C.: A new password-based multi-server authentication scheme robust to password guessing attacks. Wireless Pers. Commun. **71**, 1977–1988 (2013). https://doi.org/10.1007/s11277-012-0918-6
9. Chow, Y.-W., Susilo, W., Au, M.H., Barmawi, A.M.: A visual one-time password authentication scheme using mobile devices. In: Hui, L.C.K., Qing, S.H., Shi, E., Yiu, S.M. (eds.) ICICS 2014. LNCS, vol. 8958, pp. 243–257. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-21966-0_18
10. Prabhu, S., Shah, V.: Authentication using session based passwords. Procedia Comput. Sci. **45**, 460–464 (2015). https://doi.org/10.1016/j.procs.2015.03.079
11. Abdellaoui, A., Khamlichi, Y.I., Chaoui, H.: A novel strong password generator for improving cloud authentication. Procedia Comput. Sci. **85**, 293–300 (2016). https://doi.org/10.1016/j.procs.2016.05.236
12. Habib, M., Alqatawna, J.: A proposed password-free authentication scheme based on a hybrid vein-keystroke approach. In: International Conference on New Trends in Computing Sciences, pp. 173–178 (2017). https://doi.org/10.1109/ICTCS.2017.27
13. Bilgi, B., Tugrul, B.: A shoulder-surfing resistant graphical authentication method. In: International Conference on Artificial Intelligence and Data Processing, pp. 1–4 (2018). https://doi.org/10.1109/IDAP.2018.8620934
14. Yıldırım, M., Mackie, I.: Encouraging users to improve password security and memorability. Int. J. Inf. Secur. **18**(6), 741–759 (2019). https://doi.org/10.1007/s10207-019-00429-y
15. Alsunaidi, S.J., Saqib, N.A., Alissa, K.A.: A comparison of human brainwaves-based biometric authentication systems. Int. J. Biometrics **12**(4), 411–429 (2020). https://doi.org/10.1504/IJBM.2020.110814
16. Liu, C.H., Chen, T.L., Chang, C.Y., Wu, Z.Y.: A reliable authentication scheme of personal health records in cloud computing. Wireless Netw. 1–11 (2021). https://doi.org/10.1007/s11276-021-02743-7
17. Siddiqui, Z., Tayan, O., Khan, M.K.: Security analysis of smartphone and cloud computing authentication frameworks and protocols. Special section on security analytics and intelligence for cyber physical systems. IEEE Access **6**, 34527–34542 (2018). https://doi.org/10.1109/ACCESS.2018.2845299
18. Mehrnezhad, M., Ghaemi Bafghi, A., Harati, A., Toreini, E.: PiSHi: click the images and I tell if you are a human. Int. J. Inf. Secur. **16**(2), 133–149 (2016). https://doi.org/10.1007/s10207-015-0311-z
19. Khalifa, W., Hasan, A.: A survey of current research on CAPTCHA. Int. J. Comput. Sci. Eng. Surv. **7**(3), 1–21 (2016). https://doi.org/10.5121/IJCSES.2016.7301
20. Wang, D., Wang, P.: Offline dictionary attack on password authentication schemes using smart cards. In: Desmedt, Y. (ed.) ISC 2013. LNCS, vol. 7807, pp. 221–237. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-27659-5_16

21. Bošnjak, L., Sreš, J., Brumen, B.: Brute-force and dictionary attack on hashed real-world passwords. In: 41st International convention on information and communication technology, Electronics and microelectronics, pp. 1161–1166 (2018). https://doi.org/10.23919/MIPRO.2018.8400211
22. Kirushnaamoni, R.: Defenses to curb online password guessing attacks. In: International Conference on Information Communication and Embedded Systems, pp. 1–6 (2013). https://doi.org/10.1109/ICICES.2013.6508230
23. Chen, L., Huang, K., Manulis, M., Sekar, V.: Password-authenticated searchable encryption. Int. J. Inf. Secur. **20**(5), 675–693 (2020). https://doi.org/10.1007/s10207-020-00524-5
24. Ferrag, M.A., Maglaras, L., Derhab, A.: Authentication and authorization for mobile IoT devices using biofeatures: recent advances and future trends. Secur. Commun. Netw. **2019**, 1–20 (2019). https://doi.org/10.1155/2019/5452870
25. Munonye, K., Péter, M.: Machine learning approach to vulnerability detection in OAuth 2.0 authentication and authorization flow. Int. J. Inf. Secur. **21**(2), 223–237 (2021). https://doi.org/10.1007/s10207-021-00551-w
26. Ahmed, K.I., Tahir, M., Habaebi, M.H., Lau, S.L.: Machine learning for authentication and authorization in IoT: taxonomy, challenges and future research direction. Sensors **21**(15), 1–34 (2021). https://doi.org/10.3390/s21155122
27. Aniche, C., Yinka-Banjo, C., Ohalete, P., Misra, S.: Biometric e-voting system for cybersecurity. In: Misra, S., Kumar Tyagi, A. (eds.) Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities. SCI, vol. 972, pp. 105–137. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-72236-4_5

Analysis and Survey of Soil Moisture Prediction Techniques for Agricultural Applications

Seema J. Patil(✉) and B. Ankayarkanni

Sathyabama Institute of Science and Technology, Chennai, India
seema.patil@mitwpu.edu.in

Abstract. Soil Moisture (SM) is an important factor disturbing the growth of crop. Thus, sophisticated understanding or precise prediction of future SM states are important in scheduling of irrigation, improving utilization of agricultural water, and forecasting of yield. Hence, the detection and prediction of SM are of major concern in the present era. This review article provides the detailed review of latest research papers presenting the SM prediction approaches for the prediction of SM. The papers are classified as conventional methods of SM prediction, Remote sensing based SM prediction approaches, Machine learning based SM prediction methods, and the deep learning based SM prediction approaches. In addition to this, various research gaps and the challenges associated with the existing works of SM prediction are discussed. The reviewed works are analyzed in the basis of performance metrics, performance attained using various methods, and the datasets employed for analysis. In addition, this review presents the future scope for the researchers with the analysis of issues associated with the existing literary works.

Keywords: Soil moisture · Prediction · Agriculture · Irrigation scheduling · Yield forecast

1 Introduction

India is a nation with greater part of the people depending on agriculture for their living. Indian soils are less productive specifically in terms of micronutrients. In present years, it has been noticed that the health of soil is some way connected with the sustainability in the area of agriculture and also the present levels of crop yield can be enhanced by controlling the soil fertility. Agriculture requires decision support system in various ways such as the type of crop to be planted [1]. By screening the SM, the usage of water can be optimized to a considerable range due to the reduction in water table day by day. SM is advantageous for the production of crops so, the processes that involve in the growth of crops can be promoted with the successful prediction of SM content of any location. By evaluating the content of SM, the farmers can obtain the data about what could be the best time of planting and cultivating the crops [2]. Changes in static soil properties can be more simply evaluated as they are relatively steady in time, while dynamic soil properties are rather difficult as they change with respect to time [3].

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 225–241, 2023.
https://doi.org/10.1007/978-3-031-13150-9_20

There is a complexity associated with the uninterrupted evaluations of soil dynamic properties, including for key hydraulic properties, like SM all over the world [4, 25]. SM relies on number of factors, such as the rainfall, irrigation and level of water in the soil, water taken from the soil through evaporation, transpiration, and so on. SM content could vary the rate of minerals in the water when the soil dries or wets and eventually influences the pH of the soil [14]. For the better understanding of the interaction between soil, water and plant, expert models are considered in the present era to handle real-life issues in precision agriculture [5] for the maximization of returns [6]. It is important that the modelers of agricultural system develop and utilize present knowledge-based models for the prediction of SM content. The modeling of predictive strategies that are incorporated with the decision-support systems can lower the cost of operation, and save the time spend in instrumental evaluations. The integration of AI models in the presence of nature inspired optimization is confirmed to attain the model parameters optimally in most of the present studies that concentrated on the modeling of knowledge-oriented analytical models [7, 8].

The main intent of this article is to analyze and categorize the methods that involved in the prediction of SM through various approaches. The conventional methods of SM prediction are crucial to encourage the growth of the plants, in turn assisting in the development of agricultural field. In this paper, the most popular methods commonly used for the prediction of SM are reviewed using a total of 25 research articles. The difference between the methods of SM prediction is highlighted with their efficiency, advantages, and drawbacks. The methods generally vary with respect to the prediction strategy used, type of datasets considered, the evaluation metrics, and the implementation tools used for the experimentation. The four major categories of the SM prediction methods are the conventional methods, remote sensing based methods, machine learning methods, deep learning methods based on which most of the strategies are implemented.

The organization of the paper is, Sect. 1 describes a short prologue about the paper, Sect. 2 details the categories of classification models in SM prediction, Sect. 3 contributes the analysis and discussion about the research articles under review, Sect. 4 deliberates the limitations associated with the existing methods and provide some future directions for the development of better methods, and finally Sect. 5 concludes the paper.

2 Categorization of Soil Moisture Prediction Methods

The review of the various methods used for the prediction of SM is presented in this section. Figure 1 depicts the various SM techniques and its classification.

The techniques are mainly classified based on four approaches, namely conventional methods of SM prediction, remote sensing based methods of SM prediction, deep learning methods of SM prediction, and machine learning methods of SM prediction. The taxonomy of the various SM prediction methods provides a clear idea about the classification of SM and provides a complete deliberation over the available strategies with their advantages and limitations.

In Fig. 2, the percentage of various methods used in the research papers are depicted. Among the considered 25 research papers, 36% of the papers are based on deep learning approaches. The conventional methods occupy the least of 16% of the research papers,

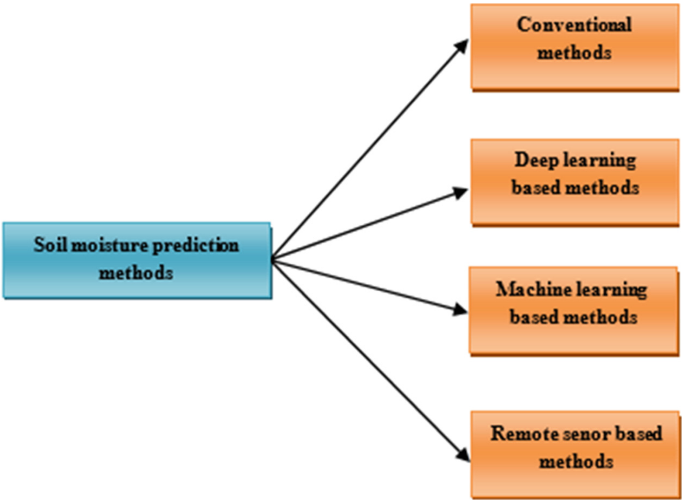


Fig. 1. Taxonomy of the soil moisture prediction methods

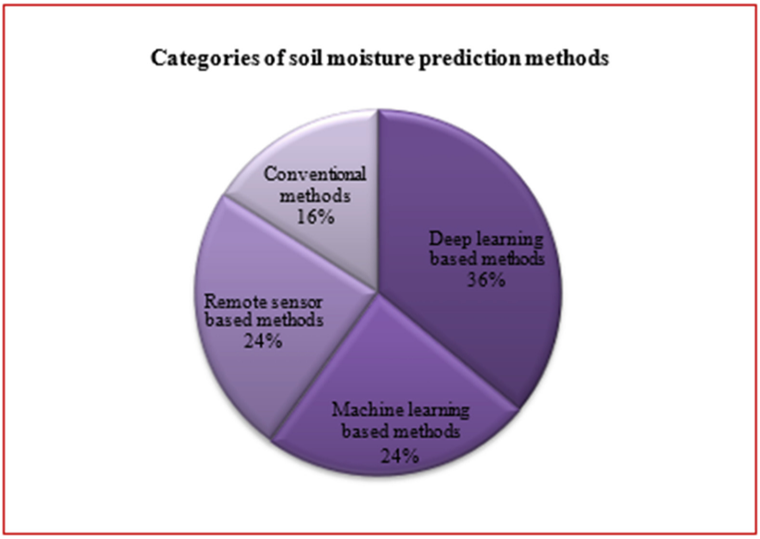


Fig. 2. Methods of soil moisture prediction

and the rest 48% of the research papers are shared equally by the machine learning strategies and the remote sensing based methods. The dominating deep learning based approach area is due to the increased efficiency and accuracy of them in making decisions, in case of new data. The deep learning based methods are capable of handling the data of high dimension without any deterioration in the performance of the system.

2.1 Conventional Methods of Soil Moisture Prediction

The conventional methods of SM prediction are capable of providing prediction in such a way to assist highly efficient irrigation. The SM prediction based on conventional methods are discussed as follows,

Dhruva Kathuria *et al.* [9] developed a geo-statistical model for the prediction and upscale of SM through a flexible spatial replica whose variance model differs by varying characteristics of the land surface. The major benefit of the developed strategy is that the strategy can be utilized for the prediction and the upscale of SM in diverse environments.

Shangrong Wu *et al.* [10] developed a microwave scattering strategy-based semi-empirical model for evaluating the SM of areas that are enveloped with winter wheat. The outcomes represent that the SM evaluations of high accuracy may be attained, and the designed model possessed enhanced performance in local functions in the analysis area at main growth levels of winter wheat.

Rajat Pandey et al. [11] designed a strategy of SM prediction with the aid of TOTRAM (thermal optical trapezoid) technique that depends on the relation between the normalized difference vegetation index (NDVI) and land surface temperature (LST).

Mohammad Hossein Jahangir and Mina Arast [12] introduced a new concept for the evaluation of the surface SM on the basis of multiindex strategies using thermal and reflective metrics that can be utilized even in lightly vegetated regions.

2.2 Remote Sensing Based Methods of Soil Moisture Prediction

The SM sensors help in enhanced organization of irrigation that sequentially produces better crops with the aid of fewer efforts. The methods based on remote sensing in the prediction of SM are,

Solmaz Fathololoumi *et al.* [13] presented a strategy that concentrates on evaluating the feasibility of static and dynamic environmental covariates and their resources, like digital elevation model (DEM) and RS images to predict SM. DSM in this research has shown a precise forecast, and hence can be suggested to predict SM, and is very cooperative in number of studies.

Velmurugan *et al.* [14] presented an open-source model on the basis of smart models for the prediction of irrigation needs of grassland with the consideration of constraints, such as SM, temperature of soil, and environmental states in addition with the forecast data of weather from web. The understanding of presented system depends on smart algorithm that make in use of the sensed data in addition with the parameters of weather forecast.

Mireguli Ainiwaer *et al.* [15] aimed to discover the viability of precisely evaluating SM level at a local scale by integrating the hyperspectral information with the multi-spectral remote sensing (Sentinel-2) data. This combination offers a scientific indication for land-space incorporated remote sensing monitoring of SM content.

Oliviu *et al.* [16] introduced a data mining strategy that gathers the data related to weather from number of weather stations to predict the SM content of next day. The prediction accuracy of the system is noticed to be high and the system is capable to operate at any geo-climatic conditions as a mature platform for agriculture.

Sabareeswaran and Guna Sundari [17] focused on designing a new technology for supervising the health of the plant by performing SM prediction Using Data Mining strategies. The outcomes are immediately forwarded to the farmers through mobile phones.

Swadhina Koley, and Jeganathan [18] tried to associate the space and incorporate multi- resolution and multi-sensor feature gap using different processes in such a way to evaluate the drought and SM. The major benefit of the developed method was the highly precise evaluation results.

2.3 Machine Learning Based Methods of Soil Moisture Prediction

The SM predictions based on machine learning techniques are efficient in prediction without the need for any human intervention. The methods based on machine learning in the prediction of SM are.

Engin Pekel [19] applied a decision tree regression for the estimation of SM with the consideration of various parameters, like time, air temperature, soil temperature, and the relative humidity. The method possesses a powerful benefit of evaluating SM as the stimulant of the decision tree regression is a model that develops a decision tree from the presented illustrations.

Masrur Ahmed et al. [20] revealed the ability of a hybridized LSTM predictive model to imitate SM under the circumstances of global warming. The strategy can be effectively executed in agriculture, hydrology, soil use organization and ecological supervision.

Sankhadeep Chatterjee et al. [21] designed a hybrid model of various methods of regression algorithms for the prediction of SM. The developed method initially groups the dataset using K- Means Clustering, and then individual regression models are applied on each cluster to train the model.

Mingshuai Liu et al. [22] introduced a SM prediction strategy on the basis of Gaussian Process Regression (GPR). For reducing the evaluation of the execution of GPR model, the Radially Uniform (RU) design strategy was integrated during training process into the selection of sample.

Nian Zhang et al. [23] developed a LSTM model, based deep learning technique for the forecast of historical monthly SM time series data. The predictions are highly accurate when revising the state of the network with examined values instead of the predicted ones.

Conrad J. Foley et al. [24] used a sequence of LSTM models to measure the evaluations of SM and vegetation metrics developed from satellite images. The model assists in predicting the future measures of such values.

2.4 Deep Learning Based Methods of Soil Moisture Prediction

The SM predictions based on deep learning techniques are capable of handling the data of larger dimension and assist in achieving enhanced prediction accuracy. The methods based on deep learning in the prediction of SM are.

Anoushka Vyas and Sambaran Bandyopadhyay [25] introduced a dynamic graph neural network that makes in use of the dependence of associated spots over a area to predict SM. The designed algorithm, termed as DGLR, offers an end-to-end learning that can predict SM over different areas in a region over time and also revise the structure of graph in between.

Sankhadeep Chatterjee et al. [26] employed a method termed as modified Flower Pollination Algorithm (MFPA) for training the Artificial Neural Network (ANN) model to predict the quantity of SM, and is found to be highly appropriate for the prediction of SM.

Zhe Gu et al. [27] modeled a NN model to learn from a process-based agricultural systems model, termed as the Root Zone Water Quality Model (RZWQM2) for the prediction of root zone SM during the time of growth of the crop.

Saman Maroufpoor et al. [8] developed an integrated intelligent model for the estimation of SM content. Based on the effectiveness of the adaptive neuro fuzzy inference system model tuned with grey wolf optimization algorithm (ANFIS-GWO), SM content was calculated.

Yang Xiaoxia and Zhang Chengming [28] developed a new model based on BPNN and PSO algorithm for the forecast of time series of SM data obtained from wireless sensor networks. The method attained enhanced convergence and accuracy in prediction, which is considered as the major advantage of the method.

Xiaoyu An and Fuxing Zhao [29] developed a longicorn beetle search algorithm (BAS) optimized BPNN prediction model. The limitation of extensive training time and slow convergence speed rectified using the BAS-BPNN, and the correctness of prediction is enhanced.

Zhe Gu et al. [30] employed a neural network ensemble (NNE) strategy to predict SM to eradicate the consequences of random parameters of NN on the accuracy of the model. The model analyses the SM dynamics properly and adequately enhanced the strength of SM prediction.

Ji Ronghua et al. [31] introduced a multilayer NN with multi-valued neurons (MLMVN), which is a different type of complex-valued NN with derivative-free back-propagation algorithm. The method showed enhanced performance in long-term prediction of SM and possesses less accumulating errors for multi-step ahead predictions.

Mars Hong Xuan Wai et al. [32] introduced a strategy using an optical system integrated with ANN for nondestructive forecast of SM range. This work states that the model developed may be reasonable for use in the improvement and future modeling of soil management.

3 Discussion and Analysis

This section deliberates the discussion and evaluation of the SM prediction techniques based on the performance metrics, dataset used, and the software tools used in the research papers.

3.1 Analysis Based on Metrics

Figure 3 shows the evaluation of the strategies in terms of evaluation metrics. From the analysis, it is noticed that most of the methods considered Root mean square error

(RMSE), Determination co-efficient (R2) as the evaluation metrics for the analysis of the performance of the methods.

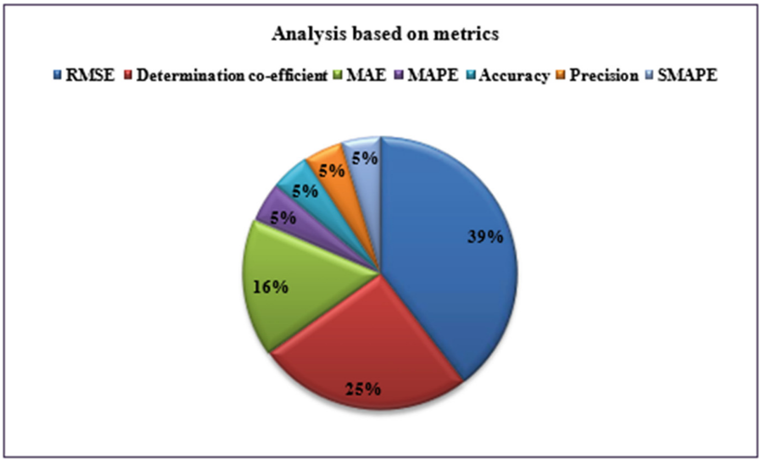


Fig. 3. Analysis based on performance metrics

Table 1 depicts the examination of 25 research papers performed based on performance indices employed for the prediction of SM. The common metrics employed for the analysis of the methods are, RMSE, R^2, Accuracy, Mean absolute percentage error (MAPE), Symmetric Mean absolute percentage error (SMAPE), Mean absolute error (MAE), and precision.

Table 1. Analysis based on metrics

Metrics	Research papers
RMSE	[8–10, 12, 15, 16, 18, 20–26, 30–32]
$R2$	[8–10, 12, 15, 18–20, 27, 30, 32]
MAE	[8, 18, 19, 22, 24, 27, 29]
MAPE	[22, 24]
Accuracy	[17, 21]
SMAPE	[25]
Precision	[17]

3.2 Analysis Based on Dataset Used

The common datasets used by the researchers for the prediction of the SM are the satellite data, Airborne data, and the randomly collected data. Figure 4 shows the analysis of the research articles based on the datasets used for analysis.

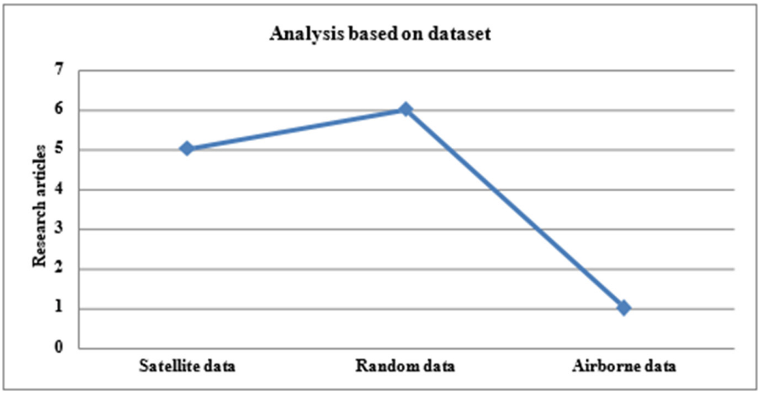


Fig. 4. Analysis based on dataset

3.3 Achievements

The achievements of the methods based on the measure of RMSE value is tabulated in Table 2. From the analysis, it is evident that most of the methods possessed negligible amount of RMSE value, stating the enhanced performance of the methods. However, some methods exhibit increased value of RMSE showing their poor performance in prediction.

Table 2. Achievement in terms of RMSE value

S. No	RMSE value	Research articles
1	1% to 2%	[1, 8, 10, 12, 22, 23]
2	2% to 6%	[2, 11]
3	3% to 4%	[17]
4	4% to 5%	[7, 29]
5	5% to 6%	[5]
6	>6%	[15, 18, 20, 25]

3.4 Survey of Papers Under Consideration

The advantages and the limitations experienced by the researches under consideration are deliberated in Table 3 as below.

Table 3. Summary of existing methods

S. No	Authors	Methods	Advantages	Limitations
1	Solmaz Fathololoumi *et al.* [13]	Digital soil mapping (DSM)	Exact prediction	Hard to verify the significance of static and dynamic covariates to extrapolative models at the big spatial scales and over longer temporal scales
2	Anoushka Vyas and Sambaran Bandyopadhyay [25]	Dynamic graph neural network	Offers an end-to-end learning that can forecast SM over different places in a region	Uncertainty in graph structure to detain the spatial correlation
3	Dhruva Kathuria *et al.* [9]	Geo-statistical framework	Can be used to forecast and upscale SM in assorted settings	Costly framework
4	Sankhadeep Chatterjee *et al.* [26]	MFPA trains ANN	Highly capable for sustainable applications related to agriculture	Highly precise and stable replica is needed to develop the model reliable
5	Velmurugan *et al.* [14]	Open-source technology based smart system	Calculate the needs of irrigation in a field with the analysis of ground parameter	Not cost effective
6	Zhe Gu *et al.* [27]	NN model	Forecasts the root zone SM throughout the growing season of the crop	May under-or over-estimate the SM
7	Engin Pekel [19]	Decision tree regression	Possess a strong benefit to conclude SM	Time consuming and requires more labour cost
8	Saman Maroufpoor *et al.* [8]	ANFIS-GWO	Highly competent	It is important to analyze the strategy with soils of different possessions to assure the use in real-time

(*continued*)

Table 3. (*continued*)

S. No	Authors	Methods	Advantages	Limitations
9	Masrur Ahmed *et al.* [20]	Hybridised LSTM predictive framework	Can be effectively used in hydrology, soil use management, agriculture, and environmental management	Data overfitting may take place
10	Shangrong Wu *et al.* [10]	Microwave scattering model-based semi-empirical method	SM evaluations of High accuracy	Need tremendously rich series of input features
11	Sankhadeep Chatterjee *et al.* [21]	Hybrid model of various kinds of regression algorithms	Reduced error of prediction	RMSE increases when the value of k increases affecting the performance of the system
12	Mireguli Ainiwaer *et al.* [15]	Multi-source remote sensing parameter based models	Offers a scientific suggestion for land-space integrated SM content remote sensing monitoring	Affects the prediction accuracy
13	Mingshuai Liu *et al.* [22]	Gaussian Process Regression (GPR)	Reduced computation time	Cannot analyze the true distribution with enhanced accuracy with fewer training data
14	Yang Xiaoxia and Zhang Chengming [28]	BPNN with PSO	Possessed higher convergence speed and prediction accuracy	May converge to local optimal solution
15	Xiaoyu An and Fuxing Zhao [29]	BAS optimized BP neural network prediction method	Improved accuracy in prediction	The prediction is high, and the effect of prediction is not perfect
16	Zhe Gu *et al.* [30]	NNE model	Improved the robustness of SM	Difficult to accurately evaluate the SM, especially when the field inconsistency is under consideration

(*continued*)

Table 3. (*continued*)

S. No	Authors	Methods	Advantages	Limitations
17	Ji Ronghua *et al.* [31]	MLMVN	Possessed enhanced performance in long- term prediction	May lead repetition and failure of information, reducing the generalization ability of the model
18	Nian Zhang *et al.* [23]	LSTM	Predictions are more precise	Poor performance
19	Oliviu *et al.* [16]	data mining strategy	Capable to operate at any geo-clmatic states as a established platform for agriculture	Complex model
20	Rajat Pandey *et al.* [11]	TOTRAM model	Enhanced prediction accuracy	Need more time and is a calculative model
21	Sabareeswaran and Guna Sundari [17]	Data Mining Techniques	The outcomes are forwarded to the cultivators via mobile phones through Messages	Complex model
22	Conrad J. Foley *et al.* [24]	Series of LSTM architectures	Learns to predict the future measures	Poor performance
23	Mohammad Hossein Jahangir and Mina Arast [12]	Estimate surface SM based on multiindex models	Can be used even in lightly vegetated areas	However, highly time consuming
24	Swadhina Koley, and Jeganathan [18]	Different scalable procedures	Highly precise evaluation results	Highly expensive
25	Mars Hong Xuan Wai *et al.* [32]	ANN	Practicable for utilization in future design	Becomes hard to measure the SM in TS- VI domain

4 Research Gap and Challenges

The limitations of reviewed techniques of SM prediction from number of literatures are discussed in this section.

4.1 Conventional Methods

Drawbacks
The drawbacks associated with the conventional methods of SM prediction are stated as below,

- The traditional techniques of SM prediction are basically critical, and time consuming necessitate more cost of labor.
- Physics based prediction of SM can be relatively precise, but they require mainly rich set of input features, like various soil properties, crop and landscape information that are difficult to obtain.
- The physical techniques are also computationally intense, making them inefficient to scale over a wider region.

Future directions
Some of the future directions while considering the conventional approaches for the prediction o SM are conveyed as,

- The relation among SM and the factors of weather with time series evaluation of SM will be concentrated, to lessen the subsistence of difficulty, and non-linear relation over SM and other associated factors of weather.
- The labor and cost of the traditional methods of SM prediction will be reduced with the introduction of better prediction strategies.
- It is suggested in future analysis to study the characteristics of the methods for a longer stage and various appliances [12].

4.2 Methods Based on Remote Sensing

Drawbacks
The drawbacks of the remote sensing based methods of SM prediction are stated as below,

- It is complex to corroborate the significance of the covariates to analytical models at the superior spatial levels and over extended temporal levels [13].
- There is a necessity to perform a water saving evaluation on the basis of the developed model in the presence of multiple nodes along with reducing the cost of the system to make the model cost-effective [14].
- The hyper-spectral data of soil comprise more unnecessary and unacceptable information, resulting in extremely intricate replica disturbing the accuracy in prediction [15].

- SM can be evaluated using soil sensors in the field or physics based land surface models. However, they possess several drawbacks. The usage of SM sensors on a vast area is costly and they cannot offer forecasts.

Future directions
Some of the future directions while considering the remote sensing based approaches for the prediction o SM are conveyed as,

- The research in [14] can be further be generalized with camera feeds for monitoring the staining of plants or leaves and hence forwards the outcomes to manage the infection from any place.
- In future, the prediction model for observing the range of growth of plant may be considered to enhance the productivity of the crop [17].
- In future, water saving analysis based on different algorithms will be conducted with different nodes along with the minimization of system cost [14].

4.3 Machine Learning Based Methods

Drawbacks
The drawbacks associated with the machine learning based methods of SM prediction are stated as below,

- The traditional AI models can come across some problems with respect to data overfitting, and this is particularly true for datasets of large dimension [20].
- It is clear from [21] that high count of clusters, the RMSE value is minimized. But when the k value is increased further, the RMSE value raises that affect the performance of the system.
- The GPR model trained using 100 samples attained the worst interval prediction characteristics over the three models. This may due to the fact that the GPR model cannot analyze the true distribution better with fewer data sample [22].

Future directions
Some of the future directions while considering the machine learning based approaches for the prediction o SM are conveyed as,

- With the expansion of the scope of developed strategies, future models can use the multivariate EMD and empirical mode decomposition (EMD) techniques. This may provide the concluding decision-making in water resources and agricultural management to implement and react to the disputes of climate variations [20].
- In future, the incorporation of RU design models and the learning algorithms, like DNN [33] and boosted regression trees [34], will be analyzed for the prediction of SM [13].
- The future analysis will obtain the SM index to make in use of it for the prediction of deficiency indicator [23].

4.4 Deep Learning Based Methods

Drawbacks

The drawbacks associated with the deep learning based methods of SM prediction are stated as below,

- The issue of SM prediction or similar indices for precision agricultural relevance is relatively different due to the dependence of numbers of external aspects and also ambiguity in the structure of graph to detain spatial relationship [2].
- The evaluation of stability has showed that more precise and constant replica is significant to formulate the system reliable [26].
- The RZWQM2 representation however still require user-written model to supply data to the instantaneous irrigation control models [27] Additionally, the developed NN technique may occasionally under or over evaluate SM [27].
- The model developed in [8] possessed enhanced capability to evaluate the high and low SM contents. However, it is important to analyze the technique with the soils of different properties to assure the usage of these strategies in real-time.
- The consideration of SM evaluations using direct strategies need time and cost, and hence emerging data-driven strategies can be commenced and utilized in various operations of agricultural fields [8].
- The error of prediction by BP technique is high, and in addition, the consequence of forecast is not perfect [29].
- It is tedious to accurately evaluate the SM, particularly when the variability of field is under consideration [30].
- In NN, with complex environmental factors as inputs and SM without any practices, may lead to duplication and failure of information, affecting the capacity of simplification by the model [31].
- The drawback of the strategy in [25] is that the nondestructive evaluation can only evaluate the surface of soil; however, it is inadequate for further deeper access of the lighting capacity.

Future directions

Some of the future directions while considering the deep learning based approaches for the prediction of SM are conveyed as,

- A future direction can be made concerning the optimization of multi objectives for training the ANN for the enhancement of performance in identifying the quantity of SM. In addition, the developed strategy can also be used in other engineering applications and sustainable science [26].
- Future task may discover development of NN oriented SM forecast and its strength over different conditions, which is the solution to dependable schedules of irrigation [27]
- The future work should be focused on the determination of a real-time scheduling system for irrigation based on the model, named NNE SM strategy [30].

5 Conclusion

This paper presents a review taxonomy that categorizes the various methods of SM prediction on the basis of techniques presented in the research articles. The major intention of the article is about to revise and analyze different types of SM prediction methods. The review and analysis is carried out using 25 research papers, which is based on the four main classifications, such as conventional strategies, remote sensing strategies, machine learning strategies, and deep learning strategies. The factors utilized for analysis includes the various performance metrics, datasets, and the strategies used for prediction. Along with this, the research gaps and the issues are presented that contributes towards a better and effective prediction strategy for SM prediction. Despite the fact, potential results have been accounted in the literature, and the results are presented in terms of RMSE value. Based on analysis, we have concluded that Deep learning based SM prediction methods possess enhanced prediction performance as compared with other methods. Moreover, the results generated by different methods are compared to perform effective analysis of the methods involved in the prediction of SM.

References

1. Hemageetha, N.: A survey on application of data mining techniques to analyze the soil for agricultural purpose. In: Proceedings of 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), IEEE, pp. 3112–3117 (2016)
2. Prakash, S., Sharma, A., Sahu, S.S.: Soil moisture prediction using machine learning. In: Proceedings of 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), pp. 1–6 IEEE (2018)
3. Aguilera, H., Moreno, L., Wesseling, J.G., Jiménez-Hernández, M.E., Castaño, S.: Soil moisture prediction to support management in semiarid wetlands during drying episodes. Catena **147**, 709–724 (2016)
4. Böhner, J., Selige, T.: Spatial prediction of soil attributes using terrain analysis and climate regionalization. 13–28 (2006)
5. Baggio, A.: Wireless sensor networks in precision agriculture. In: ACM Workshop on Real-World Wireless Sensor Networks (REALWSN 2005), vol. 20, pp.1567–1576. Stockholm, Sweden (2005)
6. Bolten, J.D., Crow, W.T., Zhan, X., Jackson, T.J., Reynolds, C.A.: Evaluating the utility of remotely sensed soil moisture retrievals for operational agricultural drought monitoring. IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens. **3**(1), 57–66 (2009)
7. Ahmad, S., Kalra, A., Stephen, H.: Estimating soil moisture using remote sensing data: a machine learning approach. Adv. Water Resour. **33**(1), 69–80 (2010)
8. Maroufpoor, S., Maroufpoor, E., Bozorg-Haddad, O., Shiri, J., Yaseen, Z.M.: Soil moisture simulation using hybrid artificial intelligent model: hybridization of adaptive neuro fuzzy inference system with grey wolf optimizer algorithm. J. Hydrol. **575**, 544–556 (2019). https://doi.org/10.1016/j.jhydrol.2019.05.045
9. Kathuria, D., Mohanty, B.P., Katzfuss, M.: A nonstationary geostatistical framework for soil moisture prediction in the presence of surface heterogeneity. Water Resour. Res. **55**(1), 729–753 (2019)
10. Wu, S., Ren, J., Chen, Z., Yang, P., Li, H.: Soil moisture estimation based on the microwave scattering mechanism during different crop phenological periods in a winter wheat-producing region. J. Hydrol. **590**, 125521 (2020)

11. Pandey, R., Goswami, S., Sarup, J., Matin, S.: The thermal–optical trapezoid model-based soil moisture estimation using Landsat-8 data. Model. Earth Syst. Environ. **7**(2), 1029–1037 (2020). https://doi.org/10.1007/s40808-020-00975-8
12. Jahangir, M.H., Arast, M.: Estimation of surface soil moisture based on improved multi-index models and surface energy balance system. Nat. Resour. Res. **30**(1), 789–804 (2020). https://doi.org/10.1007/s11053-020-09728-x
13. Fathololoumi, S., Vaezi, A.R., Alavipanah, S.K., Ghorbani, A., Saurette, D., Biswas, A.: Effect of multi-temporal satellite images on soil moisture prediction using a digital soil mapping approach. Geoderma **385**, 114901 (2021)
14. Velmurugan, S.: An IOT based smart irrigation system using soil moisture and weather prediction. Int. J. Eng. Res. & Technol. 8 (2020)
15. Ainiwaer, M., Ding, J., Kasim, N., Wang, J., Wang, J.: Regional scale soil moisture content estimation based on multi-source remote sensing parameters. Int. J. Remote Sens. **41**(9), 3346–3367 (2020)
16. Matei, O., Rusu, T., Petrovan, A., Mihuţ, G.: A data mining system for real time soil moisture prediction. Procedia Eng. **181**, 837–844 (2017)
17. Sabareeswaran, D., Guna Sundari, R.: A hybrid of plant leaf disease and soil moisture prediction in agriculture using data mining techniques. Int. J. Appl. Eng. Res. **12**(18), 7169–7175 (2017)
18. Koley, S., Jeganathan, C.: Estimation and evaluation of high spatial resolution surface soil moisture using multi-sensor multi-resolution approach. Geoderma **378**, 114618 (2020)
19. Pekel, E.: Estimation of soil moisture using decision tree regression. Theoret. Appl. Climatol. **139**(3–4), 1111–1119 (2019)
20. Masrur Ahmed, A.A., et al.: LSTM integrated with Boruta-random forest optimiser for soil moisture estimation under RCP4.5 and RCP8.5 global warming scenarios. Stoch. Env. Res. Risk Assess. **35**(9), 1851–1881 (2021). https://doi.org/10.1007/s00477-021-01969-3
21. Chatterjee, S., Kumar, S., Saha, J., Sen, S.: Hybrid regression model for soil moisture quantity prediction. In: Proceedings of 2019 International Conference on Opto-Electronics and Applied Optics (Optronix), pp. 1–5. IEEE (2019)
22. Liu, M., Huang, C., Long Wang, Y., Zhang, X.L.: Short-term soil moisture forecasting via Gaussian process regression with sample selection. Water **12**(11), 3085 (2020). https://doi.org/10.3390/w12113085
23. Zhang, N., Dai, X., Ehsan, M.A., Deksissa, T.: Development of a drought prediction system based on long short-term memory networks (LSTM). In: Han, M., Qin, S., Zhang, N. (eds.) ISNN 2020. LNCS, vol. 12557, pp. 142–153. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-64221-1_13
24. Foley, C.J., Vaze, S., El Amine Seddiq, M., Unagaev, A., Efremova, N.: SMArtCast: Predicting soil moisture interpolations into the future using Earth observation data in a deep learning framework. arXiv preprint arXiv:2003.10823 (2020)
25. Vyas, A., Bandyopadhyay, S.: Semi-supervised Soil Moisture Prediction through Graph Neural Networks. arXiv preprint arXiv:2012.03506 (2020)
26. Chatterjee, S., Dey, N., Sen, S.: Soil moisture quantity prediction using optimized neural supported model for sustainable agricultural applications. Sustain. Comput.: Inform. Syst. **28**, 100279 (2020)
27. Gu, Z., Zhu, T., Jiao, X., Junzeng, X., Qi, Z.: Neural network soil moisture model for irrigation scheduling. Comput. Electron. Agric. **180**, 105801 (2021)
28. Xiaoxia, Y., Chengming, Z.: A soil moisture prediction algorithm base on improved BP. In: Proceedings of 2016 Fifth International Conference on Agro-Geoinformatics (Agro-Geoinformatics), pp. 1–6. IEEE (2016)

29. An, X., Zhao, F.:Prediction of soil moisture based on BP neural network optimized search algorithm. In: IOP Conference Series: Earth and Environmental Science, vol. 714, no. 2, p. 022046 (2021)
30. Gu, Z., Zhu, T., Jiao, X., Junzeng, X., Qi, Z.: Evaluating the neural network ensemble method in predicting soil moisture in agricultural fields. Agronomy **11**(8), 1521 (2021)
31. Ronghua, J., Shulei, Z., Lihua, Z., Qiuxia, L., Saeed, I.A.: Prediction of soil moisture with complex-valued neural network. In: Proceedings of 2017 29th Chinese Control And Decision Conference (CCDC), pp. 1231–1236. IEEE (2017)
32. Wai, M.H., Xuan, A.H., Ngu, X.: Soil moisture level prediction using optical technique and artificial neural network. Int. J. Electr. Comput. Eng. **11**(2), 1752 (2021)
33. Verma, K., et al.: Latest tools for data mining and machine learning. Int. J. Innovative Technol. Exploring Eng. **8**(9S), 18–23 (2019). https://doi.org/10.35940/ijitee.I1003.0789S19
34. Sharma, M.N., Goel, R., Jain, A., Bhushan, M., Kumar, A.: Smart cities using internet of things: recent trends and techniques. Int. J. Innovative Technol. Exploring Eng. **8**(9S), 24–28 (2019). https://doi.org/10.35940/ijitee.I1004.0789S19

LSTM Based Advanced Fake News Detection

Aditya[1], Vikas Sihag[1(✉)], and Gaurav Choudhary[2]

[1] Sardar Patel University of Police, Security and Criminal Justice, Jodhpur, India
{spu19csa,vikas.sihag}@policeuniversity.ac.in
[2] DTU Compute, Technical University of Denmark (DTU), Lyngby, Denmark

Abstract. The digital era is proliferating, and we are in a time where we interact with lots of information in many ways. Life has become more sensitive with social media, and in the present scenario, users' activity on social media has become more frequent. The impact of social media and the news shared over it directly impacts the user. Social media is a powerful tool that can spread word of mouth in a fraction of a second. There is a variety of content and information shared all over social media and other information sources. This mystifies the user to agree on whether it is genuine or fake news. Social media has given so much power to the user that they immediately start expressing their views and concerns without checking the authenticity of the posted content. As a result, the user shares the news and becomes a spreader of fake news. This is a challenging task for the government and the country's citizens. The most popular form of unauthenticated information is rumors and fake news, and this should be combated as early as possible before it takes any dramatic consequence. For this, we propose a solution where a long short term memory(LSTM) model is used to detect the fake news, and the proposed approach attained the accuracy of 98%.

1 Introduction

Technology has surrounded humans in such a manner that it has become a crucial part of human life. The Internet has made a place in the daily routine of a person. There is the same probability that a person with screen time can see and share information that might not be genuine. Fake news is not a new term for the human era. It has always been here, but now it affects life like an intruder. Earlier, there were only traditional media, and its reach was very limited due to its propagation speed. Now, the time has completely changed, and news consumption on online platforms has increased, and now according to the survey, 68% audience uses the online platform to view news [17,22]. It is crystal clear that both the medium of news, whether traditional or digital, have a particular set of audiences. The young generation is more inclined towards digital media. In the present time, the term "Viral" is populated.

Social media is the fastest medium to spread the news in a biological virus manner. Undoubtedly, print media is reduced, and social networking sites like

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 242–256, 2023.
https://doi.org/10.1007/978-3-031-13150-9_21

Instagram, Twitter, Facebook, and YouTube have taken a new boost. This boost has taken the reach of the news to the following extent. Social media has evolved as a new medium for the consumption of news. Fake news propagates faster than usual news [3,8]. The way fake news is decorated and written, the only motive behind that is to create doubt and inflame the present dynamics of cultural and social by misapplying political, religious, and regional undertone [23]. There have been many chances in the world and in India where we have seen many riots where the root cause was fake news.

When we talk about more prominent brands and organizations, they have much bigger issues; one critical issue is nullifying the spread of false or malicious news. Suppose fake news promotes a specific viewpoint or deliberately changes the thought regarding an organization, brand, product, or any issue, social, political, or religious. In that case, it will mislead the end user [12]. There have been many examples by which some brands had got so much hate that their rating has got 1 star. The term fake news got massive popularity in the year 2016 during the presidential campaign of USA president [10]. Pollution into the information is known as fake news [11]. There are a variety of forms which can be seen in Fig. 1 and Table 2. That can justify the importance of fake news detection; it can be used to define whether news or any article can be elaborated as the procedure for estimating whether an article or any topic from any stream leads towards false or fake news. This issue is raised by the tech companies like Twitter, Facebook, Google time to address this problem, but the efforts are so less that they have hardly contributed to this issue. The authorities have not denied the Association of such tech companies and these kinds of news and sites generate a good amount of revenue for the companies (Table 1).

On the other hand, the user suffers a lot because the end person will be dealing directly with the sites that have false and fake information. This ultimately reduces the capacity of the user to interact with the healthy and good news material. The consumption of actual news is reduced, and fake is increased [1]. Social media platform aims to share material in an efficient and fast manner. Most social media platform gives the user the right to share the content. The user can share any stuff by just clicking on to share button. Many Accounts of Cambridge Analytica were compromised Twitter, and other huge giants like Facebook came forward to do more to stop the fake news spread [19]. There is much availability of fake news, which can be easily found on spamming and malicious websites. These kinds of websites have a particular intention to spread fake news. Further, this news is shredded through social networking sites and the people into it also the role of social bots cannot be denied. The user plays both roles; one is the creator, and when a user does not bother to check the authenticity of the news, it becomes the spreader of misinformation, which is another role of the user. The most effective method by which fake news can be combated is to know the news sources. Some websites are specially designed to imitate the popular news store by mimicking the name and visual. If we see adidasnews.com exactly copies to aadidasnews.com. The basic objective or we can say the motive is to trick the user and make them believe that the source they are browsing is an utmost reliable and authentic source of information. Other fake news sources can be video platforms with attractive lines on the thumbnail, facts, or any website that promotes misinformation theories. By these kinds of websites, such kinds are articles and news is grown and later on, it is harvested due to high probability of being fake. There are various sources through which we can verify fake news; for example, Politifact is a popular website to verify fake news related to politics. Basic consciousness of the user is highly recommended for fake news. Sometimes a simple fact is manipulated and presented so that the reader gets influenced by the news. The authors [16] has shown an exciting and reliable overview of the key requirement to analyze and encounter the false news. Honest and beguiling, both of the news stories must be gathered.

Moreover, that is a significant task to check the actual real facts to verify every component in the collection. For the authors, the basic key factor is length, and writing should be in a homogeneous manner. They overall suggest the importance of news delivery for the contextualization news piece. The key Aspect for gathering fake news is that facts should be checked for the false and original news set of data. The authors [18] give and superficial outline of present reality check techniques with respect to the knowledge base false news model and its identification. The expertise fact-checking of the news completely relies upon the person sitting behind to cross-check the news's authenticity. The Snopes8 and FactCheck are using similar kinds of process.in, pib.gov.in/factcheck kinds of websites. The main disadvantage with export-oriented fact-checking is that it is much costlier and time-consuming. The best alternate option for this issue can be a system that checks the facts with crowd-sourced help. This system can be used to exploit the sagacity of the population for the malicious type of news content similar to Fiskkit. The authors [18] discussed the fact-checking model that is based upon computation. Its work is based upon the algorithm and the external resource to verify the sagacity of the worthy news.

The expert-based and crowd-based factualness verification can easily be tempered to the reliable annotated data sets of the malicious news. Additionally, the mentioned facts verification services could be used to build a reliable bulk collection and false news. Snopes kind of website gives false info in the form of statements. The status of the news can be false, or it can be True.

Some websites which produce humor satirical content are also the core producer of false or malicious news. The source of the false news or the malicious news can be mostly available in the false news articles and social media(Facebook, Twitter) posts. It can be worth the task to detect content for satire and irony. One of the best examples is The Onion 11, one of the most popular USA-based satirical websites. The actual true events and stories mainly inspire the content and article this website produces. The content used in this is false and hard to believe. The writer, or the leading composer of the content, has a prominent set of mind and comes to amuse the audience. However, the writing skills and the links provided in the article will give the reader an illusion. There is a possibility that the targeted audience might believe the actual event-based false content and may share it among the surroundings.

These kinds of websites have been used as the source of data by [15] for the sake of satirical news recognition. Still, there is no filtration method for fake news detection & this is still a hugely challenging task from a research perspective. The basic task that is very complicated is gathering the media news that can be either verified or unverified.

2 Types of News

Frequently used terms that are being used in the media are Hoax, fake news, rumors. However, the research community has more concentrated and has analyzed other valuable aspects related to malicious information circulating over the internet, for example, clickbait, social media spam, and false reviews. In this section, we give a brief introduction to definitions on key aspects of news and mainly e-news which has a base of the fake info and the description of the various information origin of particular data on to the internet. This part will categorize the news wholly based upon the source and the data used in the analysis. Figure 1 gives a standard view of different types of false information.

Fig. 1. Types of misinformation

2.1 Fake News

It has been in practice to identify false information, especially for content related to the web. If we see the 2016 U.S. Presidential Campaign, it was mainly spreading during and after this. In India, 2016, Mr. Narendra Modi, the Prime Minister

Table 1. The fake news terms and their descriptions.

S.No	Term	Description	Effect
1.	Fake news	It is piece of information just to mislead the user	Targeted to damage the reputation of any organization or a person
2.	Hoax	This is simply a trick of news which is written and spread in such a way that the user believes this and in actual this is completely false.	Hides reality and spread the false
3.	Clickbait	Especially for the webpage with the intent and motive to make the user click on the link to increase the traffic on a particular.	Revenue generation and phishing attack
4.	Rumour	Piece of information which can either be true or can be false it is completely unverified.	Actual facts are hidden and user gets mislead and confuse
5.	Juke news	Completely mislead information which is written in sensationalized manner and claims to be true.	Cheap news is served to the user
6.	Prapoganda	Written in such a manner with the motive to benefit a particular political party or any particular issue.	Political or revenue profit

of India, announced the demonetization due to this cash that was under the citizen's possession became worthless. The older currency had to get deposited and exchanged with the newer one in a very short span of time that was only one month. Due to this incident, the chain reaction of a series of false and fake news was being published and circulated for clickbait and political gains. A rumor was saying that new currency had a GPS tracker, and the banks' transaction limit or deposition limit were spreading like anything. In general, it is not such a huge thing. However, the impacts created by these articles were so humongous that at one point in time Ministry of Finance released an official statement that assured the citizens that all this news was false. This incident is just a small example of how false news gets a bigger audience reach. If we talk about the definition, it should be more precise and restrictive. According to [2,6] describes that fake news can be described as an intention-based and verified false news article. It directs us to the two essential points the first is Intention and the second is variation. We can say that fake news is malicious information written with a clear mindset to mislead the targeted audience. We should not forget about the sources of verification of the misleading news. There are various sources through which we can verify the information, whether it is true or not. Some recent studies have added this definition.

In [16] there is a clear line that distinguishes the different variations of fake news. The author mainly focuses on the extreme modification of the hoaxes into large-scale and false humor. These modifications are the prototype form of fake news, a write-up with the clear intent of the malicious these things become viral very frequently on social media platforms.

Hoax, which is scaled and categorized are large are data of the false info which is disguised as the proper news [16]. These kinds of hoaxes are meant to be propagated on a large scale, not just as in the news article. The main target for these kinds of hoaxes is to target popular personalities. When we talk about the humor fake, the target and intent are very clear that they want to amuse the target audience. The author's nature should be aware that the intent is pure humor. If we talk about the example, then there are such websites as The Onion and Lercio that have shaped the news, which was satirical article as the real one. If we conclude this, there are three aspects of fake news:

1. Form in which the news article is drafted
2. Basic motivation behind the article
3. Authentication of the article

2.2 Rumour

As per the newest research literature, rumors have secured their place to study widely throughout the internet as false information. Rumors can be said to be misinformation or false news that the official authority has not confirmed. This kind of information is mainly circulated through social media platforms by the users. Social media and the internet provide the most suitable ground for the nourishment of this kind of information which are not confirmed [21]. The definition of this is as per the person defining it. The most widely accepted definition is given by [4]. Here the author describes it as the unauthorized and irrelevant information circulating in the instrumentally relevant information. [25] gives a more specific description of it. Authors say that the circulating story of questionable veracity but its credit status is questionable, producing sufficient curiosity. Rumour has the basic feature to create a direct impact reaction to the audience. We can further categorize it into, True, Partly True, Entire False and Unverified.

The rumor can be categorized concerning type and characteristics, and scope. The authors [25] say that the unverified rumor that is being spread for a more extended period and they are not verified can be said as a long-standing rumor. The spread of this is more dangerous and harmful when it is unverified. This needs to be treated with the utmost priority as a safe side. As a result, it can not be spread further, and the malicious intent gets nullified. Besides fake news & rumors, this enlightens the main interest topic for this work. There are various types of misinformation and fake content on the web, which has also been considered for the literature.

If there is a motive to attract traffic on a particular website or any news article, or any social media post, then this kind of activity is termed as Clickbait [13]. The main motive behind this is to boost the traffic on a particular website. As a result, the website gets flashed into the search results and can generate revenue. This is the major contributor to the fake news [20]. There is another community of social spammers on social media platforms. They strategically target various attacks like spreading the viruses through ads or any link. There is one more kind of term related to social spamming: fake reviews. These reviews are mostly found on an e-commerce website and many others. The motive behind this is to disrupt or make popular any product, place. If we talk about the hotel industry, the passenger is booking the hotel through a website or any online platform. The person will rely upon the reviews, and these fake reviews will misguide the person.

3 DataSet

We face several issues and challenges during the sample collection of data. We have a vast number of malicious content located in websites, crafted reviews. These kinds of stuff are created and spread the fake news daily. Finding out the fake news is itself a challenging process, and for further analysis, the sample collection of the data is far more formidable. Although there is some strict policy and rules that social media giants are using nowadays for the concerned data. The main issue for analyzing the fake news is gathering the relevant data collection intending to analyze the fake news.

When there is a discussion on collecting the data set, there should be one more point that should be kept in mind: quality. This factor is directly propositional with the supervised learning model. There should be some benchmarks and criteria that should be followed for the quality. The below Table 2 compares and shows the available set of data.

Benjamin Political News Dataset: The main target and motive behind the creation of the dataset were to promote online satirical and political stories. When we talk about the numbers, this data set has 75 stories of different categories: satire, real, and fake. It is a list that consists of fake and anonymous websites. The other part where we collect the authentic news is "Most Trusted" by business insider [7].

Burfoot Satire News Dataset: This is a kind of data set that is collected manually. There is a sample that is real 4000, and 233 satirical samples. The actual stories are collected from EN.Gigaword Corpus and the satire news are chosen according to the content chosen earlier.

BuzzFeed News: This data set is created with the help of buzzfeednews. This contains a sample that was published in Sep 2016 by facebook. This sample size is more than 2000. The source of verification is a journalist of the website. To authenticate the news relevant content like web address of the post, date of publication, the total number of share, emotions, and comments.

Credbank Dataset: This data set mainly collects the tweets in the timespan from Oct 2014 to Feb 2015. We can say that almost a year of data has been collected. In this, more than 60 million tweets with relevancy to real-world events were covered [9].

Fake News Challenge Dataset: This data set gives a massive collection of stances and tuple with more than 50000. News body and headline are the main ingredients of the tuple. This has shown all categories, whether the headline is positive or negative or discussed. The stance-based analysis is done by examining the consistency of the two, the title and the article for malicious information detection [14].

Fake News Net: This data set is a group of false and true news with number 211 accordingly. The source of data collection is BuzzFeed and Politifact. The sample has all related information like the source of publication, the content of the news, spread over social media [18].

LIAR: The main motive behind the publication of this data set is the online detection of false news. This contains more than 13000 short statements labeled in various contexts from Politifact. The data set is categorized into different categories: true, mostly true, half true, barely true, false, and pants-fire. The supporting list of the authentication of the source is also provided [24].

4 Fake News Detection

When we start with the news analysis, there are mainly two parts of it as Characterization. This part contains the viewing part of news content and Detection, which contains the detection part that means to investigate. Text data is the main content of a news article. Consequently, changes in the documents must be made within the mind of another portrayal to choose the objective to extract the feature with sufficient data that assure similarly Furthermore, reasonable to be kept up by machines. To extract feature vectors that contain enough data to guarantee an exact outline picture. The News data Classifications are shown in Fig. 2.

4.1 Digital

Meta information of the content can be author, editor, publisher, news title, and any attached multimedia. It entirely depends upon the content available in the data to extract various types of features. Syntax and lexical features can be URLs, length of words, tweets and re-tweets, hashtags. Through any multimedia, we can easily extract the visual and statistical feature with clarity score, histogram, image ratio. [18]. The creator/distributor of the news archive, next to being a portion of the news content, is likewise profoundly related to the news set. News setting is the social commitment of the news story utilization via web-based media stage. This social commitment speaks to the news engendering over time and the gathering of clients that drew in with this news archive.

Table 2. The available data set for Fake News.

S.No	DATASET	AIM
1	FEVER	Fact Extraction
2	KaggleFN	FND
3	FNC-1	Stance Detection
4	LIAR	FND
5	Weibo	FN and Rumor Detection
6	PHEME	FN and Rumor Detection
7	Twitter16	FN and Rumor Detection
8	Twitter15	FN and Rumor Detection
9	BuzzfeedPolitical	Extraction of fact
10	Cred 1 and cred 2	FND
11	NewsFN-2014	FND
12	Fake v/s Satire	FND
13	Politi Fact	FND
14	Buzzfeed news	FND
15	Gossipcop	FND
16	Information credibility	Fake news propagation in Emergency
17	Phishtank	URL Spamming link in Fake news
18	BS detector	Fake news
19.	WEKA machine learning	Fake news and clickbaits detection
20	RR Data Set	Emergency situation of twitter event

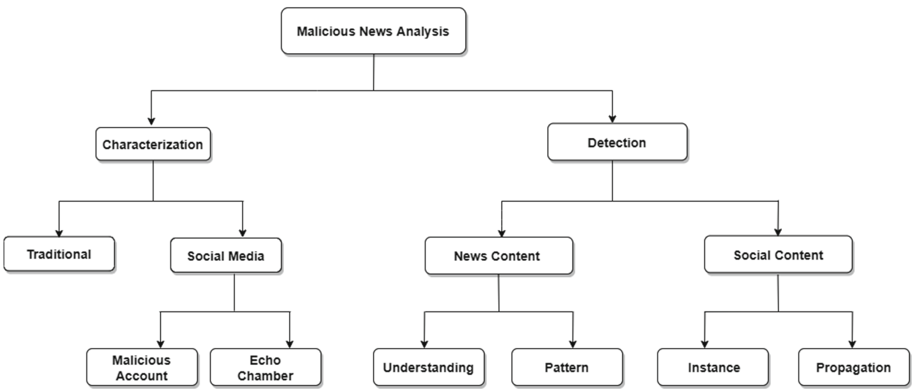


Fig. 2. News data Classifications.

Subsequently, we could remove from people, gathering, what's more, postings, social-based highlights, for example, number of devotees, companions check, enlistment age, number of composing posts/tweets, related social gatherings, segment data, client position, normal believable scores, and so on. Besides, we could extricate highlights about the space that the news story has a place with by extricating engendering highlights that consider attributes identified with the engendering tree that can be constructed from the re-tweets of a message in a specific space. These incorporate highlights, for example, the profundity of the re-tweet tree and the quantity of starting tweets of a point. A portion of the investigations on text order utilized the weighted element vectors to improve order results when all is said and done. The heaviness of each highlight shows the element's significance hence improving the arrangement results.

4.2 News Content Based

This section discusses the content of the news. More broadly, the content of the news can be categorized into two-parts

Understanding Based. A huge number of attraction has been to fact-checking and many strenuous efforts made to make an automated fact-checking system. Now the existing approach and that can be used are :

1. Expert Based: It completely relies upon a human effort to investigate relevant data and documentation to verify. The process of this is highly intellectual and time-consuming. Example- PolitiFact11, Snopes12

2. Crowd Source. It is entirely up to the "crowd wisdom." It enables the user for a description comment. These comments allow assessment of the veracity of the news. Fiskkit13 allows users to discuss a specific part of the news article, and computational notations are forwarded to produce the summarized assessment of the veracity of the news.

3. Computational Based: It allows a computational-based fact-checking method to check whether the claim is genuine or not. It Tries to entertain major issues like Identity Check Claim. For this content of news is extracted that conveys the motive and view. It mainly relies upon the external source of news. The main source can be an open web and knowledge graph(DBpedia). Distinguish the veracity of the factual claim.

Identity Check Claim. For this content of news is extracted that conveys the motive and view. It mainly relies upon the external source of news. The main source can be an open web and knowledge graph(DBpedia). Distinguish the veracity of the factual claim

Pattern. The intention for the publisher to spread the fake news is to mislead and influence the user with wrong and false information. These all are written into a particular pattern and writing style to directly communicate with the end-user and influence the mass.

Basically, there are two patterns:

Deception Based. This method takes the claims from the news content. This is a part of forensic psychology. An analysis based upon the criteria and scientific tools has also been developed. The CNN (convolutional neural networks) model, which belongs to deep network models, has been implemented to categorize fake news.

Objectivity Based. This type captures a particular signal of news material. The motive behind this is to mislead the consumers. Favoring a particular political agenda or a party in motivation to create fake news. Clickbait is the best example of this as it is written with catchy headlines to attract the reader immediately.

4.3 Social Based

This kind of scenario gives the researchers some extra resources to enhance the news content models. This includes relevant social media engagement in analyzing and capturing Info from a different perspective. This can be classified into two categories:

Particular Instance. It gains the viewpoint with the most relevant post content to see the difference with the original news. The instance can be searched by the different kinds of used emoji, the live reaction of thumbs up and down. The goal should be whether the post is in favor or against or in neutral mode.

Spreadation Based. This type of method aims towards the interrelation of social media relevant posts for the news credibility. For this two kinds of networks are proposed homogeneous, which is based on a single entity like a post or any kind of event, and heterogeneous include various entities like the post, event, sub-event. The authors [5] introduced a new credibility feature which is based upon the page rank. The algorithm works by encoding the user's credibility and tweets. This is implemented on three-layer user tweet event heterogeneous information network.

5 Fake News Detection Mechanism

Since the world is going towards digitization, technology is getting reformed day by day. The spread of false and malicious news is the biggest challenge in this digital era. This paper focuses on resolving this issue with accuracy. Although there has been much work on this side, it still seems to be insufficient for it. This paper tries to solve this problem with the help of LSTM (Long Short-Term Memory) with the help of collected data from Internet trained and test the data.

Data Collection. The dataset source is from various Internet sources, and the main source is the open datasets. There are two types of data.

Test. This data has 4 attributes which contain the id, title, author, and text.

Figure 3 shows how LSTM work. LSTM has a forward layer in the hidden layer. After inputting the data, it will forward to each node and process to the next until it reaches the output. The data contained some noise that was being removed. Then the appropriate model is being set for better results and performance.

Figure 4 is the functional diagram of proposed scheme. There are various nodes in the proposed solution; these nodes pass the information to the next node. The nodes that play the input role pass the information to the current

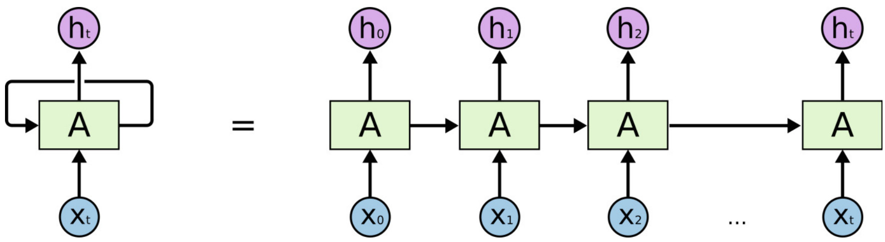


Fig. 3. The working scenario of LSTM.

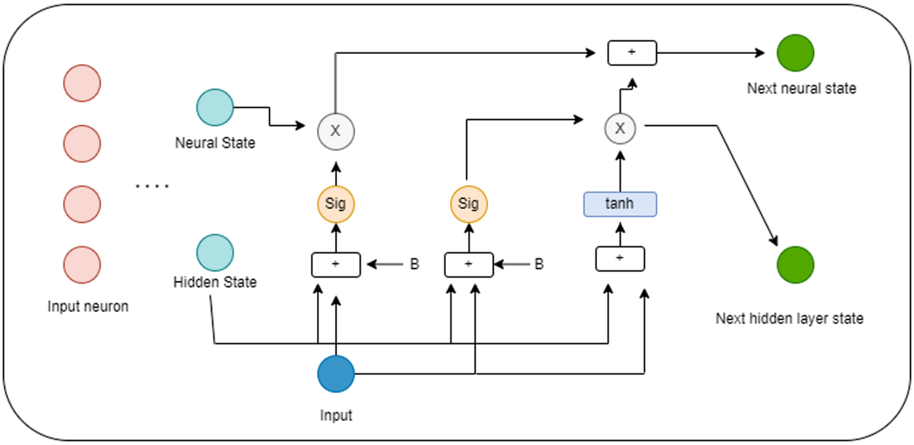


Fig. 4. The functional diagram of proposed scheme.

node. Logical operations are being performed in the hidden state, and the information is transferred to the sigmoid function. The sigmoid function is responsible for checking out the acceptance. There is one more step where biases are added before performing the logical operation to avoid fitting issues. The exact process is repeated till the tench function. Then the information is passed to the next neural node or hidden node. In the end, the relu function is used.

6 Results

This section defines the performed test results. We have performed LSTM on data sets which are discussed earlier. Before applying LSTM, the data has to go through different stages like pre-processing, cleaning, and extraction. These all enhance the strength of this model. The accuracy and Precision are shown in Table 3.

TP	3084
TN	3072
FP	20
FN	64
Pr	0.99
Re	0.97
Acc	0.98

Table 3. Result table

Model	Result
LSTM	Precision=0.99
	Recall =0.97
	Accuracy =0.98

7 Conclusion

In the present scenario, fake news is one of the most threatening issues for social media. Malicious entities can utilize this medium to manipulate the decision and various options. Fake news has influenced many sectors in various activities like shopping, education, and even elections were influenced by the fake news. This paper provided a superficial view of online fake news detection—understanding of online fake news like creators or fake news spreaders, news contents, and social context. It proposed an LSTM based fake news detection mechanism. Furthermore, In this paper, we have tried to cover the potential topic regarding false information based on computer-based communication media. In today's digital life, fake news and rumors have played a crucial role. As a result, they have been proved to be very dangerous in a digital system and outside of this devitalized ecosystem. Our motive is to provide a clear definition and distinctions for fake news and rumors and their various types. We have tried to distinguish the various aspects of big news and the terms related to fake news. We have to try the relevant data and techniques to collect valuable fake news. Fake news and clickbait can divert a user's mind from important news, and it becomes more critical when the user has to make any decision. As the business scenario in the digital world is completely changing, it warns the user regarding fake news. There needs to be a solution that can nullify this kind of information from the root level in future work. As this is traveling into a tree, there is a need to identify the primary root. Early detection techniques can also work out for the same.

References

1. Aldwairi, M., Alsalman, R.: MALURLs: malicious URLs classification system. In: Annual International Conference on Information Theory and Applications (2011)

2. Allcott, H., Gentzkow, M.: Social media and fake news in the 2016 election. J. Econ. Perspect. **31**(2), 211–36 (2017)
3. Choudhary, A., Arora, A.: Linguistic feature based learning model for fake news detection and classification. Expert Syst. Appl. **169**, 114171 (2021)
4. DiFonzo, N., Bordia, P.: Rumor, gossip and urban legends. Diogenes **54**(1), 19–35 (2007)
5. Gupta, A., Lamba, H., Kumaraguru, P., Joshi, A.: Faking sandy: characterizing and identifying fake images on twitter during hurricane sandy. In: Proceedings of the 22nd International Conference on World Wide Web, pp. 729–736 (2013)
6. Gupta, T., Choudhary, G., Sharma, V.: A survey on the security of pervasive online social networks (POSNs). J. Internet Serv. Inf. Secur. (JISIS) **8**(2), 48–86 (2018)
7. Horne, B.D., Adali, S.: This just in: fake news packs a lot in title, uses simpler, repetitive content in text body, more similar to satire than real news. arXiv preprint arXiv:1703.09398 (2017)
8. Mendoza, M., Poblete, B., Castillo, C.: Twitter under crisis: can we trust what we RT? In: Proceedings of the First Workshop on Social Media Analytics, pp. 71–79 (2010)
9. Mitra, T., Gilbert, E.: CREDBANK: a large-scale social media corpus with associated credibility annotations. In: ICWSM, pp. 258–267 (2015)
10. Niklewicz, K.: Weeding out fake news: an approach to social media regulation. Eur. View **16**(2), 335–335 (2017)
11. Pierri, F., Ceri, S.: False news on social media: a data-driven survey. ACM SIGMOD Rec. **48**(2), 18–27 (2019)
12. Potthast, M., Kiesel, J., Reinartz, K., Bevendorff, J., Stein, B.: A stylometric inquiry into hyperpartisan and fake news. arXiv preprint arXiv:1702.05638 (2017)
13. Qbeitah, M.A., Aldwairi, M.: Dynamic malware analysis of phishing emails. In: 2018 9th International Conference on Information and Communication Systems (ICICS), pp. 18–24. IEEE (2018)
14. Riedel, B., Augenstein, I., Spithourakis, G.P., Riedel, S.: A simple but tough-to-beat baseline for the fake news challenge stance detection task. arXiv preprint arXiv:1707.03264 (2017)
15. Rubin, V.L.: Disinformation and misinformation triangle. J. Documentation (2019)
16. Rubin, V.L., Chen, Y., Conroy, N.K.: Deception detection for news: three types of fakes. Proc. Assoc. Inf. Sci. Technol. **52**(1), 1–4 (2015)
17. Sahoo, S.R., Gupta, B.B.: Multiple features based approach for automatic fake news detection on social networks using deep learning. Appl. Soft Comput. **100**, 106983 (2021)
18. Shu, K., Sliva, A., Wang, S., Tang, J., Liu, H.: Fake news detection on social media: a data mining perspective. ACM SIGKDD Explor. Newsl. **19**(1), 22–36 (2017)
19. Smith, J., Leavitt, A., Jackson, G.: Designing new ways to give context to news stories. Facebook Newsroom (2018). https://newsroom.fb.com/news/2018/04/inside-feed-article-context
20. Talwar, S., Dhir, A., Singh, D., Virk, G.S., Salo, J.: Sharing of fake news on social media: application of the honeycomb framework and the third-person effect hypothesis. J. Retail. Consum. Serv. **57**, 102197 (2020)
21. Vosoughi, S., Mohsenvand, M.N., Roy, D.: Rumor gauge: predicting the veracity of rumors on Twitter. ACM Trans. Knowl. Discov. Data (TKDD) **11**(4), 1–36 (2017)
22. Wang, Y., Wang, L., Yang, Y., Lian, T.: Semseq4fd: integrating global semantic relationship and local sequential order to enhance text representation for fake news detection. Expert Syst. Appl. **166**, 114090 (2021)

23. Wardle, C., Derakhshan, H.: Information disorder: toward an interdisciplinary framework for research and policy making. Council of Europe report, 27, 2017
24. Wu, L., Liu, H.: Tracing fake-news footprints: characterizing social media messages by how they propagate. In: Proceedings of the Eleventh ACM International Conference on Web Search and Data Mining, pp. 637–645 (2018)
25. Zubiaga, A., Liakata, M., Procter, R., Bontcheva, K., Tolmie, P.: Towards detecting rumours in social media. arXiv preprint arXiv:1504.04712 (2015)

HTL-DP: Homogeneous Transfer Learning for Defect Prediction

Meetesh Nevendra(✉) and Pradeep Singh

Department of Computer Science and Engineering, National Institute of Technology Raipur, Raipur, India
{mnevendra.phd2018.cs,psingh.cs}@nitrr.ac.in

Abstract. Most approaches to predict software defects require extensive projects under training and testing. However, sufficient training information is often not available for a new project. Therefore, a predictive model should be built using historical data from additional relevant projects, followed by using the model to predict defects in the target project. The performance of this cross-project technique still has to be increased, mainly because of the distribution divergences among the source and target projects and the ambiguity about which source project should be chosen to train the model. This study proposes a Homogeneous Transfer Learning Model for Defect Prediction (HTL-DP), which covers two phases: the conversion of images and the prediction of defects. To improve the overall performance of this system, we use the popular ResNet18 to compare it with several state-of-the-art techniques and five different pre-defined deep models. We demonstrate that the framework proposed in this paper provides higher performance with exterior analysis of a 10-software project image data set than that available in the existing literature. Literature also shows that transforming multidimensional software metrics into images is more significant than direct conversion from code into images.

Keywords: Software defect prediction · Transfer learning · Deep learning

1 Introduction

Software defects can ultimately lead to system failures, substantial financial and human losses. Deficiencies of this type can be detected and removed at various test levels prior to software release. But software testing is a labour-intensive and time-consuming activity. Valuable resources must be effectively allocated for the success of a project. In this context, precise prediction of software defects is crucial for improving software quality by assigning precious resources to defective modules. There is a need for a good set of historical data to create a defect prediction model to achieve high prediction performance. Cross-project defect prediction (CPDP) can be employed without sufficient data within a company, whereas other companies use data to create predictors. The differences between sources and target projects have resulted in a significantly lower prediction performance for the defect predictor data learned from cross-project (CP) data than that obtained by the within project (WP) data [1]. Therefore, the use of sufficient CP data and

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 257–267, 2023.
https://doi.org/10.1007/978-3-031-13150-9_22

insufficient WP data to build a predictor could be a significant issue before an adequate amount of WP data are collected.

Transfer learning (TL) has recently been intended to conquer the difference in distribution amongst two domains, which means that general information can be obtained from one domain and transferred to the other. CPDP can be considered a TL branch, namely domain adaptation [2]. It requires that the source domain data set is used as the marked training set, whereas the target domain dataset is used as the non or only weakly marked test set. However, even though the data distributions are different, information from the source domain can still be used in the target domain to complete a task since it is associated.

A feature-based TL method, namely the transfer component analysis (TCA), has been suggested by Pan et al. [3], which represents data from diverse fields into the same latent feature space. Nam et al. [4] examined that, when combined with TCA, different standardization approaches for source and target domain data can have diverse transfer performances. As a result, it has developed the most appropriate standardization method for supporting TCA, based on the similarity between source/target domains and proposed TCA+. They used it for the CPDP, achieving the better performance of predictions.

This work brings together a limited availability of target area data and deeper learning mechanisms in the context of the research and transfer of learning in the context of software image classification. Adapting the deep learned and more abstract representation of the source domain produces higher prediction results in the target domain. In short, the contribution of this paper shows the effect of augmentation and DP in homogeneous scenarios using deep transfer learning (DTL). The model is made on the original feature space, which is then used to predict the defects in the target project. The contribution of the paper is:

- We suggest a new methodology for defect prediction based on software metrics as an image to capture their semantic and structural information.
- We suggest a deep learning end-to-end framework consisting of a DTL model that considers program feature images either 'defect' or 'not defects'.
- Our experiments on 10 open-source Java projects demonstrate that our approach improves in the CPDP scenarios.

The remainder of this paper is organized as follows. First, we review related work in Sect. 2. The proposed approach HTL-DP is explained in Sect. 3. The result is defined in Sect. 4. Statistical tests and threats to validity are explained in Sects. 5 and 6. Finally, we conclude our work.

2 Related Work

Software defect prediction (SDP) is a mechanism for predicting defective software modules. SDP can optimize the necessary resources for testing. Many approaches have been proposed [5–8] to find more effective SDP models. Most approaches focused on within project defect prediction (WPDP) models, which are applicable only when there is a sufficiently large number of historical data. More recent attention has been shown to whether CPDP applies to a project when there are no or insufficient local data for an organization in the development sector.

Zimmermann et al. [3] have pointed out that CPDP has little or insufficient data to build project predictors. 622 CPDPs were delivered, and only 3.4% succeeded. The data and process characteristics are crucial to the CPDP's success. The CPDP was a challenging issue to be investigated by more researchers. Turhan et al. [5] have proposed a nearest-neighbour filtering CPDP mechanism. They noted that a defect classification learned from WP information is higher than that learned from CP data. They proposed a two-phase approach based on the findings. In phase one, companies are recommended to use CPDP and start collecting WP data. Once sufficient WP information is collected, companies should stop using CP data and use WP data predictors in Phase two. They noted the importance of WP data for prediction performance improvement. Machine learning approaches assume the distribution of features between training data and test data. If such a presumption fails, prediction models will be ineffective. To resolve this problem, TL techniques derived knowledge from a source project to build models for the target project. There are some approaches to addressing the problem, given sufficient labelled source data and insufficient labelled target data.

The transfer defect approach was initially proposed by J. Nam et al. [2]. This article used TCA to make functional distributions similar in source and destination projects to the state-of-the-art transfer study approach. They also proposed a new approach to learning defects, TCA+, through TCA extension. The experimental results for 8 open-source projects show that TCA+ dramatically improves the performance of cross-project prediction. D. Ryu et al. [6] proposed a cost-sensitive transfer boosting method, which considers both the transmission of knowledge and class imbalance if a small number of the targets are identified. The proposed approach boosts that weighs both the distributional properties and the class imbalance in the training instances. The model provides significantly higher accuracy in defect detection while keeping a better overall performance through comparative experiments with TL and class imbalance learning techniques. J. Chen et al. [7] suggested a multiview software defect prediction TL, known as MTDP, which automatically learns labels using neural network models to accomplish various dimensions and granularity features. The results of the experiments show that virtually real instances have similar effects than real instances. In another study by J. Chen et al. [8] offer a DTL framework for software defects prediction that can directly get results for programs without using feature extraction tools. Experiments have been conducted on ten PROMISE datasets open-source projects to demonstrate that the method can improve cross-project and within-project defect prediction. The collective TL mechanism for defect prediction has also been demonstrated by J. Chen et al. [9]. The approach compares the feature distributions of the source and target projects through TL and uses the particle swarm optimization algorithm to take the multiple source projects fully into consideration to predict the target project.

There are no existing DTL methods that show the effect of image conversion from multidimensional software metrics data. This article shows DTL's effect to prevent defects by converting images from multidimensional software metrics data.

3 Methodology

Figure 1 shows the overall framework for our approach HTL-DP. It consists of 2 phases, 1) Data creation and 2) DTL modelling. In the first stage, we convert the multidimensional software metrics project into images. Then we develop a DTL model that uses the ResNet18 Network Structure to build an end-to-end prediction framework in the second stage. We predict whether or not a new instance file is defective by using this framework.

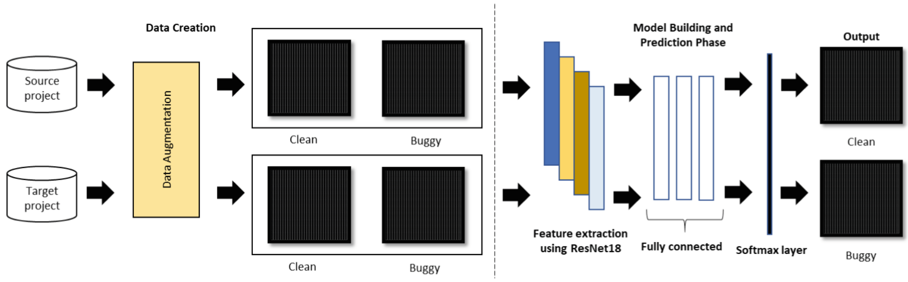


Fig. 1. The overall framework of HTL-DP.

In our approach, first, we convert the multidimensional software metrics into images. First, the square image dimensions of the array are calculated, and the flat array is converted into 2D. From this array, we produce an image by placing its values in rows and columns and interpreting it as a rectangular image. The 0 = black and 245 = white, grayscale would be an easy way to view 8-bit values as colour intensity. However, because our original training set is relatively small in size, we have a deep and insufficiently trained model. Fortunately, the added benefit of using training images is that the original data set can be expanded to make a larger dataset with the same semanticists. Data augmentation is a strategy that allows practitioners to considerably increase the diversity of data for training models without actually collecting new information. Data augmentation techniques include flipping, rotating, cutting, padding, gaussian noise zooming, and scaling. We used symmetrical padding to enlarge our project image. Once the image is created, we choose each image one by one for training and testing, then use it to build the evaluation model for defect prediction using ResNet18.

For CPDP, we use different projects and versions as listed in Table 1. One version of the project is used to generate the training data, and the other version of the different projects is used as test data. An average of 10 runs collected the performance measure for the models.

He et al. [7] proposed residual networks (ResNet) for the 2015 ILSVRC classification project deliver state-of-the-art performance and allow the training of extremely deep networks with up to 1,000 levels. It was the top-5 error of 3.57% in the ILSVRC 2015 classification competition. ResNet core idea introduces an "identity shortcut" that skips one or more layers, as illustrated in Fig. 2.

Padding is commonly used to accommodate the finite image area and permit the convolutional kernel's support to stretch across an image and reduce the impact of the border effects [8]. In this paper, we used symmetric padding techniques to enlarge

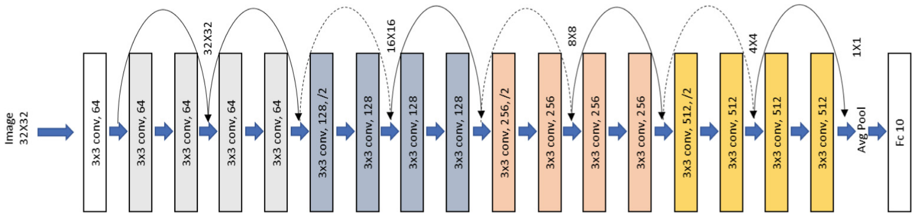


Fig. 2. The architecture of the ResNet18 model.

the image that created from the source project. Because the pre-defined deep model RestNet18 takes 221 $\times$ 221 $\times$ 3 as an input dimension. In the symmetric padding, it pads with the reflection of the vector mirrored along the edge of the array. Figure 3 shows the image padding using the symmetric padding technique.

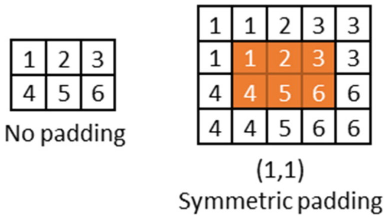


Fig. 3. Symmetric padding techniques.

We used data from the PROMISE data repository to compare our findings with previous research [9]. The datasets are imbalanced in nature. The description of the datasets is shown in Table 1.

Table 1. Dataset description

Project	Description	Version	Defective %
ant	Java based build tool	1.5,1.6,1.7	13.4
camel	Enterprise integration framework	1.2,1.4,1.6	18.7
jEdit	Text editor designed for programmers	3.2,4.0,4.1	19.2
log4j	Logging library for Java	1.0,1.1	49.7
lucene	Text search engine library	2.0,2.2,2.4	35.8
xalan	A library for transforming XML files	2.4,2.5	29.6
xerces	XML parser	1.2,1.3	15.7
ivy	Dependency management library	1.4,2.0	20.0
synapse	Data transport adapters	1.0,1.1,1.2	22.7
poi	Java library to access Microsoft format files	1.5,2.5,3.0	40.7

Precision, recall, and F-measure are the most often used performance measures for DP. The F-measure can indicate both accuracy and recall, providing a more complete assessment of predictive ability [10, 11]. As a result, it is used as the performance metric in this work.

$$P = TP/(TP + FP) \tag{1}$$

$$R = TP/(TP + FN) \tag{2}$$

$$F - measure = (2 \times P \times R)/(P + R) \tag{3}$$

4 Result

In this section, we discuss HTL-DP results compared to the other models. For CPDP, we utilized all the generated datasets and predicted the defectiveness using the ResNet18 pre-trained model. Table 2 shows the comparison of the proposed approach with a different well known pre-defined deep model. From Table 2, we can see the different obtained outcomes of deep models compared to the proposed HTL-DP. The proposed approach HTL-DP shows a significant effect over the all-other pre-defined deep model for WPDP scenarios. It achieves 0.714 F-measure, which is the highest amongst all.

Table 2. Comparison of proposed-approach with a different well known pre-defined deep model.

Source	Target	AlexNet	DenseNet201	ResNet50	GoogLeNet	Squeeze Net	HTL-DP
ant1.6	camel1.4	0.898	0.891	0.786	0.907	0.894	**0.902**
jedit4.1	camel1.4	0.903	0.892	0.901	0.877	**0.904**	**0.904**
camel1.4	ant1.6	0.847	0.892	0.832	0.849	**0.897**	0.849
poi3.0	ant1.6	0.585	0.459	0.579	**0.694**	0.333	0.585
camel1.4	jEdit4.1	0.863	**0.873**	0.821	0.858	0.855	0.830
log4j1.1	jEdit4.1	0.817	0.846	0.819	**0.863**	0.855	0.771
jEdit4.1	log4j1.1	0.819	0.830	0.820	0.800	0.814	**0.893**
lucene2.2	log4j1.1	0.438	**0.533**	0.460	0.317	0.238	0.481
lucene2.2	xalan2.5	0.307	0.499	0.581	0.453	0.268	**0.644**
xerces1.3	xalan2.5	0.679	0.612	0.683	**0.692**	0.684	0.683
xalan2.5	lucene2.2	0.431	0.371	0.373	**0.466**	0.357	0.388
log4j1.1	lucene2.2	**0.496**	0.460	0.459	0.455	0.473	0.478

(*continued*)

Table 2. (*continued*)

Source	Target	AlexNet	DenseNet201	ResNet50	GoogLeNet	Squeeze Net	HTL-DP
xalan2.5	xerces1.3	0.741	0.715	0.769	0.824	0.756	**0.888**
ivy2.0	xerces1.3	0.919	0.903	**0.921**	0.919	0.918	0.914
xerces1.3	ivy2.0	0.884	0.919	0.885	0.938	**0.940**	0.782
syapse1.2	ivy2.0	0.883	0.913	0.832	0.887	**0.921**	0.820
ivy1.4	synapse1.1	**0.844**	0.814	0.823	**0.844**	**0.844**	0.838
poi2.5	synapse1.1	0.553	0.489	**0.794**	0.356	0.297	0.485
ivy2.0	synapse1.2	0.806	0.763	0.792	0.798	0.798	**0.808**
poi3.0	synapse1.2	0.620	0.396	0.573	0.542	0.246	**0.673**
synapse1.2	poi3.0	**0.621**	0.532	0.560	0.534	0.552	0.537
ant1.6	poi3.0	0.532	0.528	0.532	0.540	**0.562**	0.554
Average		0.704	0.688	0.709	0.701	0.655	**0.714**

We compare our approach to the four baseline approaches, representing two different kinds of defect prediction methods. TCA+, LSTM, CNN, and DTL-DP are the baselines for deep learning-type methods based on extracting features from AST. Table 3 shows the F-measure values for the WPDP experiments. The highest F-measure values of the 6 methods are shown in bold. On average, the F-measure of our approach HTL-DP is 0.714, and the TCA+, LSTM, CNN, and DTL-DP achieve 0.479, 0.485, 0.528 and 0.618, respectively. The results demonstrate that our approach is competitive and improve defect prediction compared to TCA+, LSTM, CNN, and DTL-DP. Thus, we can demonstrate that converting multidimensional software metrics into images is more relevant than directly converting code into images because extracting historical data and converting an image is getting more important characteristics than direct conversion of code to an image.

Table 3. Comparison of the HTL-DP with the state-of-the-art approaches.

Source	Target	TCA+	LSTM	CNN	DTL-DP	HTL-DP
ant1.6	camel1.4	0.292	0.321	0.323	0.395	0.902
jedit4.1	camel1.4	0.330	0.318	0.651	0.407	0.904
camel1.4	ant1.6	0.616	0.448	0.607	0.591	0.849
poi3.0	ant1.6	0.598	0.386	0.532	0.693	0.585
camel1.4	jEdit4.1	0.537	0.394	0.547	0.531	0.830

(*continued*)

Table 3. (*continued*)

Source	Target	TCA+	LSTM	CNN	DTL-DP	HTL-DP
log4j1.1	jEdit4.1	0.419	0.389	0.423	0.639	0.771
jEdit4.1	log4j1.1	0.574	0.574	0.656	0.783	0.893
lucene2.2	log4j1.1	0.571	0.578	0.632	0.794	0.481
lucene2.2	xalan2.5	0.530	0.680	0.540	0.689	0.644
xerces1.3	xalan2.5	0.581	0.676	0.562	0.686	0.683
xalan2.5	lucene2.2	0.561	0.750	0.621	0.783	0.388
log4j1.1	lucene2.2	0.524	0.750	0.663	0.769	0.478
xalan2.5	xerces1.3	0.394	0.340	0.391	0.400	0.888
ivy2.0	xerces1.3	0.398	0.261	0.421	0.420	0.914
xerces1.3	ivy2.0	0.409	0.264	0.467	0.472	0.782
synapse1.2	ivy2.0	0.383	0.261	0.371	0.494	0.820
ivy1.4	synapse1.1	0.348	0.451	0.491	0.545	0.838
poi2.5	synapse1.1	0.376	0.435	0.436	0.597	0.485
ivy2.0	synapse1.2	0.570	0.530	0.456	0.620	0.808
poi3.0	synapse1.2	0.542	0.503	0.532	0.623	0.673
synapse1.2	poi3.0	0.651	0.785	0.671	0.827	0.537
ant1.6	poi3.0	0.343	0.785	0.627	0.827	0.554
Average		0.479	0.495	0.528	0.618	0.714

5 Statistical Test

The study uses the Friedman statistical test and Tukey's Honest Significant Difference (HSD) test to evaluate the predictive capability of various techniques. These tests are non-parametric in nature, thus being used without violating the various underlying data assumptions necessary for parametric tests. Tukey's HSD test allows you to determine the significant difference between the different means pairs, if any of them.

From the observation of Table 4, the proposed approach overpasses the other state-of-the-art techniques. It demonstrates that the f-ratio is 10.14025, with a p-value is .00001, where the result is significant at $p < .05$. The important values are displayed in bold. The test, descriptive, and mean range comparisons are shown in Tables 5 and 6 of the Friedman report. For the observation of Table 5 and Table 6, the proposed approach obtained the highest median value and reached the highest mean rank.

Table 4. Tukey's HSD pairwise comparison.

Pairwise comparisons		$HSD_{.05} = 0.1211$ $HSD_{.01} = 0.1457$	$Q_{.05} = 3.9255$ $Q_{.01} = 4.7239$
TCA+: LSTM	TCA+ = 0.48	0.02	Q = 0.49 (p = .99687)
	LSTM = 0.49		
TCA+: CNN	TCA+ = 0.48	0.05	Q = 1.58 (p = .79627)
	CNN = 0.53		
TCA+: DTL-DP	TCA+ = 0.48	0.14	Q = 4.48 (p = .01692)
	DTL-DP = 0.62		
TCA+: HTL-DP	TCA+ = 0.48	0.23	Q = 7.61 (p = .00000)
	HTL-DP = 0.71		
LSTM: CNN	LSTM = 0.49	0.03	Q = 1.09 (p = .93792)
	CNN = 0.53		
LSTM: DTL-DP	LSTM = 0.49	0.12	Q = 3.99 (p = .04453)
	DTL-DP = 0.62		
LSTM: HTL-DP	LSTM = 0.49	0.22	Q = 7.12 (p = .00002)
	HTL-DP = 0.71		
CNN: DTL-DP	CNN = 0.53	0.09	Q = 2.90 (p = .25105)
	DTL-DP = 0.62		
CNN: HTL-DP	CNN = 0.53	0.19	Q = 6.02 (p = .00042)
	HTL-DP = 0.71		
DTL-DP: HTL-DP	DTL-DP = 0.62	0.10	Q = 3.13 (p = .18320)
	HTL-DP = 0.71		

Table 5. Descriptive statistics of the results from the Friedman test.

	N	Minimum	25th percentile	Median	75th percentile	Maximum
TCA+	16	0.2920	0.383	0.527	0.571	0.651
LSTM	16	0.2610	0.340	0.450	0.676	0.785
CNN	16	0.3230	0.436	0.536	0.627	0.671
DTL_DP	16	0.3950	0.494	0.621	0.769	0.827
HTL-DP	16	0.3880	0.554	0.777	0.849	0.914

Table 6. Friedman test means rank comparisons.

Variable	Mean rank	Different (P < 0.05) from variable nr
(1) TCA+	2.1591	(4) (5)
(2) LSTM	2.0682	(4) (5)
(3) CNN	2.7727	(4) (5)
(4) DTL_DP	3.8636	(1) (2) (3)
(5) Proposed approach	4.1364	(1) (2) (3)

6 Threats to Validity

Experimental mistakes and baseline replication methods cause internal validity threats. This paper reproduces no changes for the baseline method. The pre-defined methods were used directly. Because ResNet is already a pre-trained model without further modifications. Nevertheless, we collected the dataset from the well-known ROMIOSE repository, which converted an image to predict project defectiveness. We do not change the project's instance, function or label. To predict the target project, it must be predicted that unlabeled instances will assist in identifying the defect. Consequently, labelled source instances are used in this paper to generate weights and thresholds when the CPDP is reproduced and then used to predict unlabeled samples.

The external threat to the validity of the results is lies in the generalizability of the results. We have already testified to our method in 10 projects groups, including 26 open-source projects. We will be experimenting with more datasets to alleviate this threat in the future. The data set's quality is a possible influence. Further experiments must verify the conversion of an image and different data augmentation schemes in the future.

Validity threats depend on the adequacy of assessment measurement. We use F-measure as our key assessment method to evaluate its effectiveness in many past defect prediction studies. It does not contain sufficient detailed code characteristics because of the coarse grain of the data set used in this experiment. Therefore, the improvement of its cost performance cannot be evaluated, such as how many actual defects are predicted to be defective in the first 20% of codes. This is why we use F-measure to consider the prediction's accuracy and recall rate fully.

7 Conclusion

SDP is critical for increasing software quality since it helps focus resources on problematic modules. When local data are insufficient, CPDP uses defect data from other projects to increase prediction accuracy. For the most part, the distributional difference is addressed by calculating and transferring similarity weights based on distributional characteristics from the source to the target projects. In this paper, we show the effect of padding concerning DTL. Our experimental results on 10 open-source projects show that deep learning can be used to prevent defects. In particular, our approach is one of the most advanced CPDP approaches. It also bests the other deep learning and state-of-the-art approaches TCA+, LSTM, CNN and DTL-DP by 39.39%, 36.22%, 29.95% and 14.41%, respectively. Moreover, the direct conversion from code into images, the image conversion of multidimensional software metrics data proves more relevant. The superior performance delivered by the HTL-DP proves an effective solution when training data is limited and sparse.

References

1. He, Z., Shu, F., Yang, Y., Li, M., Wang, Q.: An investigation on the feasibility of cross-project defect prediction. Autom. Softw. Eng. **19**, 167–199 (2012). https://doi.org/10.1007/s10515-011-0090-3
2. Long, M., Wang, J., Ding, G., Pan, S.J., Yu, P.S.: Adaptation regularization: a general framework for transfer learning. IEEE Trans. Knowl. Data Eng. **26**, 1076–1089 (2014). https://doi.org/10.1109/TKDE.2013.111
3. Pan, S.J., Tsang, I.W., Kwok, J.T., Yang, Q.: Domain adaptation via transfer component analysis. IEEE Trans. Neural Netw. **22**, 199–210 (2011). https://doi.org/10.1109/TNN.2010.2091281
4. Nam, J., Pan, S.J., Kim, S.: Transfer defect learning. In: 2013 35th International Conference on Software Engineering (ICSE), pp. 382–391. IEEE (2013). https://doi.org/10.1109/ICSE.2013.6606584
5. Turhan, B., Menzies, T., Bener, A.B., Di Stefano, J.: On the relative value of cross-company and within-company data for defect prediction. Empir. Softw. Eng. **14**, 540–578 (2009). https://doi.org/10.1007/s10664-008-9103-7
6. Chen, J., Yang, Y., Hu, K., Xuan, Q., Liu, Y., Yang, C.: Multiview transfer learning for software defect prediction. IEEE Access. **7**, 8901–8916 (2019). https://doi.org/10.1109/ACCESS.2018.2890733
7. He, K., Zhang, X., Ren, S., Sun, J.: Deep residual learning for image recognition. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 770–778 (2016). https://doi.org/10.1002/chin.200650130
8. Liu, G., et al.: Partial Convolution based Padding. arXiv (2018)
9. tera-PROMISE: Welcome to one of the largest repositories of SE research data. http://openscience.us/repo/. Accessed 30 Nov 2017
10. Xia, X., Lo, D., Pan, S.J., Nagappan, N., Wang, X.: HYDRA: massively compositional model for cross-project defect prediction. IEEE Trans. Softw. Eng. **42**, 977–998 (2016). https://doi.org/10.1109/TSE.2016.2543218
11. Chen, J., Hu, K., Yang, Y., Liu, Y., Xuan, Q.: Collective transfer learning for defect prediction. Neurocomputing **416**, 103–116 (2020). https://doi.org/10.1016/j.neucom.2018.12.091

Development of a Chi-Square Approach for Classifying Ischemic Stroke Prediction

Micheal Olaolu Arowolo[1], Victor Ashem Akubor[1], Sanjay Misra[2](✉), Lalit Garg[3], Marion Olubunmi Adebiyi[1], and Joseph Bamidele Awotunde[4]

[1] Department of Computer Science, Landmark University, Omu Aran, Kwara, Nigeria
{arowolo.olaolu,marion.adebiyi}@lmu.edu.ng
[2] Department of Computer Science and Communication, Ostfold University College, Halden, Norway
sanjay.misra@hiof.no
[3] University of Malta, Msida, Malta
[4] Department of Computer Science, University of Ilorin, Ilorin, Kwara, Nigeria
awotunde.jb@unilorin.edu.ng

Abstract. Stroke is a subsequent cause of death in the world and a primary reason for infirmity, with a high rising in developing countries. Most strokes are caused by an ischemic stroke which is a result of arterial occlusion. In most cases, strokes are found in people aged 55 and above. They occur more often in men than women although women tend to fall, victim, when they are older, they are more likely to die from it. A doctor will usually use physical examination and family history to diagnose stroke. They could also get an idea of the location of the symptoms. The best way to determine the root cause is through a Magnetic Resonance Imaging (MRI) scan. However, Doctors are humans and can have eye defects which could cause misreading of the diagnosis. Emotions could also affect our judgment as we are all humans. Therefore, this paper proposes a Convolutional Neural Network (CNN) and Support Vector Machine (SVM) for stroke classification. Chi-square was used for feature selection to remove irrelevant features from the dataset. The dataset used is obtained from the Kaggle website, the dataset contains several risk factors with more than 500 instances. The risk factors contain features that can cause blockage or cut off of blood flow to the brain. An accuracy of 95.91%, a precision of 95.37%, and a sensitivity of 98.10% were attained. The study will help the physicians to accurately predict ischemic stroke with ease and faster than conventional methods. They will also give future directions for researchers to build and make improvements on the method to enhance prediction and diagnosis for strokes and other relevant diseases.

Keywords: Ischemic stroke · Machine learning · Chi-square · CNN · SVM

1 Introduction

Stroke is a primary reason for disability and the world's second greatest cause of death, with rates rising in developing countries. Most strokes are caused by an ischemic stroke

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 268–279, 2023.
https://doi.org/10.1007/978-3-031-13150-9_23

which is a result of arterial occlusion [1]. One of the three types of strokes is Ischemic stroke and it is more common compared to the others, it is also stated as cerebral ischemia and brain ischemia. There are two key causes of stroke. The obstruction in an artery supplies blood to the brain (ischemic stroke), after which the brain cells begin to die as they are being deprived of nutrients and oxygen. The other is leaking or a burst blood vessel (hemorrhagic stroke) [2].

Most cases of stroke are found in people aged 55 and above. They occur more often in men than women although women tend to fall, victim, when they are older, they are more likely to die from it. Some of the factors that increase stroke risk include; COVID 19 infection, high blood pressure, diabetes, use of drugs like cocaine, smoking cigarette, bingeing on drinking, being overweight or obese. A doctor will usually use physical examination and family history to diagnose stroke. They could also get an idea of the location of the symptoms. The best way to determine the root cause is through a Magnetic Resonance Imaging (MRI) scan.

When testing for stroke, a Computed Tomography (CT) or Magnetic Resonance Imaging (MRI) scan of the head is usually the first resort. The Computed Tomography scan combines distinct X-ray apparatus with complex computers to produce pictures of the head, which will be examined to determine if it was a result of bleeding inside the brain or a blood clot. Computed Tomography Angiography (CTA) scans may be performed as well (i.e., a different material could be injected intravenously to obtain pictures). Pictures that sense blood flow called Computed Tomography Perfusion (CTP) could also be used. The combination of all three helps the physician decide the best therapy for the patient [3].

Machine Learning (ML), which uses pattern recognition algorithms to diagnose, treat, and forecast problems and diagnose individual outcomes in a variety of neurological illnesses, is quickly becoming a valuable tool. Over the last few years, the treatment and assessment of Acute Ischemic Stroke (AIS) have advanced significantly, necessitating the use of neuroimaging more frequently. ML is a computer science discipline that borrows from engineering to aid the extraction of data based on pattern recognition and is considered a branch of artificial intelligence [5]. After repeated data analysis and mastering tasks previously considered too complicated for machines to perform, a computer study earlier mistakes and makes the appropriate corrections. The creation of these methods for interpreting neuroimaging data has yielded useful data for study into the connection, mechanisms, and structure of the brain and its behavior in specific neurological illnesses [6].

Problems encountered while using the Convolutional Neural Networks include difficulty inaccuracy of proper reading from the CTA or MRI scans because those readings are made by doctors causing extra cost and stress for patients so a method is needed to classify the image effectively and accurately. Most of these models need a better feature selection to improve their accuracy. Therefore, this study proposes that Convolutional Neural Networks and Support Vector Machine algorithms with Chi-Square as a feature selection method are used to improve the classification of the ailment. The paper is structured as per guidelines suggested in Misra [4]. Related work section in presented in Sect. 2, methodology in Sect. 3, result and discussion in Sect. 4 and conclusion drawn in Sect. 5.

2 Related Works

In recent years, ways to improve machine learning use for an increase in productivity and positivity have been found. Though improvement is still required, it has done a lot of great deeds and has brought awareness.

In [7], the authors wrote a paper (Classification of Ischemic Stroke using Machine Learning Algorithms). They found that there are many similarities between the different forms of ischemic strokes, making it difficult to appropriately diagnose the cases using medical methods. They also noticed that there are no clear distinctions between these categories. The recent studies on ischemic stroke categorization were reviewed and analyzed in this paper. In addition, the study used a decision tree algorithm and K Nearest Neighbour to construct a classification model for ischemic stroke. A dataset with 400 instances was obtained from various Sudanese hospitals to create the classification model. The experiment indicated that the performance of the decision tree classification algorithm is superior to that of the KNN algorithm. Medical specialists can utilize the decision tree algorithm's output to diagnose and classify ischemic stroke patients. The findings discovered that the symptoms of irritability, convulsions, and mouth deviation are present in patients and that the CT data can be utilized to dictate the kind of ischemic stroke. These findings aid medical professionals in the classification of ischemic strokes. Furthermore, the findings revealed that thrombotic ischemic stroke accounts for the majority of ischemic stroke cases in Sudan [7].

The authors in [8] proposed machine intelligence in stroke prediction where they noted that machine intelligence can be projected as one of the significant tools in decision-making in the field of medicine. The system extracts hidden knowledge from a stroke database. They proposed a machine learning-based strategy using ANN and SVM to predict the risk of stroke in a group of healthy and stroke patients aged 35 to 90 years old. Predictions from the suggested method utilizing ANN were 98.1% accurate, while SVM predictions were only 91% accurate. Implementing this model, which can assist physicians in giving better medication, can enable early prognosis and diagnosis of stroke. Larger research is needed, based on the creation of more public databases that would collect huge valid stroke data sets from all patients diagnosed with the disease. The researchers' use of them would make their modeling studies easier, resulting in more reliable results and integrated clinical decision-making [8].

In [9], the authors carried conducted a study and discovered that the paper proposes a machine learning-based IoT-based smart brain hemorrhage detection system. Automatically detecting a brain hemorrhage is a difficult task that often results in death or long-term impairments. Their article offered a smart IoT application that precisely diagnoses brain hemorrhage to lessen the danger of causalities or lifetime disability, as well as to give excellent therapy at the patient's doorstep. The feedforward neural network and support vector machine are used in this smart IoT application to classify the different forms of brain hemorrhages. The SVM and FNN, on average, have accuracies of 80.67% and 86.7%, respectively. Built from the classification results, it was determined that the feedforward neural network produces superior results in a short period when compared to the support vector machine. The planned study work could be expanded in the future to include cardiac disease diagnosis utilizing machine learning methods [9].

In [10], the authors proposed the use of Deep Learning to Predict Stroke Patient Mortality) They created a deep learning model using scaled PCA based on the data of 15,099 participants to automatically predict stroke based on medical use history and health activities. The model did not contain any subjective variables. Our research allows for the early discovery of patients at high risk of stroke who require additional testing and treatment before the disease worsens. Their strategy eliminates the need to manually choose variables. They employed a DNN to examine the variables of interest using scaled PCA to provide enhanced continuous inputs for the DNN because the input data is straightforward (albeit of low resolution, that is, binary or with a limited number of options). Their approach has 64.32% sensitivity, 85.56% specificity, and an AUC value of 83.48%, respectively. Their technology can be used to forecast not only strokes but also other diseases utilizing minimal data.

The authors in [11] proposed the classification of stroke disease using CNN. CNN can assist neurologists in categorizing stroke based on the results of classifying stroke from CT head scan pictures. The accuracy attained is also influenced by the number of data points received for the training dataset. Their proposed method provides 90% accuracy for testing 15 pictures of each kind of stroke in this study. The number of pictures utilized in the training process has a big impact on the classification outcome. The higher the accuracy, the more pictures are used in the training process. Other approaches for classifying stroke can be used in future studies and compared to the convolutional neural network.

In [12], the authors proposed a computer-aided imaging analysis in acute ischemic stroke – background and clinical applications) The market for automated image analysis of ischemic stroke using artificial intelligence or machine learning algorithms is rapidly expanding. CAD products, both commercial and non-commercial, have so far focused on the analysis of CTA, NCCT, and perfusion imaging based on MR or CT imaging. They attempt to automatically identify and measure the ischemic core, ischemic penumbra, collateral flow status, and the site of arterial occlusion. CAD algorithms are not meant to be used as diagnostic tools on their own. They do, however, aid physicians in obtaining more uniform and accurate interpretations of stroke-related results, which may enhance stroke management and the selection of appropriate (sometimes time-critical) treatments for patients. To widen and generalize therapy selection measures for acute ischemic stroke patients, future clinical studies are required to properly validate, evaluate, and compare the many available software solutions. Future research could also look towards integrating CAD algorithms into the workflow of stroke referral networks [12].

In [13], the authors review a paper on DL for Medical Image Processing and discovered that, based on their outstanding performance, most academics think that deep learning-based applications will supplant humans in the next 15 years, with autonomous machines performing the majority of daily tasks. However, when compared to other real-world challenges, deep learning's adoption in healthcare, particularly in medical imaging, is gradual. They underlined the obstacles to extension in the wellbeing area, just as best in class profound learning applications in clinical picture handling. However, the rundown is a long way from comprehensive, it gives a sign of the drawn-out impact of profound learning in the clinical imaging area today. Taking everything into account, they accentuated the inexplicable examination issues.

Many huge exploration organizations are growing profound learning-based arrangements that advance the utilization of profound learning in clinical imaging. Looking on the great side of AI, the sooner people are supplanted in most clinical applications, especially finding, the better. It ought not, be that as it may, be viewed as the solitary issue because there are others. Perhaps the main obstacle is the absence of named datasets. As a result, the question of whether enough training data can be obtained without impacting the performance of deep learning algorithms remains unanswered. Larger data implies better results, according to recent developments in other applications. Big data, on the other hand, could be employed in healthcare. Although deep learning-based applications have received excellent reviews thus far, due to the sensitivity of healthcare data and obstacles, more sophisticated deep learning algorithms that can efficiently deal with complicated healthcare data will be investigated. They concluded that there are numerous ways to improve the healthcare system.

3 Methodology

The proposed model of this study uses Chi-Square as a feature selection method with Support Vector Machine and Convolutional Neural Network for ischemic stroke classification. The methods to be used in this model research are split by the main phases of the development process, to formulate the problem, data set collection, prepare the data, build the model, implement the model and then conclude the results. It is important to train the data using various algorithms and then compare selected features with trained data [19]. To extract the patterns from the dataset, and then create a model based on the patterns extracted. The trained data set is now supplied to the machine learning model which is then trained based on the data set. After the testing operation, the model predicts whether or not the pictures are for ischemic stroke or otherwise. The result is then evaluated based on this flow (Fig. 1);

3.1 Convolutional Neural Network (CNN)

A convolutional neural network is often made up of several layers that are arranged according to their functions. The anatomy of the cortical area, in particular, has energized CNN [14]. CNN is a supervised approach, unlike uncontrolled methods like Fuzzy C-Means and ADBSCAN clustering [15]. An input and output layer, as well as numerous hidden layers, make up a Convolutional Neural Network (CNN). CONV, POOL, and FC are three different sorts of these layers (short for fully-connected). We'll also explicitly write the nonlinearity activation function as a layer that applies elementwise nonlinearity. We'll go through how these layers are usually combined to make full ConvNets in this part. CNN relies on the premise that data contains pictures, which focuses the architecture to be created in a way that most accurately suits the requirement for dealing with the specific type of data.

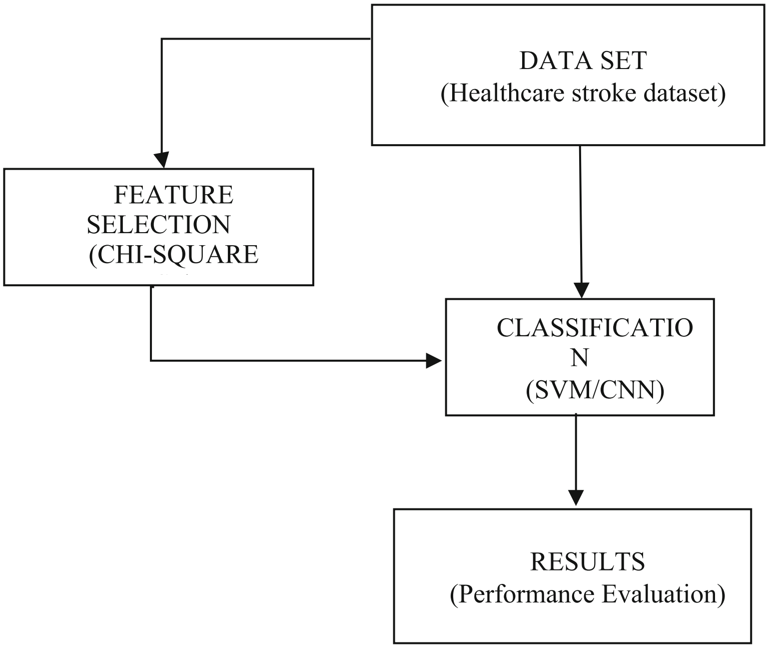


Fig. 1. Proposed design of the model

Algorithm 3.1: Convolutional Neural Network
1: algorithm Parallel-CNN
2: input: d: dataset, 1: dataset true labels, W: Word2Vec matrix
3: output: score of the parallel-CNN trained model on the test dataset
4: let f be the features 3d matrix
5: for I in dataset do
6: let fi be the feature set matrix of sample i
7: for j in I do
8: vj ← vectorize(j, W)
9: append vj to fi
10: append fi to f
11: ftrain, ftest, 1train, 1test ← split feature set and labels into train subset and test subset
12: M ← Parallel-CNN (ftrain, 1train)
13: score ← evaluation (i, 1test, M)
14: return score

3.2 Support Vector Machine

SVM (Support Vector Machine) is a supervised ML technique for solving classification or regression issues [16, 17]. It is, however, mostly used to tackle categorization problems. Every information thing in the SVM technique is addressed as a point in n-dimensional space (where n is the number of components), with the worth of each element being the organized esteem. The order is then done by finding the hyper-plane that best recognizes the two classes. Individual perception organizes are what Support Vectors are. The SVM classifier is a wilderness that isolates the two classes of hyper-plane and lines the best [18].

Algorithm 3.2: Support Vector Machine
While there are violating points, candidateSV = "closest pair from opposite classes"
Locate a transgressor.
candidateSVU infringer = candidateSVV infringer
If any p 0 occurs as a result of adding c to S, then
candidateSVp = candidateSVp candidateSVp candidateSVp candidateSVp candidateSVp candidateSV
Rep until all such points have been pruned.
if it's over
in the meantime

4 Results and Discussions

The chi-square algorithm was implemented using the Jupyter platform, precisely this section is a presentation of the results of the studies for the proposed model. Thereafter data preprocessing and data splitting were carried out to normalize the data. Comparison between the results was each performed using the different classifiers. This study implements a model with classification techniques using Convolutional Neural Networks, SVM, and Deep Neural Networks. The data was normalized and consists of 32 attributes and 569 instances. In this study, chi-square is used to select the relevant features which will be suitable for the performance. The reason for the data drop in chi-square is to drop other columns and focus on the most important columns in the data set. The data features are 32 attributes and 569 instances.

In this study. The diagnosis of stroke was performed using a stroke healthcare dataset. This dataset was classified using SVM and CNN. However, to further enhance the diagnosis of the experiment Chi-square was introduced as a feature selection method. The confusion matrix classification of SVM without Chi-Square is shown in Fig. 2. Figure 3 depicts the Chi-Square confusion matrix categorization using SVM. Figure 4 demonstrates the Chi-Square confusion matrix categorization using CNN. The confusion matrix classification of CNN without Chi-Square is shown in Fig. 5.

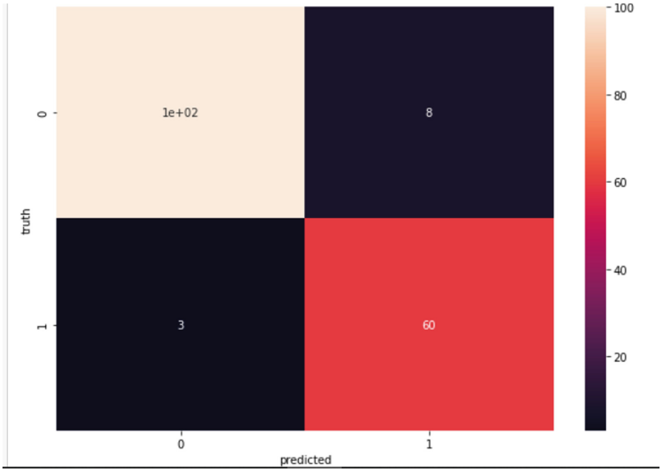


Fig. 2. SVM classification without chi-square (TP = 100, TN = 60, FP = 8, FN = 3).

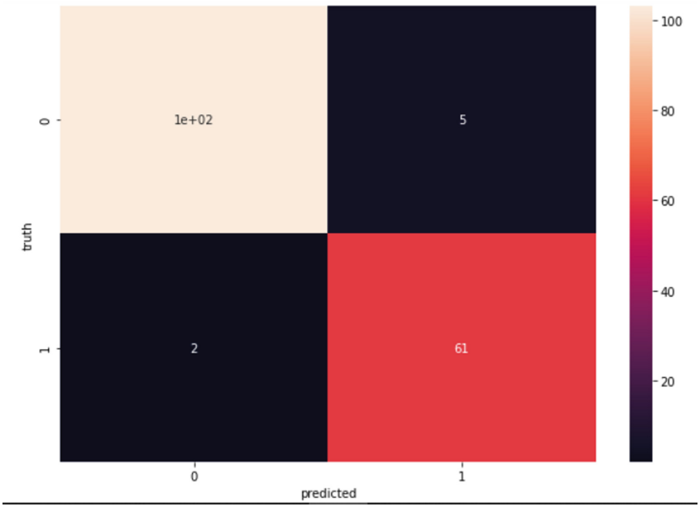


Fig. 3. Chi-Square with SVM classification (TP = 103, TN = 61, FP = 5, FN = 2).

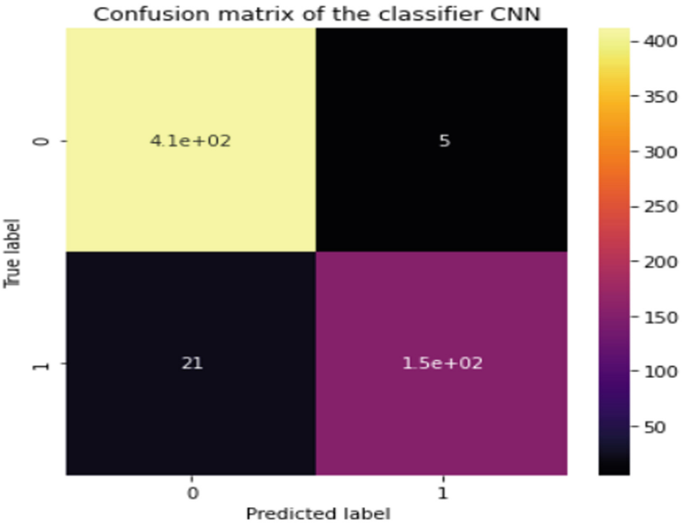


Fig. 4. Classification of Chi-Square with CNN (TP = 411, TN = 21, FP = 5, FN = 154).

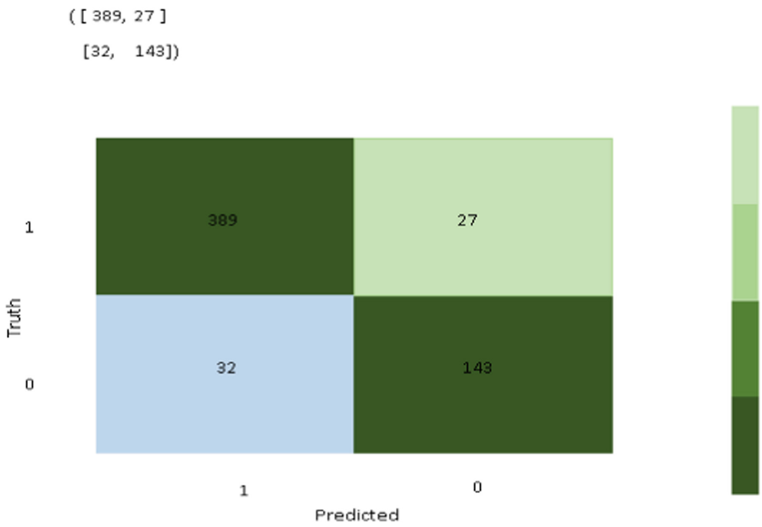


Fig. 5. Classification of CNN without Chi-Square (TP = 389, TN = 143, FP = 27, FN = 32).

Figure 6 shows the Receiver Operating Characteristics (ROC) Curve for Chi-Square with Support Vector Machines. The ROC Curve shows the performance of the classification threshold. The curve plots the true positive rate against the false-positive rate.

This study used SVM and CNN for classification, the data is passed into the stated classifiers, before being passed to Chi-square separately to be passed into the classifiers respectively.

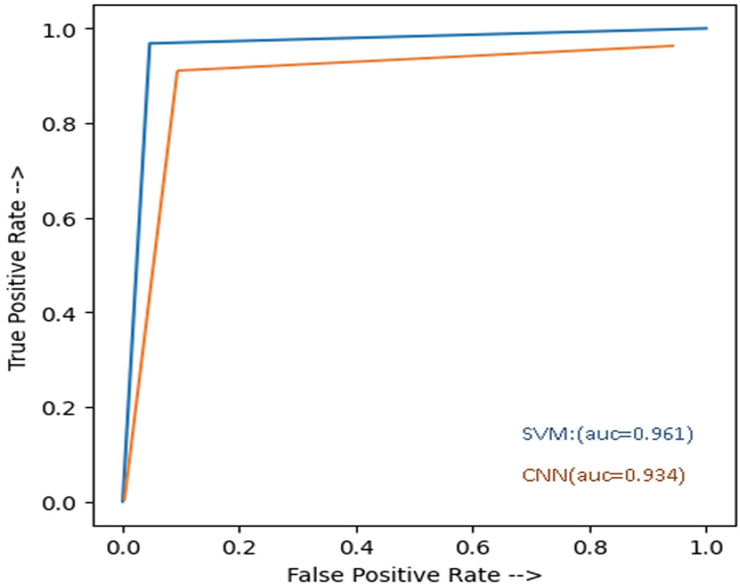


Fig. 6. ROC curve for Chi-square with SVM

The confusion matrices obtained were evaluated using performance metrics; sensitivity, specificity, precision, accuracy, and f1 score. Table 1 shows the performance measures of each classifier with and without the Chi-square.

Table 1. Calculation and comparison of performance

Performance	SVM	Chi-square + SVM	CNN	Chi-square + CNN	Formular
Sensitivity	97.09	98.10	92.40	95.14	TPR = TP/(TP + FN)
Specificity	88.24	92.42	84.12	96.86	SPC = TN/(TP + TN)
Precision	92.59	95.37	93.51	98.80	PPV = TP/(TP + FP)
Accuracy	93.57	95.91	90.02	95.60	ACC = (TP + TN)/(P + N)
F1 score	94.79	96.71	92.95	96.93	F1 = 2TP/(2TP + FP + FN)

This study performed numerous experiments were and the table shows the evaluations. Table 2 shows the comparison of the results obtained.

Table 2. Comparison of algorithms used

Authors	Algorithms/methods used	Accuracy
[7]	K-nearest neighbour	97.5%
[11]	Convolutional neural network	90%
[8]	Artificial neural network + SVM	98.1%, 91%
[10]	PCA + deep neural network	83.48%
[9]	SVM + feedforward neural network	80.67%, 86.7%
Proposed Model	SVM + convolutional neural network + Chi-square	95.91?%

5 Conclusion

The ischemic stroke should be diagnosed early for proper actions to be taken. As a result of this, early diagnosis can be done by this model after considering the risk factors that are being measured in the dataset. The dataset has been trained and tested using this model. Support Vector Machine and Convolutional Neural Networks were taken into consideration in this research because Support Vector Machine is a supervised learning technique that serves as a classifier in this research, the dataset was sanitized and Chi-Square as a feature selection method for the data. Python programming language was used in this research. Jupyter notebook development environment was used for the implementation process. An accuracy of 95.91%, a precision of 95.37%, and a sensitivity of 98.10% were attained. No matter the discovery in health informatics, there is always room for improvement. There was difficulty in procuring a dataset within a small reach but a good dataset was attained. This model was trained and tested with more than 500 cases. It gives space for future researchers to make improvements but, it can be concluded that it could predict the stages of Ischemic stroke and could also predict for many patients worldwide. In the future, more data in millions should be considered especially when using a predictive algorithm. Also, further works should be developed as a web app and mobile app for doctors to interact with the diagnosed patient for easy mobility and better use. People should take better care of themselves and stay away from substances that could lead to stroke. Also, awareness of this disease should be improved.

References

1. Campbell, B.C., et al.: Ischaemic stroke. Nat. Rev. Dis. Primers **5**(1), 1–22 (2019)
2. Xie, L., Li, W., Hersh, J., Liu, R., Yang, S.H.: Experimental ischemic stroke induces long-term T cell activation in the brain. J. Cereb. Blood Flow Metab. **39**(11), 2268–2276 (2019)
3. Hersh, J., Yang, S.H.: Glia–immune interactions post-ischemic stroke and potential therapies. Exp. Biol. Med. **243**(17–18), 1302–1312 (2018)
4. Misra, S.: A step-by-step guide for choosing project topics and writing research papers in ICT-related disciplines. In: International Conference on Information and Communication Technology and Applications, pp. 727–744. Springer, Cham (November 2020). https://doi.org/10.1007/978-3-030-69143-1_55

5. Awotunde, J.B., Folorunso, S.O., Jimoh, R.G., Adeniyi, E.A., Abiodun, K.M., Ajamu, G.J.: Application of artificial intelligence for COVID-19 epidemic: an exploratory study, opportunities, challenges, and future prospects. Stud. Syst. Decis. Control **358**, 47–61 (2021)
6. Awotunde, J.B., Ogundokun, R.O., Misra, S.: Cloud and IoMT-based big data analytics system during COVID-19 pandemic. In: Chakraborty, C., Ghosh, U., Ravi, V., Shelke, Y. (eds.) Efficient Data Handling for Massive Internet of Medical Things. IT, pp. 181–201. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-66633-0_8
7. Adam, S.Y., Yousif, A., Bashir, M.B.: Classification of ischemic stroke using machine learning algorithms. Int. J. Comput. Appl. **149**(10), 26–31 (2016)
8. Jeena, R.S., Kumar, S.: Machine Intelligence in stroke prediction. Int. J. Bioinform. Res. Appl. **14**(1–2), 29–48 (2018)
9. Chen, H., Khan, S., Kou, B., Nazir, S., Liu, W., Hussain, A.: A smart machine learning model for the detection of brain hemorrhage diagnosis based internet of things in smart cities. Complexity **2020**, 1–10 (2020)
10. Cheon, S., Kim, J., Lim, J.: The use of deep learning to predict stroke patient mortality. Int. J. Environ. Res. Public Health **16**(11), 1876 (2019)
11. Marbun, J.T., Andayani, U.: Classification of stroke disease using convolutional neural network. In: Journal of Physics: Conference Series, vol. 978, no. 1, p. 012092. IOP Publishing (March 2018)
12. Mokli, Y., Pfaff, J., Dos Santos, D.P., Herweh, C., Nagel, S.: Computer-aided imaging analysis in acute ischemic stroke–background and clinical applications. Neurol. Res. Pract. **1**(1), 1–13 (2019)
13. Razzak, M.I., Naz, S., Zaib, A.: Deep learning for medical image processing: overview, challenges and the future. In: Dey, N., Ashour, A.S., Borra, S. (eds.) Classification in BioApps. LNCVB, vol. 26, pp. 323–350. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-65981-7_12
14. Folorunso, S.O., Awotunde, J.B., Ayo, F.E., Abdullah, K.K.A.: RADIoT: the unifying framework for IoT, radionics, and deep learning modeling. Intell. Syst. Ref. Libr. **209**, 109–128 (2021)
15. Kundu, R., Basak, H., Singh, P.K., Ahmadian, A., Ferrara, M., Sarkar, R.: Fuzzy rank-based fusion of CNN models using Gompertz function for screening COVID-19 CT-scans. Sci. Rep. **11**(1), 1–12 (2021)
16. Mahesh, B.: Machine learning algorithms-a review. Int. Jo. Sci. Res. (IJSR). **9**, 381–386 (2020)
17. Jakkula, V.: Tutorial on support vector machine (SVM). Sch. EECS Wash. State Univ. **37**, 3 (2006)
18. Chandra, M.A., Bedi, S.S.: Survey on SVM and their application in image classification. Int. J. Inf. Technol. **13**(5), 1–11 (2018). https://doi.org/10.1007/s41870-017-0080-1
19. Awotunde, J.B., Ogundokun, R.O., Jimoh, R.G., Misra, S., Aro, T.O.: Machine learning algorithm for cryptocurrencies price prediction. Stud. Comput. Intell. **972**, 421–447 (2021)

Anomaly Detection for Industrial Control Networks Using Hamming Distance

Rajneesh Kumar Pandey and Tanmoy Kanti Das(✉)

National Institute of Technology, Raipur, India
{rkpandey.phd2019.mca,tkdas.mca}@nitrr.ac.in

Abstract. Cyber security threats on Industrial Control Systems (ICS) to disrupt physical systems such as power grids and water treatment plants are a harsh fact of today's world. Anomalous activities, such as cyber-attacks, must be detected and prevented as soon as possible. ICSs are used in a wide range of fields and industries, including water treatment plants, power distribution and generation, transportation, medical systems, defence, and many others, which make them an attractive target for security attacks for various reasons, including economic, criminal, military, espionage, political and terrorism as well. Supervisory control and data acquisition (SCADA) systems are used to control industrial control systems. It collects data from sensors linked to a physical process and remotely controls the process using electronic control of actuators, switches, and valves to handle complex and potentially dangerous operations. System data from a real water treatment process with attacks is analyzed in this paper. This paper uses a collection of supervised learning algorithms to investigate attacks and intrusions in the Secure Water Treatment (SWaT) testbed. The study aims to detect abnormal activity in vulnerable sensors, actuators, HMIs, and SCADA systems and develop a methodology for countering intrusions. Matrix Profiles, a motif discovery algorithm for time series, is extended to perform the analysis. Binary and tertiary actuators may be introduced into the research in a meaningful manner by expanding Matrix Profiles with a Hamming distance metric. This algorithm has a low learning curve and produces reliable results. It also has the capability of being used in real-time. The applicability of the extended Matrix Profiles is demonstrated by analyzing selected actuators from the data collection.

Keywords: Industrial control system · Anomaly detection · Cyber physical systems · Operational data · Hamming distance · Deep learning

1 Introduction

Anomaly detection in cyber-physical systems or Industrial Internet of Things (IIoT) has got enormous attention from industrial practitioners and academia as part of the fourth industrial revolution, i.e. Industry 4.0. More and more devices

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 280–290, 2023.
https://doi.org/10.1007/978-3-031-13150-9_24

are being linked together in the IIoT, resulting in vast amounts of industrial data being generated every day [1]. The data is generated from sensors, actuators, and other instruments is part of industrial automation. IIoT gives us the power to utilize these data in intelligent machines and real-time analysis to increase productivity and reduce human error.

The increase in critical infrastructure automation has resulted in a fragile system. This automation ushered in a slew of new cyber threats, resulting in financial losses, life-threatening hazards, and societal ramifications. Stuxnet [2], WannaCry, and attacks on the Ukrainian power grid [3] are just a few examples. Initially, the critical infrastructure used to be restricted to a single geographic area, but it is now dispersed throughout the world. All critical infrastructure has adopted a shared information technology stack and remote access to monitor and manage goals to meet the current scenario. Because of the disparity in geographical position, vital infrastructure interconnection is reliant on public communication networks. Cyber security vulnerabilities and accidents are more likely as a result of these reforms. All confirmed cyber-attacks have one goal in common: to disrupt the underlying physical process [4]. Many other vital infrastructure industries, such as power generating stations, substations, and electric grid operations, depend on equipment from a variety of vendors. Due to the diversity of equipment, one thumb rule can not be applied for secure interconnection and communication between devices. Increasing the interconnectedness and digitization of these systems is a key component of improving operational efficiency, but it is not without risk [5].

Intruder alarms are often compared to intrusion detection systems, and IDS solutions [6]. They're mostly utilized to get real-time visibility into possible network breaches; by examining the packets that pass across your network and the network traffic patterns, IDS devices look for unusual behaviour or signals of a potential compromise [7]. An anomaly-based IDS creates a prototype of normal behaviour and detects attacks by comparing observed behaviour to the template and measuring deviations. Anomaly detection can detect unknown attacks since it requires only standard working conditions to learn the normal profile. In this article, we concentrate on anomaly-based techniques.

When it comes to ICS anomaly identification, there are two major concerns. Modelling the complex system requires good domain knowledge of physical processes. The behavioural changes in the system need to be classified as per pattern and based on domain knowledge. Initial system start-up and maintenance activity does not follow the common collective pattern of the majority of the data points. It hence can be easily separated or distinguished from the rest of the data patterns. The same needs to be refined while modelling the system. Methods for locating abnormal functioning devices may aid the investigator in properly checking the system in real-time, reducing losses caused by anomalies. Several anomaly detection techniques have been developed specifically for ICS [8]. The control and process actions are represented using a discrete multi-input, and multioutput (MIMO) device model [9]. However, the model does not apply to the nonlinear model. Goldenberg and Wool [10] used deterministic finite automata to model Modbus/TCP traffic, based on the phenomenon that traffic between devices is periodic (DFA). Their model, on the other hand, is only suitable for single-period traffic patterns. Deep learning has shown promise in the learning of complex variable relationships. Anomaly identification has been attempted with deep learning methods [11,12].

There is a difference between modelling a CPS IDS and a standard cyber security IDS. Cyber security in information technology is a three-step process that includes (i) safeguarding, (ii) detecting, and (iii) reacting to threats. In a similar way, physical process IDS is being modelled. Changes in the behaviour or pattern of CPS equipment like programmable logic controllers (PLC), sensors, actuators, and supervisory elements such as human-machine interfaces (HMI's)) data and network traffic may be due to an intrusion. The analysis of behaviours of the system becomes more important as cyber attacks in ICS increase day by day. The role of detecting cyber-attacks in near real-time on ICSs has become a major challenge.

We concentrate on detecting the abnormal activity of the Secure Water Treatment System (SWaT) [13] at the physical level in this study. Since the attacker's ultimate aim is to disrupt the underlying physical process. Supervised machine learning algorithms have been used to detect the behaviour of the system at the physical level. A number of studies have been published that uses supervised/unsupervised machine learning algorithms for anomaly detection in ICSs [14,15]. The SWaT testbed [16] was created to aid research into the design of stable cyber-physical systems (CPSs). It's crucial to consider the activity patterns of both normal and abnormal behaviours (cyber-attacks). Historian data can be used to create a model that can distinguish between normal and abnormal behaviour.

The motivation for the present work is to identify the main CPS security threats, vulnerabilities and attacks. We have modelled the SWaT dataset using a decision tree classifier. After modelling the system, Hamming-Distance matrix is used for predicting the attacks or/and normal state of the system.

The rest of the paper is organized as follows: Sect. 2 discusses the related work in the field of CPSs, whereas in Sect. 3, we have given a description of Testbed and Dataset. Section 4 explains the dimensions used for CPS IDS classification and the result associated with it. Section 5 presents our conclusion and suggests future research directions.

2 Related Work

The cyber-physical system is an integration of embedded systems to the environment for monitoring modern critical infrastructures. Anomaly detection in critical infrastructures or industrial control systems has gotten enormous attention by the industrial practitioner and academia. A key aspect of a cyber-physical system is integrating communication and operational process to meet new functionality. Intrusion Detection System (IDS) design concepts and techniques for cyber-physical systems are investigated by Brandon Phillips et al. [17]. Malicious traffic can be detected on the generated dataset of Remote Terminal Unit

(RTU) communications using the Modbus protocol, and Machine learning-based anomaly detection algorithms were used to identify the attacks.

Sridhar Adepu et al. [18] described how they used distributed attack detection to detect a single-stage multipoint cyber-attack in a secure water treatment plant(SWaT). The method is based on physical invariant's calculated from the CPS's design for each point. Jun Inoue et al. [19] performed another study in which they used an unsupervised machine learning approach to solve the intrusion detection problem in SWaT. He compares two classifications in this paper: Deep Neural Networks (DNN) adapted to time series data created by a CPS and one-class Support Vector Machines (SVM).

The research work in the paper is motivated by Tanmoy Kanti das et al. [4] logical analysis of data (LAD) which shows how a laptop class computer can be used to detect anomalous sensor or actuator activity using the LAD technique. Without the assistance of domain experts, LAD extracts rules from previous observations that control the activity of a CPS. Nikolaos Bakalos and colleagues presented a multimodal data fusion and adaptive deep learning approach for monitoring and securing water infrastructure [20].

Block-chain based CPS security was explained by Zhao et al. [21], as per his work, blockchain can play a critical role in cyber-physical systems (CPS) where Internet of Things (IoT)are used to collect sensing data regarding the environment. The captured data being monitored using a blockchain to enhance CPS in various aspects, ranging from securing the data for offline storage to protecting key operations from cyber attacks in real-time. A semi-supervised approach was used for intrusion detection by extending the logical analysis of data by Tanmoy Kanti das et al. [22]. [22] Using the autoregressive behaviour of the device, the proposed model will readjust its parameters to adapt to changing dynamically environment.

The objective of all security CPS testbeds is to execute simulated attacks and evaluate the system's vulnerabilities and defences mechanism. According to requirements, different goals are set, which yield other testbed implementations.

3 Dataset Description

The Singapore University of Engineering and Innovation has created the SWaT dataset. There are a variety of instruments in the testbed that are divided into sensor and actuator categories. As shown in Fig. 1, the devices are distributed in six phases.

Throughout the 11 d of operation, all data from sensors and actuators is logged every second, resulting in multivariable time series data. The first seven days of the run, data were in relatively good shape. In the last four days of Data, 36 attacks have been carried out. There are four types of attacks in the attack data: SSSP, SSMP, MSSP, and MSMP, which are defined in detail in Table 1. J Goh et al. [23] given a complete overview of the dataset. The dataset reported here contains network traffic and all the values obtained from all the 51 sensors and actuators. Description of all the sensors and actuators is annexed as Table-4.

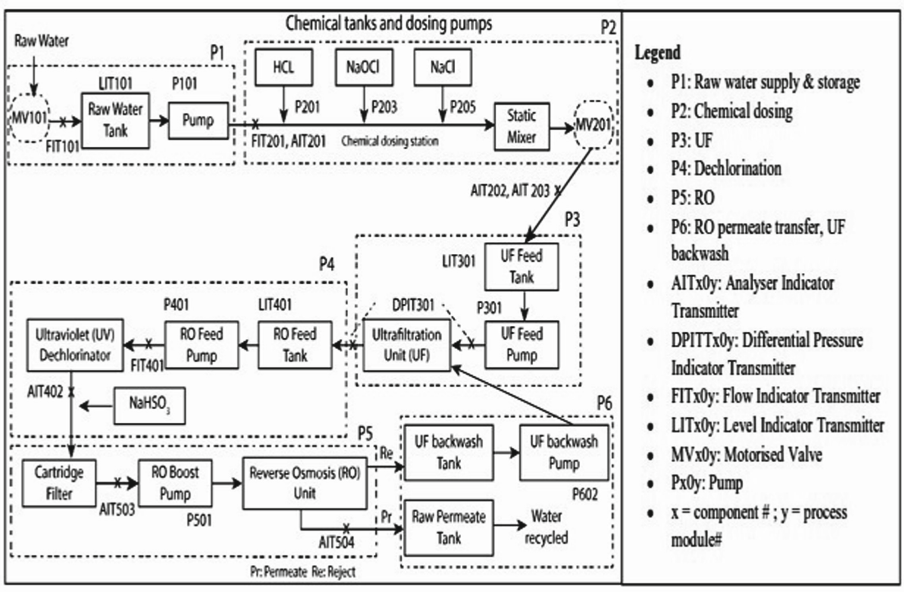


Fig. 1. Functional diagram for SWaT architecture

Data labelled according to normal and abnormal behaviours. The physical Data consist of 14,41,719 rows and 52 attributes along with the result attribute. Out of the total records, the attack records are 54,621. However, in this paper, we will be predicting the attack using hamming distance matrix.

Table 1. Type of attacks

Attack category	No. of attacks
Single Stage Single Point (SSSP)	26
Single Stage Multi Point (SSMP)	4
Multi Stage Single Point (MSSP)	2
Multi Stage Multi Point (MSMP	4

4 Performance Evaluations

In this section, the anomaly detection method for industrial control systems on Secure water treatment networks using Hamming Distance has been proposed. The section divided in two major parts (i) Methodology is used for prediction of anomolous behaviour and (ii) Experiment result. The proposed anomaly detection system employs C4.5 decision tree classification. Furthermore, the hamming distance is used to improve the identification of suspicious activity in industrial control systems.

4.1 Methodology

Control systems provide a recurrent behaviour as they are used in industries. This enables the system's actions to be compared to expected behaviour. ICS equipment operates within predefined parameters, and such operations are simple to profile. The proposed anomaly detection system uses a dual detection approach to detect abnormal activity by analyzing both the equipment's readings with their thresholds and the discrete-event traces produced by the industrial control system.

One of the most widely used tree classifiers is C4.5 used in the experiment. To define the classifier, the C4.5 algorithm creates a decision tree, which is then used to generate the ruleset. Complex decision trees can be challenging to understand due to the dispersed knowledge about a single class in a tree. As a result, classifies cases using groups of if-then rules for each category. The case is classified by the first rule that suits the conditions specified in the case. If there is no correspondence rule, the standard class for the case is assigned by the classifier.

A Hamming Distance calculation based method is proposed for anomaly detection using decision tree classifier is presented below.

Step 1: First select the one actuator and initial seven days of sensor value(No attack mounted), used for training the corresponding actuator model using the C4.5 classifier.
Step 2: We save the actuator model, and it will be used for testing from remaining 4 d sensor value.
Step 3: We will carry out the test for the remaining 15/20 actuators and save the model.
Step 4: Now uses the last 4 d of sensor data(when the attack has been mounted) for predicting the actuator value from the previously saved model.
Step 5: After completing the Step-4 we have(Hamming distance Matrix) mentioned in Table 2:
Step 6: Now we have two matrices one is of actual value, and the other is predicted value.
Step 7: Now Calculate the Hamming distance between the 15/20 actual actuator values versus 15/20 predicted actuator values.
Step 8: After this calculation we have set of threshold value. Be precise on choosing threshold values so that minimum variation between actual and predicted values. Let's Fix some threshold values, The value more than the threshold value will be considered an attack, and less than that will be regarded as normal.
Step 9: The calculated Accuracy is Shown in Fig. 3

Table 2. Hamming distance matrix

Actual Actuator Value	Predicted Actuator Value
MV101-ACTUAL	MV101-PREDICT
P101-ACTUAL	P101-PREDICT
....	......
....	......

4.2 Result

A decision tree model is similar to a tree, shows a branching of decisions and future results. Commonly, discrete goals are used for decision tree classifiers (which, in this case, maybe only referred to as "trees"), the outcome is a binary variable that categorizes the participants as being either 'Normal' or 'Attack'. Two different experiment using 15 or 20 actuator has been carried out as mentioned in Sect. 4.1. The comparative result is shown in Table 3. The accuracy of the classification is shown in Fig. 3.

Table 3. Comparison of results

Actuator's	Precision	Recall	F1 Score	Accuracy
20 Actuators	84.1	91.3	87.5	78.63
15 Actuators	87.4	91.3	89.3	81.3

The graphical representation of result is shown in the Fig. 2:

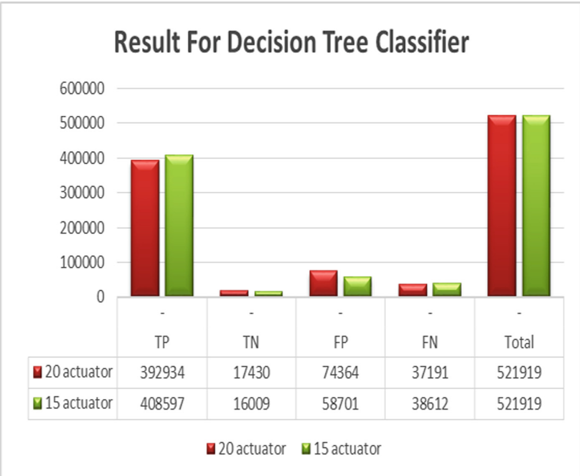


Fig. 2. Result for C 4.5 decision tree classifier

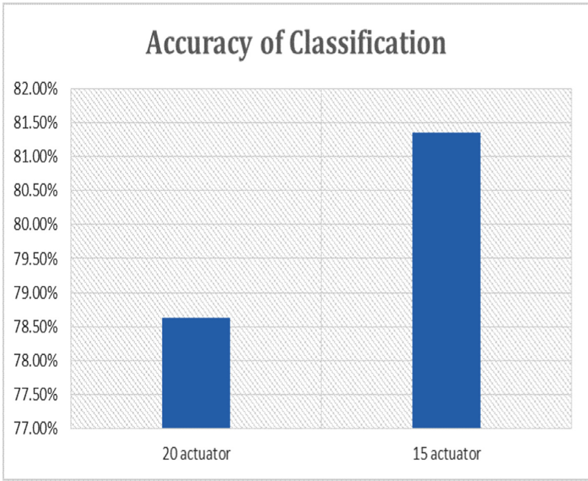


Fig. 3. Accuracy comparison

Table 4. Sensor and actuator description of the SWaT testbed

No	Name	Type	Description
1	FIT-101	Sensor	Flow meter; Measures inflow into raw water tank
2	LIT-101	Sensor	Level Transmitter; Raw water tank level
3	MV-101	Actuator	Motorized valve; Controls water flow to the raw water tank
4	P-101	Actuator	Pump; Pumps water from raw water tank to second stage
5	P-102 (backup)	Actuator	Pump; Pumps water from raw water tank to second stage
6	AIT-201	Sensor	Conductivity analyser; Measures NaCl level
7	AIT-202	Sensor	pH analyser; Measures HCl level
8	AIT-203	Sensor	ORP analyser; Measures NaOCl level
9	FIT-201	Sensor	Flow Transmitter; Control dosing pumps
10	MV-201	Actuator	Motorized valve; Controls water flow to the UF feed water tank
11	P-201	Actuator	Dosing pump; NaCl dosing pump
12	P-202 (backup)	Actuator	Dosing pump; NaCl dosing pump
13	P-203	Actuator	Dosing pump; HCl dosing pump
14	P-204 (backup)	Actuator	Dosing pump; HCl dosing pump
15	P-205	Actuator	Dosing pump; NaOCl dosing pump
16	P-206 (backup)	Actuator	Dosing pump; NaOCl dosing pump
17	DPIT-301	Sensor	Differential pressure indicating transmitter; Controls the backwash process
18	FIT-301	Sensor	Flow meter; Measures the flow of water in the UF stage
19	LIT-301	Sensor	Level Transmitter; UF feed water tank level
20	MV-301	Actuator	Motorized Valve; Controls UF-Backwash process
21	MV-302	Actuator	Motorized Valve; Controls water from UF process to De-Chlorination unit
22	MV-303	Actuator	Motorized Valve; Controls UF-Backwash drain
23	MV-304	Actuator	Motorized Valve; Controls UF drain
24	P-301	Actuator	UF feed Pump; Pumps water from UF feed water tank to RO feed water tank via UF filtration
25	P-302 (backup)	Actuator	UF feed Pump; Pumps water from UF feed water tank to RO feed water tank via UF filtration
26	AIT-401	Sensor	RO hardness meter of water
27	AIT-402	Sensor	ORP meter; Controls the NaHSO3 dosing(P203), NaOCl dosing (P205)
28	FIT-401	Sensor	Flow Transmitter; Controls the UV dechlorinator

(*continued*)

Table 4. (*continued*)

No	Name	Type	Description
29	LIT-401	Sensor	Level Transmitter; RO feed water tank level
30	P-401 (backup)	Actuator	Pump; Pumps water from RO feed tank to UV dechlorinator
31	P-402	Actuator	Pump; Pumps water from RO feed tank to UV dechlorinator
32	P-403	Actuator	Sodium bi-sulphate pump
33	P-404 (backup)	Actuator	Sodium bi-sulphate pump
34	UV-401	Actuator	Dechlorinator; Removes chlorine from water
35	AIT-501	Sensor	RO pH analyser; Measures HCl level
36	AIT-502	Sensor	RO feed ORP analyser; Measures NaOCl level
37	AIT-503	Sensor	RO feed conductivity analyser; Measures NaCl level
38	AIT-504	Sensor	RO permeate conductivity analyser; Measures NaCl level
39	FIT-501	Sensor	Flow meter; RO membrane inlet flow meter
40	FIT-502	Sensor	Flow meter; RO Permeate flow meter
41	FIT-503	Sensor	Flow meter; RO Reject flow meter
42	FIT-504	Sensor	Flow meter; RO re-circulation flow meter
43	P-501	Actuator	Pump; Pumps dechlorinated water to RO
44	P-502 (backup)	Actuator	Pump; Pumps dechlorinated water to RO
45	PIT-501	Sensor	Pressure meter; RO feed pressure
46	PIT-502	Sensor	Pressure meter; RO permeate pressure
47	PIT-503	Sensor	Pressure meter; RO reject pressure
48	FIT-601	Sensor	Flow meter; UF Backwash flow meter
49	P-601	Actuator	Pump; Pumps water from RO permeate tank to raw water tank (not used)
50	P-602	Actuator	Pump; Pumps water from UF back wash tank to UF filter to clean the membrane
51	P-603	Actuator	Not implemented in SWaT yet

5 Conclusion

In this study, we have presented a way to build an enforceable system with minimal computing resources, thus elevating the current levels of accuracy. To describe a set, the tags that are sufficiently using model-based enlargement have been done using Hamming distance. This article demonstrates that Matrix Attack Recognition using the Hamming-distances could detect all examined attacks without any false positives. Additionally, preparation was done by a computerized system. More work may be involved in understanding and analyzing the comprehensive computational study of the algorithm's capabilities could yield benefits in the future. As the sequences are always the same, the number of times that motif occurs in the dictionary is less than that in the actual protein sequences. Using a known and assigned motif reduces the number of comparisons required but provides the exact details. Since an outlier occurs twice, it is described as a high when the number of occurrences increases, detecting this anomaly will mean we know something is out of the ordinary. It will also be fascinating to explore the detection's feasibility using resource-constrained degradable devices, particularly considering the long term abundance of precious resources.

References

1. Jiang, J.R.: An improved cyber-physical systems architecture for industry 4.0 smart factories. In: 2017 International Conference on Applied System Innovation (ICASI), pp.918–920 (2017)
2. Langner, R.: Stuxnet: dissecting a cyberwarfare weapon. IEEE Secur. Priv. **9**(3), 49–51 (2011)
3. Liang, G., Weller, S.R., Zhao, J., Luo, F., Dong, Z.Y.: The 2015 Ukraine blackout: implications for false data injection attacks. IEEE Trans. Power Syst. **32**(4), 3317–3318 (2016)
4. Das, T.K., Adepu, S., Zhou, J.: Anomaly detection in industrial control systems using logical analysis of data. Comput. Secur. **96**, 101935 (2020)
5. Cintuglu, M.H., Mohammed, O.A., Akkaya, K., Uluagac, A.S.: A survey on smart grid cyber-physical system testbeds. IEEE Commun. Surv. Tutorials **19**(1), 446–464 (2016)
6. Mitchell, R., Chen, I.-R.: A survey of intrusion detection techniques for cyber-physical systems. ACM Comput. Surv. (CSUR) **46**(4), 1–29 (2014)
7. Fovino, I.N.: SCADA system cyber security. In: Markantonakis, K., Mayes, K. (eds.) Secure Smart Embedded Devices, Platforms and Applications, pp. 451–471. Springer, New York (2014). https://doi.org/10.1007/978-1-4614-7915-4_20
8. Jones, A., Kong, Z., Belta, C.: Anomaly detection in cyber-physical systems: a formal methods approach. In: 53rd IEEE Conference on Decision and Control, pp. 848–853. IEEE (2014)
9. Zhanwei, S., Zenghui, L.: Abnormal detection method of industrial control system based on behavior model. Comput. Secur. **84**, 166–178 (2019)
10. Goldenberg, N., Wool, A.: Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems. Int. J. Crit. Infrastruct. Prot. **6**(2), 63–75 (2013)
11. Malhotra, P., Vig, L., Shroff, G., Agarwal, P.: Long short term memory networks for anomaly detection in time series. In: Proceedings, vol. 89, pp. 89–94. Presses universitaires de Louvain (2015)
12. Malhotra, P., Ramakrishnan, A., Anand, G., Vig, L., Agarwal, P., Shroff, G.: LSTM-based encoder-decoder for multi-sensor anomaly detection. arXiv preprint arXiv:1607.00148 (2016)
13. Mathur, A.P., Tippenhauer, N.O.: SWaT: a water treatment testbed for research and training on ICS security. In: 2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater), pp. 31–36 (2016)
14. Goh, J., Adepu, S., Tan, M., Lee, Z.S.: Anomaly detection in cyber physical systems using recurrent neural networks. In: 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), pp. 140–145. IEEE (2017)
15. Beaver, J.M., Borges-Hink, R.C., Buckner, M.A.: An evaluation of machine learning methods to detect malicious SCADA communications. In: 2013 12th International Conference on Machine Learning and Applications, vol. 2, pp. 54–59. IEEE (2013)
16. iTrust Labs Dataset Info iTrust. Swat dataset
17. Phillips, B., Gamess, E., Krishnaprasad, S.: An evaluation of machine learning-based anomaly detection in a SCADA system using the modbus protocol. In: Proceedings of the 2020 ACM Southeast Conference, pp. 188–196 (2020)
18. Adepu, S., Mathur, A.: Distributed attack detection in a water treatment plant: method and case study. IEEE Trans. Dependable Secure Comput. **18**(1), 86–99 (2018)

19. Inoue, J., Yamagata, Y., Chen, Y., Poskitt, C.M., Sun, J.: Anomaly detection for a water treatment system using unsupervised machine learning. In: 2017 IEEE International Conference on Data Mining Workshops (ICDMW), pp. 1058–1065. IEEE (2017)
20. Bakalos, N., et al.: Protecting water infrastructure from cyber and physical threats: using multimodal data fusion and adaptive deep learning to monitor critical systems. IEEE Signal Process. Mag. **36**(2), 36–48 (2019)
21. Zhao, W., Jiang, C., Gao, H., Yang, S., Luo, X.: Blockchain-enabled cyber-physical systems: A review. IEEE Internet Things J. (2020)
22. Das, T.K., Gangopadhyay, S., Zhou, J.: SSIDS: Semi-supervised intrusion detection system by extending the logical analysis of data. arXiv preprint arXiv:2007.10608 (2020)
23. Goh, J., Adepu, S., Tan, M., Lee, Z.S.: Anomaly detection in cyber physical systems using recurrent neural networks. In: 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), pp. 140–145 (2017)

A Web-Based Instant Messaging System for Effective Communication Among Organic Farmers and Researchers

Oluwasefunmi Arogundade[1], Aderonke Sakpere[2], Sanjay Misra[3](✉), Christianah Alonge[1], Lalit Garg[4], Adebayo Abayomi-Alli[1], and Oluwaseyi Bello[1]

[1] Department of Computer Science, Federal University of Agriculture, Abeokuta, Nigeria
{arogundadeot,abayomiallia}@funaab.edu.ng
[2] Department of Mathematical Sciences, Anchor University, Lagos, Nigeria
[3] Ostfold University College, Halden, Norway
sanjay.misra@hiof.no
[4] University of Malta, Msida, Malta

Abstract. Agriculture is undergoing a revolution from the deployments of traditional methods in carrying daily operations with the advent of Information Technologies and web based computing. As the activities involved in the agricultural practices become more bogging in recent times, the need for more instant communication becomes essential amidst key practitioners. Hence, a technology that enables an effective interaction is required. In this paper, a web-based instant messaging application for farmers and customers with information that supports knowledge dissemination and farm-produce transactions is proposed. The design of the system was developed and implemented using various front-end and back-end technology tools. These tools are HTML, CSS, Bootstrap, Javascript, Vue JS, Laravel, PHP, MySQL and AJAX. The web application reduces communication costs and afford farmers and customers the opportunity to send and receive vital information rapidly. The system fosters a farming centered conversation that makes agricultural goals achieved amidst farmers without the distractions that would have been provided by social communication platforms.

Keywords: Instant messaging · Organic farmers · Communication · Agriculture · Web-based

1 Introduction

In the global economic space, agriculture is regarded as Africa's highest areas with the most competitive advantage [1, 2]. The abundance of arable and fertile farmland, vast expanse of water of bodies and favourable climatic conditions disposes African countries to the profession of agriculture and food production over the years. Presently, proceeds from agricultural proceed at-tracts 15% of continental GDP and nearly 50% national GDP contribution in some low-income countries in Africa [3] (OECD-FAO, 2016). Emerging fronts in Agro-business reveal a promising future in the sec-tor; governmental

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 291–300, 2023.
https://doi.org/10.1007/978-3-031-13150-9_25

and non-governmental efforts are being harness to encourage rural-urban participation in crop production and the importance of technology cannot be over-emphasized [4, 5]. Technology-enabled strategies to improve agricultural practices have attracted significant attention within the past decade. Very notable innovations are smart and precision agricultural approaches are regarded as an important tool in the struggle to mitigate the effect of climate change on agricultural yield and practices around the world [6, 7]. The utilization of in-formation technology to observe, control and optimize the entire processes of agricultural production for profitability and environmental sustainability is the crux of precision agriculture. Smart agricultural practices multiply the capacities of digital information and data technologies to synergise the complex interactions between structures in the farming system [8]. This also help field agents to increase quality and yield in agricultural practices and cli-mate-friendly production [9]. In some climes, strategies from smart-climate agriculture are being adopted to improve irrigation for farming in region bordering the Sahara belt in Africa.

The advent of mobile telecommunication devices has improved the access to information amongst farmers in many part of the world which has sufficiently improved awareness to climate matters, pest and viral infections as well as soil fertility amongst others [10, 11]. Mobile communication and ICT based devices telecommunication devices have tremendous impact on inter-action and exchange of information amongst farmers [12, 13]. Android-based smart telephones usually enabled with internet applications are been described as a credible instrument of tool for agricultural extension [14]. In the community of farmers, the smart-telephones would require some level of literacy to surf around for specialized information agricultural-based information which may be out-of-the reach of the average farmers.

The utilization of social media as a communication instrument has been identified by individual farmers and ranchers as a tool that can help [4], nevertheless it is as yet unclear how these tools can best be used. Since little research has been conducted in agricultural communications investigating this phenomenon, it's crucial to see how the phenomenon has influenced and will continue to influence people from the agricultural sector. So as to ensure their success, agriculturalists have to balance a number of duties and obligations. Efficiently using social media tools necessitates effort and premonition. This re-search aims to help manage the gap of knowledge between buyers and producers considering agriculturalists' encounters using social media. Sect. 2 of this work states some related works to this research, Sect. 3 describes the methodology employed in developing the messaging system, Sect. 4 shows a clear description of the implementation of the work and the conclusion and recommendation given in Sect. 5.

2 Related Works

Wright et al. [15] highlighted the impact of ICT devices in overall improvement on health of crop and yield of farm produce for selected studies undertaken in East Africa employing a home-built Plant Online Management System (POMS). This report identified potentials of care-fully deployed ICT and telecommunication devices to provide information on plant health, perform consultation on pest control and hand-on guidance for rural farmers. Tegegne and Alemu [16] de-signed information systems for agricultural extension services using protocols of short-messaging services in Central Ethiopia.

Mobile tele-phone was utilized as the backbone tool for implementing the messaging aperture for efficient propagation of information on farming activities and market analysis. A clear advantage posed by the authors revealed that high throughput delivery speed and vast coverage of in-formation could benefit a broad spectrum of end-user farmers in knowledge transmission. A gallery of mobile services dedicated to farming and agro-based activities reported by Saravanan and Bhattacharjee [17] showed the increasing awareness of technology providers to seamless communication strategies in agricultural production sector to address essential information on fertilizer distribution, climate forecast amongst others.

The increase in the penetration of mobile telephones opens a new front for telephone-based application for conversation amongst farmers, consultation with expert systems and professional extension workers. Exchange of climate information for cultivation purposes using mobile device was reported by Market Light, the authors utilized mobile technology to inform and educate farmers on climate-related risks and to provide expert counsel on cultivation strategies that could improve farm yield in austere weather conditions. An integrated SMS-web based protocol was designed by Churi et al. [18] to furnish agrarian workers with an expert system for decision on crop and weather related information that may improve the yield and productivities based text-reply-text model. The model was built on knowledge based architecture to provide a spectrum of scientific procedure to prescribe simple techniques from cultivation to post-processing activities on farmland.

Although Decision Support Systems for agro-technology transfer (DSSAT) has been around for some time, there are limiting issues sur-rounding access restriction to extension scientist. Hence, Trigodo et al. [19] provide an interface option by developing SMS inquiry architecture transmitting from the dedicated DSSAT for farmers in selected cities in Philippines. The advent of smart phones is up scaling communication strategies in agro-based value chain because of the promising feature in the android based telecommunication technology. For instance, soft applications enabled on smart phones could be instrumental in propagating information between distant farmers. Barh and Balakrishna [20] presented an array of agro-based android application technologies based on cultivation, information, diagnostic and professional applications. Prasad et al. [21] implanted an AgroMobile technology leveraging on cloud computing framework to connect farmers over distances on pertinent to crop productivity. Similar re-ports from Lomotey et al. [22] demonstrated the capabilities of an agro-assistant system on android-enabled mobile telephone to support farmer's decision real time basis in the agricultural environment. Market and price determination of agricultural produce is critical to the agricultural value chain, to harness basic information required for farmers to determine pricing of produce, Sharma et al. [23] designed an agro-based expert system to provide real-time information on market pricing. The author alluded the feasibility of the same model for distribution of seedlings, pest control and agro-chemicals such as fertilizer. Ghanshyam et al. [24] developed architecture to integrate a wide collection of common problems associated to the cultivation of selected crops in a single-click approach. Table 1 shows a summary of existing instant messaging agricultural application and their ratings from 1 to 5.

Table 1. Table showing existing instant messaging web applications for farmers.

S/N	Application	Features	Ratings	Remark
1	AgriApp by AgriApp Technologies Pvt Ltd www.agriapp.co.in	• Package of Practices • Chat • Videos • News • Quick Search • Buy Now • Discounts • Secure Payments	Overall: 4.3/5 Ease of Use: 4.5/5 Customer Service: 4/5	Reliable
2	Apni Kheti by Cogneesol www.apnikheti.com	• Agricultural Information • Chat • Buy Now • Quick Search • Weather Updates • Market Rates • News • Farmer Stories	Overall: 4.7/5 Ease of Use: 4/5 Customer Service: 4/5	Satisfactory
3	Cropstream by Cropstream LLC www.cropstream.com	• Chat • Market Rates • Information-sharing	Overall: 5/5 Ease of Use: 5/5 Customer Service: 4.2/5	Free to use
4	SmartFarm by CropIn Technologies www.cropin.com	• Traceability • Order Processing • Crop Management • Inventory Management • Built-in Accounting Labor management • Contract Management • Pricing Management • Supplier Management • Package of practices • Alert Log & Management • Weather Records • Crop reports & insights • Geo tagging	Overall: 5/5 Ease of Use: 4/5 Customer Service: 4/5	Reliable and has a free trial

3 Methodology

A key concern is to develop a flexible system in a manner that future changes will be possible. This is important so that the solution won't be neglected after launch. As a result, the evolutionary development approach was adopted. The application of this approach as illustrated in Fig. 1, resulted into having two major tasks, project management and development process. The management of the project convers considering the scope of system by looking into the extent at which the system would cover. This was followed by the technical & farmers' usability which looks at what technical requirements need to be considered and the farmers that would use the system. With this, the design of the website was done and delivery follows with a review of the system. The farmers were made to test the system and give their feedback which was employed in further improving the form of the application. This evolutionary development model made interactivity effective and carrying out the process perfected. With this, an improvement or update on the system in future is easy. Figure 2 shows the design flow of the proposed system. This describes the various functionalities on the system and the users that can access them. The admin menu enables the admin add farmers, add customers, add categories, view farmers, manage farmers and view customers. The customers can access the user menu where they are able to view, chat and rate farmers.

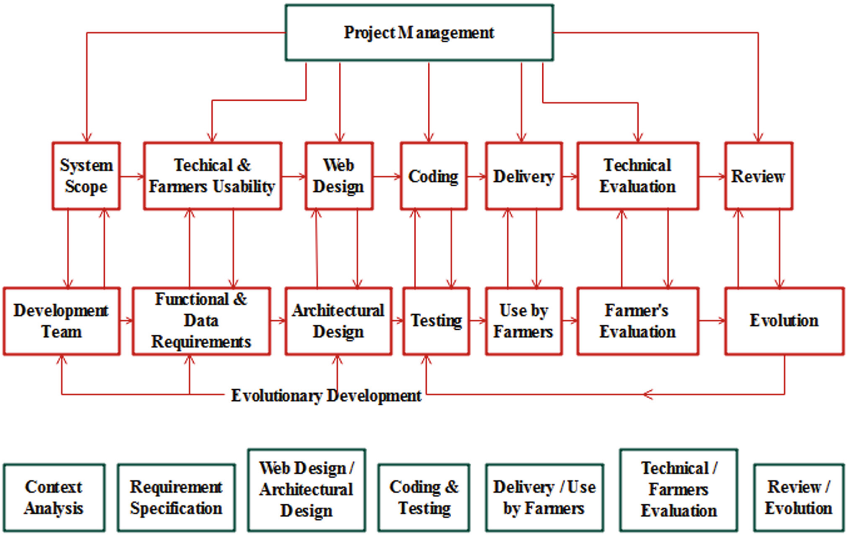


Fig. 1. An evolutionary development model for an instant messaging web application for farmer's cooperation

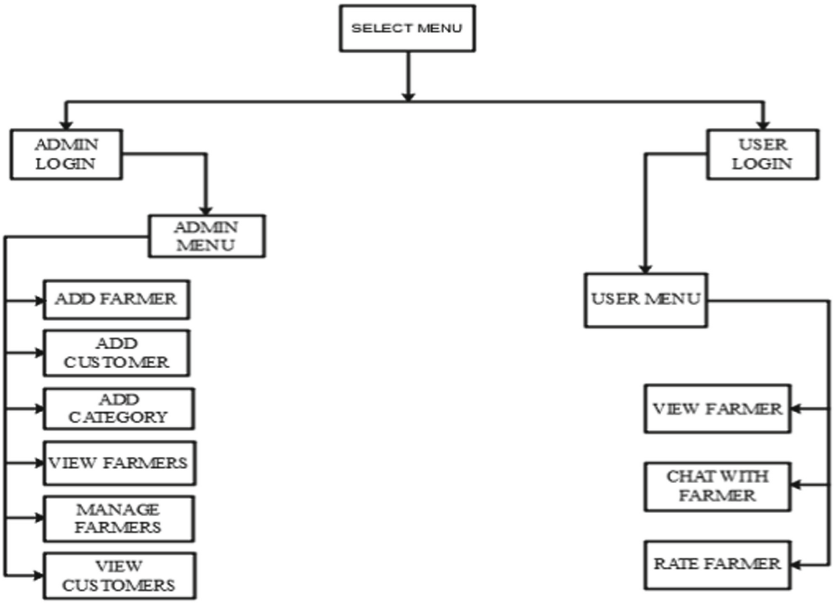


Fig. 2. System flowchart

4 Results

The design of the system was developed and implemented using various front-end and back-end technology tools. These tools are HTML, CSS, Bootstrap, Javascript, Vue JS, Laravel, PHP, MySQL and AJAX. The illustration of the system features such as the Sign in Page, Home Page, chat page and connection status view are shown in Figs. 3, 4, 5 and 6 respectively. The sign inpage is where the user enters a pre-registered username and password to be able to access information on the application. The welcome page displays to the users what the application does and the description of how it should be used. In the chat page, pre-registered customers chat with agriculturists to request for goods and services. In Fig. 6, the page shown displays the connection status as well as the time of message sent in format (YYYY-MM-DD H M S). It also shows a green online icon that appears next to the user's name to indicate that he/she is online while no icon will appear if they are offline. A user when offline can still get messages dropped by other users, when next they come online as unread messages.

This proposed application enables users to not just get information or place order for agricultural products but also embeds payment gateway for making payments securely. The traditional platform of payment will need the farmers to have their online payment platform for order separate from the platform but this application makes it easier. Customers can become aware of the number of products for a particular produce available and the farmer who is interested in selling. In a normal social media platform, the contact of the farmer is not kept securely as this could be used for malicious acts. This platform caters for this by simply using only the names of the users without breaching their details. Due to the level of trust demanded in the transactions, customers can rate the farmers

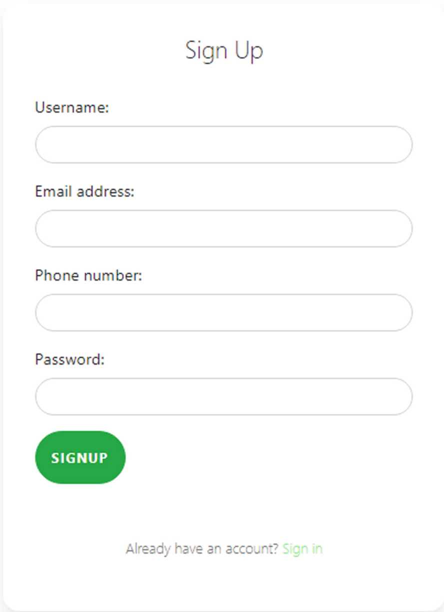


Fig. 3. Screenshot of the sign in page.

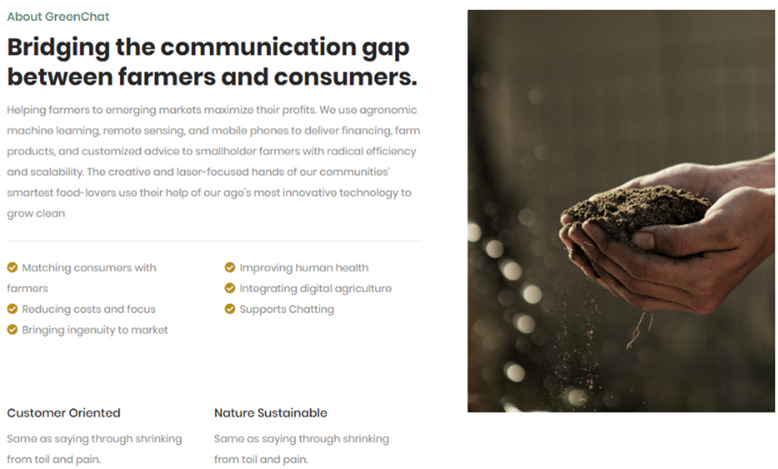


Fig. 4. The screenshot of the proposed system homepage

to enable new prospects make a choice of who they want to buy from. For example, a 4-star or 5-star farmer is more reliable than a 1-star or 2-star rated farmer. This helps ensure the provision of quality products and services as farmers would not want to keep losing customers.

Fig. 5. The screenshot showing the chatting engagement

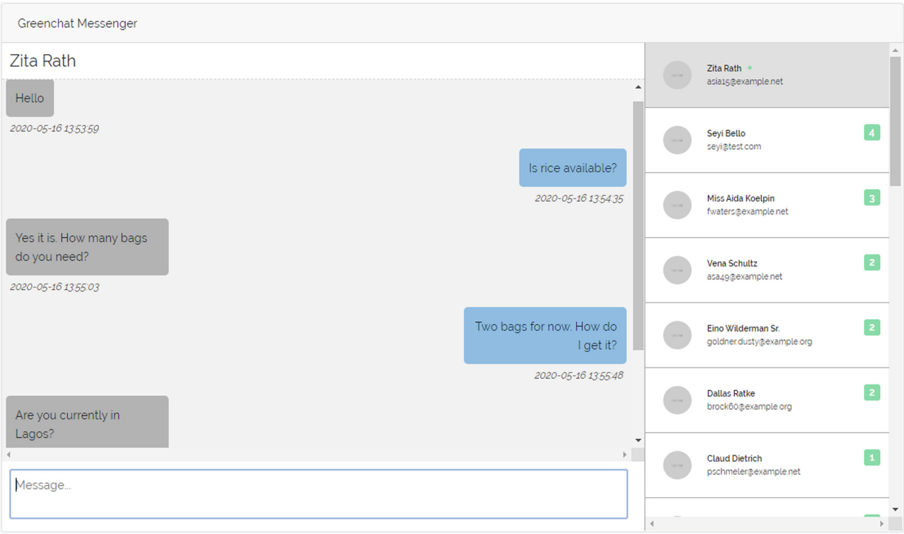


Fig. 6. Screen shot showing the connection status.

5 Conclusion

The Ease of accessing and availability of information are critical to the welfare of a nation. Where the right conversation between farmers who have agricultural produce and the prospects who long for them are not effective, there would be the loss on such goods. With the required diversification of national economy in many parts of Africa, agriculture has been seen as a critical se tor to help achieve this. This research presents an instant messaging web application which should be adopted by farmer's cooperation around to save people from communication costs, increase the efficiency of market interactions and provide access to real time information mainly by enhancing farmers' access to markets and their pricing power through the use of instant messaging via web applications and likewise to educate agriculturists by enlightening them on how to make use of technologies to yield production and profitability. This makes it possible to chat online directly with agents, traders and/farmers. This saves customers the trouble of having direct conversation every time when requesting for the supply of farm produce from agriculturists.

References

1. Oruma, S.O., Misra, S., Fernandez-Sanz, L.: Agriculture 4.0: an implementation framework for food security attainment in Nigeria's Post-Covid-19 era. IEEE Access **9**, 83592–83627 (2021)
2. Ortmann, G.F.: Promoting the competitiveness of South African agriculture in a dynamic economic and political environment. Afr. J. Agric. Econ. Res., Policy Pract. South. Afr. **133**(3), 286–320 (2010)
3. Olokundun, A.M., Falola, H.O., Ibidunni, O.S.: Agro busi-ness as a remedy for youth unemployment towards the achievement of sustainable development in Nigeria: comparative perspec-tives from the Kwara state agro business economy. J. Econ. Sustain. Dev. **5**(3), 46–57 (2014)
4. Devaux, A., Torero, M., Donovan, J., Horton, D.: Agricultural innovation and inclusive value-chain development: a review. J. Agribusiness Developing Emerg. Economies **8**(1), 99–123 (2018)
5. Saidu, A., Mohammed, A., Adamu, S.H.: Application of ICT in agriculture: opportunities and challenges in developing countries. Int. J. Comput. Sci. Math. Theory **3**(1), 1–8 (2017)
6. Pan, Y., Smith, S.C., Sulaiman, M.: Agricultural extension and technology adoption for food security: evidence from Uganda. Am. J. Agric. Econ. **100**(4), 1012–1031 (2018)
7. Kabbiri, R., Dora, M., Kumar, V., Elepu, G., Gellynck, X.: Mobile phone adoption in Agri-food sector: are farmers in Sub-Saharan Africa connected? Technol. Forecast. Soc. Change **131**, 253–261 (2018)
8. Arogundade, O.', Abayomi-Alli, A., Adesemowo, K., Bamigbade, T., Odusami, M., Olowe, V.: An intelligent marketspace mobile application for marketing organic products. In: Hattingh, M., Matthee, M., Smuts, H., Pappas, I., Dwivedi, Y.K., Mäntymäki, M. (eds.) I3E 2020. LNCS, vol. 12066, pp. 276–287. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-44999-5_23
9. Senyolo, M.P., Long, T.B., Blok, V., Omta, O.: How the characteristics of innovations impact their adoption: an exploration of climate-smart agricultural innovations in South Africa. J. Cleaner Prod. **172**(20), 3825–3840 (2018)
10. Masuki, K.F.G., et al.: Role of Mobile Phones in İmproving Communication and İnformation Delivery for Agricultural Development: Lessons from South Western Uganda. Workshop at Makerere University, pp. 22–23. Makerere University, Uganda (2010)
11. Aker, J.C., Mbiti, I.M.: Mobile phones and economic development in Africa. J. Econ. Perspect. **24**(3), 207–232 (2010)
12. Adesemowo, A.K., Abayomi-Alli, A., Olabanjo, O.O., Odusami, M.O., Arogundade, O.T., Abioye, T.E.: Harnessing the potentials of mobile phone for adoption and promotion of organic farming practices in Nigeria. In: Sharma, S.K., Dwivedi, Y.K., Metri, B., Rana, N.P. (eds.) TDIT 2020. IAICT, vol. 618, pp. 170–181. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-64861-9_16

13. Abayomi-Alli, O., et al.: Smart-solar irrigation system (SMIS) for sustainable agriculture. In: Florez, H., Diaz, C., Chavarriaga, J. (eds.) ICAI 2018. CCIS, vol. 942, pp. 198–212. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-01535-0_15
14. Singhal, M., Verma, K., Shukla, A.: Android based solution for Indian agriculture. In: 2011 Fifth IEEE International Conference on Advanced Telecommunication Systems and Networks (ANTS), Bangalore, India, 18–21 Dec 2011
15. Wright, H.J., et al.: Using ICT to strengthen agricultural extension systems for plant health. J. Agric. Food Inform. **17**(1), 23–36 (2016). https://doi.org/10.1080/10496505.2015.1120214
16. Tegegne, A.K., Alemu, T.A.: SMS-based agricultural Information systems for rural farmers in Ethiopia. J. Usability Stud. **15**(1), 47–62 (2019)
17. Saravanan, R., Suchiradipta B.: Mobile phone and social media for agricultural extension: getting closer to hype & hope? In: International Conference on Extension Educational Strategies-for Sus-tainable Agricultural Development A Global Perspective, University of Agricultural Sciences, Bangalore, Indıa, pp. 140–148. 5–8 Dec 2013
18. Churi, A.J., Mlozi, M.R., Mahoo, H., Tumbo, S.D., Casmir, R.: A decision support system for enhancing crop productivity of smallholder farmers in semi-arid agriculture. Int. J. Inform. **3**(8), 838–847 (2013)
19. Trigodo, R., Ebardaloza, J.B., Sabido, D.J.: SMS-based Smart-er Agriculture decision support system for yellow corn farmers in Is-abela2015. In: IEEE Canada International Humanitarian Technology Conference (IHTC2015) (2015)
20. Barh, A., Balakrishnan, M.: Smart phone applications: Role in Agri-information dissemination. Agric. Rev. **39**(1), 82–85 (2018)
21. Prasad, S., Peddoju, S.K., Ghosh, D.: AgroMobile: a cloud-based framework for agriculturists on mobile platform. Int. J. Adv. Sci. Techno. **59**, 41–52 (2013)
22. Lomotey, R.K., Jamal, S., Chai, Y., Deters, R.: Mobicrop: supporting crop farmers with a cloud-enabled mobile app. In: Proceedings of the 6th Service-Oriented Computing and Applications, vol 1, pp. 182–89. Koloa, HI, USA (2013)
23. Sharma, S., Patodkar, V., Simant, S., Shah, C.: E-agro android application-integrated farming management systems for sustainable development of farmers. Int. J. Eng. Res. Gen. Sci. **3**, 368–372 (2015)
24. Kirubi, C., Jacobson, A., Kammen, D.M., Mills, A.: Community-based electric micro-grids can contribute to rural development: evidence from Kenya. World Dev. **37**(7), 1208–1221 (2009)

Machine Learning Approaches for Classifying the Peace-War Orientations of Global News Organizations' Social Media Posts

Ada Peter[1], Rose Omole[1], Sanjay Misra[1,1](✉), Lalit Garg[2,3], and Jonathan Oluranti[1]

[1] Covenant University, Ota, Ogun State, Nigeria
{ada.peter,jonathan.oluranti}@covenantuniversity.edu.ng, rose.omole@stu.cu.edu.ng, sanjay.misra@hiof.no

[2] Department of Computer Science and Communication, Ostfold University College, Halden, Norway

[3] University of Malta, Msida, Malta

Abstract. The study used the existing conceptualizations of peace and war journalism to create supervised machine learning text classifiers trained and tested to identify the war or peace orientations of news stories posted on social media. Peace-oriented journalists promote peace initiatives, ignore differences, and promote conflict resolution. In contrast, war-oriented journalists promote differences between opposing parties and instigate violence as means to resolving conflicts. Using Naïve Bayes, Logistic Regression, Decision Trees, Random Forests, and Support Vector Machines (SVM), the study trained and tested five computational models to detect the peace or war orientations of the news posted on social media. The results indicate that Random Forest has the highest predictive accuracy for predicting war or peace orientations of online news stories. Naïve Bayes ranked the least accurate algorithm for predicting peace or war orientations of online news stories.

Keywords: Naïve bayes · Logistic regression · Support vector machine · Random forest · War and peace journalism

1 Introduction

Galtung [1, 2] suggests that peace-oriented frames promote peace initiatives, ignore differences, and encourage conflict resolution, while in contrast, war-oriented frames enable differences between opposing parties and instigate violence as means to resolving conflicts. Social Science researchers have used Galtung's competing frames of war coverage to examine and critique how journalists represent different conflict situations in other countries [3–5]. For Instance, Lee [5] used Galtung's model to examine and compare the framing of two different levels of conflicts, the Iraq War and Asian conflicts, by eight newspapers in India, Pakistan, Sri Lanka, Indonesia, and the Philippines.

The trained algorithms are available on Streamlit: https://share.streamlit.io/ade-rose/peace-and-war-journalism-classifier/app.py.

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 301–317, 2023.
https://doi.org/10.1007/978-3-031-13150-9_26

Lee [5] content analyzed 1558 stories on the Iraq War and the Asian conflicts involving Pakistan and India's tussle over Kashmir, the Tamil Tigers in Sri Lanka, the Muslim separatist movement in the southern Philippine province of Mindanao and the Aceh and Maluku civil wars in Indonesia showed that the Asian newspapers used a war journalism frame in covering local conflicts but deployed a peace journalism frame in covering the Iraq war. Fahmy and Neuman [4] also used Galtung's classification of war and peace to investigate visual frames provided by three leading newswire services covering the 2008–2009 Gaza War. Zaheer [6] also used Galtung's peace and war journalism lenses to examine newspaper coverage of the Kashmir conflict caused by the murder of a Kashmiri freedom fighter, Burhan Wani. Zaheer [6] looked at four generally distributed Pakistani newspapers of Urdu and English language.

Many more studies [4, 7–15] have used the model to suggest the ideal role of the media and to propagate a different type of framing for war. But like Fahmy [4], Lee [5] and Zaheer [6] other social scientists continue to manually examine the war or peace content of traditional news story coverage of various conflicts. Several factors often constrain these empirical studies, primarily subject to classic newspaper stories, broadcast news transcripts, manual coding, and analysis. The first factor is that the method inevitably limits sample sizes, both in terms of the range of media outlets and the periods covered. As Flaounas et al. pointed out, manual form of content analysis is labor-intensive [16], relying upon people to physically examine and interpret media content (texts or pictures) as war or peace oriented is gradually becoming problematic. The range of media outlets and citizen journalists has increased with news media organizations posting fleeting news content on social media platforms, like Facebook.

Is an automated approach to classifying the peace or war orientations of global news organizations' social media posts possible? Which algorithm can best predict the war or peace frames of a news post? Automating news analysis for war and peace content on traditional international media organizations (Aljazeera, BBC, CNN, Deutsche Welle, and France24) has significant applications. First, an automated model will evaluate large datasets on time, classify these extensive news contents as war or peace oriented. If plugged into various sites, it can provide real-time analytics on multiple media coverage on specific wars, like the recent Israel-Gaza conflict. Besides saving considerable time for researchers, the analytics will provide deep insights on possible relationships between media slants and war/conflict outcomes. Social media platforms may also opt to improve the model for flagging content as war or peace-oriented when it emanates from news organizations. This practice is like flagging an individual's post as hate speech. Students in the field of communication may also find the model resourceful for research endeavors. Besides, since news posts on Facebook generate immediate reactions from the audience, an automated classification provides the opportunity to examine the types of emotions and sentiments that peace or war-driven content instigates from empirical data. There are possibilities that the outcomes may either bolster the case for peace journalism or provide counterarguments for proponents of war journalism.

The authors used existing conceptualizations [1, 5] of peace and war journalism to create and compare five supervised machine learning text classifiers trained and tested to identify war or peace-oriented texts on Facebook accounts of the selected online news entities (Aljazeera, BBC, CNN, Deutsche Welle, and France24). Separately, there are

15.15 million people following Aljazeera English on Facebook, 56.56 million following BBC, 38.2 million following CNN, 378.3 thousand following Deutsche Welle, and 1.89 million following France 24.

The authors examined which supervised machine learning model best computationally classified news contents into peace and war journalism, identified the predictive accuracy of each computational model used for the classification, and presented the datasets and components of Galtung's model used for the development of the computational model. The outcome is machine classifiers that automatically detect war or peace-orientations of the news posted on social media.

Research Questions
We posed two research questions based on Galtung's classification of war and peace journalism [1, 18] and later attempts to understand the concept both from a normative and empirical perspective.

RQ1**:** Which supervised machine learning model best classifies a journalist's news post as peace and war-oriented content?
RQ2: What is the predictive accuracy of Naïve Bayes, Logistic Regression, Decision Trees, Random Forests, and Support Vector Machines in classifying online news content as peace or war oriented?

2 Method

This study is based on a content analysis of 4674 CNN, BBC, France24, Aljazeera, and Deutsche Welle Facebook posts on the following wars from 00:00:00 WAT, March 1, 2011, to March 00:00:00 WAT 31, 2021.

Together, during the timeframe, 29,144,234 million interactions occurred on the pages of these news organizations about the following conflicts (See Table 1).

- *The Libya conflicts*
- *The Syria conflicts*
- *The Afghanistan conflicts*
- *The Yemen conflicts*
- *The Gaza conflicts*

The unit of analysis was the individual post, a definition that included any posts summarizing and redirecting readers to each news organization's website where the entire story is hosted. These posts often summarize the content of the main story published on each media organizations' website. The authors collected all Facebook texts posted by the five selected global news organizations on conflicts and wars in the following countries - Afghanistan, Gaza, Libya, Syria, and Yemen.

The posts were collected via CrowdTangle,[1] and then the content was analyzed by the authors and two additional Covenant University Mass Communication Graduate

[1] https://www.crowdtangle.com.

Table 1. Distribution of posts and interactions across the five conflicts

Conflict	All posts (Aljazeera, BBC, CNN, DW, FR24)	Interactions
Afghanistan	970	6,520,577
Gaza	685	3,935,528
Libya	359	1,349,720
Syria	2050	14,316,367
Yemen	610	3,022,042

students between March 2021 and April 2021. Crowd Tangle is a tool from Facebook to help researchers follow, analyze, and report on what is happening across social media. Access to this tool was granted through Harvard's Social Science One partnership with Facebook[17], a collaboration with access to Facebook data that focuses on the effect of social media on democracy and elections.[2] The only filter applied during the search was the preference for output of overperforming posts only. The following keywords were used to search from 15 00:00:00 WAT, March 1, 2012, to March 31, 2021, 00:00:00 WAT - Afghanistan, Gaza, Libya, Syria, and Yemen. The system collated all over performing posts by these news organizations mentioning each key term. The search result returned 4674 posts. The authors opted to use social media posts for training and testing the algorithms because these posts are shorter and less complicated for training algorithms, unlike the more extended versions of the same story posted on the respective websites of these news organizations. More so, a close examination of social media posts indicated that these posts briefly summarized the contents on the websites with links that redirect followers to the expanded versions of the story.

Coding Categories

Based on the original table of Galtung's[3] classification of what a journalist will do, the coding categories for war and peace frames involve four orientations for peace journalism and four orientations for war journalism. A peace journalist's orientation included (a) peace/conflict-oriented, (b) truth-oriented, (c) solution-oriented, and (d)people-oriented. The war journalist's orientations included (a) war/conflict-oriented, (b) victory-oriented, (c) propaganda-oriented, and (d) elite-oriented [19]. Each orientation was detected by two to eight indicators (Appendix). However, the authors used only the indicators of war/violence orientation and peace /conflict orientation. The rationale for using indicators of war and peace orientations is that after examining more than 80% of the news post stories, the authors noticed that most of the available posts were more of either peace/conflict oriented or war violence-oriented indicators. Since algorithms need a lot

[2] https://socialscience.one/our-facebook-partnership Hosted by Harvard's Institute for Quantitative Social Science.

[3] Conflict Transformation by Peaceful Means: The TRANSCEND Method by Professor Johan Galtung. UN publication 1999 cited cited by Lynch and McGoldrick's. (2000). https://www.transcend.org/tri/downloads/McGoldrick_Lynch_Peace-Journalism.pdf.

of similar data to learn, the study focused on training the algorithms with the available type of post. This implies that the existing algorithms were only trained to identify war/violence and peace/conflict-oriented stories.

The eight indicators for the war/violence oriented stories include (i) Focus on conflict arena, two parties, one goal (win), war general zero-sum orientation (ii) Closed space, closed time; causes and exits in the arena, who threw the first stone (iii) making wars opaque/secret (iv) “us-them” journalism, propaganda, voice, for “us” (v) see “them” as the problem, (vi) dehumanization of “them” (vii) reactive: waiting for violence before reporting, (viii) focus only on the visible effect of violence (killed, wounded and material damage. The six indicators for the peace/conflict-oriented stories include (i) explore conflict formation, x parties, y goals, z issues general “win, win” orientation (ii) open space, open time; causes and outcomes anywhere, also in history/culture (iii) giving voice to all parties; empathy, understanding see conflict/war as a problem, focus on conflict creativity (iv) humanization of all sides; more so the worse the weapons (v) proactive: prevention before any violence/war occurs (vi) focus on invisible effects of violence (trauma and glory, damage to structure/culture) For example, a story was judged if it is reactive (“was the post after the outbreak of the war?); whether it reported mainly on the visible effects of war (“Does the post mention injuries, injured, number of deaths, destroyed cars, houses, homes focus on casualties, death toll, property damage?”); and whether it was partisan (“does the post only mention one of the conflicting parties?”). It was nearly impossible to identify more than one indicator in each post because these posts were concise, most times between 20 - 30 words. This is different from the longer stories used by previous studies (Lee et al., 2006) where the story was classified as a peace journalism story if the total score for peace journalism indicators exceeded the total score for war journalism or classified as war journalism when the war journalism indicators exceeded peace journalism indicators. Hence, the authors measured each post’s war or peace orientations based on the war or peace indicator that best represents the post.

In terms of intercoder reliability for the human coders, a coding of 300 posts produced Scott’s pi of between 0.79 and 0.97, with the following ranges for the war oriented journalist: (i) Focus on conflict arena, (between 0.84 and 0.88) (ii) Closed space, closed time; causes and exits in arena, who threw the first stone (between 0.80 and 0.87) (iii) making wars opaque/secret (between 0.79 and 0.81) (iv) “us-them” journalism, propaganda, voice, for “us” (between 0.79 and 0.88) (v) see “them” as the problem, (between 0.80 and 0.82) (vi) dehumanisation of “them” (between 0.84 and 0.88) (vii) reactive: waiting for violence before reporting, (viii) focus only on visible effect of violence (killed, wounded and material damage((between 0.90 and 0.97). The Scott’s pi inter coder reliability ranges for the peace oriented journalist are (i) between 0.80 and 0.87 for exploring conflict formation, (ii) open space, open time; (between 0.90 and 0.93 (iii) giving voice to all parties; (between 0.90 and 0.92 (iv) humanisation of all sides (between 0.79 and 0.81); (v) proactive: prevention before any violence/war occurs (between 0.90 and 0.93 (vi) focus on invisible effects of violence: trauma and glory, damage to structure/culture (between 0.82 and 0.89). From the manually classified war or peace-oriented content, 70% was used to teach, and 30% to test all five models on identifying the writings of a peace-oriented journalist or a war-oriented journalist.

Features

The manually classified war or peace-oriented datasets were pre-processed through the Natural Language processing pipeline to ensure their usability for the machine learning classifiers. Natural Language Processing (NLP) structured the unstructured data so that the models could intelligently decipher the human language used in each post. First, all characters were converted to lowercase since the datasets had several words starting with capital letters. These included names of people, places, and single-person pronouns. For example, the Aljazeera Facebook post: '*While the country came closest ever to peace in its 18 years of war, this year, Afghanistan also saw unprecedented violence'* was converted to '*while the country came closest ever to peace in its 18 years of war, this year, afghanistan also saw unprecedented violence* using the function *lower ()*. Next, all punctuations like full stops, commas, ampersand were removed because punctuations often hinder the full performance of the models and more, so punctuations are not inevitable during classification. For example, "*while the country came closest ever to peace in its 18 years of war, this year, afghanistan also saw unprecedented violence"* was converted to "*while the country came closest ever to peace in its 18 years of war this year afghanistan also saw unprecedented violence* using the function *("".join)*. Then stop words like 'in' and 'that' were also removed using *nltk.corpus.stopwords.words*. Stop words are words that do not necessarily add any meaning to a sentence. Subsequently, we tokenized to help each model to identify each word as necessary and something to classify. The dataset was tokenized using the function *(re.split)*. After tokenization, the dataset was lemmatized. During lemmatization, words with prefixes and suffixes were converted to their original words using the function *(nltk.WordnetLemmatizer)*. For instance, the word *"closest"* was converted to *"close"*. Finally, using count vectorizer and term frequency vectorization, we then calculated the weights for every word using tokens present in each post. We find that the count vectorizer rendered the data-sparse; hence we opted for the term frequency vectorizer (TF-IDF) because it created a normalized weight score for every word in the data set and summarized how often each word appeared the most, thus giving a class of word a unique vector. For instance, when the word "killings" appeared a lot, TF-IDF assigned a vector of 0.23738848 to "killings." When the word "protest" appeared a few times, TF-IDF assigned a vector of 2.4889593938 to that word. So, wherever the word killing was mentioned [mostly war-related posts], the vector 0.23738 substituted the word. The $\textit{tf-idf}_{t,\ p}$ issues a weighted score, based on the term *t* and the post *p,* as follows: Highest if a term, t, is found across a few posts in the corpus; Lower if the term occurs a fewer number of times in a post, or occurs in too many posts in the corpus (resulting in a lower relevance of the word); Lowest when the term, t, occurs in all the posts and many times per post.[4]

The preceding process converted the datasets into numbers since machine learning models only understands numbers. For example, *"country" "came" "closest"*

[4] Excerpt From Hands-On Natural Language Processing with Python Arumugam, Rajesh; Shanmugamani, Rajalingappaa (2018) Packt Publishing.

“peace” 18 years “war”, “year”, “afghanistan” “saw” “unprecedented” “violence” were converted to ‘1 0 0 1 0 1 0 using the function *(TfidVectorizer).*

3 Models

The authors trained and tested five natural language classification algorithms: Decision Trees, Logistic Regression, Naïve Bayes, Random Forests, and Support Vector Machines (SVMs). Each algorithm was implemented differently. The SVM implementation was based on LIBSVM, where the fit time-scaled at least quadratically with the number of samples as it may be impractical beyond tens of thousands of samples. The random forest was implemented based on the meta estimator that fits several decision tree classifiers on various sub-samples and used averaging to improve the predictive accuracy and control over-fitting. The sub-sample size was controlled with the max-samples parameter. The decision tree classifier was implemented by taking as input two arrays: an array X, sparse or dense, of shape (n_samples, n_features) holding the training samples, and an array Y of integer values, shape (n_samples,), keeping the class labels for the training samples. After being fitted, the model was then used to predict the class of samples. The Multinomial Naive Bayes was used to implement the naive Bayes algorithm for multinomial distributed data, one of the two classic naive Bayes variants used in text classification. The data are typically represented as word vector counts. The number of features (in text classification, the vocabulary size) was the probability of elements appearing in a sample belonging to the class.

We tested each model using five-fold cross-validation, holding 10% of the sample for evaluation to help prevent overfitting. We excluded any grid search to tune the hyper-parameters of these models since the data sets were highly random. The non-grid search approach reduces any possibility of overfitting. Then all five models using the entire dataset were trained and tested to predict the label for each post. All modeling was performed using scikit-learn. Each algorithm was trained with 70% of the dataset with the code (train_inputs, train_classes), and then based on the training, the algorithm built a model and tested the model with the 30% using the code(test_inputs, test_classes). We trained the model with the dataset after splitting it into 70% training and 30% test sets using the following code

$$\textbf{from}\ \text{sklearn.model\_selection}\ \textbf{import}\ \text{train\_test\_split}$$
$$\text{train\_test\_split(news posts, classes, train\_size} - 0.7,\ \text{random\_state}{-}10)$$

The random state for the dataset is 10. A random state ensures that the split datasets are reproducible anytime.

4 Results

RQ1: Which machine learning model best classifies a journalist’s news post as peace and war-oriented content?

Findings suggest that Random Forest and Support Vector Machine were the machine learning models that best classifies social media news posts as peace or war oriented.

Fig. 1. BBC sample facebook news post

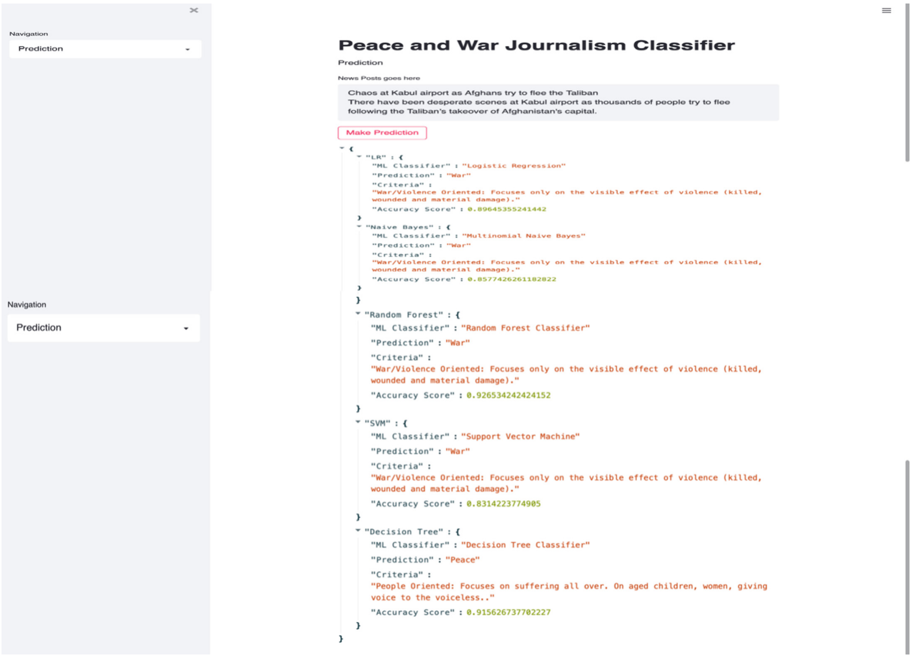


Fig. 2. A screenshot of the performance of each algorithm for one of the war-oriented posts. Decision misclassifies the war-oriented post as peace

To examine which machine learning model best ranks a journalist news post as peace or war-oriented, we experimented with all five trained and tested models ten different times with ten other random posts, five war-oriented and five peace-oriented. The experiment was conducted by copying a random social media news post from one of the news media organizations (See Fig. 1), pasted the same on the visualization tool's prediction tab, and ran the code. In all ten instances, Random Forest accurately identified each post as peace or war oriented. Support vector Machine was accurate all the time but had a lower mean predictive accuracy of 0.83 than Random Forest with a mean predictive accuracy of 0.93.

During the test for the peace-oriented posts, Logistic Regression, Decision Tree, and Naïve Bayes were incorrect at different times. Logistic regression was correct in all attempts to identify war-oriented posts but misclassified 20% of peace-oriented posts by classifying peace-oriented posts as war. Naïve Bayes had the poorest performance. All attempts to identify a peace-oriented post were misclassified as war. Naïve Bayes was

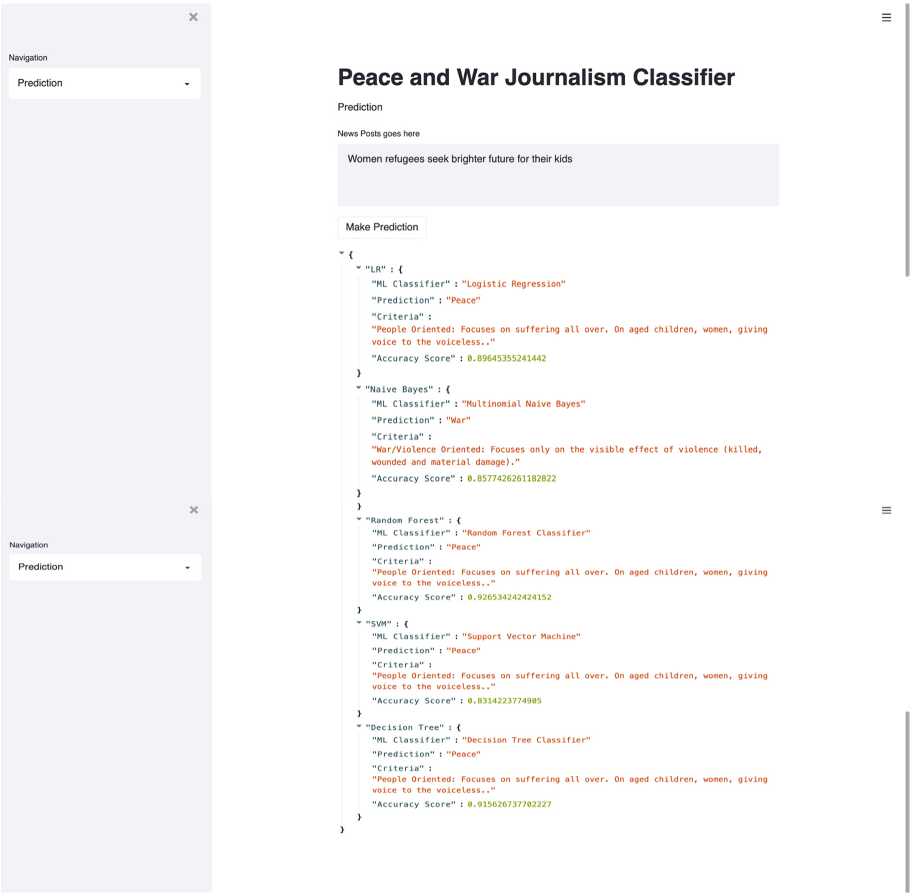


Fig. 3. A screenshot of the performance of each algorithm for one of the peace-oriented posts. Naïve Bayes misclassifies the peace-oriented post as war

more accurate in placing war-oriented posts. In only one instance, Decision Tree misclassified a war post as peace. See (Fig. 2) a screenshot of the performance of each algorithm for one of the war-oriented posts and (Fig. 3) a screenshot of the implementation of each algorithm in identifying peace-oriented posts.

Table 2 presents the summary of the performance of each model of each experiment. The stroked outcomes represent the instances that were misclassified.

Table 2. Summary of the performance of each model during the experiment

S/N	Test instance	RF	SVM	LR	DT	NB
1.	1 (war)	0.93	0.83	0.89	0.92	0.86
2.	2 (war)	0.93	0.83	0.90	0.92	0.86
3.	3 (war)	0.93	0.83	0.90	0.92	0.86
4.	4 (war)	0.93	0.83	0.90	~~0.93~~	0.86
5.	5 (war)	0.93	0.83	0.90	~~0.92~~	0.86
6.	1 (peace)	0.93	0.83	~~0.90~~	0.92	~~0.90~~
7.	2 (peace)	0.93	0.83	0.90	0.92	~~0.86~~
8.	3 (peace)	0.93	0.83	0.90	0.92	~~0.86~~
9.	4 (peace)	0.93	0.83	0.90	0.92	~~0.86~~
10.	5 (peace)	0.93	0.83	0.90	0.92	~~0.86~~
11.	Average of the times the model was correct	0.93	0.83	0.80	0.74	0.43
12.	Rank	1st	2nd	3rd	4th	5^{th}

Table 3. The accuracy test score for each model is presented in the table below[1]

Model	DT	LR	NB	RF	SVM
Predictive accuracy score	0.84	0.87	0.84	0.85	0.86
F1	0.86	0.89	0.85	0.89	0.90

[1]In classification problems, precision and recall are most often reported for measuring performance. Precision is the ratio of true positives to the sum of true positives and false positives. Recall is the ratio of true positives to the sum of true positives and false negatives. Positive and negative refer to whether a post is classified war or peace oriented. Intuitively, precision identifies the proportion of the classifications is correct, and recall identifies what proportion of the actual abstracts is correctly classified. Because both are important measures of accuracy, their harmonic mean, the F1 score, is our preferred accuracy metric

RQ2: What is the predictive accuracy of Naïve Bayes, Logistic Regression, Decision Trees, Random Forests, and Support Vector Machines in classifying online news content as peace or war oriented? (Table 3)

Measuring Performance

The best performing model is Random Forest with a predictive accuracy of 0.93, an overall precision of 0.90, recall of 0.89, and an F1 score of 0.89. (Also see Table 4).

Table 4. Sample news posts and ML prediction outcomes

Model	Post	Predictive accuracy	Source	ML classification	Remark
LR	Chaos at Kabul airport as Afghans try to flee the Taliban There have been desperate scenes at Kabul airport as thousands of people try to flee following the Taliban's takeover of Afghanistan's capital	0.89	https://bbc.in/3D17k6r	War	Correct!
NVB		0.85		War	Correct!
RF		0.92		War	Correct!
SVM		0.83		War	Correct!
DT		0.92		Peace	Wrong!
LR	Video shows Afghans clinging to outside of US military plane as it takes off Video shows people clinging to the outside of a US military aircraft before it takes off from Kabul airport. CNN's Clarissa Ward reports on chaotic scenes as the Taliban take control of Afghanistan	0.89	https://cnn.it/3syitXz	War	Correct!
NVB		0.86		War	Correct!
RF		0.93		War	Correct!
SVM		0.83		War	Correct!
DT		0.92		War	Correct!

(*continued*)

Table 4. (*continued*)

Model	Post	Predictive accuracy	Source	ML classification	Remark
LR	Taliban declares Afghanistan war over after president flees It is the first day of what the Taliban calls the "Islamic Emirate of Afghanistan" after its fighters took control of Kabul and President Ghani fled the country	0.90	https://aje.io/hrunev	War	Correct!
NVB		0.86		War	Correct!
RF		0.93		War	Correct!
SVM		0.83		War	Correct!
DT		0.92		War	Correct!
LR	Scale of Russian mercenary mission in Libya exposed The scale of operations by a shadowy Russian mercenary group, Wagner, in Libya's civil war has been revealed after a BBC investigation. A Samsung tablet, found after being left by a fighter, has exposed how the mercenaries have committed war crimes	0.90	https://bbc.in/3CDE1qk	War	Correct!
NVB		0.86		War	Correct!
RF		0.93		War	Correct!
SVM		0.83		War	Correct!

(*continued*)

Table 4. (*continued*)

Model	Post	Predictive accuracy	Source	ML classification	Remark
DT		0.92		War	Correct!
LR	UK-born man, who was a member of the ISIL (ISIS) team in Syria and accused of beheading US hostages, has pleaded guilty to eight US criminal charges, including lethal hostage taking and conspiracy to support "terrorists"	0.90	https://www.aljazeera.com/news/2021/9/3/uk-born-isil-fighter-pleads-guilty-to-murdering-us-hostages?sf150588367=1	War	Correct!
NVB		0.86		War	Correct!
RF		0.93		War	Correct!
SVM		0.83		War	Correct!
DT		0.92		War	Correct!

5 Discussion

By using existing conceptualizations of peace and war journalism, the study trained, tested, and compared the performance of five supervised machine learning algorithms in identifying war or peace-orientations of texts posted by CNN, BBC, Aljazeera, FR24, and DW on social media. The algorithms with the higher predictive accuracies, Random Forest and Support Vector Machine, are valuable for tracking and identifying war or peace-oriented texts posted on social media pages of selected online news entities. It means that researchers can deploy these algorithms for the constant classification of posts and tweets in the immediate aftermath of a conflict, terror attack, or the outbreak of war in different parts of the world.

In previous interdisciplinary empirical studies of war and peace journalism, the classification of media organizations' war and peace content has remained primarily subject to manual coding and analysis [3–5]. These previous studies focused either on the content available on each news agency's respective search engines or analyzed available content on hardcopy newspapers. If future studies plan to examine the war and peace orientations of social media posts, a manual approach to the vast amount of data available on social media platforms is nearly impossible because of the increasing quantity, variety, and speed of online news posts and interactions. Several factors constrain a manual approach to these types of text or picture analysis. First, a manual process to big data is time-consuming and lacks scalability. Besides, the method inevitably limits sample sizes, both in terms of the range of media outlets and the periods covered. Relying on such scenarios is particularly problematic as the range of media outlets and citizen journalists has increased. Second, the traditional form of analysis is labor-intensive, depending on people to physically examine, interpret media content (texts or pictures) as war or peace oriented. The highlighted limits of the manual approach are not to suggest that artificial intelligence is without challenges. Biases can occur in the AI pipeline, from dataset creation and problem formulation to data analysis and evaluation [20]. But in comparison to traditional data techniques and platforms, artificial intelligence techniques (including machine learning, natural language processing, and computational intelligence) provide more accurate, faster, and scalable results in big data analytics [21]. Thus, the approach developed and used in this study appears a viable method for making sense of fleeting news of wars generated on the social media pages of news organizations. The technique is faster, relatively accurate, more precise for massive volumes of data. It may eventually be able to discover hidden patterns and unknown correlations in massive war and peace datasets.

The sheer mass of data would be impossible to handle manually. The Facebook pages of these news organizations, for instance, together with generate millions of interactions daily. Separately, there are 15.15 million people following Aljazeera English on Facebook, 56.56 million following BBC, 38.2 million following CNN, 378.3 thousand following Deutsche Welle, and 1.89 million following France 24. The exact population of followers consists of various ethnicities, groups, classes, gender that provide a variety of responses to news posts released publicly in fleeting seconds. At the time of this study, there were nearly 30 million interactions cumulatively on CNN, BBC, Aljazeera, DW, and FR24 about Libya, Syria, Afghanistan, Yemen, and Gaza conflicts. Thus, it is nearly impossible for humans to work through this type of data without computational assistance. Even the heterogeneity and unstructured nature of these data compound the complexity of handling such enormous data.

The outcome and machine learning tools presented here are helpful for quickly tracking how journalists report specific wars over time and may be a good takeoff for monitoring the relationship between language and emotion. These include answering the question of what type of emotions over time does war or peace journalism evoke? More so, since it has been difficult making a case for peace journalism, an automated detection provides the opportunity to gather and discover hidden patterns and unknown correlations between media frames of conflicts, war outcomes, and emotions. The authors have deployed the algorithms with the most predictive accuracy for collecting and classifying ongoing data for ongoing civil wars and conflicts.

6 Conclusion

The current study used existing conceptualizations of peace and war journalism to create and compare five supervised machine learning text classifiers trained and tested to identify the war or peace orientation of news posted on social media. The texts used for the study were collected from Facebook accounts of the selected news entities (CNN, BBC, France24, Aljazeera, and Deutsche Welle). The study identified Random Forest and Support vector machine as the two top supervised machine learning models to classify news contents into peace and war journalism computationally. The study implies that the random forest algorithm may be best suited for developing more sophisticated models for predicting peace and war-oriented news posts on social media websites. Other investigations may have considered Naïve Bayes a fundamental algorithm for text classification. However, the current research indicates its limits in predicting peace and war-oriented news posts.

The study also identified the predictive accuracy of each of the five computational models. It is essential to highlight that the current attempt to classify social media posts as war or peace-oriented differs from existing hate speech classifications. More so, the classifications here only focus on social media posts of news organizations, not content posted by individual users. But since news posts on Facebook generate immediate reactions from the audience understanding from empirical data, the types of emotions and sentiments that peace or war-driven content instigates may also bolster the case for peace journalism.

The tool is available for test cases on Streamlit. Streamlit[5] is a web development framework that works with Python. A new visualization tool that allows engineers to build and share highly interactive web applications in minutes. The code is also available on Github at https://github.com/war-peace-journalism-project.

Further studies may explore the human versus machine learning performance in classifying news posts as war or peace oriented. Previous studies argue that ML classifiers trained on different training sets are also more reliable than human classifiers, meaning that different ML classifiers are more consistent in assigning the same classifications to any given abstract than different human classifiers. While the top five percentile of human classifiers can outperform ML in limited cases, selection and training of such classifiers are likely costly and challenging compared to training ML models [23]. Future studies can also explore training and testing machine learning classifiers to identify other themes of Galtung's war and peace journalism indic. Thee the current research was based only on the first theme: the peace and war-oriented journalist.

Further studies may explore neural networks, computational replications of important data analysis principles in human brains. Neural networks are the most successful methods for big data analysis. Simulating neural structure in the brain to build neural network structure models and simulating memory mechanisms in the brain to develop learning algorithms are two basic methodologies in neural networks research.

Appendix

What does a Peace Journalist do? This is the Original table by Prof Johan Galtung.[6]

The current study was based only on the first theme: Peace and war-oriented journalist.

[5] https://streamlit.io/.

[6] Conflict Transformation by Peaceful Means: The TRANSCEND Method by Professor Johan Galtung. UN publication 1999 cited cited by Lynch and McGoldrick's. (2000). https://www.transcend.org/tri/downloads/McGoldrick_Lynch_Peace-Journalism.pdf.

Peace/conflict journalism	War/violence journalism
I. Peace/conflict-orientated Explore conflict formation, x parties, y goals, z issues general "win, win" orientation Open space, open time; causes and outcomes anywhere, also in history/culture Making conflicts transparent Giving voice to all parties; empathy, understanding See conflict/war as the problem, focus on conflict creativity Humanisation of all sides; more so the worse the weapons Proactive: prevention before any violence/war occurs Focus on invisible effects of violence (trauma and glory, damage to structure/culture)	I. War/violence orientated Focus on conflict arena, two parties, one goal (win), war general zero-sum orientation Closed space, closed time; causes and exits in the arena, who threw the first stone Making wars opaque/secret "us-them" journalism, propaganda, voice, for "us." See "them" as the problem, focus on who prevails in war, Dehumanizationionn of "them"; more so the worse the weapon Reactive: waiting for violence before reporting Focus on the visible effect of violence (killed, wounded, and material damage)
II. Truth-orientated Expose untruths on all sides / uncover all cover-ups	II. Propaganda-orientated Expose "their" untruths / help "our" cover-ups/lies
III. People-orientated Focus on suffering all over; on women, aged children, giving voice to voiceless a Give name to all evil-doers Focus on people peace-makers	III. Elite orientated Focus on "our" suffering non-disabled bodied elite males, being their mouth-piece give name to their evil-doers focus on elite peace-makers
IV. Solution orientated Peace = non-violence + creativity Highlight peace initiatives, also to prevent more war Focus on structure, culture, the peaceful society Aftermath: resolution, reconstruction, reconciliation	IV. Victory orientated Peace = victory + ceasefire Conceal peace-initiative, before victory is at hand Focus on treaty, institution, the controlled society Leaving for another war, return if the old flares up again

References

1. Galtung, J.: Violence, peace, and peace research. J. Peace Res. **6**(3), 167–191 (1969). https://doi.org/10.1177/002234336900600301
2. Galtung, J.: Peace journalism and reporting on the United States. The Brown J. World Aff. **22**(1), 321–333 (2015). http://www.jstor.org/stable/24591019
3. Abdulbaqi, S., Ariemu, O.: Newspapers framing of herdsmen-farmers' conflicts in Nigeria and its implication on peace-oriented journalism. Theatre Media Stud. **11**(2), 77–105 (2017)
4. Fahmy, S., Neumann, R.: Shooting war or peace photographs? An examination of newswires' coverage of the Conflict in Gaza (2008–2009). Am. Behav. Sci. **56**(2), NP1–NP26 (2012). https://doi.org/10.1177/0002764211419355

5. Lee, S.T., Maslog, C.C., Kim, H.: Asian conflicts and the iraq war: a comparative framing analysis. Int. Commun. Gaz. **68**(5–6), 499–518 (2006). https://doi.org/10.1177/1748048506068727
6. Zaheer, L.: War or peace journalism: comparative analysis of Pakistan's English and Urdu media coverage of Kashmir conflict. South Asian Stud. **31**, 713–722 (2016)
7. De Michelis, S.: Peace Journalism in Theory and Practice. E-Int. Relat. (2018)
8. Hussain, S.: Media coverage of Taliban: is peace journalism the solution? Asia Pac. Media Educ. **26**(1), 31–46 (2016). https://doi.org/10.1177/1326365X16640340
9. Lynch, J.: What's so great about Peace Journalism? Glob. Media J. – Mediterr. Ed. **1**(1), 74–87 (2006)
10. Mashoed, B.: Peace Journalism: A Practical Handbook for Journalists in Cyprus. In: Vakfı, N.T. (ed.), (2017)
11. McGoldrick, A., Lynch, J.: Peace Journalism: What is it and how to do it? Reporting the World (2006)
12. McGoldrick, A., Lynch, J.: Audience responses to peace journalism. Journalism Stud. **17**(5), 628–646 (2016). https://doi.org/10.1080/1461670X.2014.992621
13. Peleg, S.: Peace journalism through the lens of conflict theory: analysis and practice. Conflcit Commun. Online **5**(2), 18 (2006)
14. Powers, S., O'Loughlin, B.: The Syrian data glut: rethinking the role of information in conflict. Media, War Conflict **8**(2), 172–180 (2015). https://doi.org/10.1177/1750635215584286
15. Shinar, D.: Can peace journalism make progress? The coverage of the 2006 Lebanon War in Canadian and israeli media. Int. Commun. Gazette **71**(6), 451–471 (2009). https://doi.org/10.1177/1748048509339786
16. Flaounas, I., et al.: The structure of the EU mediasphere. PLoS ONE **5**(12), e14243 (2010). https://doi.org/10.1371/journal.pone.0014243
17. King, G.: Social Science One - Our Facebook Partnership. Harvard's Institute for Quantitative Social Science (2018)
18. Galtung, J.: On the role of the media in worldwide security and peace. In: Varis, T. (ed.) Peace and Communication, pp. 249–266. Universidad para La Paz, San Jose, Costa Rica (1986)
19. Galtung, J.: Conflict Transformation by Peaceful Means: The TRANSCEND Method (2000)
20. Srinivasan, R., Chander, A.: Biases in AI systems: a survey for practitioners. Queue **19**(2), 45–64 (2021). https://doi.org/10.1145/3466132.3466134
21. Hariri, R.H., Fredericks, E.M., Bowers, K.M.: Uncertainty in big data analytics: survey, opportunities, and challenges. J. Big Data **6**(1), 44 (2019). https://doi.org/10.1186/s40537-019-0206-3
22. Goh, Y.C., Cai, X.Q., Theseira, W., Ko, G., Khor, K.A.: Evaluating human versus machine learning performance in classifying research abstracts. Scientometrics **125**(2), 1197–1212 (2020). https://doi.org/10.1007/s11192-020-03614-2

Application of Block Chain Technology by Aggregators in Complex Supply Chains

Sudhendar Hanumantha Rao[1] and Sreedhar Matam[2(✉)]

[1] Faculty of Management and Commerce, Manipal University Jaipur, Jaipur, India
[2] Bahadur Institute of Management Sciences, University of Mysore, Mysore, India
Sreedhar.Matam@gmail.com

Abstract. Aggregation is the most prevalent emerging business model of E-commerce. Block Chain is an emerging technology leveraging an open, tamper-evident ledger, which can be used in several situations requiring transparent establishment of trust between transacting parties. This offers several benefits like reduced transaction costs, transparency, traceability, and speed of execution. Most existing applications of the aggregation model involve simple supply chains on the supplier side (eg., Uber, OYO, etc.). This article explores how the application of block chain technology in aggregation models involving a complex supply chain scenario to achieve various benefits of merging the two technologies.

Keywords: Business aggregation · Aggregator model · Aggregation theory · Pharmaceutical supply chain · Block chain

1 Introduction

Aggregation is currently one of the fastest developing business models among the e-Commerce businesses. With the advancement of the internet and its spread, the Aggregation theory proposed by Ben Thompson [4] provides a great insight to how business models have changed, and how aggregation can be leveraged in E-commerce. Aashish Pahwa [1] states "The Aggregator Business Model usually organize an unorganized sector and provide their service under their brand". Kohlborn, Korthaus et al. [2] define service aggregator such that "A service aggregator acts as an intermediary between service consumers and providers. From R. Srinivasan [3], it can be inferred that a disorganized customer base could also be a good candidate for aggregation.

In this business model, the aggregator acts as a technology platform bringing together customers and providers, one or both of whom are disaggregated, and unorganized, to result in a transaction. Benefits of this model include economies of scale to vendors and ease of doing business to customers (examples include Uber and AirBnB).

While most existing examples of successful aggregation involve simple chains among providers (for example in the case of AirBnB, individual homeowners interact directly with customers through the platform), not all supply side chains are simple. We shall use the Indian Pharmaceutical Retail as an example to analyze the complexities. The more complex the supply chain is, the more challenges to track, trace and verify

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 318–329, 2023.
https://doi.org/10.1007/978-3-031-13150-9_27

authenticity- Shahid et al. [11] discuss on the challenges of tracking the provenance of data and maintain traceability throughout the supply chain network.

Gaur and Gaiha [14] discuss how to build a transparent supply chain using block chain technology. Namasudra, S., et al. discuss the challenges of the revolution of blockchain. IBM [5] and Hyperledger Foundation [8] show how block chain technology can be utilized to provide traceability in the food industry to develop transparency and trust. Juma, Shaalan, and Kamel [12], Hasan and Salah [13] discuss how the Block chain technology can be applied to solve the supply chain problems.

In implementing this aggregation model and delivering the services, Block chain technology can potentially be applied by an aggregator to achieve various benefits as the product moves across the supply chain and is delivered to the customers in a complex supply chain scenario.

One of the major challenges in the Indian pharma industry is the issue of fake drugs being sold through legitimate channels. The Indian Pharmaceutical Retail sells about one third fake drugs [6] and how technology is being increasingly leveraged to minimize this problem [7]. The Indian Pharmaceutical Retail is used as an example of complex supply chain scenario to illustrate as it has multi-level sourcing, and the Retailers are unorganized (un-aggregated, disintermediated) whereby providing a great opportunity for an aggregation model to work.

This article is an attempt to leverage the concept of the block chain as a public general ledger [10] and see how it can be used in aggregation model as applicable to complex supply chain scenarios. It will briefly discuss the block chain technology concepts, application of the aggregation model in the Indian Pharmaceutical Retail area and then delve into the use of block chain technology and its advantages for application in this area of aggregation.

2 Block Chain Technology

The Block chain is essentially a decentralized distributed ledger that can be private or public that allows blocks of data to be stored across networks, geographies, and onto various servers. By allowing access to the users to the network(s) it lets everyone who is authorized to see everyone else's data entries in near real-time. Thus, provenance of a transaction can be verified, ensuring trust between the transacting parties. Each time a business transaction event occurs, a set of validated transaction block data is added, which then becomes another block in the chain.

Key features of a Block Chain include:

1. It is a distributed ledger or record of transactions between parties involved in a block chain.
2. The transactions are time stamped and combined in chunks called blocks which are appended to the end of a chain of blocks in a linear manner.
3. The process of verifying the transactions, building them into a block and adding them to the chain is referred to as mining. The process typically involves solving a set of complex mathematical operations which are very computing and time intensive to build but are easy to verify.

4. Transactions and blocks can only be updated going forward. Thus, any attempts to retrospectively change/modify an existing transaction is practically impossible and visible. Thus, block chain can be considered as tamper evident.
5. Depending on the ownership and access control, Block Chains may be classified as

   Public and permission less

   Public and permissioned

   Private and permission less

   Private and permissioned

6. An additional feature called a 'Smart Contract' can be used to effect outside transactions based on certain, predefined conditions being met by each transaction added into the block chain.

Following are the main constituents in block chain technology [10]:

A Transaction – It is the result of a business event that manifests itself to create the smallest building block of data of a block chain system.
A Block – It comprises of data structure that is used to keep a set of transactions which is distributed to all nodes in the network
The Chain – It is a sequence of data blocks in a specific order as defined by the block chain
The Nodes – A node is a user or a computer within the block chain network. Every node has an independent validated copy of the whole block chain ledger
The Miners – These are specific nodes in the block chain network which perform the necessary block verification/validation processes before adding any new block to the block chain.
Consensus – Are a set of rules and arrangements defined by the business need that help carry out block chain operations. With each business, these rules will differ.

The following is a block chain architecture diagram [Fig. 1] that shows how it works in a transaction. This mainly applies to a public, permission less block chain.

Following are some of the basic characteristics on which the block chain is built [10]:

Cryptography – This plays a vital role in validating the data as every block chain transaction is validated and is trustworthy. Complex computations and cryptographic proof among involved parties is involved.
Immutability means that no block in a block chain can be changed or deleted thus making it tamper proof
Provenance means that it is possible to track the origin of every transaction inside the block chain ledger
Decentralization means that as the data is spread over and replicated, every member of the block chain structure has access to the whole distributed data in the network.

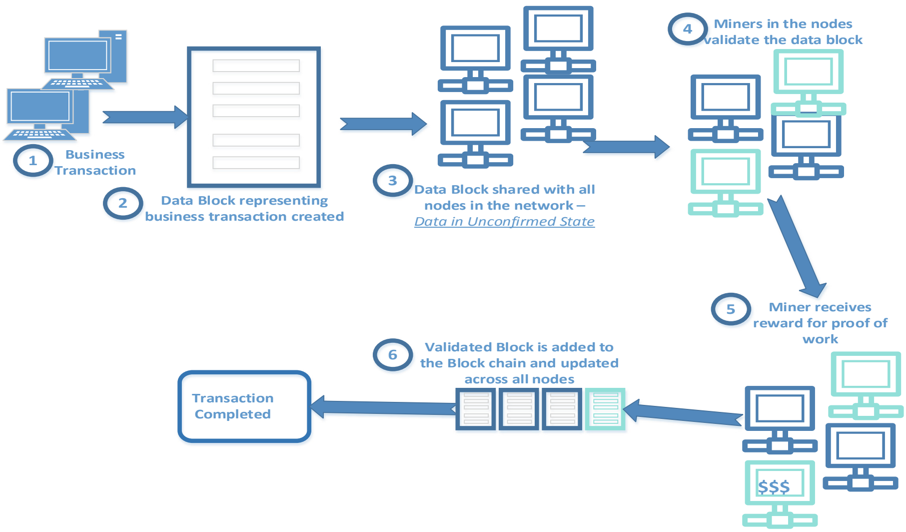


Fig. 1. Block chain architecture

3 Aggregation in Complex Supply Chain – Case of Indian Pharmaceutical Retail

The advent of the internet age has spawned E-Business to provide Products and/or services in new and innovative ways. Various business models like Storefront Model, Auction Model, Portal Model, Dynamic Pricing Models, Bartering Model, B2B Model, Online Trading Model, Online Lending Model, Online Travel Services, E-Learning Model. Aggregation model has been developed and applied for use in business with great success.

Most markets have been unorganized (un-aggregated/disintermediate[1]) historically and the advancement in Communication and Information technology has enabled to help aggregate these markets.

The unorganized (un-aggregated/disintermediated) sector can involve different levels of complexity with factors ranging from the nature of the suppliers, the Supply side complexity and the business rules involved therein between the players, the Contract arrangements between players, the Pricing agreements and incentives across players and combinations that can be used to service the customer better, Regulatory mechanisms involved and its complexity, maintaining quality standards in the supply chain and rating

[1] Un-aggregated, disintermediated are the terms used to define the marketplace models where there is no aggregation involved – for example Amazon India.

the suppliers, liability issues and ownership involved for each combination, Expected impact on the end customer with the use of aggregation, social impact and supplier business continuance for existing suppliers.

According to Pahwa [1] “The Aggregator Business Models usually organize an unorganized and populated sector like hotels, taxis, etc. and provide their service under their brand. Aggregators, just like a marketplace, are big brands which provide goods/services under their own name. The sellers are their partners but, unlike marketplace, sellers don’t sell under their own name. Goods/services are sold under the name of the aggregator and hence the price/price band is determined by the aggregator. Examples of online aggregators are Uber, Ola, Oyo, Munchery, etc.” Aggregation is also different from the Portal model where the goods/services are sold. Kohlborn, Korthaus et al. [2] define service aggregator such that “A service aggregator acts as an intermediary between service consumers and providers. This role combines certain services based on its detailed domain knowledge to add additional value to the services and provide a solution to a customer specific need. Thus, they rebrand, repurpose, and refactor certain services for a specific or anticipated customer demand. The value proposition includes selection, organization, matching, price, convenience, and fulfillment’”.

The internet has provided the means to aggregate the suppliers and match them to the need of customers.

In the article “Organising the Unorganised: Role of platform intermediaries in the Indian real estate market” by R. Srinivasan [3], it can be inferred that a disorganized customer base could also be a good candidate for aggregation.

A visual of aggregated business as described by Ben Thompson [4] is shown below in Fig. 2:

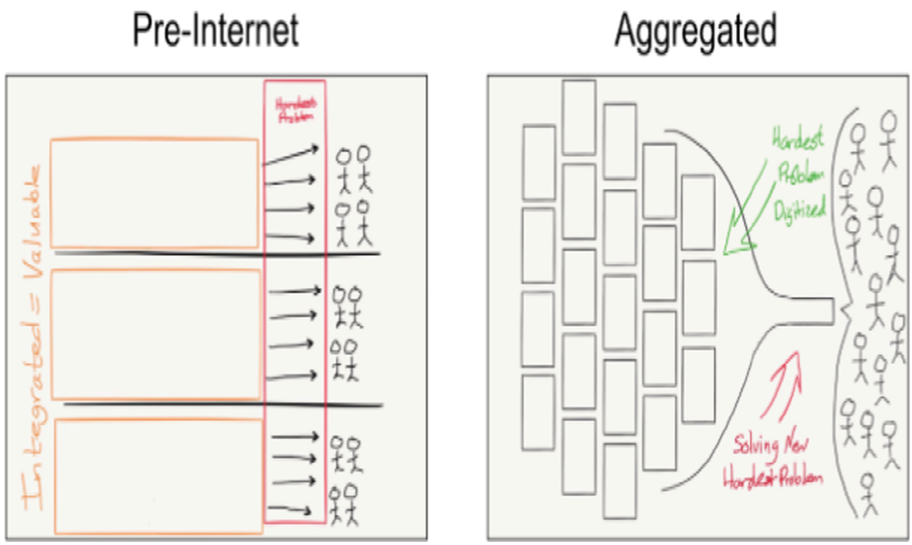


Fig. 2. Ben Thomson aggregation visual

Next we will consider a simple and complex supply chain scenario and how aggregation can be different in each case. Extending the aggregation model from Fig. 2 the UBER/Ola aggregation can be depicted in Fig. 3a **(Pre-aggregation)** and Fig. 3b **(With aggregation)**. The following are the key points of this model:

– In the pre-aggregation model, individual providers (taxis) transacted with individual customers on an ad-hoc basis.
– The price is either set by law or agreed to between the two parties
– Multiple providers interacted with multiple customers
– In the aggregated model, providers (taxis) depend on one party to provide customers
– Customers need to deal with one party for all transactions who sets the price and guarantees the quality parameters and acts as a single source to address complaints and exceptions.
– From a supply chain perspective, there is only one tier of providers/suppliers. Once a customer contacts the aggregator, the order is matched with a single pool of providers any one of whom may be assigned the order. There is only one service contract between a provider and the aggregator and no subcontracts between the provider and other providers. There is only one link between the aggregator and the provider.

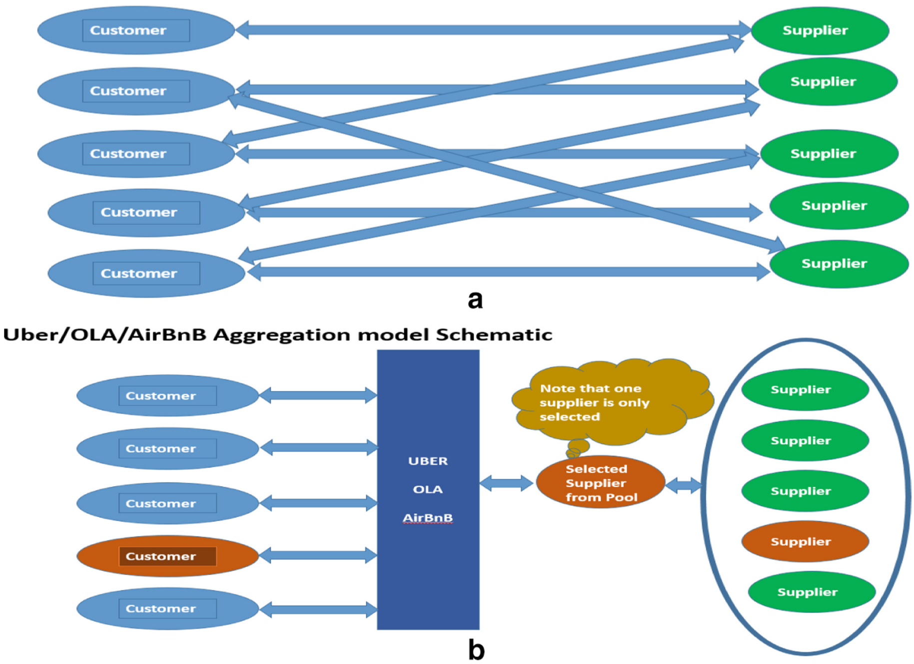


Fig. 3. a (Pre-Aggregation). b (With aggregation)

This can be compared with the supply scenario in the Indian pharma industry where there may be multiple links between the aggregator and the final delivery of the product depending on the product. This is depicted in Fig. 4a **(Pre-Aggregation)** and Fig. 4b **(Post-Aggregation)** (Note: only the supply side is shown in the post-aggregation state in Fig. 4b).

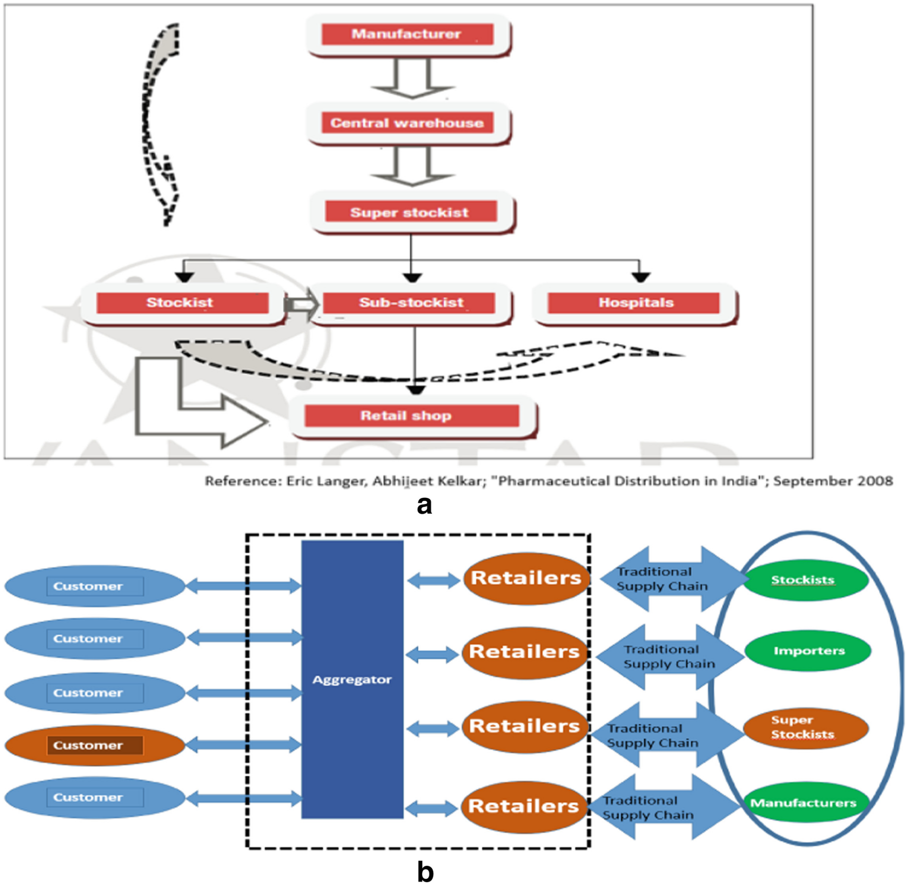


Fig. 4. a and b (Pharmacy Retail Aggregation)

Comparing the above Uber/OLA/AirBnB aggregation model where the aggregator does the matching with the aggregation in the complex supply chain scenario such as Indian Pharmacy Retail area where matching is more complex as the supplier selection and delivery mechanism is more varied and complex both in terms of variability among the level and levels themselves to cater to the customer SLAs.

We will discuss further down the complexity involved. Based on the customer demand of the prescription, we may end up with one or more suppliers who can cater to the best way to the customer need and the aggregator must work and facilitate this complexity to fulfill the customer demand on time.

The selection of the supplier(s) can be generalized as follows:

Scenario	Example
Single-Level Single Source	One single Retailer has all items as needed on the prescription
Single-Level Multi-Source	Two Retailers selected to fulfill the order
Explicitly Single-Level Single Source but Implicitly Multi-Level Single-Source	One Retailer promises to source and deliver all the items as needed on the prescription as required by the customer SLA from the Stockist
Explicitly Single-Level Single Source but Implicitly Multi-Level Multi-Source	The Retailer promises to source and deliver all the items as needed on the prescription as required by the customer SLA. He can again source from more than one of the stockist or sub-stockist or super-stockist or central warehouse
Explicitly Single-Level Multi-Source but Implicitly Multi-Level Single-Source	More than one Retailer promises to source and deliver the items as needed on the prescription as required by the customer SLA. They can again *single source* only from the stockist or sub-stockist or super-stockist or central warehouse
Explicitly Single-Level Multi-Source but Implicitly Multi-Level Multi-Source	The first level Retailers promise to source and deliver all the items as needed on the prescription as required by the customer SLA. They again source from *more than one* of stockist or sub-stockist or super-stockist or central warehouse

Based on the SLAs and expectation of the customer one of the above scenarios will be selected. The delivery mechanism also needs to be handled appropriately from the supplier side to manage the customer expectation. There can be multiple rules that may need to be applied based on the various factors underlying based on the customer SLA. For example, a diabetic patient may plan and his SLA may be 2-week delivery time to be cost effective whereas a patient with the need for antibiotics may want it delivered in 4 h at reasonable pricing. From the above, assuming we treat all the players at the same level, we end up with multiple scenarios some of which are listed below, and operational flows will differ for each combination.

A few of the scenarios are listed as below:

Sourcing Complexities in Pharma Retail (Subset)

	Retailer	Sub-Stockist	Importer	Stockist	Manufacturer
Customer-1	Single				
Customer-2	Multiple				
Customer-3	Single				
Customer-4	Single	Single			
Customer-5	Single	Multiple			
Customer-6	Multiple	Single			
Customer-7	Multiple	Multiple			
Customer-8	Single	Single	Single		
Customer-9	Single			Single	
Customer-10	Single				Single
Customer-11	Multiple	Single	Single		
Customer-12	Multiple			Single	
Customer-13	Single			Multiple	

Aggregation in complex supply chain can try to solve (Indian Pharma Retail) as below:

- A single visit does not guarantee all medications will be filled. Aggregator can
  - Provide a single point of service to provide all medications
  - Look at multiple options to fill the complete list of prescriptions
  - Inform and swap legally equivalent medicines
  - Use technology to cross check contra-indications in Rx
  - Quality not guaranteed by disaggregated pharmacy sector whereas the Aggregator can provide quality guarantee for medications (securing the product transfer in the supply chain using block chain technology)
- Price is not consistent across geographies. The aggregator can provide a standard pricing for the product across geographies with GST becoming a reality
- Contracts and Revenue management can be streamlined for better SLAs

4 Leveraging Block Chain in Aggregation

As aptly put by IBM [5] "Block chain can help reach business goals around traceability, compliance, freshness and more by enabling a holistic ecosystem. A block chain solution is not just about technology, it's about solving business problems that have been insolvable before due to the inability of the ecosystem to share information in a transparent, immutable, and trusted manner. Unlike other systems of record, block chain technology provides a trusted record of data."

In the above scenarios, block chains can be leveraged to fulfill various functions and capabilities at different points in the supply chain. One such use case is described in the following.

Providing Traceability to Minimize the Problem of Counterfeit and Substandard Drugs:
Counterfeit and Sub-Standard drugs are a major problem an according to ASSOCHAM [6] they constitute about 25% of products sold. This is a huge safety issue and needs to be tackled. The e-pharmacies are trying to provide quality products [7] by adopting various strategies.

On the other hand, block chain has proven to be a very effective tool in providing traceability in supply chains thus proving the authenticity of each item as it moves through the supply chain. This will help in quickly identifying counterfeit products and trace them to their point of origin in the supply chain and help eliminate the problem.

Examples of use of block chain put to such use are where IBM has partnered with Walmart [8] to use block chain in the food supply eco system and as a result for mangoes in the US, the time needed to trace their provenance went from 7 days to… 2.2 s. Also, another example is with IBM and Maersk [9] have also collaborated to develop using block chain technology a global tamper proof system for digitizing global trade workflow and tracking shipments and millions of containers end to end.

Considering the Aggregation model for the Indian pharmaceutical supply chain, we have multiple players on the supply side viz. Aggregator, Manufacturers' Central Warehouses, Super Stockists, Stockists, Sub-Stockists, Retail Pharmacy stores.

On the demand side we have either the Hospitals/Clinics or the end customers (Patients) themselves. The government agencies act as regulators for the Drugs manufacturers and distributors.

As with any optimal supply chain, the information flow and the goods flow are both critical. The goods move across these players from one player to the other and a block chain of information can be built with all validations in place and this public ledger can be leveraged to make block chain entries which cannot be altered. Further, depending on the type of block chain, all participants should be able to verify the entries into the block chain and trace any transaction to its point of origin.

As an example, we shall illustrate how block chain can be used by an aggregator to handle traceability of the product (Fig. 5).

As the product moves from each player of the supply chain, the details of the medicines and devices are logged in the block chain and can be verified by all participants in a transparent manner. This can be a private permissioned block chain where only certain players can make updates to the block chain data while all can view it.

The use of Smart Contracts can also be leveraged based on the business needs and at various parts of the business, like payment agreements, SLAs, margin percentages etc.

Each block is added into the chain (could also be validated based on rules) by the various authorized players in the network. The information elements in each block can contain simple to complex attributes of the product like Manufacturer name, Manufacturing Facility, Drug name, Potency, Manufacture Date, Batch number, Drug Expiration Date, Date shipped, Date received etc.

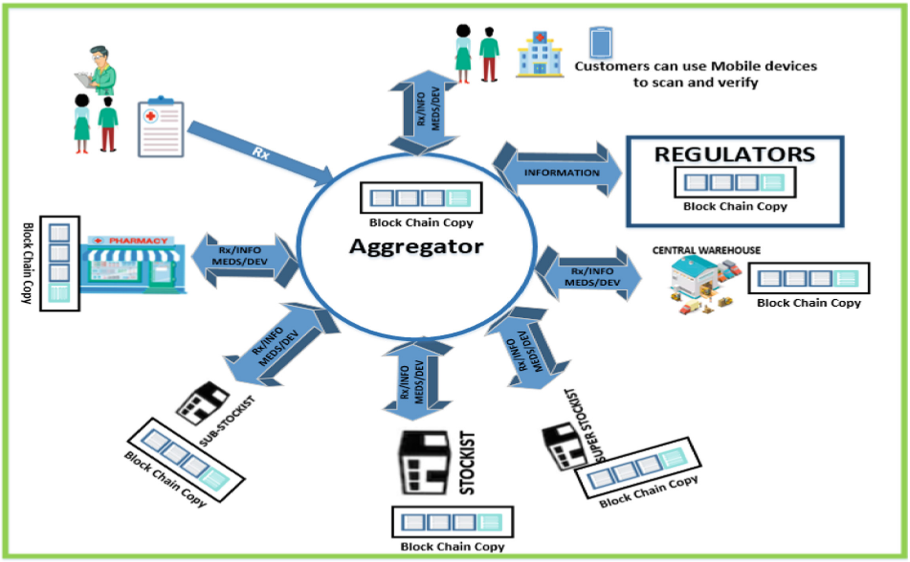


Fig. 5. Block chain use by an aggregator

Anyone with a key identifier (code) of the SKU for the product would scan the code with a smartphone App and this code along with the sellers' ID would validate if the product were genuine.

Once this code is verified by the end user after purchase at the Retailer, its life cycle is complete, and no other entries can be made into the block chain.

By tying the end user validation to the original manufacturer, we can make sure that the product is genuine.

Any unverified transaction is logged back into the block chain with details of the vendor which can further be analyzed to improve the supply chain. This information can also be used as a metric to track the vendor if any frivolous medicines or devices are sold by them.

The expiration dates can be used to see where the product movement is slow, and the business can address the issue at the right level.

Other benefits of the Block Chain while applied with the aggregator model are Track and Trace to analyze and help minimize counterfeits and spurious drugs, Legal Compliance, Use the ship and receipt details to finalize the payment mechanisms, Any product recall can also be controlled at the manufactures side where any new block chain transaction would automatically flag the product as recall and not be sold to the next level in the supply chain, The aggregator can use the data on the vendors to rate them, and Better product quality can be delivered.

5 Conclusion

This study is an attempt to bring together two of the most current phenomena in E-commerce namely aggregation and block chain, each of which is bringing significant benefits to consumers/users, intermediaries, and providers/suppliers. Aggregation as a business model has proven to be successful in bringing the benefits of organized business to unorganized and disaggregated business domains. However, till date the model has not been applied in domains where the supply chain on the provider/supplier side is complex. This study is an attempt to address the issue by leveraging the strengths and capabilities of block chain technology to bring the benefits of aggregation to such business domains. The Indian pharmaceutical retail industry is used as test case to explore the possibility of this application.

References

1. Pahwa, A.: Aggregator Business Model. What Is It And How Does It Operate? (3 September 2016). Retrieved from https://www.feedough.com/aggregator-business-model/
2. Kohlborn, T., Korthaus, A., Riedl, C., Krcmar, H.: Service aggregators in business networks. In: 2009 13th Enterprise Distributed Object Computing Conference Workshops (2009). https://doi.org/10.1109/edocw.2009.5331992
3. Srinivasan, R.: Organising the unorganised: role of platform intermediaries in the indian real estate market. IIMB Management Review **29**(1), 4 (2017). https://doi.org/10.1016/j.iimb.2017.03.007
4. Thompson, B.: Aggregation Theory (21 July 2015). Retrieved from https://stratechery.com/2015/aggregation-theory/
5. https://www.ibm.com/in-en/blockchain/solutions/food-trust
6. https://www.downtoearth.org.in/news/fake-drugs-constitute-25-of-domestic-medicines-market-in-india-assocham-45393
7. https://timesofindia.indiatimes.com/spotlight/how-are-e-pharmacies-beating-the-fake-drugs-issue-in-india/articleshow/65936562.cms
8. https://www.hyperledger.org/learn/publications/walmart-case-study
9. https://www.youtube.com/watch?v=tdhpYQCWnCw
10. https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture
11. Shahid, A., Almogren, A.S., Javaid, N., Al-Zahrani, F.A., Zuair, M.A., Alam, M.: Blockchain-based agri-food supply chain: a complete solution. IEEE Access **8**, 69230–69243 (2020). https://doi.org/10.1109/ACCESS.2020.2986257
12. Juma, H., Shaalan, K., Kamel, I.: A Survey on using blockchain in trade supply chain solutions. IEEE Access **7**, 184115–184132 (2019). https://doi.org/10.1109/ACCESS.2019.2960542
13. Haya, R., Khaled, S.: Blockchain-based Proof of Delivery of Physical Assets with Single and Multiple Transporters
14. Gaur, V., Gaiha, A.: Building a Transparent Supply Chain. https://hbr.org/2020/05/building-a-transparent-supply-chain
15. Namasudra, S., et al.: The revolution of blockchain: state-of-the-art and research challenges. Arch Computat Methods Eng (2020). https://doi.org/10.1007/s11831-020-09426-0

ATM Security System Using Gesture and Hand Vein Recognition

Yashika Kuckian(✉), Neha Bharambe, Adishree Sane, and Easther Masih

Information Technology, Fr. C. Rodrigues Institute of Technology, Navi Mumbai, Maharashtra, India
yashika.kuckian@gmail.com

Abstract. An ATM is a 24/7 banking outlet through which users can avail prompt services like cash withdrawal, cash transfer, balance enquiry, pin change, mini statement, etc. Due to the risk of theft in ATMs, it is important to deploy high security measures while carrying out transactions. This paper presents a more secure method to carry out ATM transactions using hand gesture recognition and hand vein verification. In order to avoid pin hacking using techniques like shoulder surfing, pin verification using hand gesture recognition model is implemented. The 4-digit security pin will be entered by posing hand gestures inside a chamber. This method also focuses on easing the use of ATMs for blind people. The voice based instruction module helps the blind people to carry out the transactions without any assistance from other people. The security is enhanced with the help of a hand vein recognition system which is one of the newest biometric techniques. The vein patterns under the skin are difficult to replicate thereby making it very secure. The hand vein images captured using NoIR camera are preprocessed followed by extraction of features for vein recognition. Since the model is deployed on raspberry pi, it provides a cost effective approach as compared to sensor technology. The results of the proposed model of hand gesture recognition showed an accuracy of around 98% for both the train and test dataset.

Keywords: Hand vein · ATM security · Gesture · NoIR · Blind · Raspberry pi

1 Introduction

ATMs enable the users to carry out transactions easily and are available to us 24/7. But ATMs are also becoming targets for criminals due to the large amounts of cash stored in the machines. It is also possible to find out the four-digit verification pin using thermal cameras, shoulder surfing and many other techniques. In the battle of functionality versus security, the functionality wins more often. But in the case of banking transactions, security should possess the highest priority. The developers should consider security as their primary aspect in order to reduce these increasing threats of robbery in ATMs. There is a need for introducing a multifactor authentication approach in ATM systems. The knowledge factor ("something only the user knows") [1] is provided by the 4-digit ATM pin. But it is important to add the possession factor ("something only the user has")

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 330–341, 2023.
https://doi.org/10.1007/978-3-031-13150-9_28

in this authentication process in order to provide more security to the transactions. This possession factor should be as unique as possible, something which cannot be replicated.

In this paper, the concept of hand gesture recognition for 4-digit pin verification is implemented in order to secure the knowledge factor of the authentication process. In this, the person has to enter the four-digit pin using hand gestures which will be posed in front of the camera fitted inside a closed camber. The hand gesture recognition system will prove to be useful in reducing shoulder surfing and other techniques used for pin hacking. Using fingerprints as a possession factor can prove to be less secure, because it is easy to replicate fingerprints. Therefore, the possession factor in the proposed system is provided by a hand vein verification system which is a powerful biometric technique which uses infrared lights to capture data points on the palm. The entire model is deployed on raspberry pi since the NoIR camera module in raspberry pi helps to capture the infrared light which is reflected from the hand veins. Since hand veins exist beneath the skin and are unique for each person, they are hard to be stolen and hence prove to be more secure as compared to other biometrics [2]. Along with the security factor, it is important to focus on easy access to ATMs for blind people. The system provides a voice based instruction module that helps the blind people to carry out the transactions without any assistance from other people.

2 Literature Review

ATMs are convenient systems, allowing consumers to carry out quick transactions such as cash withdrawals, deposits, bill payments, and cash transfers between accounts. There are many systems that are implemented in order to enhance the security of the ATM. The systems provide security based on biometrics and other techniques.

In the ATM Security using Fingerprint Authentication and OTP system, the fingerprint of the user is registered in the bank database when the user opens his/her account in the bank. Further, when the user carries out any transaction, first the authentication is done by matching the input fingerprint with the registered fingerprint in the bank database. Once the fingerprint is matched, an One-Time-Password (OTP) is sent to the user. Thus, the system proposes to use unique pincode (OTP) every time a transaction is carried out from a particular account. Thus, for every transaction, a new OTP will be sent to the account holder's mobile number, thus there will not be a fixed PIN number for every transaction [3] thereby contributing to the enhanced security of the ATM.

While the idea of sending a unique pincode for each transaction does eliminate the threat of pin hacking, it still has a disadvantage. The technology used in this system is based on the user's fingerprints. Fingerprints are unique to a person but they can be easily duplicated using materials like gelatine and silicon thereby deceiving the commonly used sensors [4]. It has been recorded that a better biometric system can be used to increase the security of the ATM. Rather than using fingerprint authentication, palm vein recognition system is more suitable for ATM. Hand veins are complex and unique to a person. Hand is an ideal part of the body with very less hair which can pose as an obstacle for photographing blood vessels [5]. Being situated inside the human body, vein information is impossible to steal, thereby making it a highly secure and reliable factor for authentication. There are few ideas published supporting the same concept.

The design details of the palm vein capture device are researched, and preprocessing and feature extraction of palm vein image are also investigated [5] in this system. In this, first the device setup is used to capture user's hand veins by subjecting it to infrared radiations at a specific wavelength [5]. Hemoglobin is oxygenated in the lungs and the deoxidized hemoglobin is sent to the heart via veins. Since the deoxidized hemoglobin absorbs only a specific wavelength i.e. 760 nm of light in near infrared region [5], the system is able to recognize the veins but not the arteries [5]. Another similar system is proposed for palm vein image enhancement. In this algorithm is proposed to enhance a low quality vein image and reduce noise thereby detecting a clean palm vein pattern [6]. The process first consists of image normalization technique [6] used to obtain the standard image of veins which is later passed through Gaussian filter to reduce noise. Further segmentation process is carried out and later thinning technique is used to get single line vein pattern [6].

Furthering the same logic used in previous system, another system maintains a small palm vein image database and the experimental results on this database shows that the system performs well on the same. In this existing system, palm vein authentication is implemented on raspberry pi. Comparison of the registered palm vein and input palm vein is completed in a few seconds [7]. The predictions are done using libraries like tensorflow and OpenCV. Thus, there are many existing papers supporting the use of palm vein information for authentication in ATM systems.

While security is the prime focus in the ATMs, contactless biometric authentication [8] is the necessity of today's world. It is important to ensure proper hygiene as well as high security features. This can be achieved by introducing contactless hand gesture and vein recognition systems in the security process of ATMs. Modern day biometric authentication systems use convolutional neural networks which is a type of deep multilayer ANN widely used in all computer vision task [8]. CNN helps in obtaining better representation of input images with minimum preprocessing to easily identify visual patterns [9]. The system proposed in 'Static Hand Gesture Recognition Based on CNN', the proposed architectures compared CNN models with 1, 2 and 3 layers of hand gestures and obtained the accuracy of 94.7% for 1 layer CNN and 96% for the other models. Thus, the CNN models attained high success rates at relatively low computational costs [10]. Earlier the hand posture recognition methods focused mainly on RGB image datasets [11] which had several limitations. But most of the CNN-based approaches represent 2D depth images as 3D data for hand pose classification. 3D CNN-based may waste convolutional process calculation and shift the numeral networks from learning the effective features [11]. Thus, it is important to improve the hand gesture recognition systems.

In addition to security, it is also required to consider the ease of access of the ATMs. There are many cases wherein it is observed that blind people need assistance to carry out ATM transactions. They need some other person to enter their 4-digit pin for completing the transaction. This might be dangerous if the assisting person is not reliable. In order to eliminate this threat, a new concept of entering the required inputs for the ATM using hand gestures rather than using a number pad is introduced. One such system is developed which describes an approach of giving ATM inputs using British Sign Language. A high speed algorithm for gesture recognition [12] was developed in MATLAB 2011b and then deployed in Java language. Blind users can remember the instructions and commands for a particular ATM machine, but it is difficult for them to operate the different types of ATM machines on their own and hence they have to depend on a person who knows how to operate the machine for their banking [13]. Therefore, another system providing audible instructions for the person who cannot read the ATM screen was proposed. In this, the sensor output is analog values, converted to digital and processed by microcontroller, then it is given to the voice chip to produce voice using speaker [14].

Thus, by referring to all the above mentioned work, the system proposes to integrate both a hand vein authentication system for enhancing the security and hand gesture based pin verification system along with audio instructions for providing ease of access of ATMs for blind people.

3 System Implementation

ATM security system is implemented using the Django framework. HTML, CSS, JavaScript and Ajax are used for making frontend attractive and dynamic. In the hardware part, Raspberry Pi Model 3B for computing, Raspberry pi camera noir V2, 850 mm IR LED light and a USB Webcam is used. All the user information related to the bank account is stored in the PostgreSQL database. The proposed system has two modules namely hand gesture recognition module and the hand vein recognition module as depicted in Fig. 1.

The modules are explained in the further part of the paper.

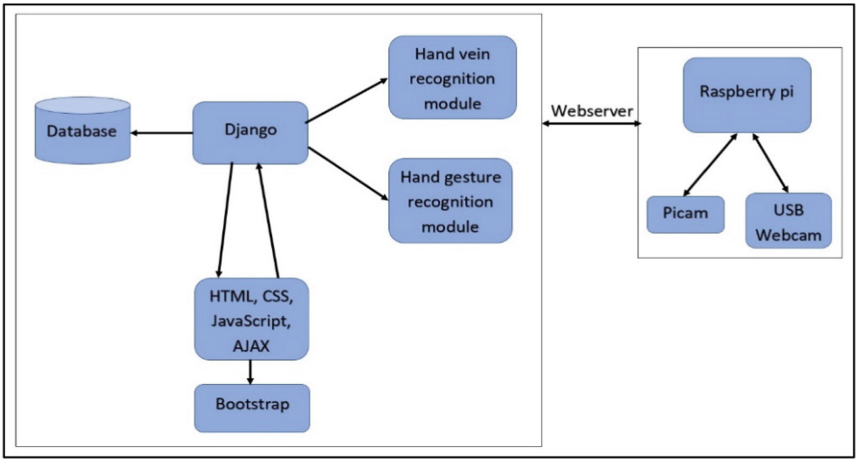


Fig. 1. Architectural block diagram

The user of this system first visits the homepage where he/she is required to enter the card number in order to retrieve the details from the database. After implementation of each step, the python gTTS (Google Text-to-Speech) module is used to give automated voice instructions to the user about the next step to be implemented. If the card number is valid it continues to the pin verification page or else it redirects to the home page with an error message. After this the user has to enter the pin using gestures. The gestures captured through the USB webcam are recognized with the help of the gesture dictionary. The pin is extracted and then compared with the one present in the database. If the correct pin is entered, it goes to the palm verification page or else redirects to the same page. After this the user has to place his/her palm over the box for the final biometric verification and that is captured through the picam. Once this is done, the entire authentication process for the transaction will be completed. The above mentioned working of the system is shown in Fig. 2.

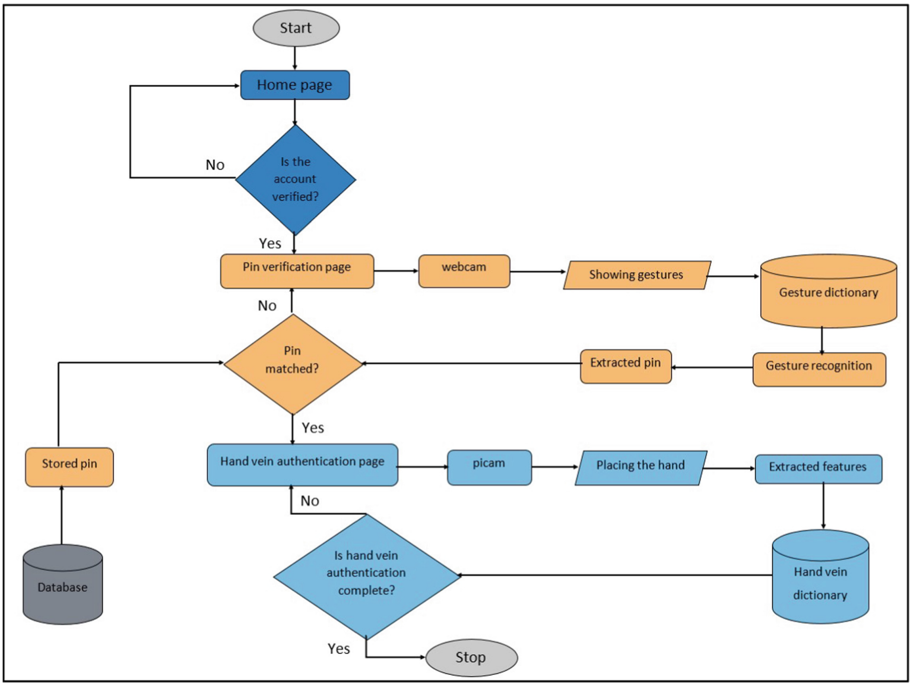


Fig. 2. Working of the system

4 Methods and Results

The ATM security system has two tracks, the first one is the hand gesture recognition model and the second one is the hand vein recognition model. The hand gesture recognition model is required to enter the 4-digit pin using gestures. The hand vein recognition model acts as a biometric authentication factor enhancing the system's overall security.

For the hand gesture recognition model a custom dataset was created. It consists of images converted into grayscale and then processed using thresholding as shown in Fig. 3. At first OpenCV function cv2.cvtColor (img, BGR2GRAY) function will be applied in order to convert the continuous frames in the form of images into grey colour.

After converting the image into grayscale image, thresholding has to be applied on to the image. In this process the pixels will be assigned the value in relation to the threshold provided. The suitable threshold for this situation will be 120. All pixel values less than 120 will be set to 0 and greater than 120 will be set to 255. The thresholding function used is Simple thresholding binary i.e. THRESH_BINARY. The size of the image used is 64 × 64.

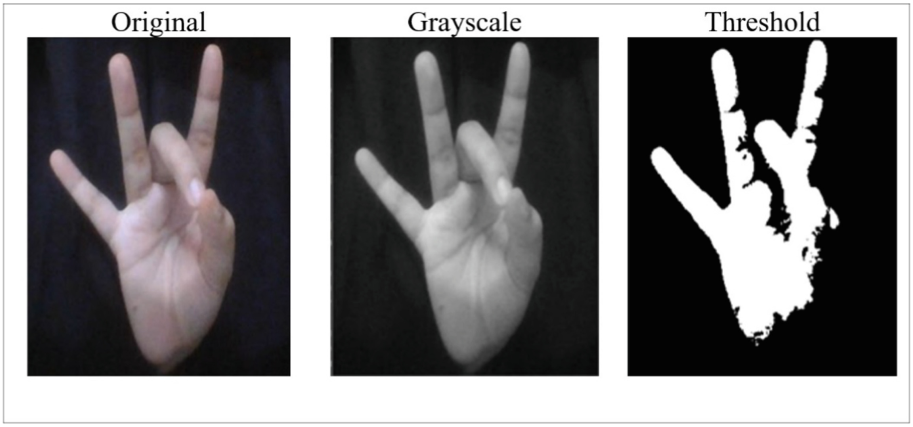


Fig. 3. Filters for hand gesture recognition

The dataset consists of 1000 images in the training set and 300 images in the test set. 100 images were used for each gesture in the training set and 30 images in the test set. The subjects whose hands were used for data collection consisted of 4 women and 3 men. The gestures used for the digits 0–9 are as shown in Fig. 4.

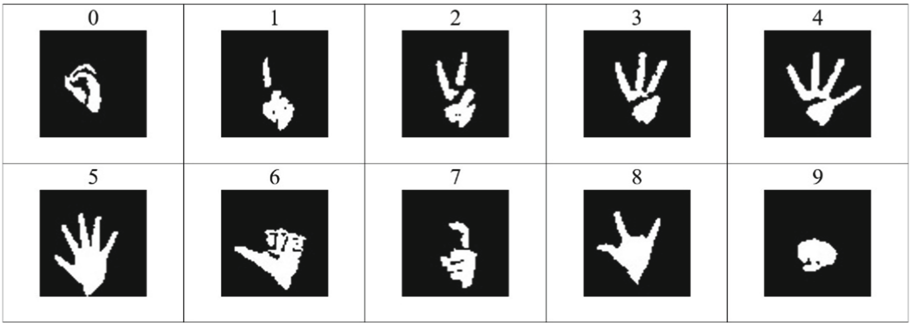


Fig. 4. Hand gestures for digits from 0 to 9.

The model was trained using simple CNN classification. The model is 2 layered and was trained using Keras API and tensorflow backend. The input to the CNN architecture consisted of 64 × 64 sized hand gesture processed images. The network architecture consists of two convolutional layers, two dense layers and a softmax classification layer. Each layer has 32 filters with Rectified Linear Unit (ReLU) activations. The output shape is (None,10) i.e. it outputs 10 samples for each batch. The model has a total of 813,802 weights, all trainable. The summary of the hand gesture recognition model is as shown in Fig. 5.

```
Model: "sequential_2"
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
conv2d_4 (Conv2D)            (None, 62, 62, 32)        320
_________________________________________________________________
max_pooling2d_4 (MaxPooling2 (None, 31, 31, 32)        0
_________________________________________________________________
conv2d_5 (Conv2D)            (None, 29, 29, 32)        9248
_________________________________________________________________
max_pooling2d_5 (MaxPooling2 (None, 14, 14, 32)        0
_________________________________________________________________
flatten_2 (Flatten)          (None, 6272)              0
_________________________________________________________________
dense_4 (Dense)              (None, 128)               802944
_________________________________________________________________
dense_5 (Dense)              (None, 10)                1290
=================================================================
Total params: 813,802
Trainable params: 813,802
Non-trainable params: 0
_________________________________________________________________
```

Fig. 5. Model summary

The results of the gesture recognition model are as shown in Fig. 6. The process of gesture recognition has been speeded up with the help of image processing. The filters used in Fig. 3 are used to speed up the process as it removes most of the unnecessary details such as colour and noise. It also helps in detecting the hand gesture faster as a white object against a black background is used in the system as shown in the final result of Fig. 3. Fixing an ROI also speeded up the process.

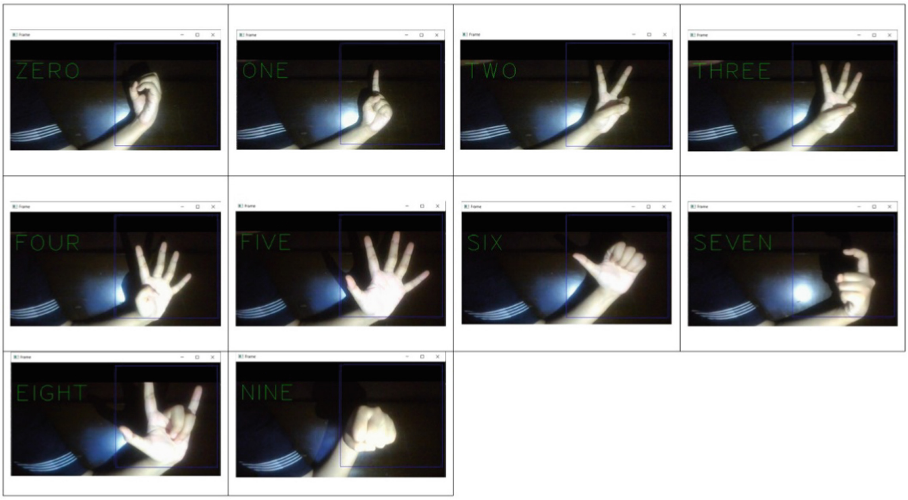


Fig. 6. Predictions of hand gestures

The model is evaluated on the basis of the metrics- accuracy and loss. The accuracy metric is as shown in Fig. 7. According to the graph it has been observed that the training accuracy increases and then at the end of the 4th epoch the accuracy is 100% which remains constant between 0.99 to 1.00 towards the 10th epoch.

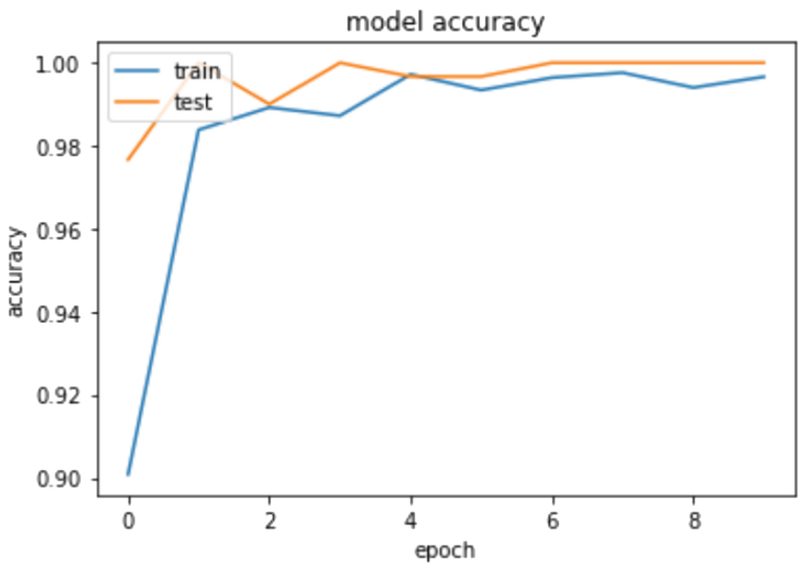


Fig. 7. Model accuracy

The model train and test loss becomes 0% towards the end after the 6th epoch. The loss during the training process of the model is as shown in Fig. 8.

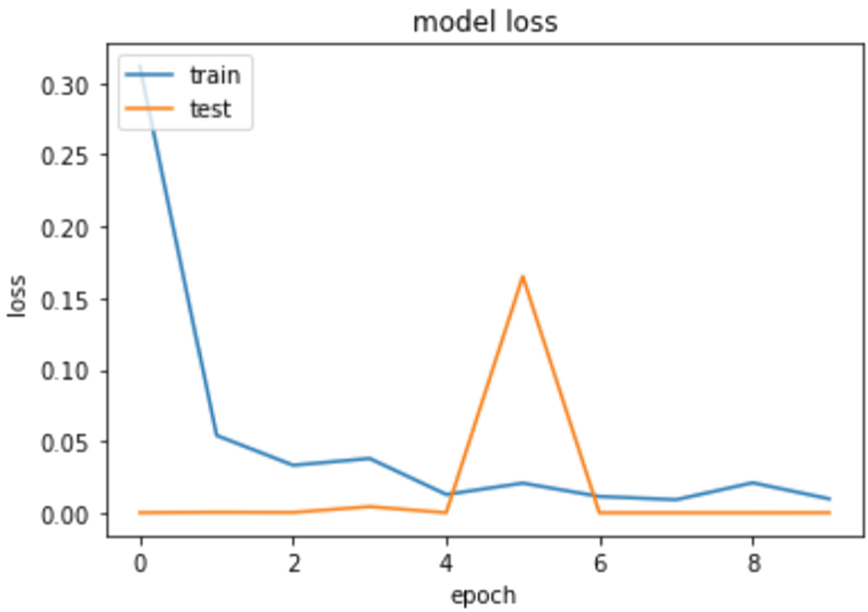


Fig. 8. Model loss

The hand vein authentication part of the project is used to authenticate the person on the basis of the pattern of the hand vein patterns. The gesture identification generally includes three parts: Capturing the IR image, applying Image Processing to it and then classification. Figure 9 shows the setup consists of raspberry pi model 3B which is used for computing. It also consists of Raspberry Pi camera noir V2 which is capable of filtering the IR light. 850 mm IR light of 3W is used. The IR light is connected to the GPIO pins and the camera module is connected to the camera slot on the raspberry pi.

The reason behind using 850 mm is because it is in the near infrared region. The haemoglobin in blood consists of oxygen when it is transported from lungs to the tissues in the body by arteries. By the time the blood flows back to heart via different arteries this oxygen releases. Vein pattern recognition uses this difference between deoxygenated and oxygenated haemoglobin. Deoxidized haemoglobin absorbs infrared light, making the vein pattern visible if a scanner is used to illuminate it with infrared light. There is a need to make use of opencv filters in order to make the veins captured more visible. The filters used are as shown in Fig. 10.

1. BGR2GRAY is used to convert the rgb format of the image into grayscale to remove all the unnecessary details such as skin colour.
2. The equalising Histogram filter is used to create a contrast between the darker and lighter pixels.

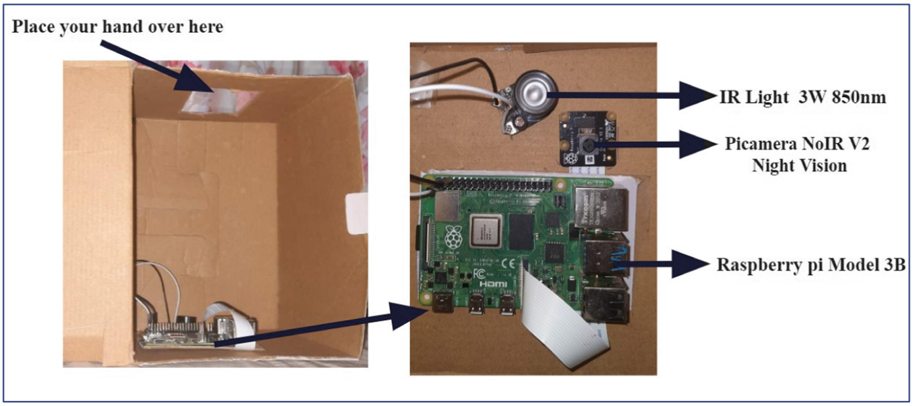


Fig. 9. Raspberry pi setup

3. Contrast Limited Adaptive Histogram Equalisation (CLAHE) is used to take care of over amplification of the contrast.
4. Gaussian Blur is used to smoothen the image that removes all the unwanted information. These filters help to reduce the complexity and the weight of the model. After that a model was trained on similar lines as the gesture model using 30 images for left hand and 30 images for right hand as shown in Fig. 11.

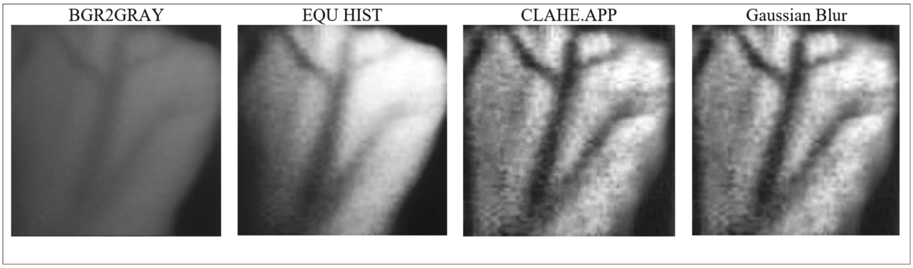


Fig. 10. Filters for hand vein recognition

There is a need to make use of opencv filters in order to make the veins captured more visible. The filters used are as shown in Fig. 10.

- Image input: After inputting the image, the image was displayed in the form of a matrix m $\times$ n according to the size of the image
- RGB Image to Grayscale Conversion: After the matrix reading process, the image produced a digital image matrix with pixel value 0–255 in 3-dimensional colors i.e. Red, Green, and Blue (RGB). So to simplify the following process, it is necessary to process the conversion of RGB digital image into Grayscale [15].
- Histogram Equalization: It is a histogram leveling process, in which the distribution of gray degree values of an image is made evenly.

- Filtering Process: This process is used for noise reduction obtained from the processing of histogram equalization [15]. Gaussian filtering is used.

The classification of the veins is the next step. The vein model is an image classification model. The dataset was made using the same image processing techniques used in capturing the video feed.

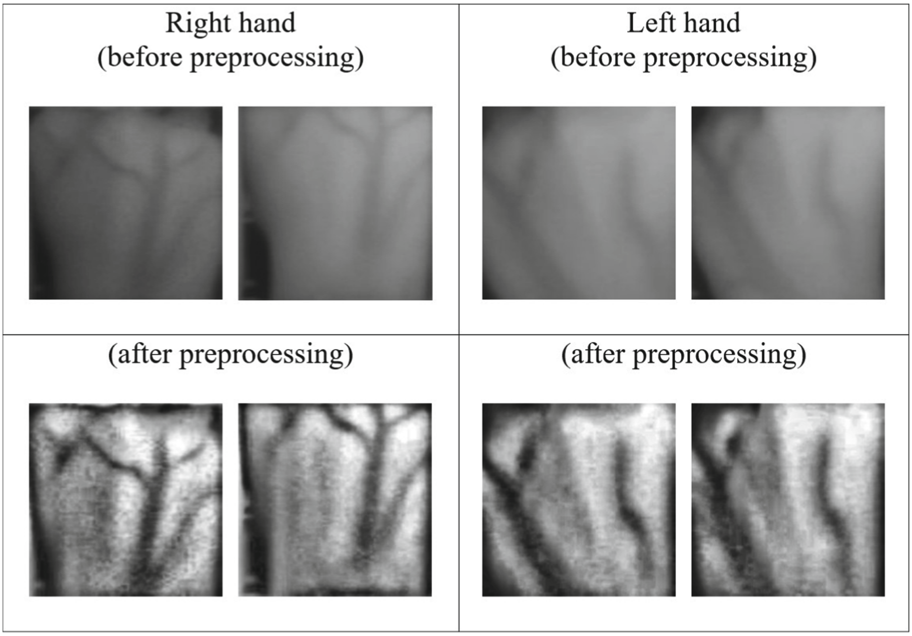


Fig. 11. Training set

Image quality can be improved using the combination of histogram equalization and guassian filtering [15]. After preprocessing images, the model is trained on similar lines as the gesture model using 30 images of left hand and 30 images of right hand as shown in Fig. 11.

5 Conclusion

Thus, the ATM security system using hand gesture and hand vein recognition is more secure as compared to other methods such as OTP based security and fingerprint or face recognition based biometric authentication. It can prevent malpractices such as shoulder surfing techniques to hack the pin or hacking of OTPS and also duplication of fingerprints. Hand vein recognition also has higher accuracy than other biometric authentication methods. The system costs less than $80. Making use of sensors can cost up to $400 which makes the proposed model affordable as well. The proposed model's accuracy can be increased by including more number of subjects for hand gesture dataset collection. Also, making use of palm veins instead of hand veins can increase the accuracy of the model even more. In the present scenario, ATM has become one of the most important and useful facilities in our day to day life. The progress in science and technology has grown up worldwide thereby providing a better future to mankind.

References

1. Rane, P.S., Sawat, P.P., Shinde, S.B., Dawande, N.A.: ATM security. Int J. Adv. Eng. Res. Dev. **5**(06), 159 (2018)
2. Aoki, T., Shinzaki, T.: Palm vein. In: Li, S.Z., Jain, A.K. (eds.) Encyclopedia of Biometrics. Springer, Boston (2015). https://doi.org/10.1007/978-1-4899-7488-4_129
3. Aruna, R., Sudha, V., Shruthi, G., Usha, R.R., Sushma, V.: ATM security using fingerprint authentication and OTP. Int. J. Eng. Res. Electron. Commun. Eng. (IJERECE) **5**(5), 1157–1159 (2018)
4. Coli, P., Marcialis, G., Roli, F.: Fingerprint silicon replicas: static and dynamic features for vitality detection using an optical capture device. Int. J. Image Graph. **08**, 495–512 (2011). https://doi.org/10.1142/S0219467808003209
5. Zhang, H., Hu, D.: A palm vein recognition system. In: 2010 International Conference on Intelligent Computation Technology and Automation, pp. 285–288 (2010). https://doi.org/10.1109/ICICTA.2010.425
6. Yusoff, S., Ramli, A.R., Ahmad, I., Mustafa, Z.: Palm-dorsa vein image enhancement algorithm using webcam for biometric system. AIP Publishing (30 July 2019). https://aip.scitation.org/doi/pdf/10.1063/1.5118147. Accessed 5 Jan 2022
7. Ghute, M., Korde, M., Kamble, K., Khade, S., Chavan, Y.: Design of palm vein authentication system. Biosc. Biotech. Res. Commun. **13**(14), 273–276 (2020)
8. Dayal, A., Paluru, N., Cenkeramaddi, L.R., Soumya, J., Yalavarthy, P.: Design and implementation of deep learning based contactless authentication system using hand gestures. Electronics **10**, 182 (2021). https://doi.org/10.3390/electronics10020182
9. Gu, J., et al.: Recent advances inconvolutional neural networks. Pattern Recognit. **77**, 354–377 (2018). https://doi.org/10.1016/j.patcog.2017.10.013
10. Pinto, R.F., Borges, C.D.B., Almeida, A.M.A., Paula, I.C.: Static hand gesture recognition based on convolutional neural networks. J. Electr. Comput. Eng. **2019**, 1–13 (2019). Retrieved January 5, 2022
11. Noreen, I., Hamid, M., Akram, U., Malik, S., Saleem, M.: Hand pose recognition using parallel multi stream CNN. Sensors (Basel, Switzerland) **21**, 8469 (2021). Retrieved January 5, 2022
12. Rupanagudi, S., et al.: A high speed algorithm for identifying hand gestures for an ATM input system for the blind, pp. 1–6 (2015). https://doi.org/10.1109/IBSS.2015.7456642
13. Reddy, C.V., Ramani, D.M., Geetha, K., Harshitha, K., Babu, S.P.: Gesture recognition system for the blind. Pers. Commun. Embed.-Syst. Signal-Process. (PiCES) – Int. J. **5**, 73–75 (2021). ISSN:2566-932X
14. Kavitha, M.E., Soundariya, P., Vaishnu, J.M., Yamuna, M.: An embedded based ATM for blind people. Int. J. Eng. Sci. Comput. **9**(3) (2019)
15. Astawa, I.N.G.A., Saptarini, N.G.A.P.H., Asri, S.A., Sukarata, P.G., Atmaja, I.M.A.D.S.: shistogram equalization and Gaussian filtering combination method for face image optimization. In: 2018 International Conference on Applied Science and Technology (iCAST), pp. 190–193 (2018)

Effect of Entrepreneurial Education on Entrepreneurial Intention: Mediating Role of Entrepreneurs Personality Traits

Bhawna Chahar(✉)

Department of Business Administration, Manipal University Jaipur, Jaipur-Ajmer Express Highway, Dehmi Kalan, Near GVK Toll Plaza, Jaipur, Rajasthan 303007, India
drbhawnachahar@gmail.com

Abstract. India's post-liberalization phase is experiencing rapid economic activity growth. The information revolution and numerous government and social efforts have paved the way for the country's entrepreneurial education. Since the inception of state of Uttarakhand (India), it has focused on developing entrepreneurial skills and attempting to build entrepreneurial intention among the students taking entrepreneurial courses. However, the effect of entrepreneurial education in developing entrepreneurial personality traits needs to be studied and how these educational programs could create entrepreneurial intention among students. Present work explores the effect of entrepreneurial education on entrepreneurial intention and whether an entrepreneurial personality trait mediates the relationship between entrepreneurial education and entrepreneurial intention. To achieve objective of this study 217 students doing professional and non-professional courses at different institutes of Dehradun district, the state capital of Uttarakhand (India) was chosen. The result of the study indicates positive relationship between entrepreneurial education and entrepreneurial intention and confirm mediating role of entrepreneurial personality traits in building relationship between entrepreneurial education and students' entrepreneurial intention.

Keywords: Entrepreneurial traits · Entrepreneurial education · Entrepreneurial intention

1 Introduction

The world economy is passing through a transformation stage, and many changes have been witnessed in the past few decades. The economic development of any country solely depends upon the quality of the human resource. The entrepreneurial education concept is growing in terms of volume and value. Today, most educational institutions offering various programs ranging from elementary schools to graduate schools and post-graduate universities emphasize promoting entrepreneurial thinking and curiosity among youngsters. Entrepreneurial education is intended for driving entrepreneurship among the prospect and helping them to be the catalyst for high-value job creation. Variations of entrepreneurship education are delivered in school education through college and

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 342–364, 2023.
https://doi.org/10.1007/978-3-031-13150-9_29

university graduate programs that have recognized the importance of entrepreneurship education and attempted to encourage students' progress by a system of entrepreneurship education. Nearly all institutes of business and technology, regardless of their specialty, have a crucial role in imparting entrepreneurial education, preparing students, and preparing them in an uncertain future world. The primary role of training in entrepreneurship is applying for a job and creating new jobs.

Imparting entrepreneurship education and creating its importance among the student is the crucial task of the present education system. Several studies revealed business and entrepreneurship training (Wang and Verzat 2011). Entrepreneurship training aims to provide awareness, expertise, and inspiration for students in various settings to promote entrepreneurial success. A learning scheme designed to grow individuals for self-employment or organize, finance, and manage a company. Entrepreneurial education strives to create and equip students with the skills needed to develop entrepreneurial traits. Mycos' research group released the "China Jobs Survey" and found entrepreneurship ratio of university graduates in 2007 and 2008 was only about 1%, the entrepreneurship ratio of university graduates in 2011 was 1.6%, and the entrepreneurship ratio of university graduates in 2017 was 3%. Because of the policies of the central governmentlike "Make in India" and "Startup India," among others, the perception of entrepreneurship is on the rise in India, said a study on Tuesday. The latest report on India for the financial year 2016–17 by the Global Entrepreneurship Monitor (GEM) showed an increase in the entrepreneurial intention rate to 14.9% compared to 9% in 2015–16. At the same time, fear of failure dropped from 44% in 2015–16 to 37.5% in 2016–17. According to the survey, a correlation between India and its BRICS peers (Brazil, Russia, India, China, and South Africa) suggests that regarded potential is the most noteworthy, followed by perceived ability. Several studies have shown that entrepreneurial intent can be improved by bringing about a qualitative shift in entrepreneurial education accompanied by entrepreneurial characteristics.

2 Motivation Behind the Study

Several studies have discovered that university students' attitudes toward entrepreneurial entrepreneurship intention differ significantly depending on their unique societal ambiance; personal factors comprise self-efficacy, family background, the effect of role models, and the institutional environment of research base projects and their conversion, entrepreneurial education, faculty influence, and so on (Heuer and Kolvereid 2014, Dr. Nanu Lunavath (2015). Certain studies have found the elements that influence entrepreneurial education and entrepreneurial intent. For example, Fiet (2014) identified three factors that influence entrepreneurial intention: contextual factors such as national policy, social environment, and culture. Individual factors include personality, family environment, family and friend support, and entrepreneurial education such as teaching method, course setting, etc. Many studies have found that personal factors such as gender (Haus et al. 2013) and entrepreneurial family background (Zellweger et al. 2011), as well as cognitive aspects (Solesvik et al. 2013), play a role. Individuals with high psychological well-being are more likely to have a robust entrepreneurial intention and establish a business, according to Zhang et al. (2014). Dr. P. Sankar (2018), in his study on Entrepreneur Intention among Medical Students in Chennai City, indicated the proper curriculum design for medical students to bring positive change in the attitudes and behavior of students so that they perceive employment creation as a necessary component of their development. More emphasis must be on institutes' soft skills development training programs to improve students' entrepreneurial traits such as risk-taking, confidence, perseverance, flexibility, and so on, which are believed to be entrepreneurs' essential elements. Corresponding contradicting findings were discovered in emerging economies. According to studies of final-year business students in India, Malaysia, and Singapore, the institutional environment has a strong impact on final-year business students in India, Malaysia, and Singapore (Trivedi 2016). Similarly, academic institution-provided concept formulation support has been demonstrated to boost students' Entrepreneurial Intention (Mustafa et al. 2016). The study discovered that the university entrepreneurial environment had no significant influence when looking at the EIs of business, medical, and law students (Sesen 2013). Academic success has been demonstrated to negatively influence a student's desire to own and run a business in Malaysia (Mohamad et al. 2015). Given the emphasis on business subjects, it will be fascinating to examine if these courses increase entrepreneurial intent in developing nations where research is scarce. However, there has been significantly less research into the role of personality traits in the relationship between entrepreneurial education and entrepreneurial intent. As a result, the purpose of the study was to investigate the role of student personality traits in mediating the relationship between entrepreneurial education and entrepreneurial intention.

3 Entrepreneurial Education and Entrepreneurial Intention

Entrepreneurial Education (EE) includes creating individually and collectively applicable habits, skills, and attributes helping people and businesses build, cope, and appreciate creativity and change (Seikkula-Leino 2008). Raposo and Paco (2011) found that entrepreneurship training prepares students to be responsible and develop entrepreneurial skills and attitudes. Similarly, UNESCO (2008) described entrepreneurial education as all types of experience giving students the opportunity and dream of different kinds of opportunities to reach and turn. EE is an accessible and economical way to increase the quality and number of graduate business students entering the economy (Matlay 2006). According to Salem (2014) and Gibb (2012), Entrepreneurial universities provide communities, traditions, practices, and opportunities to develop and support student and graduate entrepreneurship while establishing synergies between current institutional operations.

In particular, entrepreneurship courses customized to the corresponding education level and entrepreneurial skills are created. This is a concept that all countries involved in entrepreneurial training have taken on board (Sánchez-García and Hernández-Sánchez 2015). Entrepreneurial education is usually conceived as a broad education that seeks to nurture self–confidence by drawing the person's ability and creativeness while developing the skills and ethics helping students expand their outlooks on education and opportunities beyond education.

Entrepreneurship training is a tool for creating jobs and economic development in any community that includes rebranding the environment of training (Lee and Wong 2008).

Entrepreneurial training focuses on providing students with requisite skills and capabilities in the working world. Obinna (2014) defines entrepreneurship training as the mechanism by which individuals develop a wide range of skills that brings an individual more significant socio-economic benefits. Enu (2012) states that entrepreneurial education's goal is providing students with the information, attitude, and skills for entrepreneurship. According to Brush (2014) and Kuratko (2005), Entrepreneurship training consists of courses, extracurricular activities, and research efforts. Entrepreneurship training includes learning goals, subject coverage, and content choice. Entrepreneurs are active in productive activities in established and emerging economies worldwide, guided by relevant education. Therefore, solid and successful entrepreneurship training will impact the broader society showing a reduction in unemployment rates and thus will lead to innovation and creativity. Entrepreneurship training is a powerful instrument in combating poverty where policies are adequately and efficiently applied. For example, researchers such as Álvaro et al. 2008 and, Iyiola examined entrepreneurship training and Azuh 2014 to help create new businesses, resuscitate struggling businesses, foster innovation, competency, and boost the living standard of the public.

Investing highly in providing education on entrepreneurship cannot increase the entrepreneurial performance of students in a minor frame; This reduces the time lag between entrepreneurship training and actual business, implying that students have a 10- year gap between adopting entrepreneurial education and starting a business (Shen et al. 2010). Academicians prefer to measure the effectiveness of entrepreneurship education by entrepreneurial desires due to the time delay in entrepreneurship education; the focus of entrepreneurial education has switched from "establishing enterprises" to "entrepreneurial attitudes" (Mwasalwiba 2010). According to Hattab (2014), individual attitudes and cognitive entrepreneurship training can enhance entrepreneurial intentions. However, the research examines the why and how aspects of providing entrepreneurial education to students to improve their entrepreneurial ambitions, helping us better understand the business process.

Multiple studies have shown that entrepreneurial education cannot produce positive results compared to the relationship between entrepreneurial training and business goals. Ezlika and Ong (2004) found that most male Malay entrepreneurs had no tertiary education relative to Chinese entrepreneurs in a sample of urban Malaysian entrepreneurs. The contractor's study concluded that no more than 11.3% of respondents had tertiary education (Yusof et al. 2008). According to detailed research, there is an essential link between family background and entrepreneurial desires (Crant 1996; Matthews and Moser 1996; Abd. Hadi 2002). It has been revealed that children are primarily involved in business wherever there is family involvement in business (Hisrich 2000).

Conversely, several studies contradict these conclusions. In research conducted in Malaysia of contractors, it was revealed that 73.2% of respondents became entrepreneurs because of their interest, while66.2% were not from families having any background in business (Nor Aishah and Yufiza 2004). Most of the previous research has shown more inclination of males towards entrepreneurship than females (Crant 1996; Nor et al. 2004).

Historically, Universities have been active in information distribution, but this expertise should also be used (Gibb and Haskins 2014). The demand from educational institutions to be a part of the economic value chain facilitates extensive analysis of how these institutions are organizing, managing, and using information flows (Gibb and Haskins 2014). Business intentions guide and direct people's activities to grow and apply novel business concepts (Bird 1988). Several factors impact and modify the incentive to conduct such activities, including expectations, interests, preferences, and behaviors (Lee and Wong 2004); a set of cognitive variables (Ajzen 1991); and situational factors (Lian and Chen 2006). Previous studies suggest entrepreneurial education as a vital tool in improving entrepreneurial approaches for future and present entrepreneurs (Linan et al. 2010), closely linked to intent (Noel 1998) as well as the teaching of the wide range of skills and qualities to exploit entrepreneurial behavior among beneficiaries (OECD 2009). Research on private university students operated by a government-linked firm showed a high level of entrepreneurial ambition (86% of 279 respondents). There was a high level of business purpose among students across programs and was not limited only to students studying business. Students' exposure to entrepreneurial courses was proven to have a significant impact. As a result, entrepreneurial education has gotten much attention. However, there is not much known about the various entrepreneurship courses and their influence on the students' entrepreneurial behavior. One of the questions concerns is determining the entrepreneurial intention, especially amongst students studying in universities. It is evident from the literature that there is a scope for further research as only a few studies have been conducted in the Indian perspective compared to Western countries to determine entrepreneurial intent. Norasmah (2006) concluded that students preferred taking jobs to become entrepreneurs. From this theoretical perspective and various arguments into consideration, the following hypothesis was assumed

> H0: Entrepreneurial education has no significant effect on entrepreneurial intention.

Entrepreneurial Education and Entrepreneurial Personality Traits

Historically, personality traits that include creativity, success, and risk-taking have been identified as essential to entrepreneurship (Knight 1921; McClelland 1961). The trait theory states that the person's interior features allow the person's for taking such risks. According to many reports, traits have been a positive indicator and entrepreneurial metric. These attributes are the need for success, the ability to take chances, the emotional intelligence (McLaughin 2012) and locus of internal control (Brice 2002)

Rauch and Frese (2007), in their study entitled Entrepreneurs' Personality Characteristics and Performance, explained how prominent personality traits called as "Big Five Personality Traits" (consciousness, competence, neuroticism, open-mindedness, and extraversion) influence particular characteristics of a person (need for success, locus of control and risk-taking). The work suggested introducing' a model called as Big Five Personality traits' to distinguish different characteristics of individuals planning to be entrepreneurs. Brice (2002) distinguished between entrepreneurs and others using several of the Five Factors. Big five personality traits have envisaged entrepreneurial intent that predicted enterprise output (Williams 2011). Many researchers have examined the influence of 5 comprehensive personality variables on students (Liang et al. 2015; Akanbi 2013; Chen et al. 2012; Ismail et al. 2009).

Many scholars identified significant entrepreneurial purpose determinants by analyzing different sets of related variables. The analysis centered on personality identifies many business-specific characteristics. For example, risk-taking behavior, locus of internal control, innovation & creativity, to name a few of the attributes frequently discussed. Even though the impact of the need for achievement and locus of control on entrepreneurial intentions has long been studied in the literature, a new study in European countries such as Romania has yielded contradicting results. Several experimental studies have shown a low or non-existent association involving tendency, including the opening of business and personality characteristics. Popescu et al. (2017) observed a marginal positive relationship between entrepreneurial intentions and locus of control in evaluating Romanian students. The findings were essential for the need for achievement at either the level of 0.15 or zero at all.

Researchers such as Wach and Wojciechowski (2016) discovered that entrepreneurial attitudes and subjective standards had a significant impact on 719 students in other European countries like Poland. Nevertheless, some Romanian students have requisite compulsory aptitudes with business development understanding. This condition might be caused by a lack of self–assurance or a perception that other causes influence the person's long–term conduct. Therefore, we question how these factors affect the intent to start a company to study further. From this theoretical perspective and various arguments into consideration, the following hypothesis was assumed

H0: Entrepreneurial education has no significant effect on entrepreneurial personality traits among students.

4 Entrepreneurial Traits and Intention

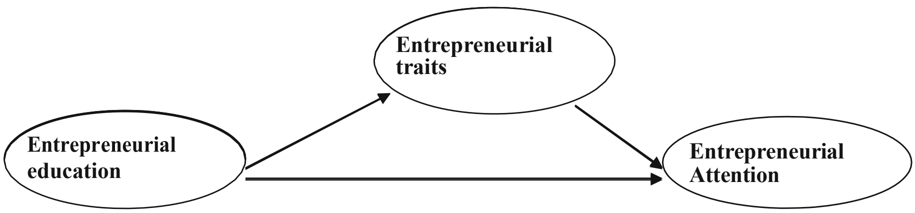
Researchers in entrepreneurial qualities have generally assumed that entrepreneur-related characteristics are embedded in the entrepreneur's personality. Personality is widely recognized as a strong predictor of entrepreneurial actions and areas of interest in entrepreneurship studies (Frese and Rauch 2000, 46). Some of the main personality traits of students, namely enthusiasm, creativity, risk-taking tendency, and competitiveness, are essential entrepreneurial traits that influence entrepreneurial purpose. Ahmed et al. (2020) explored the effect of the Big 5 personality traits on entrepreneurial intentions. He recommended that policymakers learn more about the behavior of high-profile future entrepreneurs and use a variety of incentives to encourage new start-ups among students. Farrukh et al. (2018), in their study titled "Entrepreneurial intentions: In "the significance of personality traits in the idea of planned conduct," researchers established a link between entrepreneurial intentions (EI) and personality traits. A.T. Karabulut (2016) studied the impact of personality characteristics like inner locus of control, want of success, risk tolerance, entrepreneurial awareness and stated that personality characteristics have an affirmative impact on entrepreneurial intention. M.N. In their study, Issues Affecting Entrepreneurial Intention of Students at Vietnamese National University—A Mediating Study on Perception to Entrepreneurship, Khuong and An (2016) investigated the impact of personal characteristics (locus of control, risk-taking tendency, flexibility, uncertainty sensitivity, and so on), previous experience as an entrepreneur, external environment, custom, and viability on entrepreneurship intention through positive and adverse outcomes.

Chaudhary (2017) investigated the effect of personality factors in determining entrepreneurship in Indian Universities. Results revealed that the locus of influence, uncertainty sensitivity, self-confidence, and innovativeness characteristics are essential in separating business people from those who are not doing business or are not entrepreneurs. Subsequently, these two classes also noted that the need for accomplishment and the tendency to take risks were not significantly different, contrary to expectations. Nasip et al., (2017) According to research conducted on students of a University in North Borneo area of Malaysia, need for achievement, creativity, risk-taking ability, self-confidence, and uncertainty sensitivity is related positively towards the entrepreneurial intention amongst the students who are studying in Undergraduate level. Nevertheless, there is no tangible link between the purpose of entrepreneurs and the locus of control.

In addition to these more general entrepreneurial characteristics, attempts have been made to link entrepreneurship with broader personality traits, the Big Five Factors of Personality, and mixed results (Leutner et al. 2014; Mendoza and Lacap 2015). Although they have been criticized for the importance of entrepreneurial characteristics in forecasting entrepreneurship (Gartner 1988; Kruger et al. 2000; McStay 2008; Mwasalwiba 2010), they have been substantially supported by a recent meta-analysis by Zhao et al. (2010) and Rauch and Frese (2000). However, in Rauch and Frese (2000) and Leutner et al. (2014), it is established that greater efficiency is achieved in the prediction of entrepreneurship using specific methods.

The GEM study indicates how vital entrepreneurship has become in creating jobs and creating wealth and highlighting that entrepreneurship is closely related to the country's growth and economic development (Gómez Grass et al. 2010; Nabi et al. 2010; Acs et al. 2005). Like Rasmussen, Mosey and Wright (2011), the author indicated that entrepreneurial traits are closely related to self–employment and unemployment rates reduction in economic crisis.

Some prior studies were overly optimistic, claiming no link between entrepreneurial traits and entrepreneurial intention (e.g., Block et al. 2013; Walter and Dohse 2012; Souitaris et al. 2007). Entrepreneurship researchers studied factors like organizational, environmental, and personality characteristics as the causes for new business success (Baum and Locke 2004). For this reason, Evans-Obinna (2016) investigated the relationship between entrepreneurial education, self-confidence, and entrepreneurship in achieving economic development, highlighting challenges such as insufficient funding, scarce resources, entrepreneurship teachers, among others, facing entrepreneurship education.



Based on these findings, there is every reason to argue that entrepreneurial characteristics are exceedingly narrow or unique. The conceptualization of Mould's 2013 reported a direct effect of entrepreneurial characteristics on entrepreneurial intent in which optimistic personality had a positive effect and a bivariate correlation of self-efficacy. Aspiration for perseverance and power had nothing to do with entrepreneurial purpose. On their side, Bux and Honglin (2015) reported a positive direct impact of entrepreneurial traits (control place, risk-taking tendency, self-confidence, creativity, and uncertainty tolerance) on entrepreneurial intention except for the need for achievement. Keeping these arguments into consideration following hypothesis was assumed

H0: Entrepreneurial personality traits do not mediate the relationship between entrepreneurial education and entrepreneurial intention.

5 Objectives

- To identify entrepreneurial traits among the student doing professional courses.
- To examine entrepreneurial education and its influence on entrepreneurial intention among students of professional courses.
- To examine the mediating role of entrepreneurial traits in the relationship between entrepreneurial education and entrepreneurial intention.

6 Research Methodology

For this study, data were obtained from students taking academic courses (management, engineering and law, and medical) using questionnaires from April to June 2019. Students were invited to take part in the study via personal contact. The researcher visited various professional colleges and universities in Dehradun, Uttarakhand, India; 250 students took part, final 217 questionnaires were used for analysis, and 33 inaccurate or insincerely answered questions were excluded. The current literature was assisted in preparing the questionnaire, and questions were selected based on the associated research. The works of Krueger et al. (2000), Tkachev and Kolvereid (1999), Autio et al. (1997), Kolvereid (1996), Veciana et al. (2000), Ajzen, I. (2002), Lee and Ashton (2004), Fayolle and Gailly (2004), Liñán (2004), Van der Brink, et al., (2004), and SP Kerr (2017) are explicitly focused. The researchers then changed several questions so that emphasis could be on detailed data. There were two parts of the questionnaire; the first one included a question to analyze the demographic profile of the students, while the second one dealt with different attributes associated with entrepreneurial education, entrepreneurial traits, and entrepreneurial intent. Respondents indicated their responses on a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree) for entrepreneurial education, entrepreneurial traits, and business intent (strongly agree). There were 64 attributes, 32 associated with entrepreneurial education, 16 have been associated with entrepreneurial traits, and 16have been associated with entrepreneurial intention. A panel of specialists and faculty members determined the validity of the questionnaire (survey instrument), the coherence of its interpretation of its objects, and its linkages to the study objectives. The questionnaire was validated using 25 participants, comprising 11.5

percent of respondents, considered as members of the population that will be studied to validate the accuracy.

Cronbach alpha's value was 0.970, and thus it suggested that the questionnaire was reliable as the value was at an acceptable level. The received data was arranged systematically, tabulated, and analysis was conducted using SPSS 22. The data were analyzed using descriptive statistics, regression analysis, and the Sobel test to determine the mediation effect.

Table 1. Demographic Characteristics of Respondents

	Categories	*Count*	*Percentage*
		217	100
Age (in years)			
	Up to 18	47	21.7
	19–22	62	28.6
	23–25	81	37.3
	Above 25	27	12.4
Gender			
	Male	144	66.4
	Female	73	33.6
Family Size (Number of Members)	Up to 2	33	15.2
	3 to 4	111	51.2
	5to 6	40	18.4
	More than 6	33	15.2
Income Level	Upto Rs50000 PM (USD 700)	181	83.4
	From 50001 to Rs100000PM (USD 701–1400)	19	8.8
	100001–125,000 PM (USD 1401–1750)	10	4.6
	125,001 to Rs150000PM (USD 1751–2050)	7	3.2
Program of Study	MBA	46	21.2
	Medical	45	20.7
	Applied Sciences	37	17.1
	Engineering	68	31.3
	Law	21	9.7

Source: Primary data

The analysis of the demographic background of the respondents has significant importance to understand clearly the different factors affecting the value orientation of the respondents, i.e., their age, caste, religion, family structure, educational attainments, economic status, etc. The demographic information in Table 1 demonstrates that the sample comprises a broad set of respondents from various segments, making the study more significant. The survey reveals that male respondents dominated the sample of the study. The majority of student respondents indicated that there are 3–4 members in their family. Most respondents indicated that their family income is Rs 50000 PM (USD 700). The sample comprises students studying management and engineering applied sciences, engineering, and law.

Table 2. Components of entrepreneurial education: descriptive statistics

	Reliability	Factor loading	Mean	Std. Deviation
Entrepreneurial oriented curriculum	.937		3.5098	.92919
Course curriculum is oriented toward giving Legal knowledge and skill		.826	3.61	1.066
Higher-order and problem-solving skill		.792	3.65	1.113
Course curriculum is oriented toward giving Administration knowledge and skill		.780	3.61	1.066
Students are provided practical exposure of opportunity identification		.768	3.41	1.127
Course curriculum is oriented toward giving financial management skill		.742	3.58	1.148
Course curriculum is oriented toward giving Business planning and development Skill		.741	3.69	1.064
My present course gives me knowledge about t he functionality of t he advisory board and Network		.740	3.47	1.028
Students are provided practical exposure of environmental examining		.694	3.46	1.080
Particular emphasis is made on improving Self-awareness		.512	3.47	1.076
Knowledge Transfer Pedagogy	.949		3.6517	.91790
The stories of great entrepreneurs and video clippings are shown in the lectures		.826	3.7373	.98137
The teachers promote the interest in entrepreneurship via the teaching methods		.791	3.2857	1.13097
Everyone in the university is talking about Entrepreneurship		.785	3.5530	1.09638

(*continued*)

Table 2. (*continued*)

	Reliability	Factor loading	Mean	Std. Deviation
I assume that the college is the best place to train students in a business where I meet many people with good ideas		.691	3.8571	1.02869
The teachers present the courses on the topic of entrepreneurship in an outstanding Way		.672	3.5945	1.02360
I am inspired by the college environment to Develop new business ideas		.650	3.8018	1.01032
My university focuses on the development of business enterprise courses to encourage entrepreneurship in universities		.632	3.8065	1.04055
The instructors are experienced in teaching of entrepreneurship courses the		.799	3.8065	1.10107
Knowledge Construction	.962		3.7488	1.04147
The lecturer comprehensively teaches business plan in practice sessions that significantly contribute to understanding the subject of entrepreneurship		.777	3.7834	1.09040
The lecturer has a vast practical knowledge in teaching entrepreneurship courses and makes the course practical and interesting		.723	3.6774	1.18521
Course focus towards Enrichment in Creativeness of students		.705	3.75	1.233
The instructor contributes a lot to make the course relevant for real world		.700	3.7143	1.08501
The teacher teaches the subject related to implementation of detailed business plan template		.693	3.7604	1.11708
Instructors focus more on giving knowledge about Production/managing office space		.752	3.8065	1.10107
Application-Oriented Knowledge	.906		3.5221	.89442
This course instructor emphasis giving knowledge on organizing and supervising skill		0.718	3.7834	1.09040

(*continued*)

Table 2. (*continued*)

	Reliability	Factor loading	Mean	Std. Deviation
Instructor focus more on improving operational knowledge of students		0.713	3.6774	1.18521
Course curriculum is oriented toward giving Marketing/Sales skill		0.777	3.75	1.233
Instructor provides raw materials knowledge to students		0.645	3.7143	1.08501
Instructor focus more on giving management and planning kill		0.735	3.7604	1.11708
Instructor provide knowledge about Equipment/plant/technology		0.725	3.58	.997
Professionalism and Emotional coping	.845		3.6244	.99685
Course work is more focused towards developing professionalism and accountability		.743	3.61	1.040
Students are developed for Improved Emotional coping		.734	3.64	1.101

Data summarized in Table 2 reveals that the knowle dge construction through entrepreneurial education has secured the highest mean (m = 3.7488 and SD = 1.04147), followed by Knowledge Transfer Pedagogy (3.6517). Professionalism and Emotional Copying has scored a mean of 3.6244 and SD of .9968. The entrepreneurial-oriented curriculum as scored the lowest mean of 3.6098. Attribute like Application-Oriented Knowledge has scored a mean of 3.5221. The highest standard deviation of entrepreneurial education like Knowledge Construction (SD = 1.0414) indicates respondents' heterogeneous views on this attribute (Table 3).

Entrepreneurship is viewed as an essential process through which creative information is translated into new services and products, and thus supply and demand are balanced (Shane and Venkataraman 2000). Therefore, the present study describes the need for accomplishment, locus of control, uncertainty sensitivity, sight, determination extensively, and Resilience as components of entrepreneurial traits in the following sections before revealing the methodologies adopted to establish and validate the new tool. To illustrate the critical entrepreneurial characteristics and their relative importance among students taking entrepreneurial courses, some constructs such as Achievement orientation, self- confidence, Ambiguity tolerance, Locus of control, imitativeness, and Risk-taking were identified from the literature and measurement variables developed covering the various construct related to entrepreneurial traits. Students rated the various traits on a scale of 1 to 5. From the mean, it can be concluded that variable like "Achievement Orientation (m = 3.6037)" is the most important entrepreneurial traits available among the students as it has scored the highest mean. It was followed by Ambiguity Tolerance with a mean of 3.5688. However, traits like "Achievement Orientation" have a

Table 3. Entrepreneurial traits components: a descriptive statistics

	Reliability	Mean	Std. deviation
Achievement Orientation	.873	3.6037	1.00443
I intend to achieve excellence in everything I do		3.5622	1.00326
I try to learn lessons through my mistakes and educational experience		3.6452	1.12562
Ambiguity Tolerance	.639	3.5668	.80939
I am able to work in stressful situations		3.6590	1.06451
I am ambitious and focused on my goal		3.5023	1.06773
I can adapt myself to different conditions		3.5392	1.05391
Self Confidence	.593	3.4501	.84357
I am always doing things I want to do and trying until I have the right way		3.4332	1.07858
I am able to make changes to the new environment		3.6129	1.08330
I have the courage and the desire to make my way forward		3.3041	1.23964
Locus of Control		3.5092	.98831
Business education has helped me to control one's destiny	.739	3.5300	1.06731
My actions and my own performance are strongly correlated		3.4885	1.15113
Risk-Taking		3.5369	.77192
I have the ability to take the risk	.864	3.5161	.97704
I like being independent in making decisions		3.4654	.92294
I think it is worth taking higher risks for higher rewards		3.6175	.89560
I have the ability to take calculated risks to achieve potential benefit		3.5484	.86534
Imitativeness	.636	3.5438	.87621
I am a self-starter to take on a new project		3.4009	1.08466
I am creative, adventurous, and flexible		3.6866	1.10699
Valid N (listwise)			

higher standard deviation (1.00443), indicating heterogeneous respondents' perspectives on this topic (Table 4).

Entrepreneurial intentions are regarded as individuals' orientations that might direct the formation of a new venture. It is a mindset that will precede action and direct Attention to entrepreneurial behavior like starting a new venture and becoming an entrepreneur. To illustrate entrepreneurial intention, certain variables were identified from the literature, and students rated their intention on a scale of 1 to 5. SPSS calculated all the calculations

Table 4. Entrepreneurial intention: descriptive statistics

	N	Reliability	Mean	Std. Deviation
Entrepreneurial Intention	217	.953	3.5553	.78647
It will be easy for me to open a firm and keeping it viable	217		3.5622	1.00326
My friends will approve and support my decision of starting a new venture	217		3.6452	1.12562
I am willing to do whatever for becoming an entrepreneur	217		3.5484	1.07957
Amongst various options, I prefer being anything rather than entrepreneur	217		3.5760	1.05188
In the future, I have decided to create a new business	217		3.3641	1.07203
Professionally my objective is to become an entrepreneur	217		3.5668	1.01215
I feel there are more advantages compared to disadvantages for being an entrepreneur	217		3.4055	1.07650
I have a low intention for opening a new venture	217		3.6959	1.03621
I am aware of how to start a business	217		3.5392	1.04065
My ambition is to become a renowned businessman	217		3.2350	1.23418
I am going to do my best opening and managing own company	217		3.8018	.97771
In the future, I am eager to build a company	217		3.5530	.96619
The content of the entrepreneurial course is motivating for business entrepreneurship	217		3.4793	.92835
Entrepreneurship education motivates me toward starting startup venture	217		3.6406	.88705
Entrepreneurial education is only meaningful if you intend to start your own business	217		3.5484	.86534
Valid N (listwise)	217			

of variables under study. From the mean, it can be concluded that the variable like "I am going to do my best opening and managing own company" (M = 3.8018) has scored the highest mean indicating higher entrepreneurial intention among students.

Table 5. Relationship between entrepreneurial education and entrepreneurial intention: direct effect

Model		Unstandardized coefficients		Standardized coefficients	t	Sig
		B	Std. Error	Beta		
1	(Constant)	.515	.125	.862	4.121	.000
	Entrepreneurial Education	.842	.034		24.946	.000
R = .862[a] R^2 .743 F = 622.282 P = .000[b] **Std. Error of the Estimate = .39946**						

a. Dependent Variable: Entrepreneurial Intention

7 Mediating Effect of Entrepreneurial Traits on Entrepreneurial Education and Entrepreneurial Intention: Indirect Effect

Table 6. Impact of entrepreneurial education on entrepreneurial traits: regression analysis

Model		Unstandardized coefficients		Standardized coefficients	t	Sig
		B	Std. Error	Beta		
1	(Constant)	1.032	.146	.767	7.049	.000
	Entrepreneurial Education	.693	.040		17.516	.000
R = .767[a] R^2 .588 F = 306.795 P = .000[b] **Std. Error of the Estimate =** .46832						

a. Dependent Variable: Entrepreneurial Traits

Table 7. Impact of entrepreneurial traits on entrepreneurial intention: régression analyses

Model		Unstandardized coefficients		Standardized coefficients	t	Sig
		B	Std. Error	Beta		
1	(Constant)	.513	.161	.796	3.192	.002
	Entrepreneurial Traits	.861	.045		19.311	.000
R = .796[a] R^2 .634 F = 372.926 P = .000[b] **Std. Error of the Estimate = .4767**						

a. Dependent Variable: Entrepreneurial Intention

In regression, the combined factor is used to calculate the coefficients of the linear equation between entrepreneurial education, entrepreneurial traits, and entrepreneurial intention. The pooled mean of different components of entrepreneurial education

Table 8. Impact of entrepreneurial education and entrepreneurial traits on entrepreneurial intention: regression analysis

Model		Unstandardized coefficients		Standardized coefficients	t	Sig
		B	Std. Error	Beta		
1	(Constant)	.148	.126	.329	1.174	.242
	Entrepreneurial Traits	.355	.053		6.696	.000
	Entrepreneurial Education	.596	.048	.610	12.435	.000
$R = .888^{a}$ R^2 .788 F = 397.009 P = $.000^{b}$ **Std. Error of the Estimate = .**36406						

a. Dependent Variable: Entrepreneurial Intention

Table 9. Influence of mediating variable using sobel test (A)

	Input		Test Statistics	Standard Error	P-Value
A	.693	Sobel test	12.84246842	0.046460	.000
B	.861	Aroian test	12.83284124	0.046495	.000
Sa	.040	Goodman test	12.85211731	0.046426	.000
Sb	.045				

(Entrepreneurial oriented curriculum, Knowledge Transfer Pedagogy, Knowledge Construction, Application-Oriented Knowledge, and Professionalism and Emotional copying) and different trait components (Achievement orientation, Ambiguity tolerance, Self- confidence, Risk-taking, Imitativeness, and Locus of control) and 16 components denoting entrepreneurial intention were calculated using SPSS software. Following that, a regression analysis was performed. The impact of entrepreneurial education on entrepreneurial intention (Table 5) was found significant (F = 622.282, p = .000, t = 24.946, p = .000) and contributed 74.3% (R^2 = 0.743) to the entrepreneurial intention. Entrepreneurial education has a beta value of 0.842, indicating that it significantly affects entrepreneurial intention (Tables 6, 7, 8, 9 and 10).

To assess mediating effect of entrepreneurial traits between entrepreneurial education and entrepreneurial intention, the indirect effect was measured by calculating the regression impact of entrepreneurial education on entrepreneurial traits and the further impact of entrepreneurial traits on entrepreneurial intention. The impact of entrepreneurial education on entrepreneurial traits with beta = 0.693 (F = 306.795, p = .000, t = 17.516) was found to be significant and contributed 58.8% (R^2 .588) variance to entrepreneurial traits. Similarly, impact of entrepreneurial traits on entrepreneurial intention (F = 372.926, p = .000, t = 19.311, p = .000) was also found significant. Analyzing the combined effect of entrepreneurial education and entrepreneurial traits on entrepreneurial intention, it is observed beta value (EE = 0.596, ET = 0.355) and (F = 397.009 p = .000, t =

6.696 and 12.435, p = .000). The result indicates that entrepreneurial education and entrepreneurial traits significantly affect developing entrepreneurial intention among students getting entrepreneurial education.

Table 10. Influence of mediating variable using sobel test (B)

	Input			
ta	24.274	Sobel test	12.97397587	.000
tb	7.336	Aroian test	12.96444284	.000
		Goodman test	12.98352997	.000

The effect of the mediating variable (entrepreneurial traits) of the independent variable (Entrepreneurial education) on the dependent variable was evaluated using the Sobel, Aroian, and Goodman tests (entrepreneurial intent). MacKinnon and Dwyer (1993) and MacKinnon et al. (1995) popularized statistical methods for systematically testing mediation. According to the Sobel test, if a two-tailed z-test is more significant than 1.96, p-values are less than.05. As a result, the null hypothesis is rejected, implying that entrepreneurial personality traits mediate the relationship between entrepreneurial education and intention.

8 Discussion and Conclusions

The present study examined impact of entrepreneurial education on building entrepreneurial intention and whether entrepreneur's personality traits mediate the relationship between entrepreneurial education and entrepreneurial intention. Finding indicated majority students are of opinion that entrepreneurial education system is more focused on developing knowledge construction as compared to application-oriented knowledge. Looking at the entrepreneurial personality traits, it is observed that "Achievement Orientation (M = 3.6037)" is the most important entrepreneurial personality traits available among the students. The regression analysis results demonstrate that entrepreneurial education has a significant effect on entrepreneurial traits, and entrepreneurial traits significantly impact entrepreneurial intention. Entrepreneurial intention is strongly affected by the combined effect of entrepreneurial education and entrepreneurial traits (R2 =.788). Sobel's test supports the alternate hypothesis that entrepreneurial personality traits mediate entrepreneurial education and entrepreneurial intention. Previous research supports these findings, emphasizing the value of entrepreneurial education and the role of entrepreneurial personality traits in fostering entrepreneurial intention (Susetyo Darmanto 2018, Chao Miao 2015, Gaddam, (2008). Gupta and Muita (2012).

The present study analyzed the role of education in developing entrepreneurial qualities and entrepreneurship among prospects. If entrepreneurial education can foster entrepreneurship or whether it is a personality trait. We looked at the stages at which entrepreneurial education is most successful in developing entrepreneurial qualities.

According to the findings, most respondents (60 percent) believe it should be introduced at the post-secondary/undergraduate level. The findings are also consistent with previous research by Chamard (1989), Singh (1990), Gasse (1985), Filion (1994). The research on the entrepreneurship program supports this program's importance in building a network of alumni, collaborating with other institutions, and providing coaching and mentorship.

Furthermore, entrepreneurial initiatives at the graduate level are more effective in garnering financing and investment and continuing community entrepreneurship activities. Hence, for activation of the entrepreneurial education programs, it is essential to search for direction like development and improvement. On the other hand, many studies back up the idea that early state entrepreneurial education programs at the school level are crucial in promoting student interest in entrepreneurship. As a result, methods should be investigated for directing entrepreneurial education at various stages to make it more feasible and successful for the community.

9 Limitation and Suggestions for Future Research

In the study, all factors recognized as potential causes of entrepreneurial education and entrepreneurial traits have not been accounted for. This work does not address demographic, environmental, and personality factors, which play a vital part in the entrepreneurial intent. Over time, the capacity to discern changes in characteristics and purposes is limited when using a cross-sectional technique. The best method to understand becoming an entrepreneur is to use a systematic approach to research that follows people across time. Because the respondents were all entrepreneurial students from a single city (Dehradun, India), more significant respondents from a single state (Uttarakhand, India) are advised for better outcomes.

Despite the enlightening results, there are certain limitations to the study that must be considered. The findings cannot be generalized because the investigation was limited to the Dehradun district of Uttarakhand State. This study can also be improved in the future by increasing the sample size. Cross-sectional data is information collected by seeing multiple things at the same time.

A longitudinal study is observational research in which data is gathered regularly from the same people across time. Longitudinal research initiatives can take years, if not decades, to complete. The participants in a longitudinal cohort study remain the same throughout the research period (Caruana et al. 2015).

Second, the scope of this research can be enlarged based on subgroups to assess the influence these groupings have on the correlations between various constructs (Ahmad 2014). For example, to examine if these classes affect the tested ideas, the dataset might be divided into other groups, such as student types and degrees of qualification. In addition, future studies may incorporate another mediator, such as information technology, or moderators, such as technological maturity.

10 Conclusion

Entrepreneurial education significantly affects developing entrepreneurial personality traits and students' entrepreneurship and enterprising behaviors. The organization can build winning personal qualities and create an opportunity for self and others to create jobs. Entrepreneurship, self-employment, and the development of businesses solve both unemployment and underemployment crises. Through widening the pool of entrepreneurs in society, they have a definite role in promoting entrepreneurship. The Indian government should therefore take appropriate action to encourage and improve entrepreneurial training in India. Extensive effort must be on developing entrepreneurial personality traits at a different level. This will improve the effectiveness of entrepreneurial education in influencing entrepreneurial intention.

References

Ankrah, S.N., Burgess, T.F., Grimshaw, P., Shaw, N.E.: Asking both university and industry actors about their engagement in knowledge transfer: What single-group studies of motives omit. Technovation **33**(2), 50–65 (2013)

Arvanitis, S., Kubli, U., Woerter, M.: University-industry knowledge and technology transfer in Switzerland: What university scientists think about co-operation with private enterprises. Res. Policy **37**(10), 1865–1883 (2008)

Baum, J.R., Locke, E.A.: The relationship of entrepreneurial traits, skill and motivation to subsequent venture growth. J. Appl. Psychol. **89**, 587–598 (2004)

Bekkers, R., Bodas Freitas, I.M.: Analyzing knowledge transfer channels between universities and industry: to what degree do sectors also matter? Res. Policy **37**(10), 1837–1853 (2008)

Bodas Freitas, I.M., Marques, R.A., Silva, E.M.D.P.: University–industry collaboration and innovation in emergent and mature industries in new industrialized countries. Res. Policy **42**(2), 443–453 (2013)

Brush, C.G.: Exploring the concept of an entrepreneurship education ecosystem. In: Advances in the study of entrepreneurship, Innovative Pathways for University Entrepreneurship in the 21st Century **24**, 25–39 (2014). by Fayolle, A. and Redfords, D.T. Edward Elgar Publishing Limited, Cheltenham, United Kingdom, 25–63

Byrnes, J., Paez, D., Blacker, J., Jackson, A., Dwyer, C.: The future of higher education in the knowledge-based economy: Developing innovative approaches to integrated articulation and credit transfer in Australia. In: Proceedings of the International Higher Education Partnerships and Innovation (IHEPI) Conference Budapest: From Higher Education to Innovation: Management and Entrepreneurship in a Changing Market. Pp. 91–101. Publikon Publishers, ID Research Lt (2010)

Miao, C,: Individual Traits and Entrepreneurial Intentions: The Mediating Role of Entrepreneurial Self-Efficacy and Need for Cognition (2015). Retrieved from: https://scholarscompass.vcu.edu/do/search/?q=author_lname%3A%22Miao%22%20author_fname%3A%22Chao%22&start=0&context=5233864&facet

Chaudhary, R.: Demographic Factors, Personality and Entrepreneurial Inclination: A Study among Indian University Students. Education Training **59**, 171–187 (2017). https://doi.org/10.1108/ET-02-2016-0024

Clarysse, B., Wright, M., Lockett, A., Van de Velde, E., Vohora, A.: Spinning out new ventures: a typology of incubation strategies from European research institutions. J. Bus. Ventur. **20**(2), 183–216 (2005)

Cohen, W.M., Nelson, R.R., Walsh, J.P.: Links and impacts: the influence of public research on industrial R&D. Manage. Sci. **48**(1), 1–23 (2002)

Dolfsma, W., Van der Panne, G.: Currents and sub-currents in innovation flows: explaining innovativeness using new-product announcements. Res. Policy **37**(10), 1706–1716 (2008)

Dr. Lunavath, N.: A Study on the Entrepreneurial Intention among Studen. The American Research Journal of Business and Management **1**(1) (2015). ISSN 2379–1047

Sankar, P.: Entrepreneur Intention among Medical Students in Chennai City - An Empirical Analysis. Int. J. Pharm. Sci. Rev. Res. **53**(2 and 03), 15–18 (2018). ISSN 0976 – 044X

Duncan, F.: South Africa's small business problem - why are SMMEs in South Africa struggling to establish a foothold? (2012). Retrieved from http://led.co.za/story/2012/05/07/sas-small-business-problem-why-are-smmes-in-sa-struggling-to-establish-a-foothold

Farrukh, M., Alzubi, Y., Shahzad, I.A., Waheed, A., Kanwal, N.: Entrepreneurial intentions: the role of personality traits in perspective of theory of planned behaviour. Asia Pacific Journal of Innovation and Entrepreneurship **12**(3), 399–414 (2018). https://doi.org/10.1108/APJIE-01-2018-0004

Fetters, M., Greene, P.G., Rice, M.P.: The development of university-based entrepreneurship ecosystems: global practices. Edward Elgar Publishing, Cheltenham (2010)

Fiet, J.O.: The relationship between entrepreneurship education and entrepreneurial intentions: a meta-analytic review. Entrep. Theory Pract. **38**(2), 217–254 (2014)

Fin: Zulu: Most SMMEs fail in year one (2014). Retrieved from http://www.fin24.com/Entrepreneurs/News/Zulu-Most-SMMEs-fail-20141028

Franco, M., Haase, H.: Entrepreneurship: an organizational learning approach. Journal of Small Business and Enterprise Development **16**(4), 628–641 (2009). From http://www.innovationandentrepreneurship.net/index.php/aie/article/view/16742

Gaddam, S.: Identifying the relationship between behavioral motives and entrepreneurial intentions: an empirical study-based participations of business management students. The Indian Journal of Management Research. **7**(35), 5 (2008)

Gallo, M.: Beyond philanthropy: recognizing the value of alumni to benefit higher education institutions. Tert. Educ. Manag. **18**(1), 41–55 (2012)

Gibb, A.: Exploring the synergistic potential in entrepreneurial university development: towards the building of a strategic framework. Annals of Innovation and Entrepreneurship (2012). Retrieved from https://doi.org/10.3402/aie.v3i0.17211

Gibb, A.A., Haskins, G.: The university of the future: An entrepreneurial stakeholder learning organization. Handbook on the Entrepreneurial University as edited (2014)

Gibb, A.A., Haskins, G., Robertson, I.: Leading the entrepreneurial university: meeting the entrepreneurial development needs of higher education institutions. In: Universities in Change. New York, Springer pp. 9–45 (2013). Retrieved from https://doi.org/10.1007/978-1-4614-4590-6_2#page-1

Griliches, Z.: Patent statistics as economic indicators: a survey. In: R&D and productivity: the econometric evidence, pp. 287–343. University of Chicago Press, Chicago (1998). Retrieved from http://www.nber.org/papers/w3301

Gupta, A., Muita, S.R.: Relationship between entrepreneurial personality, performance, job satisfaction and operations strategy: an empirical examination. Int. J. Bus. Manage. **8**(2), 86 (2012)

Haus, I., Steinmetz, H., Isidor, R., Kabst, R.: Gender effects on entrepreneurial intention: a meta-analytical structural equation model. Int. J. Gend. Entrep. **5**(2), 130–156 (2013)

Herrington, M., Kew, J., Kew, P.: Global Entrepreneurship Monitor: South African Report 2013. University of Cape Town Centre for Innovation and Entrepreneurship. Cape Town: University of Cape Town (2014)

Heuer, A., Kolvereid, L.: Education in entrepreneurship and the theory of planned behaviour. European Journal of Training and Development **38**(6), 506–523 (2014). https://doi.org/10.1016/j.sbspro.2016.07.109 https://doi.org/10.1108/ET-10-2015-0092

International Council for Open and Distance Education (ICDE): Growing capacities for sustainable distance e-learning provision. In: Paper presented at the 26th ICDE World Conference, Opening address: Minister of Higher Education, Sun City, South Africa (2015 October)

Karabulut, A.T.: Personality Traits on Entrepreneurial Intention. Procedia—Social and Behavioral Sciences **229**, 12–21 (2016)

Khuong, M.N., An, N.H.: The factors affecting entrepreneurial intention of the students of vietnam national university—a mediation analysis of perception toward entrepreneurship. Journal of Economics, Business and Management **4**, 104–111 (2016)

Laursen, K., Salter, A.: Searching high and low: what types of business use universities as a source of innovation? Res. Policy **33**(8), 1201–1215 (2004)

Lingappa, A.K., Shah, A., Mathew, A.O.: Academic, family, and peer influence on entrepreneurial intention of engineering students. SAGE Open **10**, 215824402093387 (2020)

Link, A.N., Siegel, D.S., Bozeman, B.: An empirical analysis of the propensity of academics to engage in informal university technology transfer. Ind. Corp. Chang. **16**(4), 641–655 (2007)

Perkmann, M.: Academic engagement and commercialization: A review of the literature on university–industry relations. Res. Policy **42**(2), 423–442 (2013)

Ahmed, M.A., Khattak, M.S., Anwar, M.: Personality traits and entrepreneurial intention: The mediating role of risk aversion (2020). Retrieved from 14 March 2021 https://doi.org/10.1002/pa.2275

Markman, G.D., Siegel, D.S., Wright, M.: Research and technology commercialisation. J. Manage. Stud. **45**(8), 1401–1423 (2008)

Masemola, M.E.: UNISA small business development hub market scoping analysis. Bureau of Market Research, Pretoria (2013)

Matlay, H.: Entrepreneurship education: more questions than answers? Educ. Train. **48**(5), 293–295 (2006)

Matlay, H.: The impact of entrepreneurship education on entrepreneurial outcomes. J. Small Bus. Enterp. Dev. **15**(2), 382–396 (2008)

Matlay, H.: The influence of stakeholders on developing enterprising graduates in UK Higher education institutions. Int. J. Entreprene. Behav. Res. **17**(2), 166–182 (2011)

Milesi, D., Petelski, N., Verre, V.: Innovation and appropriation mechanisms: evidence from argentine microdata. Technovation **33**(2), 78–87 (2013)

Minniti, M., Bygrave, W.: A dynamic model of entrepreneurial learning. Entrep. Theory Pract. **25**(3), 5–16 (2001)

Mohamad, N., Lim, H.E., Yusof, N., Soon, J.J.: Estimating the effect of entrepreneur education on graduates' intention to be entrepreneurs. Educ. Train. **57**(8/9), 874–890 (2015)

Mustafa, M.J., Hernandez, E., Mahon, C., Chee, L.K.: Entrepreneurial intentions of university students in an emerging economy: the influence of university support and proactive personality on students' entrepreneurial intention. J. Entreprene. Emerg. Econ. **8**(2), 162–179 (2016)

NAIT: The Northern Alberta Institute of Technology (2015). Retrieved from http://www.nait.ca/programsandcourses.htm?

Nasip, S., Amirul, S.R., Sondoh, S.L., Jr., Tanakinjal, G.H.: Psychological Characteristics and Entrepreneurial Intention: A Study among University Students in North Borneo, Malaysia. Education Training **59**, 825–840 (2017)

Oosthuizen, G., Butala, P., Böhm, S., Rebensdorf, A., Gergert, A.: Open community manufacturing. In: Paper presented at the SAIIE 26 Conference. Muldersdrift, South Africa (2014)

Perkmann, M., et al. : Stakeholders in university education. In: Paper presented at the 31st Annual Conference of the Production and Operations Management Society. Atlanta, GA (2003)

Popescu, C.I., Robu, I., Maxim, A., Diaconu, L.: An analysis of the determinants of entrepreneurial. Sustainability **8**, 771 (2016)
Salem, M.I.: Higher education as a pathway to entrepreneurship. Int. Bus. Econ. Res. J. **13**(2), 289–294 (2014)
Sánchez-García, J.C., Hernández-Sánchez, B.: Entrepreneurship Education in Spain. In: Entrepreneurship Education and Training. Hershey: IGI Global, pp. 39–57 (2015)
Seikkula-Leino, J.: Advancing entrepreneurship education in Finnish basic education: the prospects for developing local curricula. In: Fayolle, A., Kyrö, P. (eds.) The dynamics between entrepreneurship, environment and education, pp. 168–190, Edwards Elgar, Cheltenham, UK (2008)
Sesen, H.: Personality or environment? a comprehensive study on the entrepreneurial intentions of university students. Educ. Train. **55**(7), 624–640 (2013)
Sibanda, M.: Partnerships for innovation. In: Paper presented at the Research and Innovation Week 2015. University of South Africa, Pretoria (2015 March)
Solesvik, M.Z., Westhead, P., Matlay, H., Parsyak, V.N.: Entrepreneurial assets and mindsets: Benefit from university entrepreneurship education investment. Education + Training **55**(8/9), 748–762 (2013)
Spencer, J.W.: How relevant is university-based scientific research to private high- technology firms? A United States-Japan comparison. Acad. Manag. J. **44**(2), 432–440 (2001)
Streeter, D.H., Jaquette, J.P., Hovis, K.: University-wide entrepreneurship education: Alternative models and current trends *(*Working Paper # 2002–02). Department of Applied Economics and Management. Cornell University, New York (2002)
Darmanto, S.: Mediating Role of Entrepreneurial Self Efficacy in Developing Entrepreneurial Behavior of Entrepreneur Students Academy of Entrepreneurship Journal **24**(1) (2018)
Teixeira, S.J., Casteleiro, C.M.L., Rodrigues, R.G., Guerra, M.D.: Entrepreneurial intentions and entrepreneurship in European countries. Int. J. Innov. Sci. **10**, 22–42 (2018)
Tether, B.S.: Small and large business: sources of unequal innovations? Res. Policy **27**(7), 725–745 (1998)
Tether, B.S.: Who co-operates for innovation, and why: an empirical analysis. Res. Policy **31**(6), 947–967 (2002)
Tether, B.S., Tajar, A.: Beyond industry–university links: Sourcing knowledge for innovation from consultants, private research organisations and the public science- base. Res. Policy **37**(6), 1079–1095 (2008)
Trivedi, R.: Does university play significant role in shaping entrepreneurial intention? a cross-country comparative analysis. J. Small Bus. Enterp. Dev. **23**(3), 790–811 (2016)
Tromble, W.W.: Excellence in advancement: Applications for higher education and non-profit organizations. Aspen Publishers, Gaithersburg, MD (1998)
University of South Africa (UNISA): Institutional information and analysis portal (2015). Retrieved from http://heda.unisa.ac.za/indicatordashboard/default.aspx
Vaghely, I.P., Julien, P.A.: Are opportunities recognized or constructed? An information perspective on entrepreneurial opportunity identification. J. Bus. Ventur. **25**(1), 73–86 (2010)
Wach, K., Wojciechowski, L.: Entrepreneurial intentions of students in poland in the view of ajzen's theory of planned behaviour. Entrep. Bus. Econ. Rev. **4**, 83 (2016)
Wanzenböck, I., Scherngell, T., Fischer, M.M.: How do business characteristics affect behavioural additionalities of public R&D subsidies? Evidence for the Austrian transport sector. Technovation **33**(2), 66–77 (2013)
Wong, P.K., Ho, Y.P., Singh, A.: Towards an "entrepreneurial university" model to support knowledge-based economic development: The case of the National University of Singapore. World Dev. **35**(6), 941–958 (2007)
Zarenda, H.: South Africa's National Development Plan and its implications for regional development. Stellenbosch, Tralac (2013)

Zellweger, T., Sieger, P., Halter, F.: Should I stay or should I go? career choice intentions of students with family business background. J. Bus. Ventur. **26**(5), 521–536 (2011)
Zhang, P., Wang, D., Owen, C.: A study of entrepreneurial intention of university students. Entrep. Res. J. **5**, 61–82 (2014). https://doi.org/10.1515/erj-2014-0004
Zhao, H., Seibert, S.E., Lumpkin, G.T.: The relationship of personality to entrepreneurial intentions and performance: a meta-analytic review. J. Manag. **36**, 381–404 (2010)

Deconstructive Human Confront Acknowledgment Utilizing Profound Neural Arrange

Ratnesh Kumar Dubey(✉) and Dilip Kumar Choubey

Department of Computer Science and Engineering, Indian Institute of Information Technology Bhagalpur, Bhagalpur, India
ratneshd@lnct.ac.in, ratneshdub@gmail.com,
dkchoubey.cse@iiitbh.ac.in

Abstract. Face reconstruction or face optimization as a biometric, has a several advantages in forensic application. The size and structure of face are static of an individual. For reliable human face image reconstruction, the implementation system requires huge facial image datasets. Further the assessment of the system should be done by employing a testing procedure. This paper deals with the analysis and rectification of human face images for reconstruction and optimization of human face images. The advantage of using input human face image for reconstruction in forensic application and automatic face recognition system is that they are free from wide variety of poses, expression, illumination gestures and face occlusion. The whole research is divided into two phases; in the first phase reconstruction of destructed part of human face image is being done with template matching. Second phase deals with deep neural network applications to match the image carried out in phase one. The proposed algorithm is used to reconstruct the image and at the same time, reconstructed image is used as test image for biometrical face recognition. After reconstruction of image, it is examined with various well-known algorithms (SVMs, LDA, ICA, PCA & DNNs) of face recognition system for the evaluating the performance of speed, memory usage and metrics of accuracy.

Keywords: Human face recognition system · Deep neural networks in face recognition · Image matching · Deep neural network

1 Introduction

In today's scenario digital image processing is identified as an emerging technology finding its application in many fields. This technology is used in many areas like engineering, computer science, and many other fields. One of the most interesting areas where image processing is used is forensic science. In forensic science and archaeology, the most alluring method in image processing uses facial reconstruction method. The carver who is facial anatomy expert performs facial reconstruction. For detection of gender, age, ancestry of gopher, forensic anthropologists along with the carver analyze

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 365–380, 2023.
https://doi.org/10.1007/978-3-031-13150-9_30

skeleton features. For positive recognition of individuals, and to divulge anatomical features including affirmation of wounds like broken nose, teeth and facial asymmetry, the carver uses either the 2d or 3d reconstruction techniques [1–4].

If the carver employs a 3D technique for recognition, the tissue is placed on the skull at predefined points. This ends in a good reconstruction as the clay when placed seems to be at the maximum possible nearest location to the gopher increasing the probability of gopher identification. Conventional methods of depth measurements based on gender, age and ethnicity were used to determine the points where the markers are placed [5–8]. Fake eyes also play a part in efficient reconstruction. To determine position of eyes, length/width of nose and mouth, various iteratively measurement has been taken into consideration. When the tissue markers are affixed on the skull, the sculptor starts to place clay on the skull. This initiate sculpting and finally a face are formed [9, 10]. When the elementary or primary shape is constructed, the sculptor can work on the skull, the aim being making the skull look alike a gopher. All these steps are facilitated by means of the information provided by the forensic anthropologist, including the lifestyle of gopher and the geographical location where the gopher lived. In addition to this, for better identification of the gopher, the sculptors may add clay or wig representing hair [11–14].

The properties are not limited to the above-mentioned ones but can be anything such as articles of clothing, glasses or any other aspects that could end up in a good identification. The basics of the 2D reconstruction techniques are similar to 3D techniques involving the placement of tissue markers on the skull at pre-defined depths and particular places by means of dome measurements for finding age, sex and ancestry [15–18]. As mentioned above, once the skull is in the Frankfort horizontal position, an 1X1 image of the skull is photographed from both the profile view and frontal view.

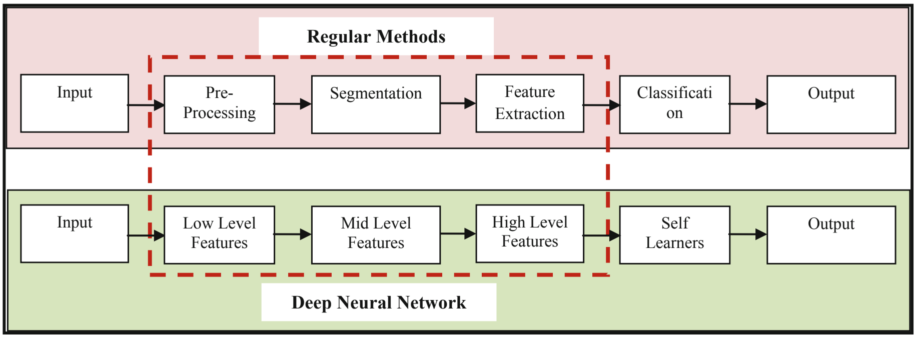


Fig. 1. Comparison between deep neural network and regular methods

The artist follows the boundaries or to be specific skull contours and by referring the tissue markers sketches the skull. By means of 3-D reconstruction techniques size and position of mouse, nose and eyes can be found. The type of hair and style is found by estimating sex and ancestry, data given by the forensic anthropologist, from scene evidences or from other methods. Another type of reconstruction technique involves reconstruction of a human face from a decaying body. Here the artist makes use of their knowledge regarding the position of the soft tissue of the skin on the skull and the process of body decomposition. The goal is to obtain an exact imagery of the gopher during the lifetime. The 2D techniques are advantageous over 3D techniques in terms of time even though they both end up in the same results.

A 3D face can be reconstructed using the anatomical condition of human head. Deep Neural Networks can be used for detecting such kind of models. In this project, a novel method for recovery of face recognition is put forward by the researcher using deep neural networks [19, 20]. Deep learning is a branch of machining learning. It helps in learning hierarchical representations of the given data. Multiple nonlinear processing layers are a major part of it and by stacking them pattern classification is enabled. The major architecture of a DNN involves an input layer followed by a huge number of hidden layers and an output layer. The network is initialized at the beginning by means of unsupervised training. Consequently, they are tuned in a supervised manner. Figure 1 shows the difference between deep learning and regular machine learning [21–24].

Amongst regular machining learning methods and deep learning methods, deep learning methods focus on learning different useful feature representations, the raw material being the available input data. This is done by means of capturing significant statistical irregularities from the input data. Next the representation features can be framed for regression, classification and other information retrieval problems [25–29]. Some of the major advantages of deep learning include human effort in feature learning and independence from prior knowledge.

In the starting module, initially the frontal human-face image has been studied. This is done to extract significant features for forming a corpus termed as human-face model. In the successive phase, a face image under test with every possible orientation's have been captured resulting in the application of high-end computing approach of advanced computing for the successful recognition of the subject's face. In the current research work based on the created data sets, a proper matching-classification- decision process has been performed [30–33]. Keeping this objective, in the present work, a methodology based on deep neural network has been proposed for the reconstruction of destructed human face image for forensic application [34, 35].

Jangir et al., [41], Choubey et al., [42, 43] have used similar data science and machine learning algorithms for the identifications and predictions of medical diabetes.

The idea conceived through the review of many published articles, text and references like comparative analysis of classification methods [24], performance evaluation of classification methods [25], rule-based diagnosis system [26] and classification techniques and diagnosis for diabetes [27, 28] are found to be of great help in accomplishment of the present work.

2 Proposed Methodology with Mathematical Formulations

Generally, two methods namely simple structure analysis and template matching approach are used to compute the estimated outline of the wavelet in noisy environment, and its occurrence time.

In order to compute the wavelet coefficients, present in the noisy images, consider a group of wavelet, $W_i(t)$ belonging to the range $i = 0, 1, \ldots, N - 1$, for an entire structural characteristic possibilities. By considering additive noise, the corrupted image can be expressed as [36–38],

$$P(m, n) = q(m, n) + Gr(m, n) \tag{1}$$

In which, q(m, n) represents the original image without noise, r(m, n) illustrates the noise present in the image and G is known as signal-to-noise ratio. Windowing of the image is expressed as represented in Eq. (2) when G is set to 1.

$$P_w(m, n) = q_w(m, n) + r_w(m, n) \tag{2}$$

Applying the Fourier transform, we get (Fig. 2)

$$P_w\left(e^{j\omega 1}, e^{j\omega 2}\right) = Q_w\left(e^{j\omega 1}, e^{j\omega 2}\right) + R_w(e^{j\omega 1}, e^{j\omega 2)} \tag{3}$$

where,

$$\begin{cases} P_w(e^{j\omega 1}, e^{j\omega 2}) Fouriertransformofwindowednoisyimages \\ Q_w(e^{j\omega 1}, e^{j\omega 2}) Fouriertransformoforiginalimage \\ R_w(e^{j\omega 1}, e^{j\omega 2}) Fouriertransformofnoisyimages \end{cases}$$

ϕ(t) signifies the fundamental mother wavelet and is illustrated as

$$\varphi(t) = e^{\left(j2\pi ft - t^2/(2)\right)} \tag{4}$$

Applying Continuous Wavelet Transform CWT (a, τ), the above expression is modified as,

$$CWT(a, \tau) = (1/\sqrt{a}) \int p(t)\phi\{(t - \tau)/a\} \tag{5}$$

Discretization of CWT is performed by applying discrete parameter wavelet transform (DPWT) and the resultant discretized output is presented in Equation (6).

$$DPWT(m, n) = 2^{-m/2} \sum\nolimits_k \sum x(k, l)\left(2^{-m}k - n\right) \tag{6}$$

In which

$$\begin{cases} m, n \; integers \\ a_0 \tau,_0 \; sampling \; interval \; for \; a \; and \; \tau \\ x(k, l) enhanced \; images \end{cases}$$

By substituting $a_0 = 2$ and $\tau_0 = 1$, the wavelet coefficient can be calculated for Eq. (6).

Sampling of the enhanced images is done at periodic time interval T to obtain sampled image sequences {q(mT, nT)}, with size X x Y, belonging to ranges m = 0,1, …, X − 1 and n = 0,1,…,Y − 1 significantly. By applying discrete Fourier transform (DFT) [39, 40], the equation is dictated as below

$$I(u, v) = \sum\nolimits_{x=0}^{x-1} \sum\nolimits_{y=0}^{y-1} i(x, y)\exp(-j2\pi(um/x + vn/N) \tag{7}$$

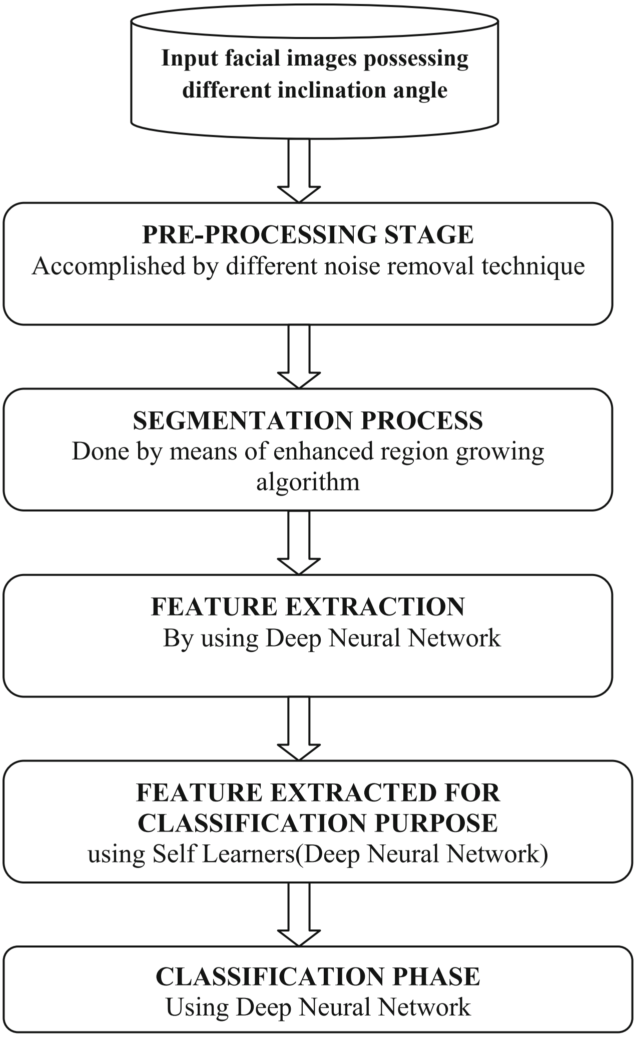


Fig. 2. Architecture of the proposed methodology

where u = 0,1,…,X − 1 and v = 0,1, ……..,Y − 1.

The magnitude, phase angle and power spectrum are evaluated by time-domain to frequency-domain transformation. If $R(u, v)$ and $A(u, v)$ signifies the real and imaginary part of $Q(u, v)$ its magnitude spectrum can be expressed as

$$|I(u, v)| = [R^2(u, v) + A^2(u, v)]^{1/2} \tag{8}$$

And the phase angle can be defined as

$$\phi(u, v) = \tan^{-1}\left[\frac{A(u, v)}{R(u, v)}\right] \tag{9}$$

The power spectrum with the inclusion of magnitude and phase angle is depicted as

$$P(u, v) = |I(u, v)|^2 = R^2(u, v) + A^2(u, v) \tag{10}$$

The dynamic range seems to be very high as the power spectrum is expressed as the squared value of the magnitude. Hence, logarithmic transformation is applied for normalization purpose and the normalized equation can be defined as

$$|I(u, v)|_{normalize} = \log(1 + |I(u, v)| \tag{11}$$

The expectation value, variance and its auto covariance of the enhanced images are represented as in Eqs. (12), (13) and (14) respectively.

$$E[I(u, v)] = \frac{1}{XY} \sum\nolimits_{u=0}^{X-1} \sum\nolimits_{v=0}^{Y-1} I(u, v) \tag{12}$$

$$Var[I(u, v)] = E\{\left|I(u, v) - I'(u, v)\right|^2\} \tag{13}$$

$$C_{xx}(u, v) = E\{\left[I(u, v) - I'(u, v)\right]\left[I(u, v) - I'(u, v)\right]\} \tag{14}$$

The power spectral density can be calculated as

$$P_E(f) = \sum\nolimits_{m=0}^{M-1} \sum\nolimits_{n=0}^{N-1} C_{xx}(m, n) W(m, n) \exp(-j2\pi f(m = n) \tag{15}$$

where, C_{xx}(m,n) and $W(m, n)$ are auto-covariance and Blackman-window function respectively with $'m'$ and $'n'$ samples.

By applying discrete cosine transform (DCT), the data can be compressed by the given equation.

$$\mathrm{DCT_c(u, v)} = \sum\nolimits_{x=0}^{X-1} \sum\nolimits_{y=0}^{Y-1} I(x, y) \cos\left(\frac{2\pi T(x + y)}{XY}\right) \tag{16}$$

For the calculation of Eigen-values and respective Eigen-vectors, a pattern vector $\overline{p_n}$ is considered that is represented by similar low dimension vector $\overline{q_n}$ which can be expressed in terms of linear transform characteristics.

$$\overline{p_x} = [X]\overline{q_x} \tag{17}$$

where $[X] = \left[I(x, y)\right], form = 0$ to $X - 1$ & $n = 0$ to $X - 1$, $\overline{q_x} = min$ ([X]), *where* $\overline{q_n} > 0$

By taking the covariance of Eq. (17), the Eigen-vectors are estimated as shown in Eq. (18),

$$\overline{P} = cov(\overline{p_n}) \tag{18}$$

$$\overline{p}.X_i = \lambda_i.X_i \tag{19}$$

where, λ_i denotes the respective Eigen-values.

Although using PCA with covariance finds the components that are useful for representing the data but may not be useful for discriminating the data between classes. Thus, Fisher's Linear Discriminate Analysis (FLDA), has been applied in present work for reducing the feature vector dimensionality from 'x' into A $= Y - 1$ (where Ydenotes the total class involved). Hence the main idea in adopting FLDA is to project the feature vector of 'x' dimension into least dimensional region. These regions are selected in such a manner that the partition among the classes have been at minimal distance from the regression line.

Clustering is an unsupervised method and needs a training set where belong to different classes are known as priori. Image clustering and categorization is a means for description of image features. When no such training set is available one should adopt unsupervised methods such as clustering. Clustering can be used for training as well as classification in an unsupervised manner. In clustering, the basic objectives to partition the feature space data points into several groups that follow a pre-defined set of procedures. Image clustering enables the creation of a user-friendly interface to the database and the implementation of efficient retrieval algorithm. There are two widely used methods namely c-means clustering and k-means clustering.

K-means is a simplest clustering approach that adopts square-error criteria algorithm where the total partitions are pre-defined. The implementation process of K-means clustering is simple and the time required for computation is minimal. For predefined number of clusters, the cluster centers are randomly initialized and every data point is allocated to any of the neighboring cluster. But the selection of the predefined cluster affects the output of k-means algorithms. If the selection of initial clusters is unclear, then the algorithm outputs wrong cluster location along with improper clustering. C-means is a clustering technique that allows single pixel of data to present in more than two clusters. A machine learning algorithm called as Support Vector Machine is applied for classifying and characterizing the progressive switching pattern of facial test images taken from the side-view (Fig. 5).

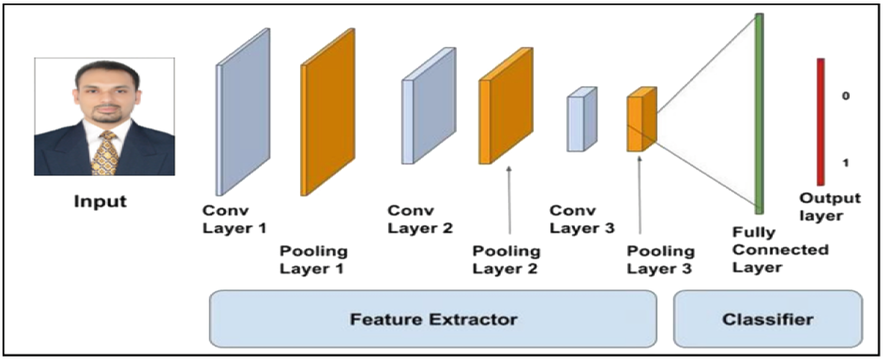


Fig. 3. Training stage of our proposed methodology

Various facial image database is collected and the proposed technique is applied for automatic generation of seven numerous facial datasets. Table 1 shows the statistic

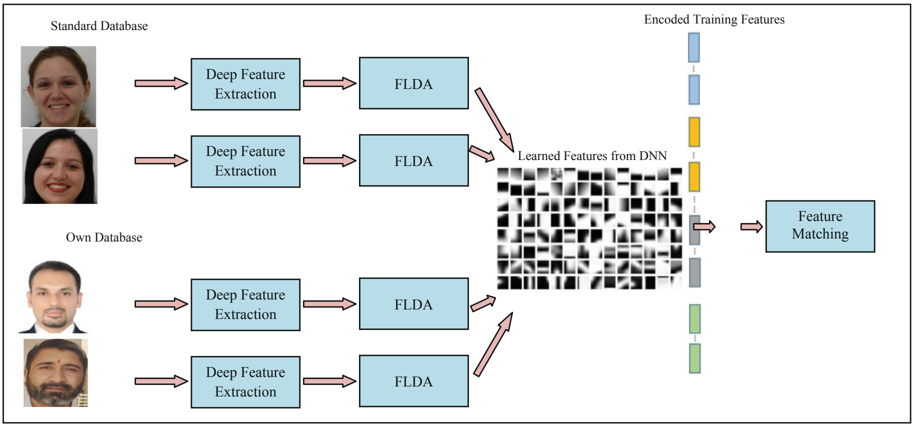


Fig. 4. Testing stage of our proposed methodology on complete face

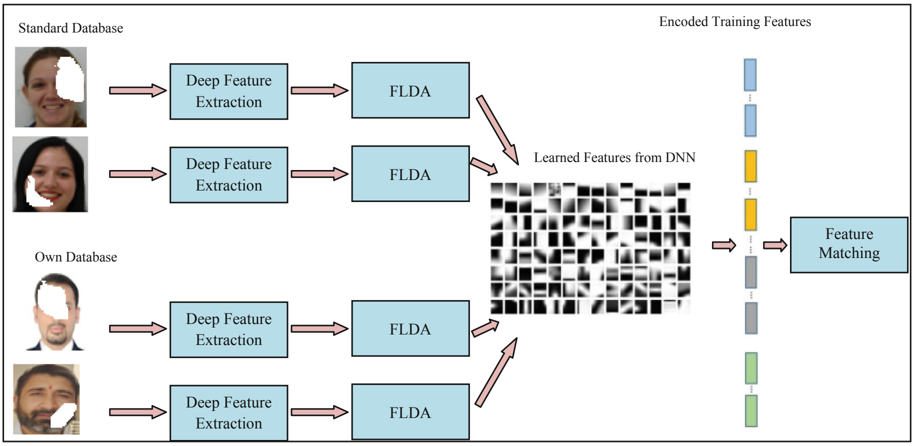


Fig. 5. Testing stage of our proposed methodology on destructive face

comparison of each database with various Database Faces given in [14]. The samples facial images of AT&T dataset are presented in Fig. 1.

Algorithm for Recognizing the Reconstructed Face Image
The methodology adopted in the present work has been depicted below.

Table 1. Statistics for various datasets

Sr. No	Dataset name	No. of person	Total images
1	ATT	40	400
2	ACR	10	282
3	BCB	22	839
4	JBK	65	4009
5	EGO	148	7950
6	RGA	215	12394
7	LLP	264	17602
8	SSB	222	18599
9	FERET	329	3290
10	IIT-Kanpur	40	400

Algorithm1. Recognition algorithm called RRFI

Step1. Read an unknown plant image

Step2. Convert into grayscale image, say R.

Step3. Filter the image using DCT

Step4. Get the Cropping counter, say, n

Step5. Set the counter for Objsel = m

Do while Objsel> 0

Select the Object of Interest (OOI) for each Objsel

Crop the selected object

Scale the Cropped and Selected object using 2D transformation technique (Scaling technique)

Segment the OOI using connected component method

Employ Flood fill algorithm for image rectification

Re-segment the filled object image

Extract the features of the object rectified

And store in the form of face model

Objsel = Objsel - 1

End Do

Step6. Store in a template and map the data with corpus for the classification process and recognition of reconstructed face image using Naïve classification method, SVM, GA.

3 Results and Discussions

In the present work an algorithm is developed for the reconstruction of destructed human face has been represented in the Fig. 3. It represents the original face image and almost all possible combination of destruction in 2d face image. The proposed work is carried out in two parts, in first part destructed face image is read and preprocessing techniques is performed after that segmentation is perform, from segmented face image the mirror image part is crop which is almost similar to the destructed part. After that the face image will be used for recognition and performance is measured as shown in Fig. 4.

Fig. 6. Original picture, Image of Case 1, Image of Case 2, Image of Case 3.

Fig. 7. Image of Case 1, Image of Case 2, Image of Case 3.

The feature clusters used for the identification of behavioral patterns of human face have been drawn by adopting fuzzy c-means clustering and the outcome is visualized in Fig. 12 (Figs. 6 and 7).

False Positive Rate (FPR)
The percentile of cases where an image was segmented to the shape, but in fact it did not.

$$FPR = \frac{FP}{FP + TN} \tag{20}$$

False Negative Rate (FNR)
The percentile of cases where an image was segmented to the shape, but in fact it did.

$$FNR = \frac{FN}{FN + TP} \tag{21}$$

Sensitivity

The sensitivity is defined as the rate of proportions of true positive that are correctly identified. It correlates the ability of the test to obtain positive outcomes.

$$Sensitivity = \frac{NumberofTP}{NumberofTP + NumberofFN} \times 100 \tag{22}$$

Specificity

The specificity is defined as the rate of proportions of true negative that are correctly identified. It correlates the ability of the test to obtain negative outcomes.

$$Specificity = \frac{NumberofTN}{NumberofTN + NumberofFN} \times 100 \tag{23}$$

Accuracy

The weight percentile of pose varied facial images is exactly categorized by measuring the accuracy. It can be expressed as given in Eq. (14) (Figs. 8, 9, 10 and 11 and Table 2).

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \times 100 \tag{24}$$

Table 2. Comparison of accuracy, FPR, FNR, sensitivity and specificity on all standard datasets

Datasets	FPR	FNR	Sensitivity (in %)	Specificity (in %)	Accuracy (in %)
ATT	4.9511	3.9222	97.1888	98.1589	98.9957
ACR	7.5504	10.0836	89.2484	94.7996	95.1185
BCB	7.1283	9.6467	87.9713	96.2767	95.4705
JBK	5.1306	7.1463	93. 3756	95.4134	97.4006
EGO	7.9959	10.191	89.0829	93.2941	94.4491
RGA	6.0173	10.9402	88.0512	94.1127	93.4955
LLP	5.7689	9.7401	84.0111	95.2611	90.1226
SSB	7.9147	8.4565	85.1005	93.2863	91. 1126
FERET	9.2179	8.2678	87.7902	90.7721	90.1939
IITK	4.9852	4.2191	98.1589	97.2597	97.3251

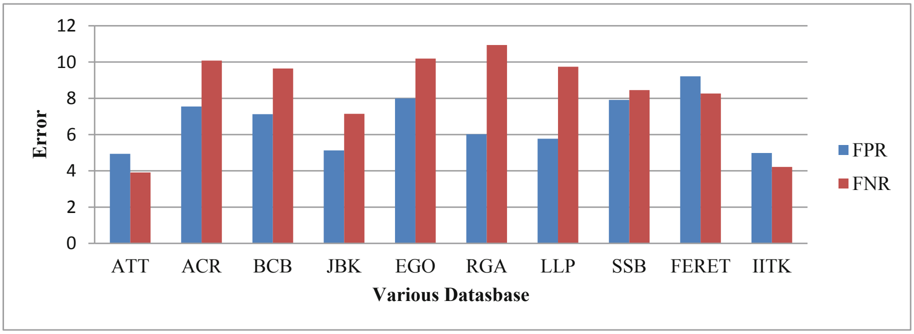


Fig. 8. Comparison of FPR and FNR on various database with proposed methodology

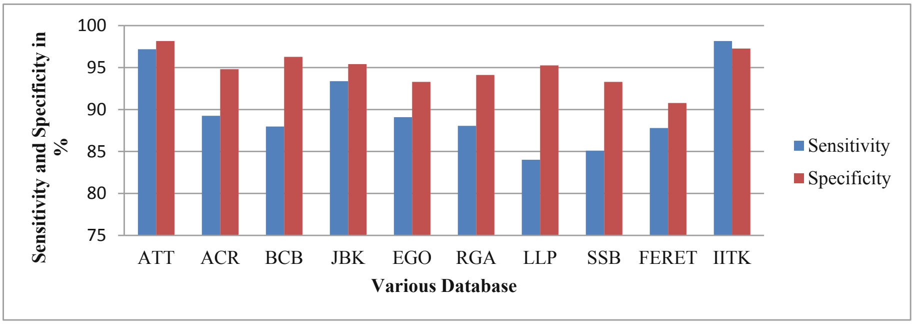


Fig. 9. Comparison of sensitivity and specificity on various databases with proposed methodology

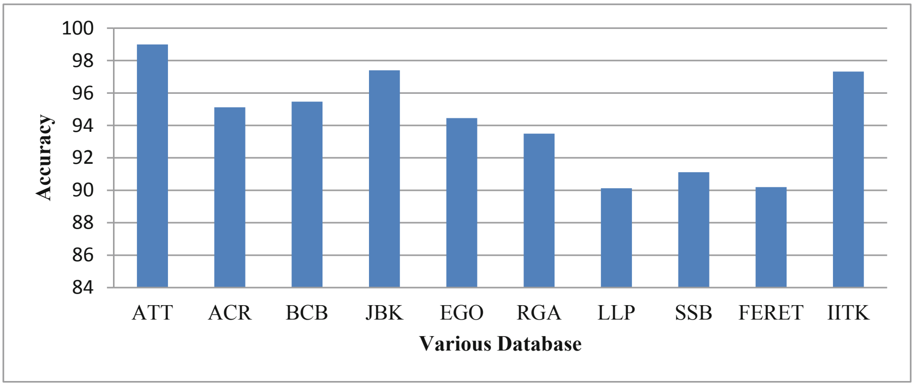


Fig. 10. Comparison of accuracy on various databases with proposed methodology

The Table 3 illustrates the achieved percentage for different methods for different datasets.

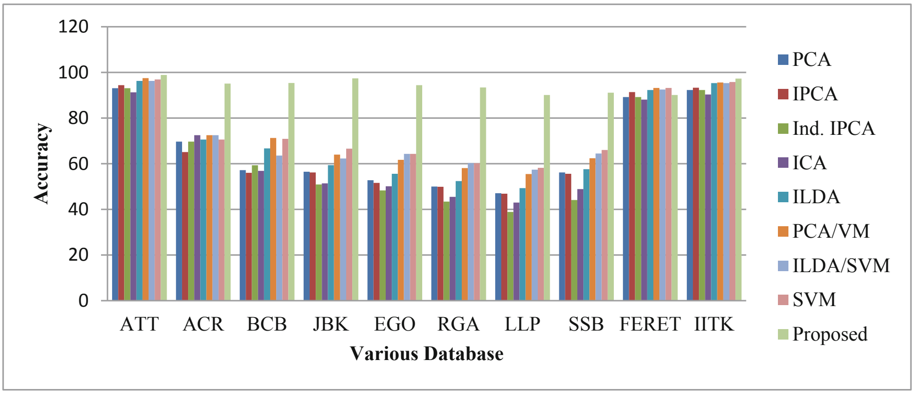


Fig. 11. Comparison of accuracy on various database with different methodology

Table 3. Accurate percent measures of datasets & approaches (in %)

	ATT DB	ACR DB	BCB DB	JBK DB	EGO DB	RGA DB	LLP DB	SSB DB	FERET DB	IITK DB
PCA	94.1	70.7	58.2	57.5	53.8	51.0	48.1	57.2	90.2	93.3
IPCA	95.4	66.1	57.0	57.2	52.6	50.9	47.9	56.6	92.4	94.3
Ind. IPCA	94.1	70.7	60.3	51.9	49.3	44.4	39.9	45.1	90.2	93.3
ICA	92.3	73.5	57.9	52.4	51.1	46.5	42.0	49.9	89.1	91.3
ILDA	97.3	71.6	67.7	60.4	56.6	53.4	50.3	58.6	93.3	96.3
PCA/VM	96.5	73.5	72.3	65.0	62.7	59.1	54.5	63.4	94.2	96.6
ILDA/SVM	95.3	73.5	64.6	63.3	63.3	62.3	58.4	68.5	93.5	96.3
SVM	97.9	71.6	71.9	67.6	65.3	61.2	59.2	67.0	94.2	96.8
Proposed	98.9	95.1	95.4	97.4	94.4	93.4	90.1	91.1	90.1	97.3

4 Conclusion

The present research work we have discussed the results obtained. In this research work knowledge-based model has been formed by considering the relevant features of human face image as case study. After that knowledge-model has been mapped with test reconstructed face image for recognition and classification. From the experimental results, the application of proposed algorithm has been found very satisfactory.

References

1. Yoshiki, K., Saito, H., Mochimaru, M.: Reconstruction of 3D Face model from single shading image based on anatomical database. In: 18th International Conference on Pattern Recognition (ICPR'06), pp. 350–353. Hong Kong (2006). https://doi.org/10.1109/ICPR.2006.982

2. Kemelmacher-Shlizerman, I., Basri, R.: 3D face reconstruction from a single image using a single reference face shape. In: IEEE Transactions on Pattern Analysis and Machine Intelligenc*e*, vol. 33, no. 2, pp. 394–405 (2011 Feb.). https://doi.org/10.1109/TPAMI.2010.63
3. Shengming, W., Hubei "Research of 3D face reconstruction based on one image". In: International Conference on Image Analysis and Signal Processing, pp. 533–537, Hubei (2011). https://doi.org/10.1109/IASP.2011.6109100
4. Bhattacharyya, S., Chakraborty, S.: Reconstruction of human faces from its eigenfaces. In: International Journal of Advanced Research in Computer Science and Software Engineering **4**(1), (2014 January)
5. Vidanapathirana, M., et al.: A novel semi-automated approach for forensic facial reconstruction in Sri Lanka. Galle Medical Journal. **18**(1), 16–25 (2013). https://doi.org/10.4038/gmj.v18i1.5517
6. Raja, R., Sinha, T.S., Dubey, R.P.: Recognition of human-face from side-view using progressive switching pattern and soft-computing technique. Association for the Advancement of Modelling and Simulation Techniques in Enterprises, AMSE Journals 2015 Series **58**(1), 14–34 (2015)
7. Raja, R., Sinha, T.S., Dubey, R.P.: Biometrical authentication of twins from side-view using hybrid approach. (BJSTH) Bharat Journal of Science Technology and Humanities **I**(1), 2015 (2015)
8. Raja, R., Tilendra, S.S., Dubey, R.P.: An empirical analysis for detection of occlusion for face image parallel to the surface plain using soft-computing technique. MATS J. Eng. Appl. Sci. **1**(2), 97–104 (2015). ISSN No. 2394 549
9. Raja, R., Sinha, T.S., Dubey, R.P.: Soft computing and LGXP techniques for ear authentication using progressive switching pattern. Published in International Journal of Engineering and Future Technology **2**(2) (2016)
10. Raja, R., Tilendra, S.S., Dubey, R.P.: Orientation calculation of human face using symbolic techniques and ANFIS. Publ. Int. J. Eng. Future Techn. **7**(7), 37–50 (2016)
11. Kumar, S., Singh, S., Kumar, J.: Live detection of face using machine learning with multi-feature method. Wireless Pers. Commun. **103**(3), 2353–2375 (2018). https://doi.org/10.1007/s11277-018-5913-0
12. Kumar, S., Singh, S., Kumar, J.: Automatic live facial expression detection using genetic algorithm with haar wavelet features and SVM. Wireless Pers. Commun. **103**(3), 2435–2453 (2018). https://doi.org/10.1007/s11277-018-5923-y
13. Soumya, S., Kumar, S.: Health Care Monitoring Based on Internet of Things the (Springer). In: International Conference on Artificial Intelligence & Cognitive Computing (AICC), 2nd -3rd Feb 2018 Hyderabad (Scopus Indexed-Published)
14. Kumar, S., Singh, S., Kumar, J.: A study on face recognition techniques with age and gender classification. In: IEEE International Conference on Computing, Communication and Automation (ICCCA), pp. 1001–1006 (2017 May)
15. Kumar, S., Singh, S., Kumar, J.: A Comparative Study on Face Spoofing Attacks. In: IEEE International Conference on Computing, Communication and Automation (ICCCA), pp. 1104–1108 (2017 May)
16. Kumar, S., Singh, S., Kumar, J.: Gender classification using machine learning with multi-feature method. In: IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). Las Vegas, USA, January 7th-9th (2019)
17. Scholkopf, B., Smola, A., Muller, K.: Nonlinear component analysis as a kernel eigenvalue problem. Proceding of Neural Computation **10**(5), 1299–1319 (1998)
18. Shafiee, S., Kamangar, F., Ghandehari, L.S.: Cluster-based multi-tasking sparse representation for efficient face recognition. IEEE Image Analysis and Interpretation (SSIAI) on 6–8 April at San Diega, CA, pp. 125–128 (2014)

19. Shah, J.D., Patil, S.H.: Biometric authentication based on detection and recognition of multiple face in image. In: the Proceeding of IC-3, pp. 87–95 (2008)
20. Shan, T., Lovell, B.C., Chen, S.: Face recognition robust to head pose from one sample image. In: Proceedings of the 18th IEEE International Conference on Pattern Recognition at Hong Kong **1**, 515–518 (2006). https://doi.org/10.1109/ICPR.2006.527
21. Sharma, A., Haj, M.A., Choi, J., Davis, L.S., Jacobs, D.W.: Robust pose invariant face recognition using coupled latent space discriminant analysis. Elsevier J. Comp. Vision and Image Understa. **116**, 1095–1110 (2012)
22. Shuang, L.: A novel face dectection algorithms based on PCA and adaboost. In: 6th IEEE International Conference on Measuring Technology and Mechantronics Automation on 10–11 Jan at Zhangjjajie, pp. 38–41 (2014)
23. Singh, G., Chhabra, I.: Human face recognition through moment descriptors. In: Proceeding of IEEE RAECS UIET Panjab University Chandigarh on 6–8 may at Chandigarh, pp. 1–6 (2014)
24. Singh, R., Vatsa, M., Ross, A., Noore, A.: A mosaicing scheme for pose-invariant face recognition. IEEE Trans. Syst. Man Cybern. B Cybern. **37**(5), 1212–1225 (2007). https://doi.org/10.1109/TSMCB.2007.903537
25. Singh, R., Vatsa, M., Ross, A., Noore, A.: A Mosaicing scheme for pose - invariant face recognition. IEEE Trans. Sys. Man and Cybernetics **37**(5), 1212–1225 (2007). https://doi.org/10.1109/TSMCB.2007.903537
26. Singh, S.K., Vatsa, M., Singh, R., Shukla, K.K.: A comparative study of various face recognition algorithms (feature based, eigen based, line based, neural network approaches). IEEE International Workshop on Computer Architectures for Machine Perception on 12–16 May at New Orleans LA, pp. 160–171 (2003). https://doi.org/10.1109/CAMP.2003.1598161
27. Sinha, T.S., Patra, R.K., Raja, R.: A Comprehensive analysis of human gait for abnormal foot recognition using Neuro-Genetic approach. Int. J. Tomograp. Statis. (IJTS) **16**(W11), 56–73 (2011). http://ceser.res.in/ceserp/index.php/ijts
28. Siraj, F., Yusoff, N., Kee, L.C.: Emotion classification using neural network. In: International Conference on Computing & Informatics(ICOCI '06) on 6–8 June at Kuala Lampur, pp. 1–7 (2006). https://doi.org/10.1109/ICOCI.2006.5276419
29. Song, Y.J., Chang, U.D., Park, W.B., Ahn, J.H.: Side view face detection using geometrical characteristics of nose and chin in color Image. J. Res. Ins. Comp. Info. Commu. **11**(3), 23–28 (2008)
30. Devireddy, S.K., Siva Nagireddy, K., Ramsaswamy, G., Ravikiran, D., Sireesha, P., Suresh Babu, Y.: A study of unimodel multimodel and soft biometric recognition. IJCSNS int. J. Comp. Sci. Netw. Secur. **8**(8), 36–46 (2008)
31. Suikerbuik, R., Tangelder, H., Daanen, H., Qudenhuijen, A.: Automatic feature detection in 3D human body scans. In: Proceeding of the Conference SAE Digital Human Modeling for design and Engineering (2004)
32. Sun, X., Zhang, Q., Wang. Z.: Face recognition based on NMF and SVM. In: IEEE Second International Symposium on Electronic Commerce and Security on 22–24 May at Nanchang, (ISECS'09.), vol. 1, pp. 616–619 (2009). https://doi.org/10.1109/ISECS.2009.98
33. Takallou, H.M., Kasaei, S.: Multiview face recognition based on Multilinear decomposition and pose manifold. IET image processing **8**(5), 300–309 (2014)
34. Tan X., Chen S., Zhou Z., Liu, J.: Face recognition under occlusions and variant expressions with partial similarity. Ieee Trans. Info. Forensics Secur. **4**(2), 217–230 (2009)
35. Tan, X., Chen, S., Zhou, Z., Zhang, F.: Recognizing partially occluded, expression variant faces from single training image per person with SOM and soft kNN ensemble. Proceedings of IEEE Transaction on Neural Networks **16**, 1–13 (2005)
36. Tan, H., Yang, B., Ma, Z.: Face recognition based on the fusion of global and local HOG features of the face images. IET comput. **8**(3), 224–234 (2014)

37. Tan, N., Huang, L., Liu, C.: Face recognition based on a single image and local binary pattern. In: International Symposium on Intelligent Information Technology Application,(IITA) on 20–22 Dec at Shanghai, vol. 2, pp. 366–370 (2008). https://doi.org/10.1109/IITA.2008.332
38. Tanaka, H.T., Ikeda, M., Chiaki, H.: Curvature-based face surface recognition using spherical correlation. In: Proceedings 3rd IEEE International Conference on Principal directions for curved object recognition, Automatic Face and Gesture Recognition on 14–16 Apr., pp. 372–377 (1998). https://doi.org/10.1109/AFGR.1998.670977
39. Tenenbaum, J.B.D., Silva, V., Langford, J.C.: A global geometric framework for nonlinear dimensionality reduction. Science Magazine **290**, 2319–2323 (2000)
40. Terzopoulos, D., Waters, K.: Analysis and synthesis of facial image sequences using physical and anatomical models. IEEE Trans. Pattern Anal. Mach. Intell. **15**(6), 5690–6579 (1993). https://doi.org/10.1109/34.216726
41. Jangir, S.K., Joshi, N., Kumar, M., Choubey, D.K., Singh, S., Verma, M.: Functional link convolutional neuralnetwork for the classification of diabetes mellitus. International Journal for Numerical Methods in Biomedical Engineering, e3496 (2021)
42. Choubey, D.K., Tripathi, S., Kumar, P., Shukla, V., Dhandhania, V.K.: Classification of diabetes by kernelm based SVM with PSO. Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science) **14**(4), 1242–1255 (2021)
43. Choubey, D.K., Paul, S.: GA_MLP NN: a hybrid intelligent system for diabetes disease diagnosis. Int. J. Intelli. Sys. Appl. **8**(1), 49 (2016)
44. Choubey, D.K., Kumar, M., Shukla, V., Tripathi, S., Dhandhania, V.K.: Comparative analysis of classification methods with PCA and LDA for diabetes. Curr. Diabetes Rev. **16**(8), 833–850 (2020)
45. Choubey, D.K., Kumar, P., Tripathi, S., Kumar, S.: Performance evaluation of classification methods with PCA and PSO for diabetes. Netw. Model. Analy. Health Info. Bioinforma. **9**(1), 1–30 (2019). https://doi.org/10.1007/s13721-019-0210-8
46. Choubey, D.K., Paul, S., Dhandhenia, V.K.: Rule based diagnosis system for diabetes. An Int. J. Medi. Sci. **28**(12), 5196–5208 (2017)
47. Choubey, D.K., Paul, S.: GA_RBF NN: a classification system for diabetes. Int. J. Biomed. Eng. Technol. **23**(1), 71–93 (2017)
48. Choubey, D.K., Paul, S.: Classification techniques for diagnosis of diabetes: a review. Int. J. Biomed. Eng. Technol. **21**(1), 15–39 (2016)

MoRec: User's Definition Inspired Analytical Approach for Movie Recommendation

Padmini Yadav[1], Venkatesh Gauri Shankar[2](✉), Bali Devi[3], Neha V. Sharma[2], and Anmol Srivastava[2]

[1] Data Science and Engineering, Manipal University Jaipur, Jaipur, Rajasthan, India
[2] Information Technology, Manipal University Jaipur, Jaipur, Rajasthan, India
venkateshgaurishankar@gmail.com
[3] Computer Science and Engineering, Manipal University Jaipur, Jaipur, Rajasthan, India

Abstract. As of 2020, streaming service giant Netflix has 204 million subscribers. Data experts suggest that Netflix users will spend just 60–90 s browsing and reviewing 10 to 20 titles before finally deciding upon watching content or not. In continuation, a robust recommender system is required to produce user definition-inspired analytics. This paper aims to derive analytical conclusions about cinema data and recommend movies to the user based on their specifications. The problem statement at hand is promptly getting a list of movies to watch next from a dataset of 45,000+ movies. The methods used for analyzing the metadata in cinema are implemented through Python libraries. For building the machine learning model that recommends movies, Natural Language Processing and other relevant statistical/programming like Regular Expression, similarity methods, etc., have been used. The key result of the paper is building a "Content-based recommendation system" based on the user's definition of similarity.

Keywords: Machine learning · Natural Language Processing (NLP) · Content-based filtering system · Term Frequency-Inverse Document Frequency (TF-IDF) · Cosine-similarity

1 Introduction

Thousands of movies are available for viewers to watch. Often users want to watch a specific type of content. This recommendation system makes it possible for users to find movies based on their definition of similarity [5–7]. Netflix, the world's largest streaming service, has 204 million customers as of 2020. According to data specialists, Netflix customers will spend just 60–90 s exploring and reviewing ten to twenty items before choosing whether to watch them. This makes it very important for the recommendation system to be excellent for the streaming service's success. Netflix's recommendation system accounts for 80 percent of the hours watched on it in total. The rest comes from the user's search function. Thus, the importance of a good recommendation algorithm is utmost [2–4].

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 381–396, 2023.
https://doi.org/10.1007/978-3-031-13150-9_31

A recommendation system is like a simple input-process-output engine [25]. It takes a few parameters as input, reads and processes them, and formulates a list of recommendations. In most programming languages, this is done by creating a method or function that takes inputs and churns out a list of outputs or recommendations in a befitting context. How the recommendations are produced could range from a statistical method being applied to the inputs, using machine learning algorithms on it, or something entirely different. Now, content-based filtering for recommendation is a method that finds similarity patterns in a given user's history. Here, The user has suggested items based on what he has liked in the past. Our engine is also primarily a content-based filtering system.

2 Key Contribution

The key contributions of our work are as follows:

- The objective is to build a recommendation system that asks the user to specify the basis of their recommendation (given actor, similar overview, best in the genre, etc.).
- A robust approach with user's definition inspired analytical approach for movie recommendation

3 Literature Review

The previous works cited on the topic tackle only model-building using Machine Learning. Our work extends the same into the filter-based search engine and can be further modeled to have more interactive filters [17, 18, 20–22]. Similar works have used Natural Language Processing (NLP) methods like CountVectroizer and Word2Vec to create a similarity matrix. SVM models have also dealt with vectorized movie overviews [8–10]. Most research has also tried to tackle the problem of keyword weights by tweaking features of the Tf-IdfVectorizer itself. Further, hybrids of collaborative filtering and content-based filtering have been built [16, 19, 23, 24]. These allow movies to be recommended based on other similar users' viewing AND based on similar content. Some larger-scale projects store the user's watch history to find patterns in their liking to improve future recommendations [11–13]. Classification algorithms have been used as well. They primarily help define if the recommended movies are similar or have been falsely labeled (due to lack of definition of scope within which two movies can be called 'similar' [14, 15].

4 Material and Method

The data used for the recommendation is mainly secondary data. The data has been fetched from various online portals and presented formally in the MovieLens dataset. User validation of the model can be taken via an experience survey which can be presented at the exit point of the program.

This third-party dataset consists of the movie title, runtime, production details, budget, revenue generated, original language, genres, cast, crew, overview, tagline, vote count (for its review), popularity, vote average (from voters), and censor rating. These files contain metadata for all 45,000 movies listed in the Full MovieLens Dataset [1]. The data contains a feature called 'movie overview,' which has an average length of 317 characters. It is a short description of the premise of the movie. The sample description of the dataset is given in Fig. 1.

```
MOVIE NAME:- NIXON
MOBIE OVERVIEW:- An all-star cast powers this epic look at American President Richard M. Nixon, a man carrying the fa
te of the world on his shoulders while battling the self-destructive demands within. Spanning his troubled boyhood in
California to the shocking Watergate scandal that would end his presidency.
*************************************************************************************************
MOVIE NAME:- STAR TREK II: THE WRATH OF KHAN
MOBIE OVERVIEW:- Admiral James T. Kirk is feeling old; the prospect of accompanying his old ship the Enterprise on a
two week cadet cruise is not making him feel any younger. But the training cruise becomes a a life or death struggle
when Khan escapes from years of exile and captures the power of creation itself.
*************************************************************************************************
MOVIE NAME:- ROCKY
MOBIE OVERVIEW:- When world heavyweight boxing champion, Apollo Creed wants to give an unknown fighter a shot at the
title as a publicity stunt, his handlers choose palooka Rocky Balboa, an uneducated collector for a Philadelphia loan
shark. Rocky teams up with trainer  Mickey Goldmill to make the most of this once in a lifetime break.
```

Fig. 1. Sample data description

Movie Overview is an excellent metric to define 'similar' movies since it quantifies how similar plots (and often genres) of any pair of movies are. In order to have a numeric description of similarity between two movies (movie overviews), the following steps are followed:

1 Take movie overview as input and output a sparse matrix for it by vectorizing the 'overview' using the 'Term frequency-inverse document frequency' (TF-IDF) statistic (from sklearn.feature_extraction.text = > TfidfVectorizer) (Fig. 2, Fig. 3).

$$w_{i,j} = tf_{i,j} \times \log\left(\frac{N}{df_i}\right)$$

$tf_{i,j}$ = number of occurrences of i in j
df_i = number of documents containing i
N = total number of documents

Fig. 2. TF-IDF formula

Each row of the sparse matrix can be considered as a vector (number of words in text overall = dimensions of the vector = Z. Each term is a value of the kth dimension where k ∈ [0, Z]).

The sparse matrix gives insight into how many keywords from 2 different movie overviews are the same and how much 'weight' they carry in the overviews. The closer the vectors in Z-dimensional space, the more similar the overviews. The algorithm finds cosine similarity between the vectorized format of the dataset feature "movie description." Each vector is stored in a table which is referred to as a sparse matrix. Following is an example of 3 sentences being converted to a sparse matrix.

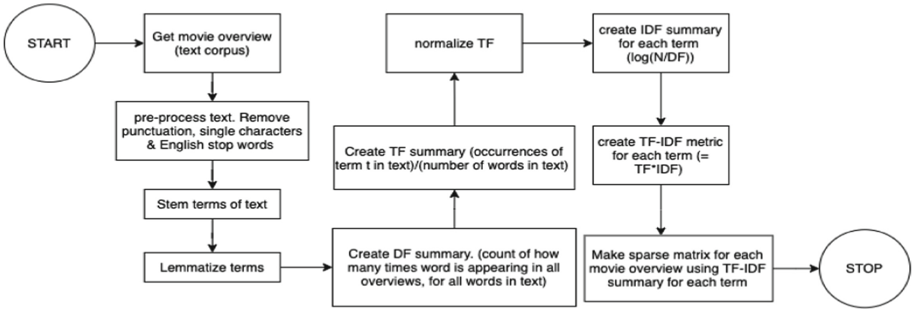


Fig. 3. Flow chart to convert 'movie overview' to TF-IDF sparse matrix

good movie
not a good movie
did not like

good	movie	not	a	did	like
1	1	0	0	0	0
1	1	1	1	0	0
0	0	1	0	1	1

Fig. 4. Converted sparse matrix

Similarly, the 'overview' parameter for all movies is converted to a sparse matrix (Fig. 4).

Now, the pairwise cosine similarity (from sklearn.metrics.pairwise = > cosine_similarity) is found between all vectors in order to find movies that have the most similar overviews (or overview vectors) (Fig. 5, Fig. 6, Fig. 7).

$$similarity(A,B) = \frac{A \cdot B}{\|A\| \times \|B\|} = \frac{\sum_{i=1}^{n} A_i \times B_i}{\sqrt{\sum_{i=1}^{n} A_i^2} \times \sqrt{\sum_{i=1}^{n} B_i^2}}$$

Fig. 5. Cosine similarity formula

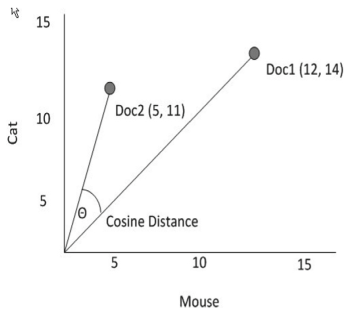


Fig. 6. Cosine distance

At the end of this step, we have a numeric summary of similarities between any given pair of movies. Higher the cosine-similarity value, more like the movies. Each element i of the cosine-similarity matrix is a list containing cosine-similarity scores of an ith movie with all other movies. In order to get the most similar movies, the list of the given movie can be sorted in descending order.

```
array([[1.        , 0.00566113, 0.        , ..., 0.        , 0.00250477,
        0.        ],
       [0.00566113, 1.        , 0.01457717, ..., 0.01967902, 0.00786262,
        0.00308481],
       [0.        , 0.01457717, 1.        , ..., 0.        , 0.0049893 ,
        0.        ],
       ...,
       [0.        , 0.01967902, 0.        , ..., 1.        , 0.        ,
        0.        ],
       [0.00250477, 0.00786262, 0.0049893 , ..., 0.        , 1.        ,
        0.        ],
       [0.        , 0.00308481, 0.        , ..., 0.        , 0.        ,
        1.        ]])
```

Fig. 7. Cosine – similarity matrix for each movie with every other movie

```
MOVIE NAME:  TOY STORY
SIMILARITY SCORES - TOP 10 SCORES:
[0.23975131556999332, 0.22894701329715916, 0.11548116554127433, 0.11154595749232298, 0.10656567097446677, 0.092153314
68150254, 0.0891414300481215З, 0.08439907504604399, 0.08269048947452533, 0.0697077466767437]
**************************************************************************************************
MOVIE NAME:  PLATOON
SIMILARITY SCORES - TOP 10 SCORES:
[0.09589306201299465, 0.09260721756270975, 0.08499473634569936, 0.08381296060408461, 0.07450063482573344, 0.071044546
22877292, 0.05785873995733123, 0.05564412891380726, 0.05459282905327572, 0.05352387933124722]
**************************************************************************************************
MOVIE NAME:  SCARLET DIVA
SIMILARITY SCORES - TOP 10 SCORES:
[0.1238458233599887, 0.10687742834149315, 0.09687934113807099, 0.0945816147905297, 0.09177686743499208, 0.09077296232
184544, 0.08682331472252709, 0.08636288326654627, 0.08375359084247466, 0.08180172319561367]
```

2. Fetching movies that have a similar overview to the given movie (input from the user is the movie's name) (Fig. 8)

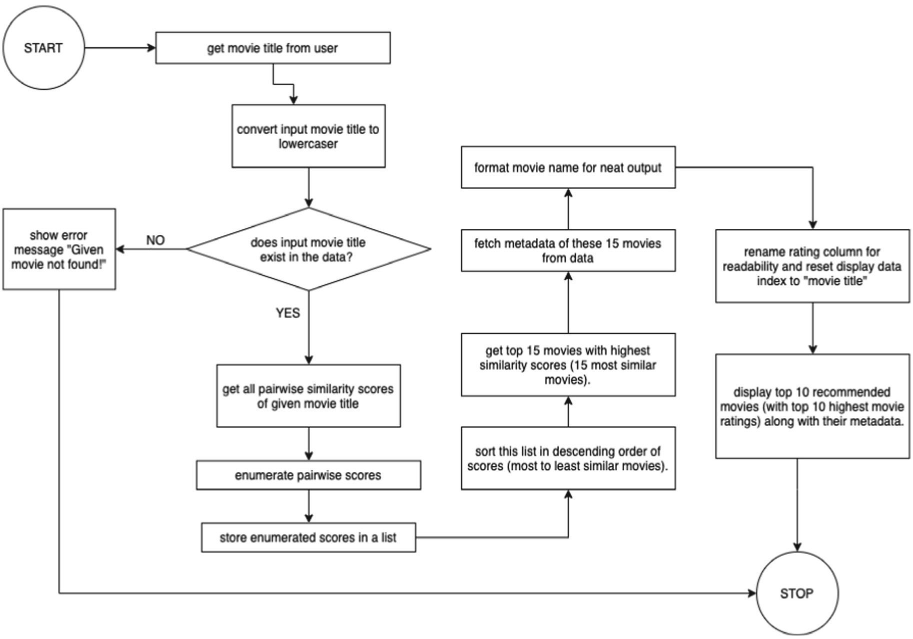


Fig. 8. Flow Chart of fetching movies that have a similar overview

3. A regex function is used to perform queries on data features. The user can enter the basis on which they want a list of movies. The recommendation can be movies with given crew members, movies with cast members, movies made in the given language, and movies of a given genre. Flowchart for ‘cast member search’ (Fig. 9).

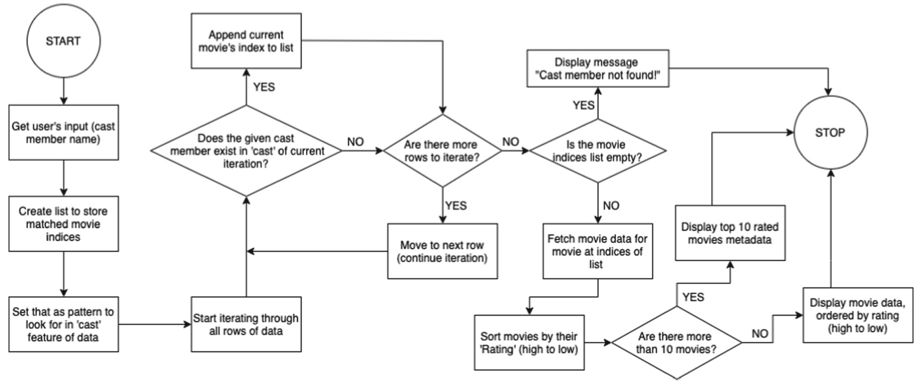


Fig. 9. Flow Chart of logic is used for crew/language/genre filters

The novelty of the given approach is how it lets the user define what they mean by “similar.“ Current models assume that the user would almost always want to watch movies similar to his history. However, this poses a problem since the user no longer has control over his recommendations. Our technique simplifies the process by asking the user on what basis he wants the similarity, and subsequently, to provide a movie/movie metric he liked. Therefore, in comparison to existing models, our approach gives out a simpler yet equally elegant methodology for movie recommendation.

5 Results

The model successfully delivers a framework that takes the user input and delivers a recommendation summary list based on their specification. The front end, which is a menu-driven program, follows the flow as:

1. Display menu so that users can specify what type of recommendations they want (Fig. 10)

```
ON WHAT BASIS DO YOU WANT A RECCOMENDATION?
1. Similar overview
2. Top movies from select language
3. Top movies by given actor
4. Top movies by given crew member (director, producer etc.)
5. Top movies from given genre
ENTER CHOICE NUMBER:
```

Fig. 10. Menu presented at the entry to user that asks user to specify their definition of similarity

The user can specify what sort of recommendation he wants. Option numbers 1 to 5 lay out the options available to the user to base his definition of similarity. He can then enter the option number to get started with the specific recommendation type. For example, he should enter '1' in 'ENTER CHOICE NUMBER' to get movies with a similar overview.

2. After users enter their choice code from the menu, they are directed to the suitable function that asks for further selection and gives out the recommendations.

```
**********MOVIE RECCOMMENDATION SYSTEM*************

ON WHAT BASIS DO YOU WANT A RECCOMENDATION?
1. Similar overview
2. Top movies from select language
3. Top movies by given actor
4. Top movies by given crew member (director, producer etc.)
5. Top movies from given genre
ENTER CHOICE NUMBER:1
Reccommend movies similar in story with: REPLicanT

====RECCOMMENDATION SUMMARY====

THE WAR GAME  -  Drama, War, Documentary  -  5.7 / 10 rating
OVERVIEW:  The War Game is a fictional, worst-case-scenario docudrama about nuclear war and its aftermath in and arou
nd a typical English city. Although it won an Oscar for Best Documentary, it is fiction. It was intended as an hour-l
ong program to air on BBC 1, but it was deemed too intense and violent to broadcast. It went to theatrical distributi
on as a feature film instead. Low-budget and shot on location, it strives for and achieves convincing and unflinching
realism.

*****************************************************************************************************

LONG WAY ROUND  -  Documentary, Adventure  -  5.7 / 10 rating
OVERVIEW:  This documentary series follows actors Ewan McGregor and Charley Boorman on a motorcycle trip around the w
orld. The two friends will travel through such places as Siberia, Kazakhstan, Mongolia, and Alaska, before finally en
ding the journey in New York. The filming will be done by on board cameras and one ride along cameraman.

*****************************************************************************************************

WIT  -  Drama  -  5.7 / 10 rating
OVERVIEW:  A renowned professor is forced to reassess her life when she is diagnosed with terminal ovarian cancer.

*****************************************************************************************************

MY LIFE  -  Drama, Romance  -  5.6 / 10 rating
OVERVIEW:  It seems that Bob Jones has everything a man could want, namely a fulfilling job and a beautiful, pregnant
wife, Gail. But Bob's life is turned upside-down when he is diagnosed with cancer and given four months to live -- no
t even enough time to see his first child's birth. To cleanse himself of demons in his remaining days, Bob makes a vi
deo diary, hoping to pass along some wisdom to his future child. Along the way, he discovers a lot about himself.

*****************************************************************************************************

GOD SAID, 'HA!'  -  Comedy  -  5.6 / 10 rating
OVERVIEW:  Julia Sweeney tells the viewers the monologue about the hard time in her life when her brother fought with
cancer and she was also diagnosed with a rare form of cancer.

*****************************************************************************************************

THE GRASSHOPPER  -  Romance, Drama  -  5.6 / 10 rating
OVERVIEW:  A British Columbia teenager dreams of show business but winds up as a call girl in Las Vegas.

*****************************************************************************************************

THE WORK AND THE GLORY III: A HOUSE DIVIDED  -  Drama  -  5.6 / 10 rating
OVERVIEW:  Joshua Steed returns to Missouri a wealthy man with a beautiful wife; however, the past has a way of catch
ing up. Soon Joshua is tangled in a web of rumors, deception and betrayal that threatens to tear his family apart. Ba
ck in Kirtland, financial trouble riddles the foundations of the fledgling Church causing a division, and questioning
of the Prophet Joseph Smith's divine calling. Has he lost his prophetic gift? Hundreds of Saints immigrate to Missour
i, where Governor Boggs raises an army - with Joshua at its head - to address the "Mormon Problem." When the militia
receives orders to attack the Mormon settlement, only Joshua can save his family from the gathering mob.

*****************************************************************************************************

QUINCY JONES: BURNING THE LIGHT  -  Comedy  -  5.6 / 10 rating
OVERVIEW:  This solo, one-hour, stand-up show is the culmination of a dream made public on The Ellen Degeneres Show a
fter Jones was diagnosed with cancer.

*****************************************************************************************************

MOTHER LODE  -  Adventure, Action, Thriller  -  5.6 / 10 rating
OVERVIEW:  A couple of youngish adventurers go into the wilderness of British Columbia in search of a lost colleague.
Their plane crashes and they find themselves at the mercy of a crazed old Scottish miner, who has lived in isolation
for many decades searching the mountain caves for a chamber of long lost gold. He is prepared to do anything - includ
ing murder - to keep his gold for himself.

*****************************************************************************************************

CRAZY SEXY CANCER  -  Documentary  -  5.6 / 10 rating
OVERVIEW:  Just weeks after being diagnosed with a rare and incurable form of cancer, 31-year-old actress Kris Carr t
urned the camera on herself as she embarked on the fight of her life. The result is this moving and funny inspiration
al documentary. In need of experimental treatment, Carr travels the country seeking experts on alternative medicine a
nd, along the way, meets other cancer-stricken women driven to survive.

*****************************************************************************************************
```

Fig. 11. Result for similar movies to the input movie 'Replicant.'

Now, about Fig. 11, the user has chosen option '1,' i.e., he wants movies with a similar plot to the movie he enters. Next, the program asks him to specify 'recommend movies similar in plot to:' He enters the desired movie name, 'Replicant.' Now, the program churns out a list of 10 movie recommendations. The output contains the recommended movie's name, genre, IMDb rating, and a short movie overview.

3. Recommendation based on similar overviews

Figure 12 showcases another list of recommendations produced when users want movies similar to 'Heavyweights' in the plot.

4. Recommendation based on selected cast member

As for Fig. 13, the user has chosen option '3,' i.e., he wants movies with a similar cast to the movie he enters. Next, the program asks him to specify 'cast member(s)' to which he enters the desired actor's name, which in this case is 'uma thurman.' The program churns out a list of 10 movies with 'uma thurman' in them. The output contains the recommended movie's name, genre, IMDb rating, and a short movie overview.

5. Recommendation based on selected crew member

As for Fig. 14, the user has chosen option '4,' i.e., he wants movies with a similar crew to the movie he enters. Next, the program asks him to specify 'crew member(s)' to which he enters the desired crew member's name, which is 'stanley kubrik'. Now, the program churns out a list of 10 movies with 'stanley kubrik' as part of their crew. The output contains the recommended movie's name, genre, IMDb rating, and a short movie overview.

6. Recommendation based on a selected genre

As for Fig. 15, the user has chosen option '5,' i.e., he wants the best movies from the given genre. Next, the program asks him to specify the genre he enters 'drama.' Now, the program churns out a list of 10 movies with the highest rating in the given genre, sorted in descending order to rating. The output contains the recommended movie's name, genre, IMDb rating, and a short movie overview.

```
**********MOVIE RECCOMMENDATION SYSTEM*************

ON WHAT BASIS DO YOU WANT A RECCOMENDATION?
1. Similar overview
2. Top movies from select language
3. Top movies by given actor
4. Top movies by given crew member (director, producer etc.)
5. Top movies from given genre
ENTER CHOICE NUMBER:1
Reccommend movies similar in story with: heavyweights

====RECCOMMENDATION SUMMARY====

CAMP ROCK 2: THE FINAL JAM  -  Comedy, Music  -  5.7 / 10 rating
OVERVIEW:  Mitchie can't wait to go back to Camp Rock and spend the summer making new music with her friends and supe
rstar Shane Gray. But the slick new camp across the lake, Camp Star, has drummed up some serious competition — featur
ing newcomers Luke (Matthew "Mdot" Finley) and Dana (Chloe Bridges). In a sensational battle of the bands, with Camp
Rock's future at stake, will Camp Star's flashy production and over-the-top antics win out, or will Camp Rockers prov
e that music, teamwork, and spirit are what truly matter?

****************************************************************************************************

SCOOBY-DOO! CAMP SCARE  -  Animation, Comedy, Family  -  5.7 / 10 rating
OVERVIEW:  Scooby and the gang experience outdoor fun as they go back to Fred's old summer camp.

****************************************************************************************************

RACE FOR YOUR LIFE, CHARLIE BROWN  -  Animation  -  5.6 / 10 rating
OVERVIEW:  The Peanuts gang, including Snoopy and Woodstock, have gone off to summer camp. After a few days of the us
ual summer-camp activities, they all take part in a rafting race. Battling treacherous rapids, wild animals, and bull
ies from a rival camp, the teams make their way downriver to the finish line.

****************************************************************************************************

INDIAN SUMMER  -  Comedy, Drama  -  5.6 / 10 rating
OVERVIEW:  A group of childhood friends, now in their thirties, reunite at Camp Tamakwa. Only a few of the original c
ampers show up, but they still have a good time reminiscing. The people share experiences and grow while at the camp.
They are dismayed to discover that the camp's owner, Unca Lou, is going to close the camp down.

****************************************************************************************************

KISS AT PINE LAKE  -  Romance  -  5.6 / 10 rating
OVERVIEW:  A boy and a girl fall in love during summer camp and promise to stay in touch, but they don't. Fifteen yea
rs later they meet again in the same camp under very different circumstances. What will happen to the camp and will t
hey try again?

****************************************************************************************************

ADULT CAMP  -  Comedy  -  5.6 / 10 rating
OVERVIEW:  Adult Camp is a comedy about the bumpy road to personal growth. A group of men and women, strangers to eac
h other, choose to spend a different kind of summer holiday week by traveling to the beautiful Turku archipelago to p
articipate in an inviting, upgraded version of an adult camp. When they discover that the galloping horses from the c
amp's sales video are just symbols of a free mind, and the guru of the camp takes off to witness his dog in labour, t
he participants are forced to examine themselves and each other to find the necessary elements for growth. Perhaps th
e camp doesn't fulfill its promise of the "most wonderful week of your life", but one thing's for sure - no one retur
ns home the same.

****************************************************************************************************

PARTY CAMP  -    -  5.6 / 10 rating
OVERVIEW:  A teenage boy takes a job as a counselor at a summer camp. He finds that the camp is run like a military t
raining camp, and he resolves to turn it into Party Central.

****************************************************************************************************

PINBALL SUMMER  -  Comedy  -  5.6 / 10 rating
OVERVIEW:  It's a summer of fun for two teenaged boys who spend their time chasing two sisters, annoying a biker gan
g, and basically getting into typical sophomoric hijinks whenever they can.

****************************************************************************************************

BAIGNADE EN MER  -  Documentary  -  5.6 / 10 rating
OVERVIEW:  Several little boys run along a pier, then jump into the ocean.

****************************************************************************************************

SUMMER CAMP  -  Comedy  -  5.6 / 10 rating
OVERVIEW:  The director of a failing summer camp decides to invite campers from ten years ago for a free weekend even
t, hoping that he can trick them into fixing up the place and also get their families to provide them some financial
support. The boys and girls return to the camp and play pranks on each other and try to score with the other campers
and the staff.

****************************************************************************************************
```

Fig. 12. Result for similar movies to the input movie 'Heavyweights'

```
**********MOVIE RECCOMMENDATION SYSTEM*************


ON WHAT BASIS DO YOU WANT A RECCOMENDATION?
1. Similar overview
2. Top movies from select language
3. Top movies by given actor
4. Top movies by given crew member (director, producer etc.)
5. Top movies from given genre
ENTER CHOICE NUMBER:3
Enter cast member name (only 1 name allowed): uma thurman

====RECCOMMENDATION SUMMARY====

PULP FICTION  -  Thriller, Crime  -  8.1 / 10 rating
OVERVIEW:  A burger-loving hit man, his philosophical partner, a drug-addled gangster's moll and a washed-up boxer co
nverge in this sprawling, comedic crime caper. Their adventures unfurl in three stories that ingeniously trip back an
d forth in time.

****************************************************************************************************

KILL BILL: VOL. 1  -  Action, Crime  -  7.4 / 10 rating
OVERVIEW:  An assassin is shot at the altar by her ruthless employer, Bill and other members of their assassination c
ircle – but 'The Bride' lives to plot her vengeance. Setting out for some payback, she makes a death list and hunts d
own those who wronged her, saving Bill for last.

****************************************************************************************************

KILL BILL: VOL. 2  -  Action, Crime, Thriller  -  7.4 / 10 rating
OVERVIEW:  The Bride unwaveringly continues on her roaring rampage of revenge against the band of assassins who had t
ried to kill her and her unborn child. She visits each of her former associates one-by-one, checking off the victims
on her Death List Five until there's nothing left to do … but kill Bill.

****************************************************************************************************

GATTACA  -  Thriller, Mystery, Romance  -  6.9 / 10 rating
OVERVIEW:  Science fiction drama about a future society in the era of indefinite eugenics where humans are set on a l
ife course depending on their DNA. The young Vincent Freeman is born with a condition that would prevent him from spa
ce travel, yet he is determined to infiltrate the GATTACA space program.

****************************************************************************************************

NYMPHOMANIAC: VOL. II  -  Drama, Mystery  -  6.1 / 10 rating
OVERVIEW:  The continuation of Joe's sexually dictated life delves into the darker aspects of her adult life and what
led to her being in Seligman's care.

****************************************************************************************************

BURNT  -  Drama  -  6.0 / 10 rating
OVERVIEW:  Adam Jones is a Chef who destroyed his career with drugs and diva behavior. He cleans up and returns to Lo
ndon, determined to redeem himself by spearheading a top restaurant that can gain three Michelin stars.

****************************************************************************************************

DANGEROUS LIAISONS  -  Drama, Romance  -  6.0 / 10 rating
OVERVIEW:  Dangerous Liaisons is the film based on the novel of the same name by Choderlos de Laclos set in 18th cent
ury France. Marquise de Merteuil's asks her ex-lover Vicomte de Valmont to seduce the future wife of another ex-lover
of hers in return for one last night with her. Yet things don't go as planned in this love triangle drama.

****************************************************************************************************

PERCY JACKSON & THE OLYMPIANS: THE LIGHTNING THIEF  -  Adventure, Fantasy, Family  -  5.9 / 10 rating
OVERVIEW:  Accident prone teenager, Percy discovers he's actually a demi-God, the son of Poseidon, and he is needed w
hen Zeus' lightning is stolen. Percy must master his new found skills in order to prevent a war between the Gods that
could devastate the entire world.

****************************************************************************************************

THE ADVENTURES OF BARON MUNCHAUSEN  -  Action, Adventure, Comedy, Fantasy  -  5.9 / 10 rating
OVERVIEW:  An account of Baron Munchausen's supposed travels and fantastical experiences with his band of misfits.

****************************************************************************************************

LES MISÉRABLES  -  Crime, Drama, History, Romance  -  5.9 / 10 rating
OVERVIEW:  Jean Valjean, a Frenchman imprisoned for stealing bread, must flee a police officer named Javert. The purs
uit consumes both men's lives, and soon Valjean finds himself in the midst of the student revolutions in France.
```

Fig. 13. Result for similar movies based on the same cast.

6 Discussion

The user can select one basis of the same above recommendation.

- Recommendations with an overview similar to a given movie
- Recommendations of top movies in a given language

```
**********MOVIE RECCOMMENDATION SYSTEM*************


ON WHAT BASIS DO YOU WANT A RECCOMENDATION?
1. Similar overview
2. Top movies from select language
3. Top movies by given actor
4. Top movies by given crew member (director, producer etc.)
5. Top movies from given genre
ENTER CHOICE NUMBER:4
Enter crew member name (only 1 name allowed): stanley kubrick

====RECCOMMENDATION SUMMARY====

THE SHINING  -  Horror, Thriller  -  7.7 / 10 rating
OVERVIEW:  Jack Torrance accepts a caretaker job at the Overlook Hotel, where he, along with his wife Wendy and their
son Danny, must live isolated from the rest of the world for the winter. But they aren't prepared for the madness tha
t lurks within.

****************************************************************************************************

A CLOCKWORK ORANGE  -  Drama  -  7.5 / 10 rating
OVERVIEW:  Demonic gang-leader Alex goes on the spree of rape, mugging and murder with his pack of "droogs". But he's
a boy who also likes Beethoven's Ninth and a bit of "the old in-out, in-out". He later finds himself at the mercy of
the state and its brainwashing experiment designed to take violence off the streets.

****************************************************************************************************

2001: A SPACE ODYSSEY  -  Mystery, Adventure  -  7.4 / 10 rating
OVERVIEW:  Humanity finds a mysterious object buried beneath the lunar surface and sets off to find its origins with
the help of HAL 9000, the world's most advanced super computer.

****************************************************************************************************

FULL METAL JACKET  -  Drama, War  -  7.4 / 10 rating
OVERVIEW:  A pragmatic U.S. Marine observes the dehumanizing effects the U.S.-Vietnam War has on his fellow recruits
from their brutal boot camp training to the bloody street fighting in Hue.

****************************************************************************************************

DR. STRANGELOVE OR: HOW I LEARNED TO STOP WORRYING AND LOVE THE BOMB  -  Drama, Comedy, War  -  7.2 / 10 rating
OVERVIEW:  Insane General Jack D. Ripper initiates a nuclear strike on the Soviet Union. As soon as the actions of Ge
neral "Buck" Turgidson are discovered, a war room full of politicians, generals and a Russian diplomat all franticall
y try to stop the nuclear strike. Near the end is a scene that is probably the most uniquely unforgettable performanc
e of Slim Pickens in his movie career. Peter Sellers plays multiple roles in this film.

****************************************************************************************************

PATHS OF GLORY  -  Drama, War  -  6.7 / 10 rating
OVERVIEW:  During World War I, commanding officer General Broulard (Adolphe Menjou) orders his subordinate, General M
ireau (George Macready), to attack a German trench position, offering a promotion as an incentive. Though the mission
is foolhardy to the point of suicide, Mireau commands his own subordinate, Colonel Dax (Kirk Douglas), to plan the at
tack. When it ends in disaster, General Mireau demands the court-martial of three random soldiers in order to save fa
ce.

****************************************************************************************************

EYES WIDE SHUT  -  Mystery, Drama  -  6.5 / 10 rating
OVERVIEW:  After Dr. Bill Hartford's wife, Alice, admits to having sexual fantasies about a man she met, Bill becomes
obsessed with having a sexual encounter. He discovers an underground sexual group and attends one of their meetings -
- and quickly discovers that he is in over his head.

****************************************************************************************************

BARRY LYNDON  -  Drama, Romance, War  -  6.4 / 10 rating
OVERVIEW:  In the Eighteenth Century, in a small village in Ireland, Redmond Barry is a young farm boy in love with h
is cousin Nora Brady. When Nora engages to the British Captain John Quin, Barry challenges him for a duel of pistols.
He wins and escapes to Dublin, but is robbed on the road. Without any other alternative, Barry joins the British Army
to fight in the Seven Years War.

****************************************************************************************************

SPARTACUS  -  Action, Drama, History  -  6.2 / 10 rating
OVERVIEW:  Spartacus is a 1960 American historical drama film directed by Stanley Kubrick and based on the novel of t
he same name by Howard Fast about the historical life of Spartacus and the Third Servile War. The film stars Kirk Dou
glas as the rebellious slave Spartacus who leads a violent revolt against the decadent Roman empire. The film was awa
rded four Oscars and stands today as one of the greatest classics of the Sword and Sandal genre.

****************************************************************************************************

THE KILLING  -  Drama, Action, Thriller, Crime  -  6.2 / 10 rating
OVERVIEW:  The Killing was Stanley Kubrick's first film with a professional cast and the first time he achieved publi
c recognition as the unconventional director he's now known for. The story is of ex-prisoners who plan to set up a ra
cetrack so they can live a life without monetary worries. One of the more exceptional films of the 1950's.

****************************************************************************************************
```

Fig. 14. Result for similar movies based on the same crew.

- Recommendations of top movies with given cast member (performs best when only one name is given).

```
**********MOVIE RECCOMMENDATION SYSTEM*************


ON WHAT BASIS DO YOU WANT A RECCOMENDATION?
1. Similar overview
2. Top movies from select language
3. Top movies by given actor
4. Top movies by given crew member (director, producer etc.)
5. Top movies from given genre
ENTER CHOICE NUMBER:5
Enter genre (only 1 genre allowed): drama

====RECCOMMENDATION SUMMARY====

THE SHAWSHANK REDEMPTION  -  Drama, Crime  -  8.2 / 10 rating
OVERVIEW:  Framed in the 1940s for the double murder of his wife and her lover, upstanding banker Andy Dufresne begin
s a new life at the Shawshank prison, where he puts his accounting skills to work for an amoral warden. During his lo
ng stretch in prison, Dufresne comes to be admired by the other inmates -- including an older prisoner named Red -- f
or his integrity and unquenchable sense of hope.

****************************************************************************************************

THE GODFATHER  -  Drama, Crime  -  8.2 / 10 rating
OVERVIEW:  Spanning the years 1945 to 1955, a chronicle of the fictional Italian-American Corleone crime family. When
organized crime family patriarch, Vito Corleone barely survives an attempt on his life, his youngest son, Michael ste
ps in to take care of the would-be killers, launching a campaign of bloody revenge.

****************************************************************************************************

THE DARK KNIGHT  -  Drama, Action, Crime, Thriller  -  8.1 / 10 rating
OVERVIEW:  Batman raises the stakes in his war on crime. With the help of Lt. Jim Gordon and District Attorney Harvey
Dent, Batman sets out to dismantle the remaining criminal organizations that plague the streets. The partnership prov
es to be effective, but they soon find themselves prey to a reign of chaos unleashed by a rising criminal mastermind
known to the terrified citizens of Gotham as the Joker.

****************************************************************************************************

FIGHT CLUB  -  Drama  -  8.1 / 10 rating
OVERVIEW:  A ticking-time-bomb insomniac and a slippery soap salesman channel primal male aggression into a shocking
new form of therapy. Their concept catches on, with underground "fight clubs" forming in every town, until an eccentr
ic gets in the way and ignites an out-of-control spiral toward oblivion.

****************************************************************************************************

FORREST GUMP  -  Comedy, Drama, Romance  -  8.0 / 10 rating
OVERVIEW:  A man with a low IQ has accomplished great things in his life and been present during significant historic
events - in each case, far exceeding what anyone imagined he could do. Yet, despite all the things he has attained, h
is one true love eludes him. 'Forrest Gump' is the story of a man who rose above his challenges, and who proved that
determination, courage, and love are more important than ability.

****************************************************************************************************

INTERSTELLAR  -  Adventure, Drama  -  7.9 / 10 rating
OVERVIEW:  Interstellar chronicles the adventures of a group of explorers who make use of a newly discovered wormhole
to surpass the limitations on human space travel and conquer the vast distances involved in an interstellar voyage.

****************************************************************************************************

THE INTOUCHABLES  -  Drama, Comedy  -  7.9 / 10 rating
OVERVIEW:  A true story of two men who should never have met — a quadriplegic aristocrat who was injured in a paragli
ding accident and a young man from the projects.

****************************************************************************************************

SCHINDLER'S LIST  -  Drama, History, War  -  7.9 / 10 rating
OVERVIEW:  The true story of how businessman Oskar Schindler saved over a thousand Jewish lives from the Nazis while
they worked as slaves in his factory during World War II.

****************************************************************************************************

WHIPLASH  -  Drama  -  7.9 / 10 rating
OVERVIEW:  Under the direction of a ruthless instructor, a talented young drummer begins to pursue perfection at any
cost, even his humanity.

****************************************************************************************************

LEON: THE PROFESSIONAL  -  Thriller, Crime, Drama  -  7.8 / 10 rating
OVERVIEW:  Leon, the top hit man in New York, has earned a rep as an effective "cleaner". But when his next-door neig
hbors are wiped out by a loose-cannon DEA agent, he becomes the unwilling custodian of 12-year-old Mathilda. Before l
ong, Mathilda's thoughts turn to revenge, and she considers following in Leon's footsteps.

****************************************************************************************************
```

Fig. 15. Result for similar movies based on genre

- Recommendations of top movies with a given crew member (performs best when only one name is given).
- Recommendations of top movies from a given genre.

Once the selection basis is specified, the input to search by can be given. This input triggers the relevant function that performs the appropriate searches in the movie's metadata. The final displayed result is a descriptive summary of the recommended movies. It has four key details about the displayed movie: Title, Genre(s), Rating & Overview. The process follows a five-step process (in cases of valid inputs) as described below in Fig. 16.

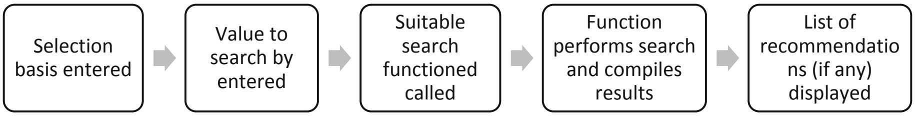


Fig. 16. The whole selection process of MoRec

The results report only top-10 (or k movies for k < 10 where only k results have been compiled) movies based on movie rating, sorted in descending order. It is assumed that once the top 15 movies have been reported, there is little to no hierarchy in their similarity to the given movie. Also, the model works irrespective of input case (lower/upper) as the function is not case-sensitive.

From observation, the following scale can define the scope of 'similar movies' based on an overview (Table 1).

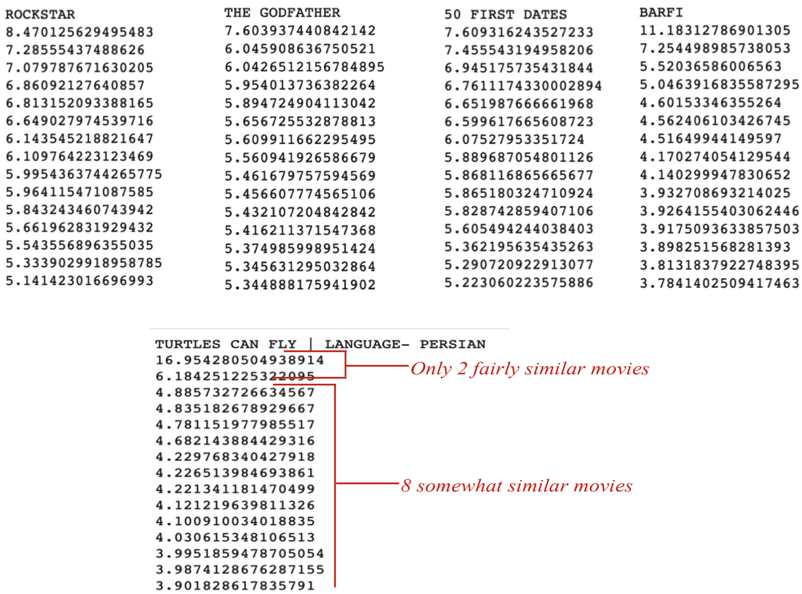
Table 1. Cosine-similarity with relative scale

(Cosine-similarity between given movie and movie 'x' $\forall \times \in$ [movie titles])*100	Similarity metric (relative scale)
Less than or equal to 3.50	No similarity between movies
More than 3.50 but less than 5.25	Somewhat similar movies
More than or equal 5.25	Fairly Similar movies

Top-10 Cosine-Similarity Scores*100 for Various Movies

It is also observed that niche movies (i.e., films of foreign languages or with relatively less famous cast/crew) have relatively small yet diverse and therefore dissimilar data to perform similarity functions on. So they do not have a rich list of recommendations. Regex filtering for genre works robustly for all inputs as the data has a good number of high-rated movies from each genre. The engine also showcases how similar storylines can be delivered in various styles and emotions in cinema. While two movies may be different in their setting, keyword identification comes across as a powerful tool in highlighting if they deal with the same theme(s) or not (Fig. 17).

Overall, the model can solve the problem statement of promptly getting a list of movies to watch next from a dataset of 45,000+ movies. It gives concise, cogent, and quick results to the user. This framework is both efficient and user-friendly.



ROCKSTAR	THE GODFATHER	50 FIRST DATES	BARFI
8.470125629495483	7.603937440842142	7.609316243527233	11.18312786901305
7.28555437488626	6.045908636750521	7.455543194958206	7.254498985738053
7.079787671630205	6.0426512156784895	6.945175735431844	5.52036586006563
6.86092127640857	5.954013736382264	6.7611174330002894	5.0463916835587295
6.813152093388165	5.894724904113042	6.651987666661968	4.60153346355264
6.649027974539716	5.656725532878813	6.599617665608723	4.562406103426745
6.143545218821647	5.609911662295495	6.07527953351724	4.51649944149597
6.109764223123469	5.560941926586679	5.889687054801126	4.170274054129544
5.9954363744265775	5.461679757594569	5.868116865665677	4.140299947830652
5.964115471087585	5.456607774565106	5.865180324710924	3.932708693214025
5.843243460743942	5.432107204842842	5.828742859407106	3.9264155403062446
5.661962831929432	5.416211371547368	5.605494244038403	3.9175093633857503
5.543556896355035	5.374985998951424	5.362195635435263	3.898251568281393
5.3339029918958785	5.345631295032864	5.290720922913077	3.8131837922748395
5.141423016696993	5.344888175941902	5.223060223575886	3.7841402509417463

TURTLES CAN FLY | LANGUAGE- PERSIAN
16.954280504938914
6.184251225322095
4.885732726634567
4.835182678929667
4.781151977985517
4.682143884429316
4.229768340427918
4.226513984693861
4.221341181470499
4.121219639811326
4.100910034018835
4.030615348106513
3.9951859478705054
3.9874128676287155
3.901828617835791

Fig. 17. Top-10 cosine-similarity scores*100 for various movies and recommendation

7 Conclusion

In conclusion, this work builds a recommendation model that allows users to define what they mean by "similar movies" based on a similar overview, given genre, language, cast, or crew. It is a hybrid project that features the following: a) Finding similarity in movies using NLP methods, b) Filtering movies using programming tools and various statistical measures. The scope of the project will be immense. More detailed data can be used to create not only a content-based system but a collaborative-filtering-based system too. Users can see what other similar users are watching (based on Mathew correlation between users-MCC). Our recommendation system can be customized based on any environment that compares similarities in items based on their literal description. For the case of movie recommendations, we input movie descriptions. For the case of product recommendations on an e-commerce platform, we can input the listed products' descriptions. Hence, our approach is customizable. Further, data for input movies can be made dynamic using web-scraping/text-mining, and then that movie can be added to the dataset.

More data from the user side can be utilized (ethically) to understand their likes/dislikes and recommend suitable movies. For example, if users follow many history pages on social media, the system can recommend historical documentaries to them. It can be extended to build a You-Tube type movie recommendation system that factors in many features like user preferences, global trends, creator details, video analytics, etc.

Acknowledgments. Our privilege is to express sincere thanks to the Information Technology and Data Science and Engineering department, School of Computing and IT, Manipal University

Jaipur, Jaipur, Rajasthan, India, for providing research platform to carry out the extensive analytical process. We are also heartiest thankful to GroupLens for providing the MovieLens dataset.

References

1. MovieLens: https://grouplens.org/datasets/movielens/. Last accessed 20 Apr 2021
2. Basu, C., Hirsh, H., Cohen, W.W.: Recommendation as classification: using social and content-based information in recommendation. In: Proceedings of the Fifteenth National Conference on Artificial Intelligence, Madison, Wisconsin. AAAI Press, pp. 714–720 (1998)
3. Harper, F., Li, X., Chen, Y., Konstan, J.: An economic model of user rating in an online recommender system. In: Proceedings of the 10th International Conference on User Modeling, Edinburgh, UK, pp. 307–216 (2005)
4. Rashid, A.M., et al.: Getting to know you: learning new user preferences in recommender systems. In: Proceedings of the International Conference on Intelligent User Interfaces (2002)
5. Robertson, S., Walker, S.: Threshold setting in adaptive filtering. J. Documentation **56**, 312–331 (2000)
6. Salton, G.: Automatic Text Processing. Addison-Wesley (1989)
7. Reddy, S.R.S., Nalluri, S., Kunisetti, S., Ashok, S., Venkatesh, B.: Content-based movie recommendation system using genre correlation. In: Satapathy, S.C., Bhateja, V., Das, S. (eds.) Smart Intelligent Computing and Applications. SIST, vol. 105, pp. 391–397. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-1927-3_42
8. Kapoor, N., Vishal, S., Krishnaveni, K.S.: Movie recommendation system using NLP tools. In: 5th International Conference on Communication and Electronics Systems (ICCES), pp. 883–888 (2020). https://doi.org/10.1109/ICCES48766.2020.9137993
9. Berger, A., et al.: Bridging the Lexical Chasm: Statistical Approaches to Answer Finding. In: Proc. Int. Conf. Research and Development in Information Retrieval, pp. 192–199 (2000)
10. Jin, C.-H., Liu, J.-G., Zhang, Y.-C., Zhou, T.: Adaptive information filtering for dynamics recommender systems, arXiv:0911.4910 (2009)
11. Mansur, F., Patel, V., Patel, M.: A review on recommender systems. In: International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), pp. 1–6 (2017). https://doi.org/10.1109/ICIIECS.2017.8276182
12. Adomavicius, G., Zhang, J.: Impact of data characteristics on recommender systems performance. ACM Trans. Manag. Inf. Syst. (TMIS) **3**(1), 3 (2012)
13. De Gemmis, M., Lops, P., Semeraro, G., Basile, P.: Integrating tags in a semantic content-based recommender. In: Proc. of the 2008 ACM Conf. on Recommender Systems, pp. 163–170 (2008)
14. Jones, K.S.: A statistical interpretation of term specificity and its application in retrieval. J. Documentation **28**(1), 11–21 (1972)
15. Pazzani, M.J., Billsus, D.: Content-based recommendation systems. In: Brusilovsky, P., Kobsa, A., Nejdl, W. (eds.) The Adaptive Web. LNCS, vol. 4321, pp. 325–341. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-72079-9_10
16. Pujahari, A., Sisodia, D.S.: Model-based collaborative filtering for recommender systems: an empirical survey. In: First International Conference on Power, Control and Computing Technologies (ICPC2T), pp. 443–447 (2020). https://doi.org/10.1109/ICPC2T48082.2020.9071454
17. Harman, D.: Overview of the 3rd Text REtrieval Conference (TREC-3). In: Proceedings of the 3rd Text REtrieval Conference, Gaithersburg, MD, Nov 1994

18. Devi, B., Shankar, V.G., Srivastava, S., Nigam, K., Narang, L.: Racist tweets-based sentiment analysis using individual and ensemble classifiers. In: Sharma, D.K., Son, L.H., Sharma, R., Cengiz, K. (eds.) Micro-Electronics and Telecommunication Engineering. LNNS, vol. 179, pp. 555–567. Springer, Singapore (2021). https://doi.org/10.1007/978-981-33-4687-1_52
19. Pujahari, A., Sisodia, D.S.: Pair-wise preference relation based probabilistic matrix factorization for collaborative filtering in recommender system. Knowl. Based Syst. **196**, 105798 (2020). ISSN 0950–7051,https://doi.org/10.1016/j.knosys.2020.105798
20. Yadav, A., et al.: Emotion recognition with facial expression using machine learning for social network and healthcare. In: Mahrishi, M., et al. (eds.) Machine Learning and Deep Learning in Real-Time Applications, pp. 273–282. IGI Global (2020). https://doi.org/10.4018/978-1-7998-3095-5.ch012
21. Shankar, V.G., Devi, B., Srivastava, S.: DataSpeak: data extraction, aggregation, and classification using big data novel algorithm. In: Iyer, B., Nalbalwar, S.L., Pathak, N.P. (eds.) Computing, Communication and Signal Processing. AISC, vol. 810, pp. 143–155. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-1513-8_16
22. Devi, B., Shankar, V.G., Srivastava, S., Srivastava, D.K.: AnaBus: a proposed sampling retrieval model for business and historical data analytics. In: Sharma, N., Chakrabarti, A., Balas, V.E. (eds.) Data Management, Analytics and Innovation. AISC, vol. 1016, pp. 179–187. Springer, Singapore (2020). https://doi.org/10.1007/978-981-13-9364-8_14
23. Shankar, V.G., Devi, B., Bhatnagar, A., Sharma, A.K., Srivastava, D.K.: Indian air quality health index analysis using exploratory data analysis. In: Sharma, D.K., Son, L.H., Sharma, R., Cengiz, K. (eds.) Micro-Electronics and Telecommunication Engineering. LNNS, vol. 179, pp. 545–554. Springer, Singapore (2021). https://doi.org/10.1007/978-981-33-4687-1_51
24. Menon, S.N., Tyagi, S., Shankar, V.G.: An efficient exploratory demographic data analytics using preprocessed autoregressive integrated moving average. In: Intelligent Data Engineering and Analytics. Smart Innovation, Systems and Technologies, vol. 266. Springer, Singapore (2022). https://doi.org/10.1007/978-981-16-6624-7_27
25. Jain, A., Bohra, M.K., Sharma, M.K., Shankar, V.G.: A modified cuckoo search for the *n*-queens problem. In: Nanda, P., Verma, V.K., Srivastava, S., Gupta, R.K., Mazumdar, A.P. (eds.) Data Engineering for Smart Systems. LNNS, vol. 238, pp. 615–620. Springer, Singapore (2022). https://doi.org/10.1007/978-981-16-2641-8_58

Design and Implementation of Secure Location Service Using Software Engineering Approach in the Age of Industry 4.0

Sumaiah Tabassum[1], Adarsh Kumar[2], Kamalpreet Kaur[3], Priyansh Arora[4], Deepraj Chowdhury[5], Sanjay Misra[6], and Sukhpal Singh Gill[1](✉)

[1] School of Electronic Engineering and Computer Science, Queen Mary University of London, Mile End, London E14NS, UK
sumaiah@se19.qmul.ac.uk, s.s.gill@qmul.ac.uk

[2] Department of Systemics, School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India
adarsh.kumar@ddn.upes.ac.in

[3] Seneca International Academy, Seneca, Toronto, Canada

[4] Microsoft, Hyderabad, India
priyansh.arora@microsoft.com

[5] Department of Electronics and Communication Engineering, International Institute of Information Technology, Naya Raipur, Chattisgarh, India
deepraj19101@iiitnr.edu.in

[6] Department of Computer Science and Communication, Østfold University College, Halden, Norway
sanjay.misra@hiof.no

Abstract. Data privacy and security are major concerns in any location-based system. In majority of location-based systems, data security is ensured via data replacement policies. Data replacement or hiding policy requires additional measures for providing required security standards for Industry 4.0. Whereas, cryptography primitives and protocols are integral part of any network and can be re-used for ensuring user's locations in Industry 4.0 based applications. In this work, an application has been designed and developed that used RSA encryption/decryption algorithm for ensuring location data's confidentiality. The proposed system is distributed in nature and gives access to location's information after users get authenticated and authorized. In the proposed system, a threshold-based subset mechanism is adopted for keys and their storage. Server is designed to securely store the location information for clients and provide this information to those set of clients or users who are able to verify sum of subset of keys. This work has elaborated the location-based data confidentiality designs in a distributed client/server environment and presented the in-depth system working with different flow diagrams. The command line and graphical User Interface (GUI)-based implementation shows that the proposed system is capable of working with standard system requirements (i5 processor, 4 GB RAM and 64-bits operating system). In addition to location information, system is able to provide much important information (including IP address, timestamp, time to access, hop count) that enhances the overall system capabilities.

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 397–418, 2023.
https://doi.org/10.1007/978-3-031-13150-9_32

Keywords: Encryption · Decryption · Latitude · Longitude · Location service · Security · RSA algorithm · Industry 4.0

1 Introduction

Location-based services are found to be rapidly evolving in various real-time applications [1]. The location-based services are integrated with application after small to large scale testing by different research groups [2]. Location-based services integrated with communication devices provides various capabilities including location tracking over Google Maps, queries execution subsystem, individual's sensitive information fetching and sharing, privacy concerns etc. [3]. These capabilities are useful if the system uses no-replacement mechanisms for providing/sharing location-based information. In replacement mechanisms, real-user data replaced with fake one and it is processed through location-dependent queries. In location-based queries, source querying location identities cannot be efficiently executed if replacement policy is followed. Thus, other data security and privacy policies need to be discussed and presented.

1.1 Motivation and Our Contributions

In existing location-based system [1–4], there are many shortcomings like (i) the replacement-based data hiding system is easy to break. This can lead to easy attack over user data. As users keep on changing the locations and data is updated regularly, the chances of tracking user's movement is much easier, (ii) similar processes of data hiding are applied to complete data. In this process, a disgruntled person can easily compromise the whole data if data security and privacy are not ensured properly. The disgruntled user can collude the stored data with unknown or fake data such that the complete data become meaningless. (iii) it is easy to find the source of location provider. Thus, any user which practices such processes in the complete execution can identify such activities easily [4]. Specifically to location-based systems or services, the various challenges in existing systems are briefly explained as follows.

- The majority of existing location-based system uses data hiding (with data replacement) policy for security. Such practices can lead to many attacks easily. Thus, they are not useful in real-time applications.
- The existing location-based system is easily prone to attacks because it is easy to manipulate data using high computational devices. Thus, formal system and software practices are required that enhances the location-based services capabilities and shows better results for real-time applications.
- Increasing the system complexity to achieve data security using cryptographic primitives need to be analysed for better performances. Thus, trade-offs between security, performance complexities and security levels are important to discuss, study and experiment.

In this work, software engineering-based methodologies are discussed to design and develop location-based system. In this system, 5 P's and their importance are discussed for location-based system [1]. The location-based system and services are required to derive and develop many real-time applications [2]. This work has discussed the location-based system project charter with detailed project plan. This plan is useful to achieve real-time application within specific, measurable, achievable, realistic and timely development process. Here, cost estimation is also performed to show the importance of discussed project charter and project plan. Thereafter, software project requirements are discussed to develop location-based secure data management system using cryptography primitives. Next, the feasibility analysis is performed that discusses economic and technical system feasibilities. In continuation, a software architecture is proposed that helps in developing location-based services for various applications. In this work, the discussed architecture explores the communication process that can help in inter-process communication for integrating location-based services. In the proposed distributed location-based system, sum of subset algorithm is used for integrating location services. These location services are useful in providing data access to authentication user only. The sum of subset approach is enhanced with encryption/decryption process using RSA algorithm [5]. To manage the distributed system, a server/client environment is suggested that helps in measuring the system performances and increases the chances of location-based system adaptability in applications. This work presents the system design as well. In the system design, system flow is explained using use-case, activity and sequence diagrams. Finally, implementation details are discussed that uses encryption/decryption processes for handling distributed architecture. The implementation section shows the system outcomes as well.

This work is organised as follows. Thereafter, Sect. 2 discusses related work, Sect. 3 focuses over system methodology. Here, software engineering practices are explored for detailed study and system development. These software engineering practices explains the project plan that can act as an example for overall system development that would be useful for any system integrating location-based services. Section 4 shows the economic and technical feasibility analysis. Section 5 explains the proposed architecture incorporating communication processes, proposed algorithm for location-based information gathering, encryption/decryption processes using RSA algorithm and distributed client/server environment. Section 6 explains the system design and flow. Section 7 presented the system integration and testing processes executed to test the system functionality. Section 8 shows the system execution. Finally, conclusion is drawn in Sect. 9.

2 Related Work

This section discusses the existing works of location-based services. Nosouhi et al. [17] identified the problem of dishonest user's fake location and provide location proof-based concept in the proposed approach. The proposed approach has concentrated over increasing the security and privacy concerns that includes prover-prover collusions with special concentration to reduce location privacy threats. Authors used Blockchain technology and proposed distributed and decentralized scheme for location proof generation and verification. Here, every prover need to broadcast its location to neighboring devices which in-turn uses peer-to-peer network for better short-range communication interface-based location sharing system. In experimentation, it has been observed that performance of the proposed approach is reliable with Prover-Prover and Prover-Witness based approach. In comparative analysis, it has been observed that the proposed approach outperforms the currently deployed proof-based scheme. The implementation is performed using Android-based platform and results show that performance is an important parameter to say that the proposed approach is comparatively better. Thus, the proposed blockchain-based architecture is capable of establishing dynamic trust and integrating score-based approach for enhancing location-based precise identification scheme. In conclusion, the proposed architecture and implementation-based solution is an effective approach to enlarge it at a large scale for realistic observations.

Tang et al. [18] concentrated over improving the healthcare services using system enabled with fog and cloud computing services. Here, location-based services play an important role in medicine, patient identification and location other healthcare services. Location-based services are useful in various healthcare's subsystems including emergence healthcare services, healthcare (medical or personal) notifications, healthcare supply chain and other subsystems. Location-based services are critical system of healthcare services. If such healthcare system can be fully implemented and followed properly with its full advantages then real advantages can be realized. For example, patient's data, its secure storage and retrieval, and sharing are important parts of any health working system. Here, location-based service can collect the required data timely and process for desired statistics and outcomes.

Tian et al. [19] discusses the characteristics of location-based services. In these characteristics, importance is given to location privacy features that may cause potential threats to different applications. Thus, security and privacy aspects are important to discuss and evaluate for application-based scenarios. Authors proposes a location privacy preserving system using cloud-of things that hides user's trajectory privacy. Here, user's moving behaviours is analysed using Markov chain that interconnects the activities. In this way, it would be much easier to identify the set of activities and provide the useful data. A cloud-based fast real data hiding and display different statistics-based system is useful in many terms including ensuring security concerns, fast data processing, statistics generation and easy to understand visualization. In experimental results, it has been found that performance can be measured in terms of moving steps, cloaking threshold score and anonymity value measures. Thus, the system is effective and efficient to tackle fast location-hiding options to various applications. This recent work gives an indication of importance of location-based system to latest applications in different sectors.

Alam et al. [20] explored the importance of IoT-based location detection services for interaction and communication in 5G technologies. The centralized approach with neighbouring devices network construction and connectivity architecture is designed and experimented to share knowledge-based data with several nodes. The integration of cloud and MANET structure creates an efficient and secure approach for data communication in Cloud, MANET and IoT integrated framework. IoT-based location detection and dynamic connection establishment and data transfer features make the proposed architecture unique and efficient to be integrated in different realistic applications.

Ratajczak et al. [21] proposed integration of location-based system with building and construction industry. The aim of this integration is to improve the overall industry performances as this industry lacks in meeting the deadlines and costs overruns. Thus, location-based system with specified key indicators are useful in meeting customer requirements. Further, system is extended with augmented reality-based system to have a walkthrough that is need to develop an application-based scenario. The complete scenario is simulated in a laboratory-based experimentation. Results show that the proposed system/solution is very effective. A feedback-based approach confirm this as well. In conclusion, the proposed system is recommended based upon semi-realistic scenario construction and outcome observations. The proposed system does not addresses the data security and privacy. The location-based data is having its own importance. This importance reduces if data is made available at no cost. Thus, there is a need to extend the proposed application-based system with security concerns.

Reddy et al. [22] discussed the importance of location-based services in Internet of Things (IoT) with short range wireless technologies including Bluetooth, Wi-Fi, ZigBee, and Global System for Mobile Communications (GSM). Integration of short range wireless technology and location-based GSM system helps in identifying various locations which in-turn is found to be helpful in control and operation of devices along with user interfaces. In this work, it has been observed that context-aware application relies over principles of context-awareness, modelling and reasoning. Various other features that includes context application facts include architecture style, abstraction, fault tolerance capabilities, uniquely identifiable services, privacy, security, data analysis etc. In the proposed system, security, privacy and open research challenges are integrated with location-based services which in-turn improves the overall system capabilities. Thus, an application-based scenario is available to study the importance of location-based services and possibilities of its integration with other systems.

Schmidtke et al. [23] discussed the importance of deploying location-based services for COVID-19-pandemic situation. In this survey, the location-aware application primarily focused over Big data construction, geospatial data analysis, visualization, data related to spreading of disease and state of other emergency services. Data privacy related to people's real location are major concern in any location-aware systems. Thus, those solutions are discussed that motivates users to share their private and comprehensive data for analysis and other benefits. The web-based variations of data collection, analysis and processing to other systems for spatial analysis and service providing are two privacy preserving COVID-19 usage. The conducted survey has gone through the pros and cons of this system. In a major finding, it has been observed that the key steps in developing privacy preserving COVID-19 contact tracking application and taking maximum usage of it are challenging but in-demand application especially during COVID-19 times. In literature, many such solutions are derived. Table 1 shows the comparative state-of-the-art work analysis for recently developed location-based system. This comparative analysis also shows the pros and cons of the techniques taken for comparative analysis.

Critical Analysis: In literature, various lightweight and traditional cryptographic primitives are discussed for different applications. These cryptographic primitives can be used for resourceful and resource constraint environments. The performance of these primitives varies from system to system under different configurations. Location-based services can be implemented over both resourceful and resource-constraint environments [24]. The major challenge in integrating location-based system with existing

Table 1. Comparative state-of-the work analysis for recently developed and/or discussed location-based systems.

Author	Year	A	B	C	D	Pros	Cons
Nosouhi et al. [17]	2020	Y	Y	Y	I	Used blockchain technology for verification Proposed trust and incentive-based	All security dimensions are not considered for implementation User-interactive location-based service is required for better statistics
Tang et al. [18]	2019	Y	N	Y	T	Generalized cloud and fog computing-based proposal is made for healthcare system The location-based services can give more precision and importance to	Lack of software practices does not ensure that the developed system is capable to integrate unknown situations which may fails the critical system understanding
Tian et al. [19]	2019	Y	N	Y	I	In this work, cloud-based architecture is proposed that handle the user's movement and capabilities to ensure data sharing functionalities This work has proposed a replacement strategy for hiding the true user's location and maintain data security and privacy concerns	Lack of software practices does not ensure that the developed system is capable to integrate unknown situations which may fails the critical system understanding Security aspects from multi-dimensional viewpoint should be considered and validated to say that the proposed system is efficient in realistic applications

(*continued*)

Table 1. (*continued*)

Author	Year	A	B	C	D	Pros	Cons
Alam et al. [20]	2020	N	N	Y	I	Cloud, MANET and IoT-based framework is unique in providing quality services to data exchange and management The proposed framework provides various features using integrated technologies that are beneficial for flexible and advanced data management	Lack of software practices does not ensure that the developed system is capable to integrate unknown situations which may fails the critical system understanding Major focus is drawn towards network construction and data management rather other data related issues including data security
Ratajczak et al. [21]	2019	N	N	Y	I & S	This work proposed location-based system with augmented reality concept for construction and building The location-based system is useful in handling construction industry efficiently as observed from laboratory-based small scale implementation	Security issues need to be addressed especially data security aspects. The location-based data is important for experimentation and if data is revealed with no cost then importance of this data reduces Smart and sustainable infrastructure solution could be proposed for construction industry

(*continued*)

Table 1. (*continued*)

Author	Year	A	B	C	D	Pros	Cons
Reddy et al. [22]	2019	Y	N	Y	I	Focused over context-aware applications, architecture and services Location-based system is one part of the complete system. Thus, it helps in understanding the possibilities of location-based system integration with other	Security and privacy concerns are partially discussed. There is need to discuss multi-dimensional security aspects to protect the system from large set of attacks GSM-based location services have large set of existing applications. However, IoT-integrated applications require distributed location-based application. Thus, new solutions are required to incorporate the additional requirements
Schmidtke et al. [23]	2020	Y	N	Y	N	This work has surveyed location-based system in recent work A classification of location-based services with different short-range technologies can be explored	Detailed survey over security aspects in location-based system is required

A: security and privacy concerns, B: prover-prover collusions, C: location-based service (generation and verification), D: implementation (I)/simulation (S)/theoretical model (T), Y: yes, N: no

real-time applications include: (i) data privacy is a major concern in location-based data collection and sharing. Thus, it should be explored with different security dimensions, (ii) location-based system need system specific solutions for integration and enhancing existing application capabilities, (iii) system specific location-based attributes are important to study and relate before designing and implement it in real-time applications, (iv) location-aware data storage is necessary to study because large user's network can generate large amount of data which require analysis accordingly, and (v) location-based services are providing advantage in many futuristic applications. Thus, the scope of location-aware data, its location and importance to other need careful considerations.

3 Methodology

In the overall system, software engineering methodologies and practices are followed to learn and analyse the progress. This section discusses methodology and more details are presented as follows:

3.1 The 5 P'S

The success of a project depends on management whether we manage it properly or not. Through the original methodology, we have prepared our own methodology [5].

- *Process:* Agile development life cycle is the base of our project. This method is opted because functional requirements of this project are explicitly stated rather than dynamic ones. Besides, more time is allowed to work on programming to assure the quality of the product.
- *Project:* Completion of project took 7 months. One of the prominent goals is to create desktop application in which one's location can be automatically retrieved that coordinate through secured channel accessed by authorized personnel.
- *Product:* It includes a mobile or web based application or web service and a manual to explain the development of this product step-wise.
- *People:* It includes the target audience such as learning institutions or common people. Adarsh Kumar, Kamalpreet Kaur and Priyansh Arora (Co-authors) are stakeholders of this project.
- *Problem:* There are many security concerns due to leakage of location information through various applications.

3.2 Project Charter

Project charter contains the following components [6]:

- **Expectations of the Customer:**
  To develop a web-based application for providing security about the user's location (user gives prior permission to share information of location)
- **Project Scope:**
  To use RSA algorithm for encryption of user's location and issue an access to certified user.
- **Analysis Technique for Interaction:**
  To implement this project after analysis of data.
- **List of Stakeholders:**
  The main stakeholders are Adarsh Kumar, Kamalpreet Kaur and Priyansh Arora (Co-authors).

- **Deliverables of Project:**
  Functional requirements are the project outcomes.
- **Evaluation Procedure of Project:**
  To run various tests to evaluate the working of project in to check whether this project is performing encryption and decryption of user location contains longitude and latitude value.
- **Projected Timeline:**
  This project has been completed in 8 months, which has been estimated using Program Evaluation and Review Technique (PERT) method.
- **User Training:**
  There is no need of user training, because it is real-time system.
- **System Maintenance:**
  This project is developed in such a way, which can be self-maintained easily. If there is a need to maintain manually, then it could be easily done without making an impact of stored data.

3.3 Project Plan

S.M.A.R.T Analysis: "SPecific, Measurable, Achievable, Realistic and Timely"
To develop a technique which is able to perform the encryption and decryption without any interference, can be completed in 7 months (99% possibility) [7]. We can create a working prototype of the proposed idea within 3 months to demonstrate its working. Table 2 show the work breakdown structure of project and length of various activities is estimated using PERT chart.

Cost Estimation/Budget
No costs for devices or system installation because whole equipment is typically owned. The development of the system will use free software that includes Qt which is also free of expenses. Most of the time would be consumed by programming and testing. Research will be on track just after the development of the software, which spends less time than expected. Programming will consume lot of time due to development based on agile model. Moreover, it is more appropriate for smaller projects with less challenge.

3.4 Requirements Specification

Function Requirements:

- Web-based application as a functional prototype, which can secure the location using encryption and decryption and also forward this information using secure network.

Non-functional Requirements:

- *Reliability:* Location of the user must be existing.

Table 2. Project tasks and their dependencies

Task ID	Task name	Duration	Start	End	Predecessor
T1	Requirement gathering	64 h	1/02/2020	09/02/2020	NA
T2	e-portfolio training	78 h	11/02/2020	22/02/2020	NA
T3	Project definition	16 days	22/02/2020	13/03/2020	NA
T4	Draft preliminary software specifications	5 days	13/02/2020	18/02/2020	NA
T5	Add feedback on specifications of software	1 day	18/02/2020	18/02/2020	NA
T6	Create timeline for delivery	1 day	19/02/2020	19/02/2020	T5
T7	Review of existing similar projects	90 h	20/02/2020	04/03/2020	MA
T8	Create working prototype	1 day	05/03/2020	05/03/2020	T7
T9	Implementation	21 days	06/03/2020	2/04/2020	T8
T10	Developer testing	21 days	06/03/2020	02/04/2020	T8
T11	Deliverables	700 h	24/03/2020	31/07/2020	NA
T12	Draft documentation	20 days	5/07/2020	9/08/2020	NA
T13	Final documentation	4 days	11/08/2020	22/08/2020	NA
T14	Prepare manual	2 days	26/08/2020	27/08/2020	NA
T15	Demonstration	1 day	07/09/202020	07/09/2020	NA

- *Performance:* The response time of developed application will me minimum as possible.
- *Safety:* No tracing can be made during the deployment stage as the samples are anonymously presented.
- *Scalability:* Should be able to maintain itself inasmuch there is no use of any data.

Software Requirements:

- To implement this application, there is a need of 64-bit Ubuntu/Windows OS.
- Geocoder

Geocoder is process of translating an address into a coordinates (longitude & latitude).

- Python language for coding
- Pyuic for changing GUI to python code
- MySQL
- Python Qt Designer

Python Qt designer designs a Graphical User Interface (GUI) for web-based applications for deployment. It is very easy to develop an application by downloading and installing it. Qt Creator Integrated Development Environment (IDE) tool [8] is available for the development of application. Moreover, the tasks such as building a project can be automated and other tasks such as actions refactoring, checking code syntax, offering semantic highlighting and writing code.

Hardware Requirements:

- 500 GB Storage
- 64-bit Architecture
- 8 GB Main Memory (RAM)
- Processor 2.16 GHz.

4 Feasibility Analysis

A feasibility study is applied for determining the possibility of a plan that includes certainty of a project whether it is legally and technically possible as well as economically acceptable or not. It informs us about the how worth the investment on the project [9]. A project may not be achievable because of plethora of reasons, such as necessitate numerous resources, which puts negative impact on these resources [11]. Consequently, the performance of other tasks get alleviated alongside might charge greater than an institute will receive back through taking on a project that isn't lucrative.

4.1 Economic Feasibility

This kind of feasibility contains a cost/benefit examination of this desktop application, supporting relations select the possibility, cost and other points associated with a task prior to the distribution of budgetary assets [10]. It upgrades the validity of project assisting users to choose the constructive financial benefits for the development of the project [12]. We have utilized open source software such as "PYUIC", "PYQT", "PYTHON" and "UBUNTU" to develop our application, which makes it economical.

4.2 Technical Feasibility

This kind of feasibility focuses on technical resources available to the institute. It provides the assistance in case of taking decisions if the particular resources meet maximum value. Technical attainability similarly comprises equipment assessment, programming, and other advanced basics of the anticipated structure. For verifying the technical feasibility, a working prototype of this application is developed [13]. The working of prototype shows that feasibility of this project technically.

5 Proposed Framework

This desktop-based application contains 4 different modules. *Command Prompt* is used to create client and server processes in this first module and then establish a connection between them. In the second module, client sends a message to server, which contains necessary input to create details of the location. In the third module, positional refinements are generated to finalize the process of encryption. In the fourth module, system provides access to the authorized users to encrypt and decrypt the message. For attaining parallelism in Python code, the threading module is used. Initially, thread class represents a process which is running in an isolated thread. The development will be decided by two ways: by rescinding run() method in the subclass or by passing a callable object to the constructor, it surpass the run() and __init__() methods for this class. Then, it calls start() method of thread to initiate the communication just after creating the thread. Moreover, it controls the thread by calling an alternate run() method. After the start of the development, thread's state considers as "alive" and further, it does not treated as "alive" once run() method stops its execution. The execution of run() method can be stopped naturally or by creating an unhandled exceptional case. If the string is "alive" then tests is alive() technique. Moreover, thread's join() method can be called by other threads. It will prevent to consider thread's join() method will finish execution.

5.1 Architecture

Figure 1 shows the process of generation of positional details and starts the communication and then apply encryption to the input utilizing the interface of a particular interface. The implementation of desktop application contains following modules:

1. Generating client and server process.
2. Use sum of subset algorithm to generate positional information.
3. Apply the encryption mechanism on details of the position.
4. Forwarding the encrypted and decrypted text to the user.

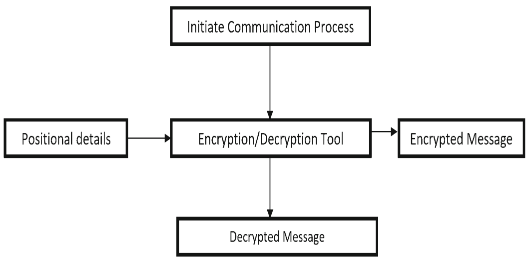


Fig. 1. System architecture of application

5.2 Start Communication Process

Command Prompt is used to create client and server processes in this first module and then establish a connection between them. Socket module provides an access to Berkeley Software Distribution (BSD) socket interface, which can be run on various platforms such as Windows, Mac or UNIX. Figure 2 shows a socket which is an anticipated representation for the one particular terminal of a network communication channel.

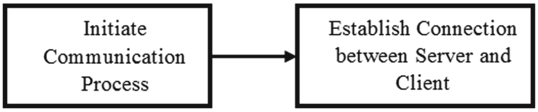


Fig. 2. Initiation of communication process

Initially, server starts the communication and then interacts with client process to verify the subset sum.

5.3 Using Sum of Subset Algorithm to Obtain Location Details

The process of using sum of subset algorithm [14] to obtain location details is shown in Fig. 3. This second module manages the transfer of message from client to server and contains the key information to make the positional refinements. In this scenario, two numbers M and n are used to define issue of Subset Sum (SS) i.e. SS (n, M). The Scenario of SS (n, M) is created by choosing a reliably irregular vector a ∈ Z n M, a reliably arbitrary vector s ∈ {0, 1} n, and producing with T = a · s mod M. The main motive of this process is to identify s using the value of T, a and n. The stability of infringement SS (n, M) is depends on the proportion between n and log M, i.e. normally indicated to as the depth of the happening of the whole subset. The Scenario, when n/log M is under 1/n or bigger than n/log2 n, the issue can be solved in polynomial time [15]. Moreover, there is no necessity of calculations which needs under 2ω(n) time when the depth is stable or uniform as little as O (1/log n). It is additionally realized that the subset aggregate issue can just get more earnestly as its thickness draws nearer to one [16]. We have developed a cryptosystem in this project and its security is relative to the stability

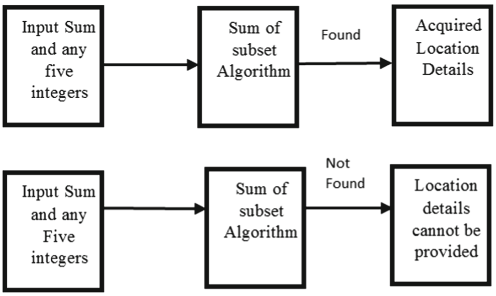


Fig. 3. Using sum of subset algorithm to obtain location details from server

of the SS (n, qn) issue, where q is a positive entire number of greatness Õ(n). Figure 3 shows the utilization of RSA algorithm for encryption of important information about the location of the user.

5.4 Encryption and Decryption of Positional Details Using RSA Algorithm

In this third module, positional details will be created to perform the process of an encryption is presented in Fig. 4. The encryption of details of the position will be performed only if client is able to offer the proper sum. The value of proper sum is required for the process of decrypt the details of position to the user. If client is not able to provide the proper sum then positional details will not be shared with client and marked client as an unauthorized user. Further, client shares its public key with the server as a sum of subset using RSA algorithm and appeals to share data. Next, public key will be used by server for encryption and shares the encrypted data with the client, who decrypts this data after receiving it. The shared data is asymmetric in nature and this data can be decrypted by the browser if third party contains the browser's public key. If required subset will be identified then position details will be encrypted with hexadecimal order of the ASCII values and share with the respective user.

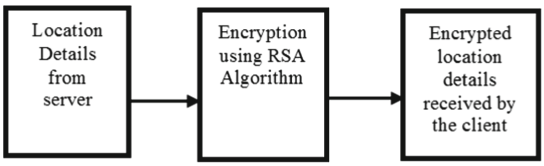


Fig. 4. Encryption and decryption process

5.5 Communication of Encrypted and Decrypted Positional Details to the Client

In this fourth module, server sends an encrypted/decrypted message to the user as presented in Fig. 5. When user shares the information about subset numbers then server starts interaction with user. If the given subset number does not satisfy the sum of subset algorithm then server denies to share positional details. Further, details of location address would be shared with user or server refuses to share encryption details with user. Server will respond with negative response "There is no subset with given sum, so location details (longitude and latitude) will not be shared" if client is not able to obtain a correct subset sum.

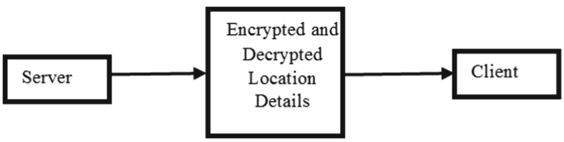


Fig. 5. Communication of location details to the client

Figure 6 shows the execution process to enter subset sum. Client will select ‘n’ to exit the loop and select ‘y’ to continue the execution process.

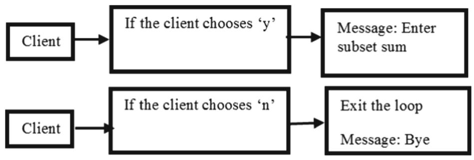


Fig. 6. Execution after acquiring the location details

6 Design Description

This section describes the design of the proposed work using three UML diagrams such as use case diagram, activity diagram and sequence diagram. Figure 7 shows a use case diagram to describe the interaction of user with the system. User initiates the communication processes and giving the input for the creation of positional description along with the information about the message to be encrypted. Further, server process performs the encryption and decryption of message. Figure 8 shows an activity diagram to start the communication process, where encryption/decryption happens and needed input for positional refinements age is specified. Otherwise, there is a need to restart the procedure. Figure 9 shows the sequence diagram to describe an interaction among client process, server process, decryption and encryption. First, client-server starts the communication using ports and give a feedback for the generation of positional details and further, message will be encrypted or decrypted.

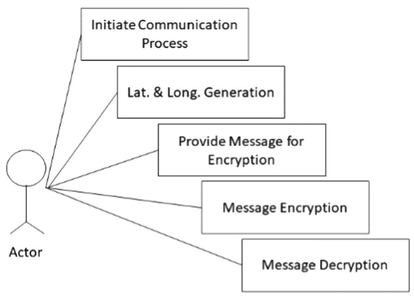


Fig. 7. Use case diagram

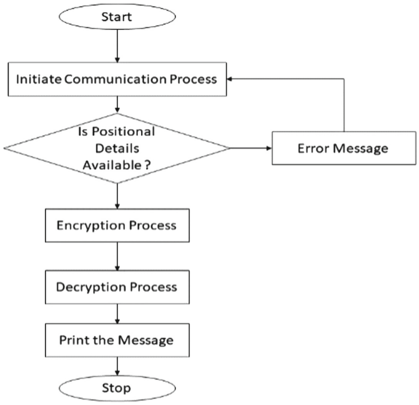


Fig. 8. Activity diagram

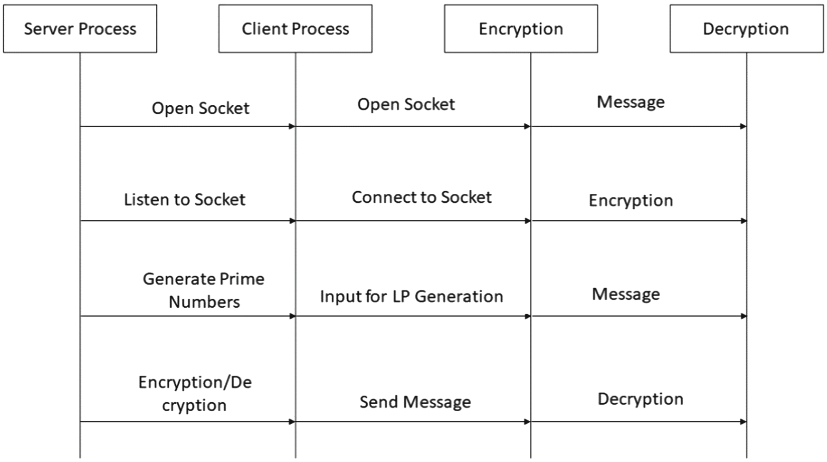


Fig. 9. Sequence diagram

7 Integration and Testing

This section describes the performance evaluation, where various different inputs are evaluated to identify the output after processing of set of operations. To start performance evaluation, encrypted location will be issued firstly. Further, programmer provides the destination address to port the server. The destination address can be edited if it is required in the server's module. Next, socket is ready to listen the request of client. Server shares that address after confirming the valid authentication. "Sum of subset problem" is considered to validate the client's authentication if client returns the required valid subset sum and numbers shadowed by colon (:). After verification of valid client, the location details will be provided by the server. After identification of correct subset sum, the server provides details of position and client process is able to check the decrypted and encrypted locations. Further, client can press *"Y"* to continue and can process *"N"* to exit the process here. The location details will not be shared with client if the sum of subset is not verified correctly and server sends the reason of not sharing location as "given subset cannot be found with given sum".

8 Implementation Details and Results

The software and hardware requirements for this research are described in Sect. 3. This section discusses the implementation details and working of proposed technique. Figure 10 shows the screen that give the option to choose the processes. We have created two processes here:

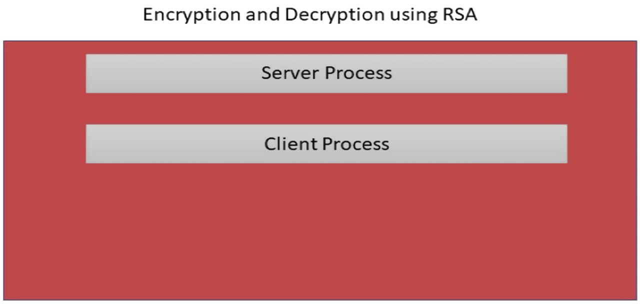


Fig. 10. Server/client process

- Server process is accessed by the person who has to share his/her location details.
- Client process is accessed by the person who wants to know someone's location details.

Figure 11 shows the window that opens when clicked on Server process. Port is opened and socket starts listening at this point.

Fig. 11. Selection of server process

Figure 12 shows the window that opens when clicked on Client process. Here in this window, sum and five numbers in the set should be given.

Fig. 12. Selection of client process

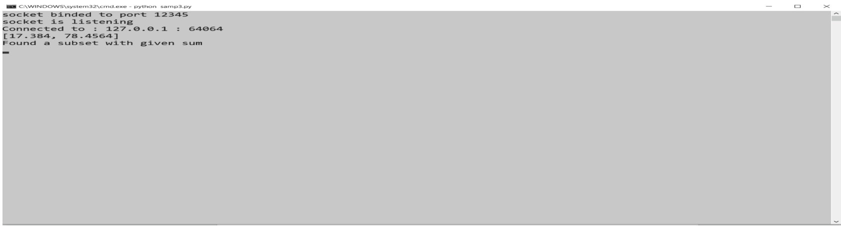


Fig. 13. An output of server process

Figure 13 shows the output of server process when the client has entered the sum and subset correctly. It discloses the location details (latitude, longitude) to the client as he/she is authorized.

Figure 14 shows the output on the client process window i.e. the location details are disclosed to him/her by the server.

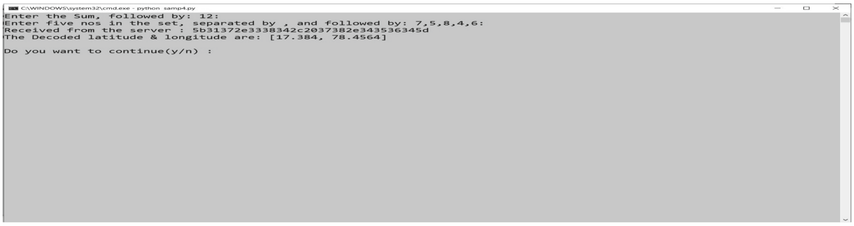


Fig. 14. An output of client process

Figure 15 shows the output where the client gives an unsatisfied sum and subset combination, which implies that the client is unauthorized.

Fig. 15. Client is unauthorized

Figure 16 shows the output where the server recognizes the client to be unauthorized and does not disclose the location.

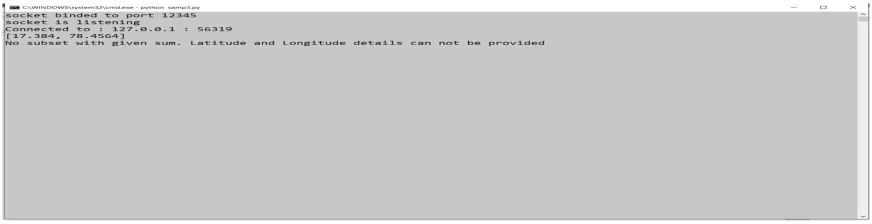


Fig. 16. Server recognizes the client to be unauthorized

9 Conclusions and Future Work

Location-aware system has advantages in various real-time applications. With these advantages, the scope of data collection, its availability for public usage and analysis for statistics are equally important to study and discuss. In traditional approach, data security uses data hiding approach for protection which in-turn uses data replacement with fake data. Such approaches are not much secure and easy to break with high computational device. Thus, there is a strong need to develop cryptographic primitives-based location-aware services that promises data security in all data stages (storage, processing and transmission). In this work, an application is developed for Industry 4.0 to enable encryption and decryption of location using RSA algorithm, which gives access to the location to only authorized users. This work has considered subset as a key and help to locate the correct location. The server keeps the details of the location in a confidential way, will be shared with only valid clients who verifies the sum of subset. The departments such as navy and army can use this application to transfer their message with high security. Further, Police personnel can also use this application for the decryption of messages of anti-social elements. Presently, this is a desktop based application, which can be extended for mobile devices in the future. Currently, this application is tested using single client and server but this application can be tested using multiple clients.

References

1. Vasilis, A., Havlena, M., Kiefer, P., Giannopoulos, I., Schindler, K., Raubal, M.: Gaze-Informed location-based services. Int. J. Geogr. Inf. Sci. **31**(9), 1770–1797 (2017)
2. Kachane, S., Feng, Y., Jayalath, D., Wang, C.: A New Location-Based Services Framework for Connected Vehicles Based on the Publish-Subscribe Communication Paradigm (2019)
3. Binh, T.N.: Location-based real-time casino data, U.S. Patent 9,626,826 (18 April 2017)
4. Chen, L., et al.: Robustness, security and privacy in location-based services for future IoT: a survey. IEEE Access **5**, 8956–8977 (2017)
5. Cicirelli, F., Fortino, G., Giordano, A., Guerrieri, A., Spezzano, G., Vinci, A.: On the design of smart homes: a framework for activity recognition in home environment. J. Med. Syst. **40**(9), 200 (2016)
6. Singh, A., Singh Gill, S.: Measuring the maturity of Indian small and medium enterprises for unofficial readiness for capability maturity model integration-based software process improvement. J. Softw.: Evol. Process **32**(9), e2261 (2020)
7. Waraga, O.A., Bettayeb, M., Nasir, Q., Talib, M.A.: Design and implementation of automated IoT security testbed. Comput. Secur. **88**, 101648 (2020)
8. Patwary, A.A.N., Fu, A., Battula, S.K., Naha, R.K., Garg, S., Mahanti, A.A.: FogAuthChain: a secure location-based authentication scheme in fog computing environments using Blockchain. Comput. Commun. **162**, 212–224 (2020)
9. Singh Gill, S., Buyya, R.: Failure management for reliable cloud computing: a taxonomy, model, and future directions. Comput. Sci. Eng. **22**(3), 52–63 (2018)
10. Rao, J., Pattewar, R., Chhallani, R.: A privacy-preserving approach to secure location-based data. In: Bhalla, S., Bhateja, V., Chandavale, A.A., Hiwale, A.S., Satapathy, S.C. (eds.) Intelligent Computing and Information and Communication. AISC, vol. 673, pp. 47–55. Springer, Singapore (2018). https://doi.org/10.1007/978-981-10-7245-1_6
11. Abidi, S., Essafi, M., Guegan, C.G., Fakhri, M., Witti, H., Ghezala, H.H.B.: A web service security governance approach based on dedicated micro-services. Procedia Comput. Sci. **159**, 372–386 (2019)
12. Lin, C., He, D., Kumar, N., Choo, K.K.R., Vinel, A., Huang, X.: Security and privacy for the internet of drones: challenges and solutions. IEEE Commun. Mag. **56**(1), 64–69 (2018)
13. Asuquo, P., et al.: Security and privacy in location-based services for vehicular and mobile communications: an overview, challenges, and countermeasures. IEEE Internet Things J. **5**(6), 4778–4802 (2018)
14. Ibarra, O.H., Kim, C.E.: Fast approximation algorithms for the knapsack and sum of subset problems. J. ACM (JACM) **22**(4), 463–468 (1975)
15. Lyubashevsky, V., Palacio, A., Segev, G.: Public-key cryptographic primitives provably as secure as subset sum. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 382–400. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-11799-2_23
16. Impagliazzo, R., Naor, M.: Efficient cryptographic schemes provably as secure as subset sum. J. Cryptol. **9**(4), 199–216 (1996). https://doi.org/10.1007/BF00189260
17. Nosouhi, M.R., Yu, S., Zhou, W., Grobler, M., Keshtiar, H.: Blockchain for secure location verification. J. Parallel Distrib. Comput. **136**, 40–51 (2020)
18. Tang, W., Zhang, K., Zhang, D., Ren, J., Zhang, Y., Shen, X.S.: Fog-enabled smart health: toward cooperative and secure healthcare service provision. IEEE Commun. Mag. **57**(5), 42–48 (2019)
19. Tian, Y., Kaleemullah, M.M., Rodhaan, M.A., Song, B., Al-Dhelaan, A., Ma, T.: A privacy preserving location service for cloud-of-things system. J. Parallel Distrib. Comput. **123**, 215–222 (2019)

20. Alam, T.: Efficient and secure data transmission approach in cloud-MANET-IoT integrated framework (2020)
21. Ratajczak, J., Riedl, M., Matt, D.T.: BIM-based and AR application combined with location-based management system for the improvement of the construction performance. Buildings **9**(5), 118 (2019)
22. Venkateswara Reddy, R., Murali, D., Rajeshwar, J.: Context-aware middleware architecture for IoT-based smart healthcare applications. In: Saini, H.S., Sayal, R., Govardhan, A., Buyya, R. (eds.) Innovations in Computer Science and Engineering. LNNS, vol. 74, pp. 557–567. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-7082-3_64
23. Schmidtke, H.R.: Location-aware systems or location-based services: a survey with applications to CoViD-19 contact tracking. J. Reliab. Intell. Environ. **6**(4), 191–214 (2020). https://doi.org/10.1007/s40860-020-00111-4
24. Gill, S.S., et al.: AI for next generation computing: emerging trends and future directions. Internet Things **18**, 100514 (2022)

Deep Learning Based Architecture for Entity Extraction from Covid Related Documents

Sushil Kumar(✉), Avantika Sahu, and Aditi Sharan

Jawaharlal Nehru University, New Delhi, India
sushilksharma.info@gmail.com, ditisharan@mail.jnu.ac.in

Abstract. Entity extraction from the text data in the biomedical domain has an essential role in biomedical research. In natural language processing entity extraction task aims to identify the terms into predefined categories. With the emergence of the covid-19, covid related digital resources increased drastically and the new type of entities is introduced. State-of-the-art named entity extraction models is heavily relying on domain-specific resources which are hard to perform adequately on covid related data. In this paper, we proposed a deep-learning-based architecture for named entity recognition. The experiment was performed on the CORD-NER dataset which was released by the University of Illinois. We compare the performance of different deep learning-based architectures on this data for a named entity recognition task.

Keywords: Deep learning · Named entity recognition · BILSTM · CRF · CNN

1 Introduction

We are living in an era of digitalization; digital resources are increasing drastically. The same applies to the biomedical domain. If knowledge can be extracted and applied appropriately from these digital resources, it has the potential to be used in various applications. In the biomedical domain, a lot of rich information is available in text form in various biomedical journals and other online resources. We are dealing with natural language text and incorporating semantics in natural language text is a difficult task. Domain-specific entity extraction can play an important role in enhancing the extraction of semantic information from the text. Named entity recognition is extensively used in the biomedical domain such as DNA identification, gene identification, drug name identification, disease name identification, question-answering model, opinion mining, text summarization, and finding the most relevant information, etc. [2]. In the biomedical domain, extensive research is going on to extract biomedical entities from the text. Some tools have also been developed to extract such entities. However, due to the covid-19 pandemic, flooding of information occurred on this topic and people required information retrieval and extraction systems that could be used for providing focused covid related information. In the context of covid, new types of entities are introduced due to which entity extraction becomes challenging, and existing entity extraction tools/models are

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 419–427, 2023.
https://doi.org/10.1007/978-3-031-13150-9_33

not suitable for such entity extraction tasks [1]. Thus it becomes important to utilize machine learning techniques for extracting covid-related entities.

In this research, we proposed a CNN Character Embedding-Based BI-LSTM (CCEBB) model for the extraction of named entities from covid-related data.

2 Related Work

"NER consists of three different problems – the recognition of a named entity in text, the assignment of a class to this entity (gene, protein, drug, etc.), and the selection of a preferred term for naming the object in case that synonyms exist" [7]. Earlier traditional NER models were based on sequence labeling, such models are Hidden Markov Models (HMM) and Conditional Random Fields (CRF) [8].

Performing handcrafted feature extraction is a difficult and time-consuming task in natural language processing, many pieces of research shows deep learning models do automated feature extraction which is better than the handcrafted feature extraction technique and less time-consuming, so if features extracted by the deep learning models are applied to traditional sequence labeling models it may show considerable good performance. [2] proposed "contextual long short-term memory networks with CRF (CLSTM)" model for named entity recognition. They are incorporating n-gram with the BI-LSTM and CRF. BI-LSTM with CRF encoding performed better in Named Entity Recognition than the RNN model [3]. To handle the out of vocabulary problem character embedding can be incorporated with the deep learning models. And to capture the relationship between entities CRF encoding layer can be added at the output layer [4]. Character embedding showed improvement in text mining in natural language processing and can also handle the inconsistency of words [4]. Most of the modern convolutional neural architectures utilize a pattern of building alternative convolutional networks and pooling layers to extract features and attach some fully connected layers for classification [9]. Covid dataset contains different type entities that We firmly believe that our findings on the spatial distribution of the present/absent amino acids over the proteins enable a better understanding of the PPIs of SARS-CoV-2. For instance, the spatial arrangements reveal the similarities and dissimilarities among the important structural proteins E, M, N and S, which further helps to establish a more complete evolutionary tree among the other CoV strains [10, 11].

3 CCEBB: CNN Character Embedding Based BILSM Model for NER

In earlier times statistical-based or rule-based models were used for the named entity recognition. Traditional models were heavily based on handcrafted features. Feature extraction from text data in natural language processing is a challenging task. With the emergence of deep learning models, one need not rely on handcrafted features. Deep learning models are self-sufficient to take care feature extraction part. In earlier days a lot of research was performed on the named entity recognition and found that some statistical models like CRF models showed significant results as these models are by nature sequential. Thus the use of deep learning has two major advantages: The sequential nature of the model and automatic learning of features.

This research aims to build a NER model with the combination of deep learning and traditional learning for the named entity extraction task. We purposed the CCEBB model that combines: character embedding with CNN, BILSTM, and CRF decoding.

3.1 Proposed Model Architecture

The main advantage of deep learning architecture is to overcome a lot of feature extraction and vectorization technique of input words. In earlier days static representation of text data like Bag of Words, one-hot encoding, etc. was used which is independent of the context. With the coming of deep learning major shift from the static representation of the text, where deep learning takes care of the context of the occurrences of the words in the sentences for getting the vector representation of the words as in word2vec, glove, etc.

Considering the popular deep learning architectures BI-LSTM and CNN, it was observed that BI-LSTM performed well for natural language processing-related tasks. In addition to word embedding, character embedding is found useful for handling out of vocabulary (OOV) problems. The context of the biomedical domain might have small variations like spelling, suffixes, prefixes, hyphenations, etc. Character embedding can also be helpful in dealing with these variations. To extract the character embedding-based feature extraction CNN can be utilized.

Therefore, in our CCEBB model, we concatenate the CNN-based character embedding and glove pre-trained embedding. The concatenated embedding was fed as the input to the BI-LSTM. In this way, we modified the input representation to the BI-LSTM. On other hand, we observed that the CRF encoding model shows good performance for the traditional Named entity extraction. However major limitation being that, it required a lot of handcrafted feature design. With the emergence of the deep learning model, the output of the deep learning model may be utilized to provide proper features to traditional sequence labeling models like CRF. It has been observed that the CRF decoding-based

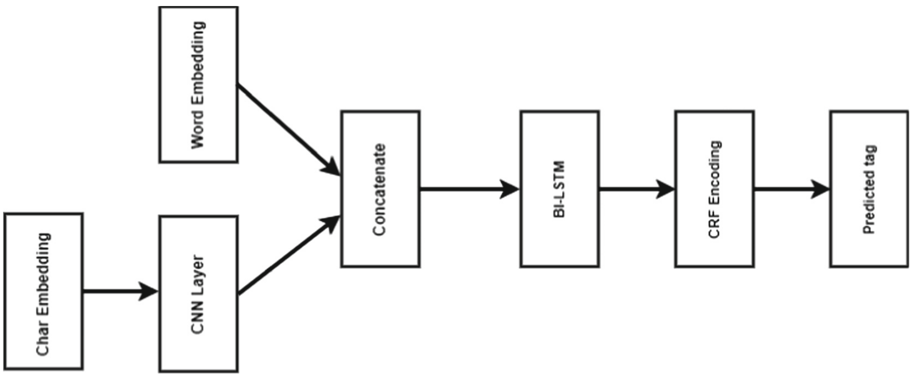


Fig. 1. Proposed model

output is more accurate than the general probabilistic classifier like Softmax. So we fed the output of the BI-LSTM to the CRF layer for predicting the tag of each term.

The architecture of our proposed model is illustrated in Fig. 1. Detailed workflow is described in the experiment section.

4 Experiments and Results

4.1 Dataset

With the emergence of the covid-19 pandemic lot of research work was done for conducting the trial and observing the effect of covid-19. In addition to this lot of research papers related to covid-19 have been published and because flooding of information it became difficult to extract useful covid-19 related information from a vast corpus. Entity extraction can be an important task that can help in extracting useful information from the covid-19 related text. For extracting the entity using the machine learning models, labeled data set is required. To perform the named entity extraction task on covid-19 related data the University of Illinois has released cord-19 data set.

The dataset includes the meta-data, full-text corpus, and CORD-19-NER results from the 29,500 documents in COVID-19 Open Research Dataset Challenge (CORD-19) corpus (2020-03-13). The size of the dataset is about 1.2 GB. It includes the following items:

- Id – unique identification for each document.
- Source – It contains the source from which documents are fetched.
- Pmcid – PMC paper records id.
- Body – body contains full-text corpus.
- Entities: entities contain CORD-19-NER results from annotation Each line represents one document in the dataset. The file schema is shown below.[1]

{'id':0, 'source':'xxx', 'doi':'xxx', 'pmcid':'xxx', 'pubmed_id':'xxx', 'publish_time':'xxx', 'authors':'xxx', 'journal':'xxx', 'title':'xxx', 'abstract':'xxx', 'body':'xxx', 'entities':[{'text':'xxx', 'start':0, 'end':3, 'type':'xxx'}, ...]}, ...]}

[1] Data set – https://uofi.app.box.com/s/k8pw7d5kozzpoum2jwfaqdaey1oij93x.

4.2 Evaluation Metric

To evaluate the performance of entity extraction task standard evaluation metrics are used, among the most important are Precision, recall, and F1. We evaluate the performance of our model using precision, recall, and F1 measures.

- **Precision** = Precision can be defined as correct prediction among all predictions.

$$\mathbf{Precision} = \frac{True\ Positive}{True\ Positive + False\ Positive} \tag{1}$$

- **Recall** = Recall can be defined as the correct prediction among all the correct labels.

$$\mathbf{Recall} = \frac{True\ Positive}{True\ Positive + False\ Negative} \tag{2}$$

- **F1-Score** = F1- score is the weighted average of precision and recall.

$$\mathbf{F1{-}score} = (2 * \frac{(Precision * Recall)}{(Precision + Recall)}) \tag{3}$$

- **Support-** it is the actual occurrence of the label in the test data.

4.3 Experiments and Results

We performed our experiments for the CCEBB model along with three more combinations of base model to compare the performance of the proposed model. These models are:

i. BI-LSTM
ii. BI-LSTM + CRF
iii. BI-LSTM + CNN

It may be noted that the dataset contains 29500 documents related to covid-19. Documents were divided into lengths 200, for the input of models. Each word in the documents has character embedding which is fed into CNN layer. We used this embedding to concatenate with the word embedding. Then we feed this embedding to the BI-LSTM layers to learn appropriate features for entity extraction. These learned features were then fed to the CRF decoding layer to predict the tag of each word. To avoid overfitting early stopping technique is used. We use Tensor Flow 2.2 along with Keras 2.3 to implement our model (Fig. 2).

Figure 3 compares the performance of our proposed CCEBB model with the other models. To evaluate the performance of the model's precision, recall, and F1 metric were used.

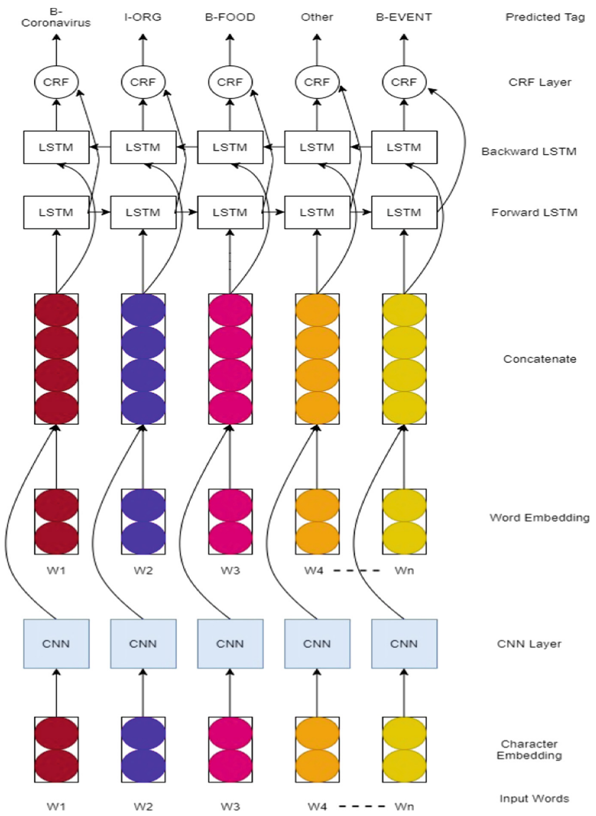


Fig. 2. Workflow of our proposed model.

Hyperparameter to train our deep learning-based models in Table 1:

Table 1. Hyperparameter table.

Hyperparameter	Value
Epochs	20
Dropout	0.2
Batch_size	128
Learning_rate	0.01
hiden_layer	64
L2_reg	1e−9
Validation_split	0.1
Filter_size	30
Kernel_size	3

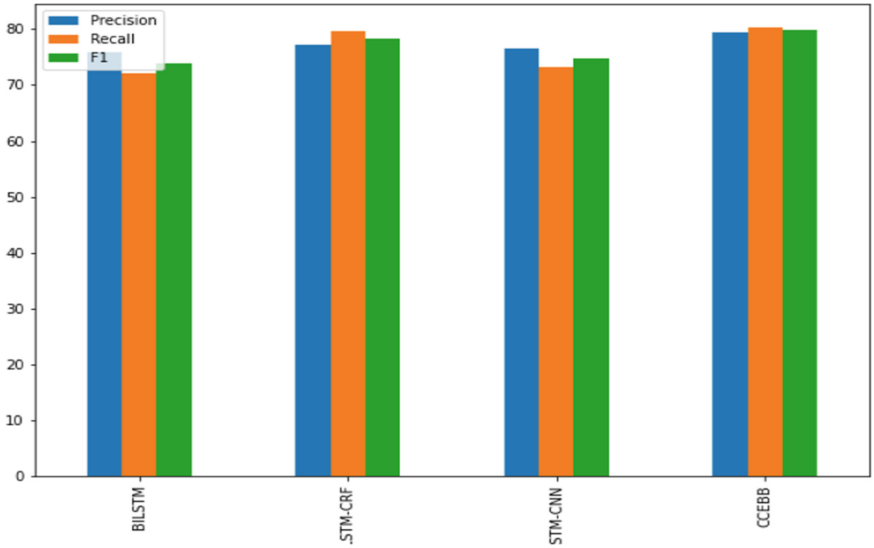


Fig. 3. Overall performance of models.

As we see in Fig. 3 our proposed CCEBB model achieves a precision of 79.51 scores and a recall of 80.38 score which is significantly better amongst all. However, in addition to just expressing overall results, it is also important to analyze the individual level performance of each entity. It is obvious that the overall accuracy of the entity is not the same, some entities might give good results comparatively others. Overall accuracy might not sufficient to analyze the result at the entity level.

We may hypothesis that an entity that has more support value has performed better. While observing the support of an entity we may think that the entity with higher support should be more accurate as more data is available for those entities. However, the analysis of the result shows that this hypothesis may not be correct always.

On more careful observation that context may also play an important role to determine the accuracy of an entity. For a particular entity, context remains stable then the entity may learn more appropriately while for some other entity context itself may be varying and it becomes difficult to catch the contexts and models not learns appropriately.

In Table 1 we can analyze some unusual performance of the entity.

From Table 2 we can infer that the support value of GROUP_ATTRIBUTE is only 275 but still it performed better than the TISSUE which has a support value much larger than the GROUP_ATTRIBUTE. As we can say that both numbers times occurrences of an entity and their context play an important role. A superficial observation can tell the context of group-attribute may be more steady as compared to the context of tissue.

Table 2. Entity-wise performance analysis.

Entity	Precision	Recall	F1	Support
Event	3.00	55.00	5.00	51
Group_attribute	96.00	96.00	96.00	275
Product	21.00	50.00	30.00	5576
Educational_activity	86.00	81.00	84.00	572
Tissue	63.00	72.00	67.00	35763
Viral_protein	90.00	86.00	88.00	6058

5 Conclusion

In this research, we proposed the CCEBB model for the named entity extraction. The proposed architecture of CCEBB consists of three layers, main model is BI-LSTM. To improve the performance of the model, we suggest the use of character embedding with a CNN filter in the input layer. The output of the BI-LSTM model feeds to the CRF layer for the tag prediction. We compare the performance of our model with the other models and found that our model performed well among them.

In addition to the overall performance, we also analyzed the individual level performance of the entity and found that some entities are easy to learn in comparison to other more difficult entities. We also observed that the support and context of the entity are important factor that is responsible to determine whether an entity is easily learnable or not.

References

1. Wang, X., Song, X., Li, B., Guan, Y., Han, J.: Comprehensive named entity recognition on cord-19 with distant or weak supervision. arXiv preprint arXiv:2003.12218 (2020)
2. Cho, H., Lee, H.: Biomedical named entity recognition using deep neural networks with contextual information. BMC Bioinf. **20**, 735 (2019). https://doi.org/10.1186/s12859-019-3321-4
3. Chalapathy, R., Borzeshi, E.Z., Piccardi, M.: Bidirectional LSTM-CRF for clinical concept extraction. arXiv preprint arXiv:1611.08373 (2016)
4. Gridach, M.: Character-level neural network for biomedical named entity recognition. J. Biomed. Inform. **70**, 85–91 (2017)
5. Wang, Y., Rastegar-Mojarad, M., Komandur-Elayavilli, R., Liu, H.: Leveraging word embeddings and medical entity extraction for biomedical dataset retrieval using unstructured texts. Database **2017**, bax091 (2017)
6. Song, H.-J., Jo, B.-C., Park, C.-Y., Kim, J.-D., Kim, Y.-S.: Comparison of named entity recognition methodologies in biomedical documents. BioMed. Eng. OnLine **17**(S2), 158 (2018). https://doi.org/10.1186/s12938-018-0573-6
7. Leser, U., Hakenberg, J.: What makes a gene name? Named entity recognition in the biomedical literature. Brief Bioinform. **6**(4), 357–369 (2005). https://doi.org/10.1093/bib/6.4.357. PMID: 16420734

8. Luo, G., Huang, X., Lin, C.-Y., Ni, Z.: Joint entity recognition and disambiguation. In: Proceedings of the 2015 Conference on Empirical Methods in Natural Language Processing, pp. 879–888 (2015)
9. Wang, D., Cui, P., Zhu, W.: Structural deep network embedding. In: Proceedings of the 22nd ACM SIGKDD international conference on Knowledge discovery and data mining, pp. 1225–1234 (2016)
10. Rout, R.K., Hassan, S.S., Sheikh, S., Umer, S., Sahoo, K.S., Gandomi, A.H.: Feature-extraction and analysis based on spatial distribution of amino acids for SARS-CoV-2 Protein sequences. Comput. Biol. Med. **141**, 105024 (2022). https://doi.org/10.1016/j.compbiomed.2021.105024
11. Hassan, S.K.S., et al.: A vicenary analysis of SARS-CoV-2 genomes. Comput. Mater. Continua **69**, 3477–3493 (2021)
12. Zhao, Z., et al.: Disease named entity recognition from biomedical literature using a novel convolutional neural network. BMC Med. Genomics. **10**(5), 73 (2017)
13. Chieu, H.L., Ng, H.T.: Named entity recognition: A maximum entropy approach using global information. In: Proceedings of the 19th International Conference on Computational Linguistics—vol. 1. Association for Computational Linguistics, Pennsylvania, p. 1–7 (2002)
14. Huang, Z., Xu, W., Yu, K.: Bidirectional LSTM–CRF models for sequence tagging. arXiv preprint arXiv:1508.01991 (2015)
15. Hochreiter, S., Schmidhuber, J.: Long short-term memory. Neural Comput. **9**(8), 1735–1780 (1997)
16. Madhu, G., et al.: Imperative dynamic routing between capsules network for malaria classification. Comput., Mater. Continua **68**(1), 903–919 (2021)

Data Sampling Methods for Analyzing Publishers Conduct from Highly Imbalanced Dataset in Web Advertising

Deepti Sisodia(✉) and Dilip Singh Sisodia

National Institute of Technology, Raipur, India
{dssisodia.cs,dsisodia.phd2017.cse}@nitrr.ac.in

Abstract. Due to the involvement of a huge amount of expenditure, the Pay-per-Click digital advertising model is affected by click fraud. The rare presence of illegitimate publishers than the legitimates makes the class distribution skewed which in turn biases the learning model towards the majority class. Moreover, the dynamic disguise activities of publishers make the task harder to investigate the actual status labels of the publishers, resulting in less accurate predictions. However, features reported in the literature detect click fraud based on analyzing the publishers' conduct but are unable to cope with the changing behavior of publishers. Therefore, we proposed a framework addressing two challenging issues: a) eight new conditional features are proposed to better capture the dynamics of click fraud behavior by merging two or more attributes over publishers on finer-grained time intervals. b) Examined the impact of data sampling methods on learners' performance for the effective identification of publisher's activity. The performance of the classification algorithms is assessed using average precision, recall, and f-measure and validated using 10-fold cross-validation. Experimental results illustrate the potential of the proposed features over a balanced dataset in improving the average precision of the learners in discriminating the fraudsters among genuine publishers.

Keywords: Pay-per-click · Online advertising · Imbalancing · Publishers · Classification algorithms · Novel features

1 Introduction

Pay-per-Click (PPC) advertising is one of the most general and effective models of Internet advertising [1, 2]. In this advertising, advertisers have to pay for every generated click on the advertisement, the system is thus influenced by suspicious activities because of the inclusion of a high amount of disbursement. This type of suspicious activity is known as click fraud [3]. Click fraud is a form of fraud where forge clicks are generated by the advertisers to deplete the competitor's budget and by the publishers for more revenue generation[4]. The ecosystem of PPC advertising is shown in Fig. 1.

Miscellaneous information like noisy data and missing samples in conjunction with the disguise activities generated by the publishers, pose complexities in click fraud detection. Moreover, high skewness [5] in the raw click dataset makes the tasks challenging

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 428–441, 2023.
https://doi.org/10.1007/978-3-031-13150-9_34

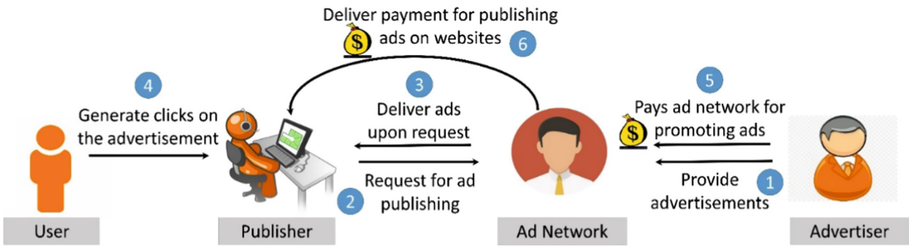


Fig. 1. PPC advertising ecosystem

and even harder in analyzing the implicit behavior of fraudulent publishers. Such findings necessitate the need for a balanced dataset and generation of robust features that can cope with their evolving patterns. Thus, new features are derived from the existing attributes that have not been examined in the literature distinguishing the fraudulent publishers among the honest ones. The main contributions of this experiment are as follows:

- Eight new features are introduced to analyze the evolving patterns of fraudulent behavior of publishers, which have never been investigated in the literature to the best of our knowledge.
- The effect of each attribute of the raw user click dataset on the behavior of a publisher is analyzed, and the total 111 composite features are generated using existing raw attributes.
- The high-class imbalance issue is being handled employing the three sampling strategies: over-sampling (BSMOTE-1, BSMOTE-2, and K-Means SMOTE), under-sampling (NearMiss1, NearMiss2, and NearMiss3), and hybrid sampling (SMOTE-TOMEK and SMOTEENN) approach for balancing the data.
- Experiments are carried out on FDMA2012 user-click dataset first, considering actual dataset, second with sampled dataset and model is validated using 10-fold cross-validation.
- The performance of the employed model is assessed using average precision, recall, and f-measure.

This work focuses on addressing the issues of click fraud detection using supervised learning. This work analyses the behavior of publishers over the skewed and balanced dataset and develops an effective model that identifies false publishers to combat click fraud. Thus, extensive work has been conducted for the identification of legitimate and illegitimate publishers where apart from employing conventional click fraud features, eight new features are also introduced which have never been utilized in the previous work to the best of our knowledge. Results have proved the utility of proposed features with improved classification performance.

The structure of the remaining paper is as follows. In Sect. 2, the related work on click fraud is described in brief. Section 3 discusses the proposed methodology, where dataset preparation and experimental design are elaborated. Experimental results are stated in Sect. 4, while Sect. 5 concludes the work.

2 Related Work

This section discusses the work associated with click fraud. Several solutions on click fraud detection have been reported in the literature, where several data mining and machine learning algorithms have been used to generate models that successfully detect fraudsters. Several works have been discussed in the literature for click fraud detection using machine learning [4–9]. One such contribution given by Haddadi [10] detected click fraud by employing bluff ads to find different sources of click fraud such as, trained-users or bots that perform fraud. To identify fraudsters, bluff ads are combined with the actual ads which served as a litmus test for the user's genuineness. A user is deemed suspicious if several bluff ads are clicked. Walgampaya et al. [11] have designed a collaborative click fraud detection and prevention system by combining the evidence obtained from several models using Dempster-Shafer evidence theory. The system keeps an online record of fraudulent sources of clicks in terms of IP, referrer, country, etc., and identifies the suspicious clicks based on three modules namely: rule-based, click map, and outlier detection module. Whenever the respective score of an IP/country etc. reaches a specific threshold level, the system puts that score into the fraud database list and reports to the ISPs for blocking the traffic generating from these suspicious sources. For the detection of distinct forms of click frauds in online advertising Antoniou et al. [12] developed a burst detection algorithm that helps in the real-time detection of click fraud by employing a splay tree (a binary search tree). Their approach is to extract the bursty webpages of websites based on the number of visits on webpages in a period and detect the click fraud by restricting an IP when the burst of clicks is received from that IP. However, simply detecting bursts might not be enough to discriminate between legitimate and illegitimate clicks; thus, more evidence is required to label clicks as false clicks. Despite the several methods made for the detection and prevention of advertising click fraud, Perera et al. [13] modeled the problem by designing novel features from the existing attributes. They had extracted features related to fraudulent publishers to characterize the behavior of the fraudsters. Pechuan et al. [14] have designed an approach for the optimization of online advertising by employing genetic algorithms as an optimizing approach. The designed approach is feasible enough for optimizing the online advertising campaign through feature selection. Another individual and ensemble approach has also detected fraud in online advertising, distinguishing fraudsters among legitimate publishers using Gradient Tree Boosting [2], Random Forest[15].

The studies discussed in the literature are not sufficient enough to combat click fraud. The features designed in prior works for the discrimination of dishonest publishers among honest need to be more specific in identifying fraudsters. Since the publisher's behavior is changing with time, examining the evolving patterns of the malicious conduct of the publishers', the dataset is balanced and new features are derived in this work concerning identifying the fraud publishers.

3 Visual Illustration of the Proposed Methodology

This section briefly discusses the dataset, extracted features, data balancing methods, and the learning models employed in the experiment. Visual representation of the proposed framework is illustrated in Fig. 2.

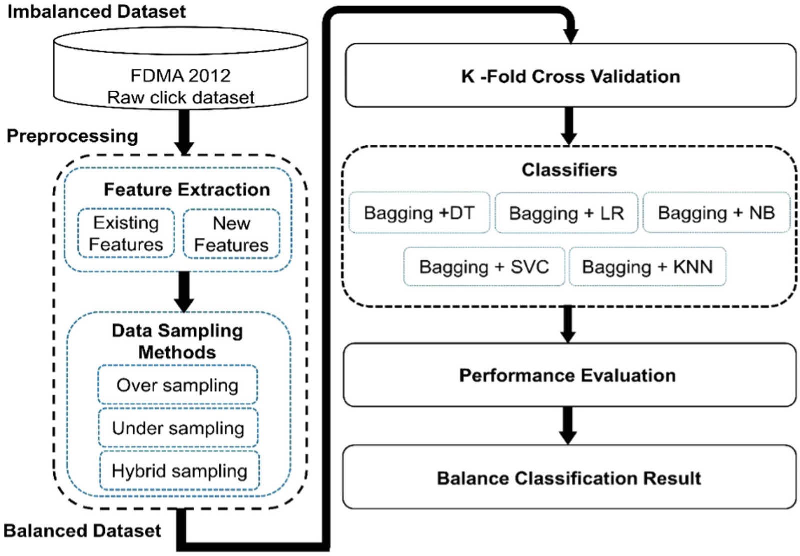


Fig. 2. Visual representation of the proposed framework

3.1 Data Preparation and Feature Engineering

FDMA 2012 user-click dataset is used in this experiment. Both the publisher and click datasets are available in the CSV format and contain the details regarding publishers and generated clicks respectively. The status of the publisher is provided as the OK (genuine publisher), Fraud (fraudulent publisher), and Observation (publisher which is neither considered as genuine nor fraudulent). The instances of fraudulent and under observation publishers outnumber the observation of genuine publishers, which poses skewness in the dataset, thus making the issue challenging for conventional machine learning methods for classification. The samples of the raw click and publisher dataset and the count statistics of publishers and clicks are summarized by Oentaryo et al. [2].

3.2 Proposed Features

New features are generated based on two observations. a) frequent change in publisher's status b) activities like generating illegitimate clicks to vanish third party's budget indicates publisher's disguise activities which harm the advertising system's viability. Therefore, to cope with these issues, newly derived features about publishers' behavior need to be extracted at different time intervals, which should be able to capture properties specific to fraudulent publishers and are more effective against their evolving behavior. Though the existing features used in the literature have shown significant improvement in classification performance but need to be more specific towards the changing behavior of publishers. Therefore, to identify the disguise activities of publishers and to investigate their changing behavior, eight new statistical features are derived based on the existing attributes.

The clicks generated by the user comprises information including, IP address of the clicker, the type of mobile device used for generating clicks, the publisher's id, the advertising campaign's id, the country user belong, date and time of the generated clicks, the channel and the referred_url. Using these attributes, 103 existing features + 8 newly proposed features are created in this experiment that is specific in capturing the characteristics of the publisher. To capture the short- and long-term behavior of the publisher, the day is divided into 4-time intervals, and composite features are extracted by recording the number of clicks received by the publisher at distinct time intervals (like, morning, afternoon, evening, and night time). A total of 111 features are generated using the following attributes which are processed separately and assessed their effect on the behavior of the publisher.

The number of clicks that every publisher receives is measured for morning, afternoon, evening, and night time, and aggregation of those clicks is performed using average and standard deviation. For instance, let the number of clicks generated by a particular publisher in one minute are 1, 5, and 9 during morning time while the number of clicks generated by the same publisher during afternoon time in one minute is 4, 5, and 6. If we calculate the average of both the publishers, we will get the same value as average = 5. This shows that on average, approximately five clicks are generated by a publisher in one minute during morning and afternoon time while the actual generated clicks are largely spread out than the calculated average number of clicks. So, to calculate the deviations of the generated clicks by a publisher, we are using standard deviation as another statistic. Considering the same example if we calculate the standard deviation, we will get two different sets of values for the generated clicks by a publisher during different time intervals. Following 8 new features are derived using null-valued referer for the identification of fraudsters.

null_referer_night_avg: a numerical-valued attribute computed as the average number of total clicks having null as the referer which occurred per minute for a particular publisher during night time.
*null_referer_night_std:*_a numerical-valued attribute computed as the standard deviation of total clicks having null as referer occurred per minute for a particular publisher during night time.
null_referer_morning_avg: a numerical-valued attribute computed as the average number of total clicks having null as referer occurred per minute for a particular publisher during morning time.
null_referer_morning_std: a numerical-valued attribute computed as the standard deviation of total clicks having null as referer occurred per minute for a particular publisher during morning time.
null_referer_afternoon_avg: a numerical-valued attribute computed as the average number of total clicks having null as referer occurred per minute for a particular publisher during afternoon time.
null_referer_afternoon_std: a numerical-valued attribute computed as the standard deviation of total clicks having null as referer occurred per minute for a particular publisher during afternoon time.
null_referer_evening_avg: average number of total clicks having null as referer occurred per minute for a particular publisher during evening time.

null_ referrer_evening_std: Standard deviation of total clicks having null as referer occurred per minute for a particular publisher during evening time.

3.3 Experimental Design

The previous section has elaborated the dataset preparation process, where a dataset is created with high skewness in class distributions. This section overcomes the issue by employing several data sampling methods, which makes the dataset balanced for further preprocessing. The training and testing of the dataset are performed using the 10–fold cross-validation to avoid the overfitting of the learning model. This sampled data is then passed to the classifiers for further classification.

Data Sampling. Table 1 represents the ratio of the instances of the classes, namely-OK, Fraud, and Observation which indicates a major class imbalance in the dataset. For significant performance assessment the issue is overcome by employing data sampling methods: oversampling- K-means SMOTE (KMS) [16], Borderline SMOTE-1(BS1) [17], and Borderline SMOTE -2 (BS2) [18], under-sampling- NearMiss-1(NM1), NearMiss-2 (NM2), NearMiss-3 (NM3) [19] and hybrid sampling SMOTETOMEK (ST), and SMOTEENN (STE) [5] techniques. Oversampling methods replicate the instances of the outnumbered class whereas, under-sampling methods reduce the instances of the majority class while balancing the dataset. The hybrid sampling method combines both over and under-sampling to make the dataset balanced.

Table 1. Ratio of instances obtained before and after sampling

Classes	Sampling methods								
	Original data	Oversampling			Under sampling			Hybrid sampling	
		KMS	BS1	BS2	NM1	NM2	NM3	ST	STE
OK	2369	2369	2369	2369	76	76	76	2357	1304
Observation	76	4662	2369	2368	76	76	76	2363	2319
Fraud	78	4660	2369	2368	76	76	62	2363	2310
Total Instances	2523	11691	7107	7105	228	228	214	7083	5933

Classification Models. The predictions obtained by combining several models yield better predictions comparative to the individual model [20]. Concerning this fact, bagging is used for the detection of click fraud in this experiment. It aggregates the results of several classifiers for better generalization of the result. It helps in avoiding overfitting and minimizes the variance related to prediction, which leads to an improved predictive performance by decreasing the misclassification rate of the classifier [21]. Decision Tree[1], Logistic Regression[5], Naïve Bayes[1], K-Nearest Neighbor[19], and Support Vector Machine[22, 23] are used as weak learners with bagging in experimentation.

Evaluation Measures. With the high-class imbalance in a dataset, performance assessment based on accuracy provide misleading results due to the biasing of the classifier towards the majority class. Thus, precision, recall, and f_1-score (f-measure) [24] are used to assess the effectiveness of the learning models, which are elaborated in Table 2. For single class i, the evaluation has been described as t_{p_i}-true positive for class i, and f_{p_i}-false positive for class i, f_{n_i}-false negative for class i, and t_{n_i}-true negative for class i respectively, l represents total number of classes.

Table 2. Performance evaluation measures for multiclass classification

Evaluation measures	Formula	Description
Average precision (AP)	$\frac{\sum_{i=1}^{l} \frac{t_{p_i}}{t_{p_i}+f_{p_i}}}{l}$	Average of precision scores
Sensitivity (TPR)	$\frac{t_{p_i}}{t_{p_i}+f_{n_i}}$	The ratio of accurately examined fraudulent observations from entire fraudulent samples
F-measure (F_1)	$\frac{2t_{p_i}}{2t_{p_i}+f_{p_i}+f_{n_i}}$	It is computed by taking the harmonic mean of the precision and recall

4 Results

Experimentations are conducted on Intel(R) Xeon(R) W-2155 CPU @ 3.30 GHz 3.31 GHz on 32.0 GB RAM utilizing various libraries of Python version 3.7. This experimentation was designed for two objectives, first, to evaluate the efficacy of newly designed features in identifying the fraudsters, and second, to assess the impact of several data sampling strategies to improve the average precision using the bagging-based classifiers. The first experiment was conducted over an actual dataset with 103 and 111 features, and another oversampled dataset with 103 and 111 features.

Several parameters are tuned for the sampling methods and classification models to achieve effective data balancing and classification. Table 3 lists the tuned parameters.

To handle the imbalance issue in the dataset, the experiment was performed first by balancing the dataset employing oversampling strategies: BS-1, BS-2, and KMS with 103 and 111 features to check whether newly designed eight features can improve the results. A slight performance improvement can be observed from Table 4 after parameter tunning based on average precision, recall, and f-measure.

Table 3. Parameter tunning a) Sampling methods and b) Classification methods

Type	Sampling Method	Parameters
a) Sampling methods		
Over-sampling	SMOTE	sampling_strategy =‘auto’, random_state = 10, k_neighbors = 3
	BSMOTE1	sampling_strategy =‘auto’, random_state = 10, kind = ’borderline-1’
	BSMOTE2	sampling_strategy =‘auto’, random_state = 10, kind = ’borderline-2’
Under-sampling	NearMiss1	sampling_strategy =‘auto’, random_state = 10, version = 1, n_neighbors = 3
	NearMiss2	sampling_strategy =‘auto’, random_state = 10, version = 2, n_neighbors = 3
	NearMiss3	sampling_strategy =‘auto’, random_state = 10, version = 3, n_neighbors_ver3 = 3
Hybrid-sampling	SMOTETomek	sampling_strategy =‘auto’, random_state = 10
	SMOTEENN	sampling_strategy =‘auto’, random_state = 10

Classifiers	Parameters
b) Classification methods	
Naïve bayes	var_smoothing = 1e−09
Logistic regression	penalty = ‘l1’, C = 1.0, random_state = 10
k-Nearest neighbor	n_neighbors = 3, leaf_size = 30, metric = ‘minkowski””
Decision tree	criterion = “gini”, random_state = 10, min_samples_split = 2
Support vector machine	C = 1, kernel = ‘linear’, degree = 3, gamma = 1, random_state = 10

Experiments are thereafter performed by handling the skewness in the data by employing under-sampling methods, namely: NM1, NM2, and NM3 over the dataset with 103 features and 111 features to evaluate the efficiency of newly designed eight features in improving the classification performance for all classifiers. Table 5 represents a slight improvement in average precision, recall, and f-measure with 111 features. However, a slight decline in the classification performance is observed using 111 features using under-sampling methods as compared to the performance achieved using over-sampling methods. This is due to the loss of data; as under-sampling methods remove the samples of over-represented classes to make the dataset balanced.

Table 4. Performance of classifiers over 103 and 111 features with over-sampling methods

			Bagging + DT		Bagging + LR		Bagging + KNN		Bagging + SVM		Bagging + NB	
			103	111	103	111	103	111	103	111	103	111
Without sampling	Original dataset	EM	Fea	Fea	Fea	Fea	Fea	Fea	Fea	Fea	Fea	Fea
		AP	48.68	49.34	39.45	40.63	36.33	37.74	45.71	47.12	36.21	37.51
		RE	45.95	46.65	37.35	37.49	34.72	36.35	43.28	44.58	34.26	35.89
		F_1	47.27	47.95	38.37	38.99	35.50	37.03	44.46	45.81	35.20	36.68
Over sampling	BSMOTE-1	AP	50.87	51.71	45.23	46.98	39.54	41.21	49.41	51.02	40.23	41.74
		RE	47.79	48.38	43.84	44.46	37.02	38.89	46.07	48.09	37.26	39.36
		F_1	49.28	49.98	44.52	45.68	38.23	40.01	47.68	49.51	38.68	40.51
	BSMOTE-2	AP	53.55	54.17	50.21	51.61	46.18	47.57	50.71	51.84	43.21	44.91
		RE	50.22	51.3	47.43	48.26	43.87	44.34	47.97	48.63	41.14	42.21
		F_1	51.83	52.69	48.78	49.87	44.99	45.89	49.30	50.18	42.14	43.51
	K-Means SMOTE	AP	62.4	63.92	55.34	56.81	49.28	50.74	52.86	53.21	49.88	50.67
		RE	60.7	60.92	52.12	52.93	47.12	48.87	50.25	51.08	47.69	48.23
		F_1	61.53	62.38	53.68	54.80	48.17	49.78	51.52	52.12	48.76	49.41

Table 5. Performance of classifiers over 103 and 111 features with under-sampling methods

			Bagging + DT		Bagging + LR		Bagging + NB		Bagging + KNN		Bagging + SVM	
			103	111	103	111	103	111	103	111	103	111
Without sampling	Original dataset	EM	Fea	Fea	Fea	Fea	Fea	Fea	Fea	Fea	Fea	Fea
		AP	48.68	49.34	39.45	40.63	36.33	37.74	45.71	47.12	36.21	37.51
		RE	45.95	46.65	37.35	37.49	34.72	36.35	43.28	44.58	34.26	35.89
		F_1	47.27	47.95	38.37	38.99	35.50	37.03	44.46	45.81	35.20	36.68
Under sampling	NearMiss (version 1)	AP	50.76	51.58	36.88	39.54	39.52	40.51	48.46	51.76	40.51	42.74
		RE	48.67	49.39	34.29	37.68	37.52	38.24	47.02	49.89	38.25	40.38
		F_1	49.69	50.46	35.54	38.59	38.49	39.34	47.73	50.81	39.35	41.53
	NearMiss (version 2)	AP	54.27	55.57	40.71	42.33	42.74	43.58	50.77	52.39	42.84	43.49
		RE	52.12	53.31	38.69	40.02	40.37	41.72	48.87	50.84	40.69	41.23
		F_1	53.17	54.42	39.67	41.14	41.52	42.63	49.80	51.60	41.74	42.33
	NearMiss (version 3)	AP	59.96	61.09	44.85	45.42	44.83	46.5	53.39	54.62	44.02	45.35
		RE	56.86	59.62	42.84	43.95	42.69	43.74	51.89	52.69	42.29	43.27
		F_1	58.37	60.35	43.82	44.22	43.73	45.08	52.63	53.64	43.14	44.29

Table 6. Performance of classifiers over 103 and 111 features using hybrid-sampling methods

			Bagging + DT		Bagging + LR		Bagging + NB		Bagging + KNN		Bagging + SVM	
			103	111	103	111	103	111	103	111	103	111
Without sampling	Original dataset	EM	Fea	Fea	Fea	Fea	Fea	Fea	Fea	Fea	Fea	Fea
		AP	48.68	49.34	39.45	40.63	36.33	37.74	45.71	47.12	36.21	37.51
		RE	45.95	46.65	37.35	37.49	34.72	36.35	43.28	44.58	34.26	35.89
		F_1	47.27	47.95	38.37	38.99	35.50	37.03	44.46	45.81	35.20	36.68
Hybrid	SMOTE-TOMEK	AP	53.63	54.82	50.94	51.21	48.27	50.01	50.38	52.63	45.68	46.65
		RE	51.12	52.94	48.79	49.18	47.19	47.11	48.36	50.38	43.11	43.63
		F_1	52.34	53.86	49.84	50.17	47.72	48.52	49.35	51.48	44.36	45.09
	SMOTE-ENN	AP	58.97	60.14	52.66	53.98	51.46	53.86	53.75	55.84	50.82	51.33
		RE	56.24	57.84	50.48	52.15	49.68	51.84	51.52	53.65	48.64	49.54
		F_1	57.57	58.97	51.55	53.05	50.55	52.83	52.61	54.72	49.71	50.42

The effectiveness of newly designed features is also evaluated on the dataset balanced using hybrid sampling methodologies, namely SMOTETOMEK and SMOTEENN, which is the combination of over and under sampling methods. A slight improvement in AP, RE, and F1 is observed in Table 6 with 111 features. A graphical representation of results discussed in Table 4, 5 and 6 is shown in Fig. 3. Table 7 demonstrates a comparison of the present work with the prior study conducted in the literature towards classifying the fraudulent publishers on FDMA 2012.

Table 7. Comparative study of current work with the previous work

Author	Classification models	Result
[15]	Random forest	36.20% AP
[2]	Tree ensemble	49.30% AP
[25]	Random forest	49.99% AP
[13]	Bagging + Random forest	51.40% AP
[26]	Random forest	52.30% AP
[2]	Random forest	58.84% AP
[2]	Gradient boosting machine	59.38% AP
[1]	Gradient tree boosting (GTB)	60.51% AP
Proposed work	**Bagging + DT**	**63.92% AP**

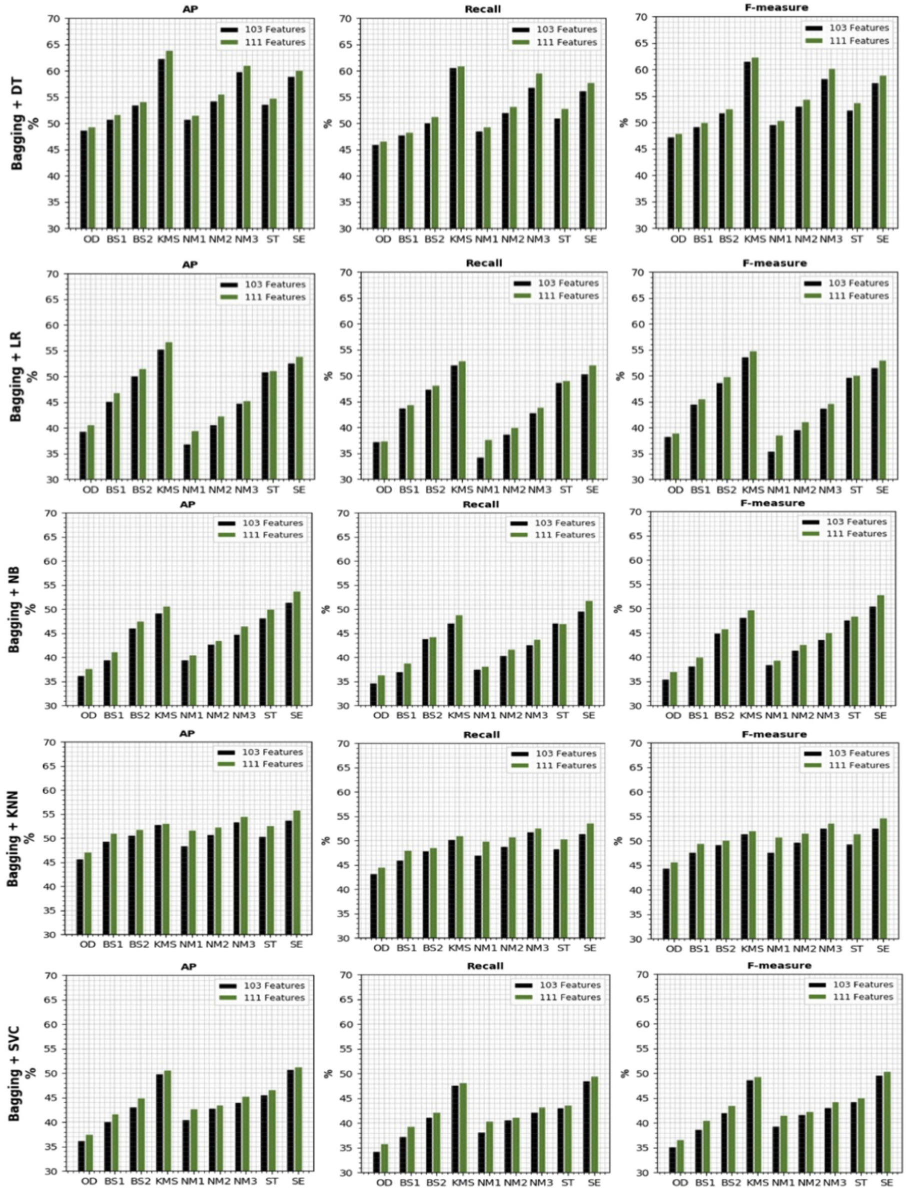


Fig. 3. Comparing the performance of existing and proposed features on a balanced dataset

5 Conclusion

This work analyzes the influence of data sampling methods towards analyzing the behavioral patterns of publishers to detect click fraud. The publisher's conduct is analyzed by balancing the dataset, thereby designing robust features and identifying if they hold a strong correlation with fraudulent behavior. Since fraudsters change their strategy continuously, inappropriate features may affect the intended working of the model. Therefore 8 new features are generated that can cope with the changing strategy of the publishers by analyzing their behavioral patterns where significant insights on the click fraud behavior are reported over a balanced dataset using machine learning ensemble methods. Following are the conclusions drawn from the work:

- Improved classification performance is achieved with Bagging over a balanced dataset of 111 features. Among all the employed sampling methods, bagging + DT outperforms other classifiers with 111 features with an achieved average precision score of 63.92%, 61.09%, and 60.14% using KMS, NM3, and STE sampling methods respectively.
- Newly generated features helped in identifying the fraudsters generating continuous duplicate clicks coming from the same IP while having no information about the type of device used for clicking. Moreover, identified another fraudulent activity, where clicks are generated from different IPs, different countries but at the same time which places that particular publisher under suspicion. The final obtained results proved that the designed model performed well over a dataset balanced using data sampling methods with newly designed eight features in identifying the illegitimate publishers among genuine publishers with an improved classification performance. Though the proposed features have improved the classification over a balanced dataset, selecting the most significant features needs to be identified in the future for effective fraudulent publishers' identification.

References

1. Sisodia, D., Sisodia, D.S.: Gradient boosting learning for fraudulent publisher detection in online advertising. Data Technol. Appl. **55**, 216–232 (2020). https://doi.org/10.1108/DTA-04-2020-0093
2. Oentaryo, R., et al.: Detecting click fraud in online advertising: a data mining approach. J. Mach. Learn. Res. **15**, 99–140 (2014). https://doi.org/10.1145/2623330.2623718
3. Haider, C.M.R., Iqbal, A., Rahman, A.H., Rahman, M.S.: An ensemble learning based approach for impression fraud detection in mobile advertising. J. Netw. Comput. Appl. **112**, 126–141 (2018). https://doi.org/10.1016/j.jnca.2018.02.021
4. Nagaraja, S., Shah, R.: Clicktok: click fraud detection using traffic analysis. In: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, Miami Florida, pp. 105–116 (2019)
5. Sisodia, D., Sisodia, D.S.: Data sampling strategies for click fraud detection using imbalanced user click data of online advertising : an empirical review. IETE Tech. Rev. (2021). https://doi.org/10.1080/02564602.2021.1915892
6. Almeida, P.S., Gondim, J.J.C.: Click fraud detection and prevention system for ad networks. J. Inf. Secur. Crytography **5**, 27–40 (2018)
7. Tripathi, D., Nigam, B., Edla, D.R.: A novel web fraud detection technique using association rule mining. Procedia Comput. Sci. **115**, 274–281 (2017). https://doi.org/10.1016/j.procs.2017.09.135

8. Skersys, T., Butleris, R., Butkiene, R. (eds.): ICIST 2012. CCIS, vol. 319. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-33308-8
9. Mouawi, R., Awad, M., Chehab, A., El Hajj, I.H., Kayssi, A.: Towards a machine learning approach for detecting click fraud in mobile advertizing. In: Proceedings of the 13th International Conference on Innovations in Information Technology, pp. 88–92. IIT, Al Ain, UAE. IEEE (2019). https://doi.org/10.1109/INNOVATIONS.2018.8605973
10. Haddadi, H.: Fighting online click-fraud using bluff ads. ACM SIGCOMM Comput. Commun. Rev. **40**, 21–25 (2010)
11. Walgampaya, C., Kantardzic, M., Yampolskiy, R.: Evidence fusion for real time click fraud detection and prevention. In: Ao, S.-I., Amouzegar, M., Rieger, B.B. (eds.) Intelligent Automation and Systems Engineering, pp. 1–14. Springer New York, New York, NY (2011). https://doi.org/10.1007/978-1-4614-0373-9_1
12. Antoniou, D., et al.: Exposing click-fraud using a burst detection algorithm. In: Proceedings - IEEE Symposium on Computers and Communications. pp. 1111–1116. IEEE (2011). https://doi.org/10.1109/ISCC.2011.5983854
13. Perera, K.S., Neupane, B., Faisal, M.A., Aung, Z., Woon, W.L.: A novel ensemble learning-based approach for click fraud detection in mobile advertising. In: Prasath, R., Kathirvalavakumar, T. (eds.) MIKE 2013. LNCS (LNAI), vol. 8284, pp. 370–382. Springer, Cham (2013). https://doi.org/10.1007/978-3-319-03844-5_38
14. Miralles-Pechuán, L., Ponce, H., Martínez-Villaseñor, L.: A novel methodology for optimizing display advertising campaigns using genetic algorithms. Electron. Commer. Res. Appl. **27**, 39–51 (2018). https://doi.org/10.1016/j.elerap.2017.11.004
15. Berrar, D.: Learning from automatically labeled data: case study on click fraud prediction. Knowl. Inf. Syst. **46**(2), 477–490 (2015). https://doi.org/10.1007/s10115-015-0827-6
16. Last, F., Douzas, G., Bacao, F.: Oversampling for Imbalanced Learning Based on K-Means and SMOTE. arXiv Prepr. arXiv1711.00837 (2017). https://doi.org/10.1533/9780857096166
17. Nguyen, H.M., Cooper, E.W., Kamei, K.: Borderline over-sampling for imbalanced data classification. Int. J. Knowl. Eng. Soft Data Paradigms **3**(1), 4 (2011). https://doi.org/10.1504/IJKESDP.2011.039875
18. Han, H., Wang, W.-Y., Mao, B.-H.: Borderline-SMOTE: a new over-sampling method in imbalanced data sets learning. In: Huang, D.-S., Zhang, X.-P., Huang, G.-B. (eds.) ICIC 2005. LNCS, vol. 3644, pp. 878–887. Springer, Heidelberg (2005). https://doi.org/10.1007/11538059_91
19. Sisodia, D., Sisodia, D.S.: Quad division prototype selection-based k-nearest neighbor classifier for click fraud detection from highly skewed user click dataset. Eng. Sci. Technol. Int. J. **28**, 101011 (2022). https://doi.org/10.1016/j.jestch.2021.05.015
20. Sisodia, D., Sisodia, D.S.: Prediction of diabetes using classification algorithms. Procedia Comput. Sci. **132**, 1578–1585 (2018). https://doi.org/10.1016/j.procs.2018.05.122
21. Sutton, C.D.: Classification and Regression Trees, Bagging, and Boosting. Elsevier (2004). https://doi.org/10.1016/S0169-7161(04)24011-1
22. Sisodia, D., Shrivastava, S.K., Jain, R.C.: ISVM for face recognition. In: International Conference on Computational Intelligence and Communication Networks, (CICN), pp. 554–559 (2010). https://doi.org/10.1109/CICN.2010.109
23. Sisodia, D., Singh, L., Sisodia, S.: Fast and accurate face recognition using SVM and DCT. In: Babu, B.V., et al. (eds.) Proceedings of the Second International Conference on Soft Computing for Problem Solving (SocProS 2012), December 28-30, 2012. AISC, vol. 236, pp. 1027–1038. Springer, New Delhi (2014). https://doi.org/10.1007/978-81-322-1602-5_108
24. Tharwat, A.: Classification assessment methods. Appl. Comput. Inform. **17**(1), 168–192 (2020). https://doi.org/10.1016/j.aci.2018.08.003

25. Berrar, D.: Random forests for the detection of click fraud in online mobile advertising. In: Proceedings of 2012 International Workshop on Fraud Detection in Mobile Advertising (FDMA), Singapore, pp. 1–10 (2012)
26. Vasumati, D., Vani, M.S., Bhramaramba, R., Babu, O.Y.: Data mining approach to filter click-spam in mobile ad networks. In: Int'l Conference on Computer Science. Data Mining & Mechanical Engg, pp. 90–94. ICCDMME Bangkok, Thailand (2015)

Analysis of the Effect of Feature Selection and Class Balancing Methods with Supervised Algorithms in Web Robot Detection Problem

Rikhi Ram Jagat(✉), Dilip Singh Sisodia, and Pradeep Singh

Department of Computer Science and Engineering, National Institute of Technology Raipur, Raipur 492010, India
{rrjagat.phd2019.cse,dssisodia.cs,psingh.cs}@nitrr.ac.in

Abstract. Accurately web robot identification is one of the most challenging problems for web robot activity detection systems. In the last few years, to accurately identify web robots, machine learning classification methods were used. However, it was discovered that the multiclass distribution in the web robot detection system is substantially skewed due to the data set's class imbalance, which causes problems with classification accuracy. The research presented in this paper examines not only the role of feature selection in improving classification accuracy but also addresses the issue of class imbalance using under-sampling of major classes and Synthetic Minority Over-sampling (SMOTE) of minor classes. After that, the classification performance is compared across a number of different classifier types. The results of this study show that oversampling (SMOTE) is more effective than under-sampling at discovering minor classes when employed with the class imbalance data set.

Additionally, it was discovered that KNN and XGBoost are more accurately classified than other classifiers throughout this research. However, no single method can be utilized to classify multiclass data. This study proposes that a combination of KNN and XGBoost may be used to classify minor classes in a web robot detection system's unbalanced class data set.

Keywords: Web robot detection · Web access log · Feature selection · Class imbalance · XGBoost · KNN

1 Introduction

In the digital era, all communication is done through the internet, as the whole world uses internet technology for different purposes such as sensitive information, business information, personal information, etc. [1, 2]. As we say, the internet means it uses the client-server system to transmit all types of data and also store it for future use [3]. Nowadays, most information travels through web servers; it provides different data using the website and web application. Some users that behave like intruders have bad intentions to damage such web servers or steal essential and sensitive information from the web servers [3]. So, they can use different methods and tools to do all these activities.

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 442–453, 2023.
https://doi.org/10.1007/978-3-031-13150-9_35

These types of activities are also known as attacks; there are various types of attacks available, and every time the new attack methods are found to breach the existing security. Some of them are web crawler, which is used for crawling the website automatically; DDOS attacks, it is used for slowing down the performance of a server. A DDOS attack is more dangerous for the servers as it slows down the server so that legitimate users cannot able to access the website of that server. It downgrades the reputations and ranking of the websites which serve on that server. So, the researchers also work to find different ways to protect these new types of security attacks using the latest technologies [4].

A web robot detection system is a system that detects the malicious activity set of intruders in a web server, which compromises the confidentiality, integrity, and availability of web information resources [5]. It is divided into three categories: network traffic based, web access logs based, and traps-based detection system. In network traffic and web access, log-based detection techniques employ the pattern recognition problem to detect the malicious activity in network traffic and web access log. Each activity is classified as web robots or normal users [6]. In contrast, the trap-based system sets a trap in the web application, and for any request to access this trap, the host making that request is marked as a robot. Web robot identification has traditionally relied on signature-based algorithms, which are time-consuming and prone to human error.

Furthermore, it is unable to detect developing cyber threats. However, a new technique, Data-Mining/Machine-Learning, has been effectively employed for online robot identification in recent years [7]. As web robot classifiers, machine learning techniques have been applied to detect web robots automatically using an example of user behavior or network data as a training set. It eliminates the requirement for the rule to incorporate any human expert knowledge.

The available datasets of NASA95 log and anonyms log have more than three million records. In the literature review, we observed that researchers perform their experiment with a standard dataset, some of them using features selection and some of them used balancing only a few of them used both balancing and feature selection. As shown in Fig. 2, both datasets have an imbalance in their classes, with the major class having a large number of instances. As a result, one of the primary goals of this research is to investigate the impact of class balance on model development and performance. The objectives which are addressed in this work are:

- Finding out what is the utility of feature selection in class imbalance data for classification,
- Which sampling technique can best solve the class imbalance problem in web robot detection, such as major class under-sampling, minor class over-sampling, and combining both?
- Which machine learning classifiers are the best for detecting and classifying web robots?

The remainder of the paper is structured as follows: the literature survey of the related work is present in the next section, followed by a methodology which includes the NASA 95 access log datasets and anonymous website access log datasets utilized in the experiments with class balancing problem discussed in details. The fourth section discussed the experimental setup and feature selection approach. Followed by the classifier's performance measure. The fifth section provides a comprehensive examination of the experimental data. Finally, in the final section of the paper, the conclusion is drawn.

2 Related Work

Gray, for his report [20], uses the autonomous software agent World Wide Web Wanderer, the first automated web agent, to collect statistics to measure the growth of the web. The number and types of autonomous software agents increase rapidly. Autonomous software agents can be of many types such as indexer, email checker, link checker, and many more; thus, generally, autonomous agents are referred to as robots. Google and yahoo use robots for page indexing. However, robots are also used for many malicious purposes; one is a DDoS attack which is a focus of the report. A detailed literature survey in the following section provides insights into the problem.

Tan and Kumar [21] use click-stream data navigational patterns to classify whether a request was generated by a robot or a human. Their model is capable of detecting a wide range of camouflaged and previously unknown robots. Kwon et al. [22] explain the three novel features whose switching factor was used in web robot detection. They extend types of web robots from only text crawler, link crawler, and email harvester to image collectors, icon collectors, download tools. Grazinic et al. [23] propose an intelligent system called Lino for detection. It's a technique that traps web crawlers by simulating a vulnerable web page. They used C4.5 and Support Vector Machine (SVM). Stassopoulou and Dikaiakos [24] propose a Bayesian network as a probabilistic modeling approach for robot detection. They use machine learning techniques to figure out the probabilistic model's parameters. Stevanovic et al. [25] investigate the effects of using seven different classifiers: C4.5, RIPPER, k-Nearest Neighbor (kNN), Naive Bayesian, Bayesian Network, Support Vector Machine (SVM), and Neural network. They also introduce two new web-session features: the consecutive sequential request ratio and page request depth standard deviation.

When it comes to web robot session identification, Sisodia et al. [26] study the efficacy of ensemble-based learners, which include Bagging, Boosting, and Voting, among other things. Learners' performance can be improved by labeling their robot sessions with multifold techniques. S. Renuka Devi et al. [27] present an effective and efficient defense method against distributed denial of service (DDoS) attacks that is based on information metrics (entropy). The technique includes a second checkpoint for distinguishing the malicious flow from the normal flow in order to detect the malicious flow. It verifies that the user is a legitimate one based on their previous activity. It determines whether a session is suspicious based on the information metric of the current session and the user's previous browsing history.

Sujatha Sivabalan et al. [28] present novel techniques for recognizing and stopping various DDoS attacks, including those involving legitimate users in flash crowds. Its primary purpose is to provide application-layer algorithms that detect attack traffic while allowing legitimate traffic to access web services. It uses CAPTCHA or AYAH to authenticate the user's signature. Tongguang Ni et al. [29] offer a novel approach to detect DDoS attacks based on the features of the DDoS attack. The project makes two contributions: (1) HTTP GET requests per source IP address (HRPI) is a new metric for detecting DDoS attacks that highlights the most important characteristics of the attacks. (2) A DDoS attack detection technique is proposed, which has a high detection efficiency and adaptability. According to Satyajit Yadav et al. [30], a model based on Logistic Regression was developed for modeling typical user browsing behavior in order to detect application-layer DDoS attack traffic, if any, from incoming traffic. Using a new constraint-based group testing (GT) model, Ying Xuan et al. [31] suggested a unique technique for identifying application DoS attacks. Three detection algorithms were proposed, and a system based on these algorithms was introduced, all of which were inspired by classic GT approaches. To combat flood attacks, Charles Tang et al. [32] suggest a meta-data-based monitoring system in which the behavior of malicious HTTP requests is captured by real-time and big-data analysis. Even when the attacking line rate is as high as 9 Gbps, the proposed DDoS defense system can continue to provide service to legitimate clients.

Takeshi Yatagai et al. [33] propose a DoS attack detection method. They consider two algorithms: one focuses on page surfing order, and the other on a correlation between browsing time and page information size on the web page. Using the access log of the Internet web server, they created the attack detection system and evaluated a false positive and false negative. Derek Doran et al. [34] describe a unique web robot identification approach based on the differences between robot and human resource request patterns. The proposed strategy is based on a behavioral difference between humans and robots that is invariant. Gregoire Jacob et al. [35] proposed the PUB CRAWL strategy for detecting and containing crawlers, as well as the first technique for crawler campaign attribution that identifies synchronized traffic from many hosts.

3 Methodology

Figure 1 is represented the flow of the model design experiment in this functional representation of the framework.

3.1 Web Access Log Dataset

Whenever a website's users make requests for resources, the webserver records these requests in a simple plain text file; this file is called a weblog file [17]. Access log, agent log, error log, and referrer log files are the four categories of server logs. For web servers such as Apache, the Common Log Format (CLF) is the standard log format [18, 19]. Each HTTP request is logged in the CLF log file. In each line, tokens are separated by spaces. A hyphen (-) represents a token that has no value. There are nine fields in a log entry shown in Fig. 2: [Ip Address] of the users, [Name] is the user name, [Login] is the HTTP-authentication of the login user, [Date/Time] is request date and time, [Request] is HTTP request which contains the HTTP Method, the resource URL, and HTTP-protocol; [Status] is a server response code which has three-digit, [Size] is the server response size in bytes, [Referrer] is the referring page URL, and [User-Agent] is the name of browser signature. The client provides the request, referrer, and agent, which are untrustworthy in terms of analysis. The remaining fields are the web server-generated fields and are hence reliable.

In this work investigating the web robot detection method for web access log-based web robot detection systems have widely used the NASA 95 dataset. Apart from this,

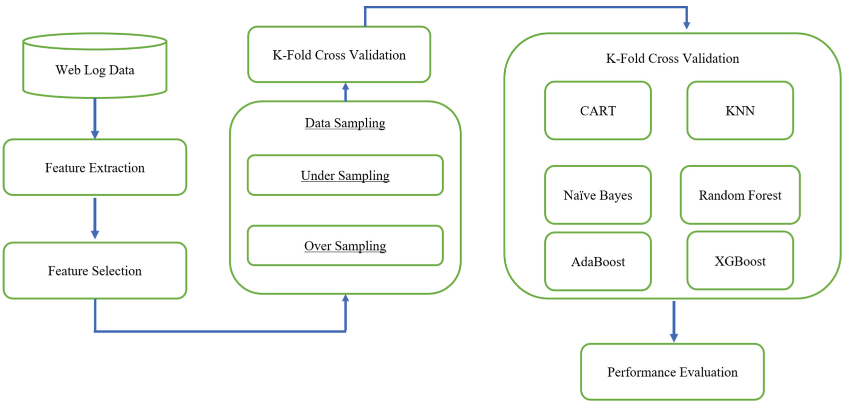


Fig. 1. Visual representation of the framework

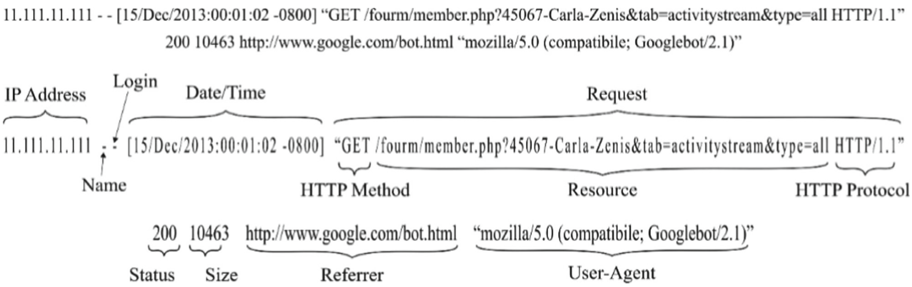


Fig. 2. Example of an entry in a weblog file with each field details

Table 1. List of features of NASA95 dataset

Sr.No	Feature Name	Sr.No	Feature Name	Sr.No	Feature Name	Sr.No	Feature Name
1	total Pages	8	per Zip	15	Repeated Access	21	width
2	per Image	9	per Multimedia	16	Error Request	22	height
3	per Binary Doc	10	per other files	17	GET	23	total Requests
4	per Binary Exec	11	Total time	18	POST	24	Referrer null
5	Robots.txt	12	Average time	19	HEAD	25	Nonunique IP
6	pre HTML	13	Stdev time	20	OTHER method	26	Nonunique Agent
7	per Ascii	14	Night				

website access log datasets of several universities have also been used, some e-commerce website access log data have also been used in a recent study. In this study, we used NASA 95 web access log and an anonymous website access log which are available in the online dataset repository. The NASA 95 web server access log data consists of 26 features shown in Table 1 and 180602 sessions. Anonyms web server access log of a portal that provides its services to worldwide visitors in the USA. It consists of 32 features shown in Table 2 and 52936 sessions. In both datasets each session is labeled as four categories' classes namely Known Browsers, Known Robots, Possible Browsers,

Table 2. List of features of Anonymous dataset

Sr.No	Feature Name	Sr.No	Feature Name	Sr.No	Feature Name	Sr.No	Feature Name
1	total_request	9	night_request_%	17	multi_agent	25	other_ext_%
2	GET_request_%	10	session_time	18	images_%	26	session_ppi
3	POST_request_%	11	avg_time	19	binary_doc_%	27	html2image
4	HEAD_request_%	12	stdev_time	20	binary_exec_%	28	std_depth
5	Other_request_%	13	width	21	html_%	29	proxy_request
6	errors_%	14	depth	22	ascii_%	30	url_resolution
7	repeated_request_%	15	request_pages	23	zip_%	31	unique_page_request_%
8	blank_referrer_%	16	multi_ip	24	multimedia_%	32	robots.txt

and Possible Robots. In both, the labeled classes' datasets are imbalanced, as shown in Fig. 3. The graph shows that the NASA 95 dataset is highly imbalanced because it has a large number of instances in one class and fewer instances in others. Anonymous datasets have a sufficient number of instances in three classes but fewer instances in one class which makes it imbalanced.

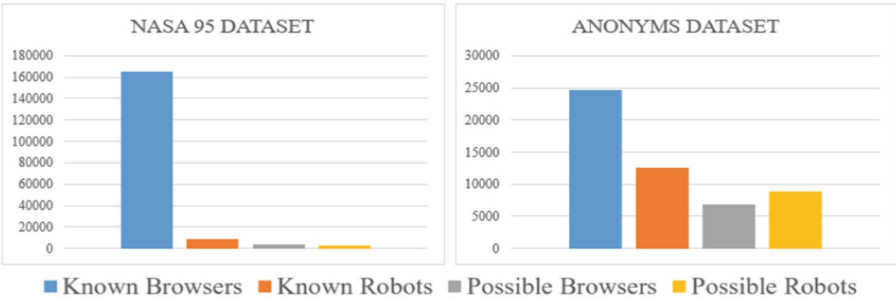


Fig. 3. Class distribution of NASA95 and Anonyms datasets

3.2 Class Imbalance

The web robot detection process, which is based on machine learning, begins with the collection of web access log data, which has a number of features, after then, the data is labeled as belonging to a human user or a web robot, and a learning algorithm is applied to the labeled data. In the process of labeling, it is found that, in general, the distribution of these labels is unbalanced; as a result, the training data sets have an uneven distribution of classes. One of the complex problems in binary or multi-class classification is the class imbalance problem because of an imbalance in the occurrences of classes. In an imbalanced data set, the class with the most occurrences is referred to as the major class, while the class with the fewest instances is referred to as the minor class. Some classifiers may be biased towards the major class (es) in such a circumstance, which can result in poor performance of the minor class(es) [8–10]. As a result, when there is an imbalance, the classifier wrongly predicts everything as belonging to the major class while completely ignoring the minor class [11, 12]. In practically all other real-world machine learning applications, this problem occurs. Some of the examples listed in [8] include text classification, medical condition diagnosis, oil spill detection, video surveillance, and network intrusion detection. Several domains have conducted an extensive study on the class imbalance problem, including intrusion and fraud detection [9], credit scoring [13], text recognition [14], bioinformatics [15], medicine [16].

To find out how feature selection and sampling procedures affect imbalanced dataset classification, the study presented in this paper. Because the accuracy of a classifier's classification is dependent on the features used to identify a pattern, it is hypothesized that adjusting the number of major and minor classes will correct any class imbalance. Hence, different feature selection approaches are studied in this study, as well as classification accuracy, major classes are under-sampled while minor classes are synthetically over-sampled.

4 Experiment Setup

All of the experiments were carried out on a workstation PC with a 64-bit Windows operating system, an Intel Xeon 3.30 GHz processor, 32 GB of RAM, and an Nvidia P1000 Graphics card. Scikit-learn, an open-source machine learning package used for different learning algorithms and feature selection. This package is a python-based machine learning algorithms collection related to data visualization, preprocessing, feature selection, classification, clustering, and regression. For class balancing, the Imbalanced-Learn library is used which is developed on top of Scikit-learn. This empirical investigation focuses on feature selection, class imbalance, and classification methods.

4.1 Feature Selection

An important step in the development of any model, particularly an empirical one, is feature selection. It not only reduces the dimensionality of the data but also allows the classifier to work more quickly and accurately as a result of this reduction. The datasets used in this experiment contain 26 features in NASA 95 dataset and 36 features in the anonyms dataset; Only significant features impacting many classes should be evaluated for model construction, as this is computationally efficient. In this study, a two-step feature selection approach is used. in the first step, a search method was used to select the set of features; in the second step, an evaluation function was used for evaluating the selected features in the first step. More than one type of search method was employed to improve the accuracy of the results. In the first phase, the genetic search method with a decision tree as an estimator was used to select features, which was then evaluated for the level of redundancy between them and their predictive performance. A subset of features with a high correlation to the class labels but a low degree of connection between them was chosen.

The rank method was also used to select the features. Two statistical metrics, info gain, and gain ratio were used to evaluate the features. Based on the information gain, gain ratio, and rank, these three algorithms generated a list of twenty features for the NASA95 Dataset and twenty-five Features for the anonymous dataset. The features used were those that were recommended by at least two of the algorithms mentioned above. Table 3 and Table 4 show the feature that was selected using this method. As shown in Table 3, the feature representing per_HTM, per_Ascii, per_other_files, POST, height, and Nonunique_IP should not be used for web robot classification in the NASA95 dataset; rather, it is the total pages, HEAD request and average time that has a significant effect on the type of robot class and should thus be monitored for web robot detection. For the anonymous dataset selected features to show in Table 4, remove the error_%, width, multiple_ip, multiple_agents, ascii_%, Zip_% and other_ext_% from the features list, which is not utilized for web robot classification.

Table 3. List of selected features of the NASA95 dataset

Sr.No	Feature Name	Sr.No	Feature Name	Sr.No	Feature Name	Sr.No	Feature Name
1	total Pages	8	per Zip	14	Night	20	OTHER method
2	per Image	9	per Multimedia	15	Repeated Access	21	width
3	per Binary Doc	11	Total time	16	Error Request	23	total Requests
4	per Binary Exec	12	Average time	17	GET	24	Referrer null
5	Robots.txt	13	Stdev time	19	HEAD	26	Nonunique Agent

Table 4. List of selected features of Anonymous dataset

Sr.No	Feature Name	Sr.No	Feature Name	Sr.No	Feature Name	Sr.No	Feature Name
1	total_request	9	night_request_%	19	binary_doc_%	29	proxy_request
2	GET_request_%	10	session_time	20	binary_exec_%	30	url_resolution
3	POST_request_%	11	avg_time	21	html_%	31	unique_page_request_%
4	HEAD_request_%	12	stdev_time	24	multimedia_%	32	robots.txt
5	Other_request_%	14	depth	26	session_ppi		
7	repeated_request_%	15	request_pages	27	html2image		
8	blank_referrer_%	18	images_%	28	std_depth		

4.2 Classifier Selection

After selecting the best features, six different classifiers were investigated for two sampling approaches. Because the data set contains a very small number of rare classes, only 30% of the total instances of large classes (such as the known browser and possible robots) were sampled, but the number of the minor class instances was maintained at the same level. The data was then utilized for model construction using a set of six classifiers with five-fold cross-validation. Using the SMOTE technique (Synthetic Minority Oversampling Technique), the second approach was taken. An informed over-sample of minorities combined with a random under-sample of the majorities is known as SMOTE. Prior to selecting any of these algorithms, it computes the nearest neighbors of the minority sample and then uses the results to create synthetic samples that connect those selected neighbors with each other. Six different classifiers were employed to create the models after the data was preprocessed with SMOTE. Five-fold cross-validation was used to test each classifier. The classifiers' performance was then assessed using the confusion matrix outlined in the following section for all classifiers under the two sampling approaches.

4.3 Classifier Performance Measure

Confusion matrices are commonly used to describe the predicted number of instances by a classifier. A large number of them are classified as either True Positive (TP), False Negative (FN), False Positive (FP), or True Negative (TN) by the classification system (TN). Where, To the extent that the classifier's predictions have been correct, this value is equivalent to the number of positive cases the classifier incorrectly predicted as negative. The number of negative instances incorrectly predicted by the classifier as positive Number of negative samples that classifier accurately predicts as positive.

5 Result and Analysis

Table 5 and Table 6 show the comparative performance of all classifiers with under-sampling of major classes and oversampling of minor classes using SMOTE. The TP-rate of the confusion matrix was used to determine the performance of the model. The table shows that the sample procedures utilized in this study, i.e., undersampling and oversampling of major and minor class, had no effect on the major class classification, with TP rates exceeding 95%, all classifiers have classified the major classes, i.e. known browser. The impact of these two sample methods, on the other hand, maybe seen in the classification of minor classes. For minor classes, the TP rate increased when classifiers are employed in conjunction with a minor class oversampling strategy. In KNN, the result shows that KNN has detected the minor classes. However, regardless of the sampling technique, this table shows that no single classifier can classify all types of classes in web robot detection. Classes with higher instances, such as known browsers, were efficiently detected at a higher TP rate of over 95% by XGBoost, KNN, Random Forest, Naive-Bayes, and AdaBoost.

XGBoost method showed 86% over accuracy but failed to detect the minor class of possible robots with a TP rate of less than 65% under both sampling techniques. Similarly, the AdaBoost classifier failed to detect possible robots with a TP rate of less than 65% for the two-sample techniques employed in this study. When using the SMOTE approach for preprocessing, the data is over-sampled, KNN had a better tendency to identify possible robots than under-sampling, with an accuracy of 74% TP rate. With respect to the Naive Bayes classifier, similar over-sampling techniques improved accuracy by identifying the possible robot with an accuracy of 65%. As a result, none of the classifiers was found to be able to identify both the minor and the large classes individually, with a TP rate of more than 90%, as shown by this result. However, the KNN classifier method showed the highest TP rate of 89% for possible browsers and 75% for the possible robot, as well as a TP rate of over 90% for other major classes, among all the examined classifiers. Other minor classes, such as know browser, have a higher TP rate using Nave Bayes (85 percent). The results suggest that an ensemble of models might be used to identify minor and major classes with a TP rate of more than 90%. KNN classifier and XGBoost are indicated as the optimum combination based on TP and FP values to obtain a robust model for classifying all classes, especially minor ones.

6 Conclusion

This research work found that only minor class classifications are affected by the sampling of web robot data, not the major class, and compared to under-sampling, SMOTE

Table 5. TP-rate of classifiers for the NASA95 dataset using two distinct sampling approaches.

Sampling/Models	Class Labels							
	Known Browsers		Known Robots		Possible Browsers		Possible Robots	
	SMOTE	Under Sample	SMOTE	Under Sample	SMOTE	Under Sample	SMOTE	Under Sample
CART	0.959	0.959	0.759	0.747	0.796	0.712	0.629	0.638
KNN	0.960	0.947	**0.768**	0.758	**0.866**	0.808	**0.742**	**0.734**
Naïve Bayes	0.959	0.960	0.760	0.760	0.753	0.709	0.628	0.601
Random Forest	0.956	0.956	0.743	0.754	0.735	0.721	0.703	0.713
AdaBoost	0.956	0.956	0.752	0.757	0.613	0.740	0.642	0.613
XGBoost	**0.970**	**0.969**	**0.768**	**0.765**	0.817	**0.821**	0.655	0.621

Table 6. TP-rate of classifiers for the NASA95 dataset using two distinct sampling approaches.

Sampling/Models	Class Labels							
	Known Browsers		Known Robots		Possible Browsers		Possible Robots	
	SMOTE	Under Sample	SMOTE	Under Sample	SMOTE	Under Sample	SMOTE	Under Sample
CART	0.972	0.969	**0.869**	0.857	0.866	0.802	0.639	0.648
KNN	0.969	0.964	0.864	**0.868**	**0.896**	0.828	**0.752**	**0.744**
Naïve Bayes	0.969	**0.970**	0.870	0.870	0.863	0.819	0.648	0.631
Random Forest	0.954	0.954	0.853	0.864	0.745	0.831	0.643	0.603
AdaBoost	0.966	0.966	0.862	0.867	0.623	**0.850**	0.652	0.653
XGBoost	**0.980**	0.969	0.868	0.865	0.807	0.831	0.645	0.637

oversampling produced more accurate minor class identification. When compared to the AdaBoost, CART, Random Forest, and naïve Bayes methods, the KNN approach combined with XGBoost is more effective in the detection of minor classes than either of these techniques. Furthermore, we discovered that no single technique can be employed for the classification of multiclass data pertaining to web robots, which is a significant finding. KNN and XGBoost are two classifiers that can be employed in conjunction for the classification of minor classes of imbalance class data in web robot detection. Therefore, we suggest that combine two classifiers, namely KNN and XGBoost, to accurately classify all of the classes, particularly minor ones. This will ensure that all of the classes, including minor ones, are correctly classified. Our goal in the future is to create a model by combining these two types of classifiers (KNN and XGBoost) and applying weight estimation approaches to create a single model.

References

1. Tan, P.-N., Kumar, V.: Modeling of Web Robot Navigational Patterns. no. March 2002 (2000)

2. Hayati, P., Potdar, V., Chai, K., Talevski, A.: Web spambot detection based on web navigation behavior. Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA, no. June 2014, pp. 797–803 (2010)
3. Kalim, A., Jha, C.K., Tomar, D.S., Sahu, D.R.: A Framework for web application vulnerability detection. Int. J. Eng. Adv. Technol. **9**(3), 543–549 (2020)
4. Jaafar, G.A., Abdullah, S.M., Ismail, S.: Review of recent detection methods for HTTP DDoS attack. J. Comput. Networks Commun, vol. 2019 (2019)
5. Marques, P., et al.: Detecting malicious web scraping activity: a study with diverse detectors. In: Proc. IEEE Pacific Rim Int. Symp. Dependable Comput. PRDC, vol. 2018-Decem, pp. 269–278 (2019)
6. Doran, D., Gokhale, S.S.: Web robot detection techniques: overview and limitations. Data Min. Knowl. Discov. **22**(1–2), 183–210 (2011)
7. Chen, H., He, H., Starr, A.: An overview of web robots detection techniques. In: Int. Conf. Cyber Secur. Prot. Digit. Serv. Cyber Secur. 2020 (2020)
8. Andrew, E., Japkowicz, N.: A mixture-of-experts framework for learning from imbalanced data sets.pdf. LNCS, pp. 34–43 (2001)
9. Cieslak, D.A., Chawla, N.V., Striegel, A.: Combating imbalance in network intrusion datasets. In: 2006 IEEE Int. Conf. Granul. Comput., pp. 732–737 (2006)
10. Chawla, N.V., Japkowicz, N., Kolcz, A.: C4.5 and imbalanced data sets: investigating the effect of sampling method, probabilistic estimate, and decision tree structure. Proc. Int. Conf. Mach. Learn. (2003)
11. Khoshgoftaar, T.M., Golawala, M., Van Hulse, J.: An empirical study of learning from imbalanced data using random forest. In: Proc. - Int. Conf. Tools with Artif. Intell. ICTAI, vol. 2, pp. 310–317 (2007)
12. Qazi, N., Raza, K.: Effect of feature selection, Synthetic Minority Over-sampling (SMOTE) and under-sampling on class imbalance classification. In: Proc. - 2012 14th Int. Conf. Model. Simulation, UKSim 2012, no. March, pp. 145–150 (2012)
13. Krause, M.: On Class Imbalance Correction for Classification Algorithms in Credit Scoring, no. February 2018 (2016)
14. Li, Y., Sun, G., Zhu, Y.: Data imbalance problem in text classification. In: Proc. - 3rd Int. Symp. Inf. Process. ISIP 2010, pp. 301–305 (2010)
15. Wald, R., Khoshgoftaar, T.M., Fazelpour, A., Dittman, D.J.: Hidden dependencies between class imbalance and difficulty of learning for bioinformatics datasets. In: Proc. 2013 IEEE 14th Int. Conf. Inf. Reuse Integr. IEEE IRI 2013, pp. 232–238 (2013)
16. Rahman, M.M., Davis, D.N.: Addressing the class imbalance problem in medical datasets. Int. J. Mach. Learn. Comput. **3**(2), 224–228 (2013)
17. Castellano, G., Fanelli, A.M., Torsello, M.A.: Log data preparation for mining web usage patterns. In: Computing, no. June, pp. 371–378 (2007)
18. Alnoamany, Y., Weigle, M.C., Nelson, M.L.: Access patterns for robots and humans in web archives. In: Proc. ACM/IEEE Jt. Conf. Digit. Libr., pp. 339–348 (2013)
19. Stassopoulou, A., Dikaiakos, M.D.: A Probabilistic Reasoning Approach for Discovering Web Crawler Sessions. In: Dong, G., Lin, X., Wang, W., Yang, Y., Yu, J.X. (eds.) APWeb/WAIM -2007. LNCS, vol. 4505, pp. 265–272. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-72524-4_29
20. Gray, M.: Measuring the growth of the web. [Online]. Available: http://www.mit.edu/people/mkgray/growth/
21. Tan, P.N., Kumar, V.: Discovery of web robot sessions based on their navigational patterns. Data Min. Knowl. Discov. **6**(1), 9–35 (2002)
22. Lourenço, A., Belo, O.: Catching web crawlers in the act. ICWE'06 Sixth Int. Conf. Web Eng., pp. 265–272 (2006)

23. Nguyen, N.T., Trawiński, B., Kosala, R.: Lino – an intelligent system for detecting malicious web-robots. In: Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 9012, pp. 1–2 (2015)
24. Stassopoulou, A., Dikaiakos, M.D.: Web robot detection: a probabilistic reasoning approach. Comput. Networks **53**(3), 265–278 (2009)
25. Stevanovic, D., An, A., Vlajic, N.: Feature evaluation for web crawler detection with data mining techniques. Expert Syst. Appl. **39**(10), 8707–8717 (2012)
26. Sisodia, D.S., Verma, S., Vyas, O.P.: Agglomerative approach for identification and elimination of web robots from web server logs to extract knowledge about actual visitors. J. Data Anal. Inf. Process. **03**(01), 1–10 (2015)
27. Renuka Devi, S.: Detection of Application Layer DDOS Attacks Using Information Theory Based Metrics, pp. 217–223 (2012)
28. Sivabalan, S., Radcliffe, P.J.: A novel framework to detect and block DDoS attack at the application layer. In: IEEE 2013 Tencon - Spring, TENCONSpring 2013 - Conf. Proc., pp. 578–582 (2013)
29. Ni, T., Gu, X., Wang, H., Li, Y.: Real-time detection of application-layer DDoS attack using time series analysis. J. Control Sci. Eng. **2013** (2013)
30. Yadav, S., Selvakumar, S.: Detection of application layer DDoS attack by modeling user behavior using logistic regression. In: 2015 4th Int. Conf. Reliab. Infocom Technol. Optim. Trends Futur. Dir. ICRITO 2015, pp. 0–5 (2015)
31. Xuan, Y., Shin, I., Thai, M.T., Znati, T.: Detecting application denial-of-service attacks: a group-testing-based approach. IEEE Trans. Parallel Distrib. Syst. **21**(8), 1203–1216 (2010)
32. Tang, C., Tang, A., Lee, E., Tao, L.: Mitigating HTTP flooding attacks with meta-data analysis. In: Proc. - 2015 IEEE 17th Int. Conf. High Perform. Comput. Commun. 2015 IEEE 7th Int. Symp. Cybersp. Saf. Secur. 2015 IEEE 12th Int. Conf. Embed. Softw. Syst. H, pp. 1406–1411 (2015)
33. Yatagai, T., Isohara, T., Sasase, I.: Detection of HTTP-GET flood attack based on analysis of page access behavior. IEEE Pacific RIM Conf. Commun. Comput. Signal Process. - Proc., pp. 232–235 (2007)
34. Doran, D., Gokhale, S.S.: Detecting web robots using resource request patterns. In: Proc. - 2012 11th Int. Conf. Mach. Learn. Appl. ICMLA 2012, vol. 1, pp. 7–12 (2012)
35. Jacob, G., Kruegel, C.: PUBCRAWL : protecting users and businesses from CRAWLers. In: Protecting Users and Businesses from CRAWLers Gregoire, pp. 507–522 (2009)

A Random Forest-Based Ensemble Technique for Malware Detection

Lalit Kumar Vashishtha[1](✉), Kakali Chatterjee[1], Santosh Kumar Sahu[2], and Durga Prasad Mohapatra[2]

[1] Department of CSE, NIT Patna, Patna, India
{lalitv.phd20.cs,kakali}@nitp.ac.in
[2] Department of CSE, NIT Rourkela, Rourkela, India
santoshsahu@hotmail.co.in, durga@nitrkl.ac.in

Abstract. With the widespread development of Internet interconnectivity, the opportunities for digital attacks have widened, many of which have damaging and severe implications. Malware is one type of cyber assault that is becoming more prevalent day by day. The conflict between security researchers and malware creators is an ongoing battle with the quick evolution of malware as technological innovation develops. Analysts are researching to identify it, while cybercriminals devise methods to conceal it. Researchers have proposed several approaches to identify malware, of which the machine learning approaches are prevalent. An ensemble-based approach has been proposed in this paper, consisting of C-means and Random Forest approaches and Local Outlier Factor, which outperforms the existing methods.

Keywords: C-means · Random Forest · UCI dataset · Local Outlier Factor · Feature selection

1 Introduction

Cybercriminals get unauthorized access to the computer system since the malware changes the attack patterns using obfuscation techniques (packing or encryption) to evade detection. Therefore, it is challenging to design a malware detection engine to detect novel attacks. According to [12] machine learning techniques play a vital role in almost all research fields. A single detection method may not be able to detect novel attacks. As a result, a sophisticated detection approach becomes utmost essential to protect the digital resources from intruders. According to [5] "It is a machine learning model in which numerous learners (individual models) are trained to solve a common problem."

Local outlier factor [8], C means clustering algorithm [15] and Random forest [4] have been used in our experiments.

Our Contribution in this paper is as follows:

– We have reviewed malware analysis techniques in detail with the limitations of the approaches.

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 454–463, 2023.
https://doi.org/10.1007/978-3-031-13150-9_36

– LOF has been used to study the exceptions.
– We have applied different machine learning algorithms in our proposed framework to measure the performances.

The following is a breakdown of the paper's structure. Section 2.1 contains related work and description of dataset on which the experiments have been performed. In Sect. 3, we shall discuss the proposed model. Section 4 involves result analysis, and Sect. 5 contains the conclusion.

2 Related Work

This section contains literature review and dataset description used in our experiments

2.1 Literature Review

We have summarized some recent work on ensemble approaches to address malware detection problems using different techniques. Tables 1, 2 and 3 shows the earlier implemented results based on the algorithm used, selected features, and their limitations year-wise.

2.2 Dataset Description

We downloaded the dataset from UCI dataset repository [1]. This dataset contains 6248 instances and 1086 attributes, of which 5654 are attacks, and 594 are benign. This dataset is in CSV format. It consists of composed of 3 datasets-

1. **staDynBenignLab.csv:** Windows 7 and 8 based features are extracted from 595 files
2. **staDynVxHeaven2698Lab.csv:** taken from 2698 files of VxHeaven
3. **staDynVt2955Lab.csv:** taken from 2955 files of Virus Total.

3 Proposed Model

In this section, we have proposed a malware detection model using machine learning techniques for malware detection. The workflow of the model is shown in Fig. 1. The architecture of our proposed model includes five steps: disassembling process to extract features, feature representation, feature optimization, training process using different classifiers, and performing testing to evaluate the model performance.

The proposed ensemble technique is discussed in Algorithm 1. The dataset D contains N instances with M features. The class label C is extracted from the original dataset D'. The LOF method is optimized by tuning its model parameters, separating the outliers, and forming an outlier group that is later labeled using the random forest algorithm. The C-Means approach clusters the

Table 1. Review on malware detection methods using AI/ML approaches

Paper	Year	Algorithm used	Features	Limitations
[2]	2016	XGBoost and Bagging	N-gram, metadata, entropy, string length, symbol, opcode, API, register, section	Obfuscation was not considered, unpacking of the sample was avoided
[13]	2021	SVM, XGB, RF and MLP	N-grams, printable strings	Database is not properly distributed
[10]	2019	Decision tree, random forest, KNN, XGBoost	Open, read, write, delete, failed	The detection accuracy fluctuates, the correlation between different characteristics of malware needs to be further explored since the characteristics of the malware are not isolated in any way there may exist some connection among them.
[7]	2019	Random forest, linear regression, polynomial regression	FindFirstFileA, FindNextFileA, LoadLibraryW, LoadLibraryA	Linear and polynomial regression show inefficient result
[9]	2021	XGBoost	Opcode, segment, secondary feature, malware images	The proposed work is for grey scale images, it could be checked for colored images.
[14]	2021	K-means clustering algorithm	TimeDateStamp, NumberOfSections, NumberOfSymbols, Machine, SizeOfCode, and CheckSum	PE header need extra study to get appropriate features for better computational complexity
[6]	2011	SVM	Graph kernel	Used small dataset
[16]	2019	K means and SVM	–	–
[20]	2020	Nearest neighbour algorithms and hamming distance	Permissions, API,intent	Cannot detect the same program with the same functionality with different features
[17]	2020	Extra tree classifier Naïve Bayes, Logistic regression, SVM	–	Useful for only unpacked samples
[3]	2020	SVM	n-gram of length 2–5	Very small data is used
[11]	2021	Naïve Bayes, Multi-level perceptron, decision tree, deep ANN	API call	Malware family classification on dynamic layer is not good
[15]	2014	K-means,C-means algorithms	–	Cannot be used for other attacks
[18]	2020	CFS-BA, C4.5, RF, Forest PA	–	Not suitable for unknown attacks
[19]	2019	SCAD-RNN intrusion detection system	–	Training time is high

data elements into two clusters. The value of C is set to be two as per the classes available in the dataset. The three clusters (one outlier cluster and two clusters generated using C-Means) are labeled using the optimized random forest method. Finally, for performance assessment, several performance matrices are calculated using the confusion matrix elements along with the ROC curve.

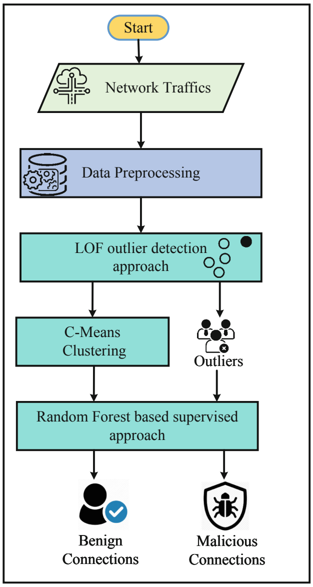


Fig. 1. Architectural diagram of proposed approach

Table 2. Initial evaluation results

Model	AUC	CA	F1	Precision	Recall
kNN	0.984	0.975	0.976	0.977	0.975
Decision Tree	0.444	0.905	0.860	0.819	0.905
Random Forest	0.999	0.987	0.986	0.987	0.987
Neural Network	0.985	0.970	0.970	0.971	0.970
Adaboost	0.970	0.990	0.990	0.990	0.990

Algorithm 1. Proposed Ensemble Approach for Malware Detection

Require: Malware Dataset D comprising of N instances with M features and C classes
Ensure: Benign and malicious class labels on malicious dataset
1: $D' = Preprocess(D(N, M, C))$
2: $Class = Extract\_Class(D')$ pc
3: *Label_LOF = Optimize(LoF(D'))*
4: *Cluster_Ind = CMeans(D')*
5: *Predicted_Class = Optimize(Rand_Forest(D', Class))*
6: [Con_Mat, ROC, Others]=*Performance_Eval(Predicted_Class, Class)*

4 Result Analysis

Experiments have been performed using machine learning approaches: Adaboost, KNN, Neural Networks, Decision tree, and Random Forest on UCI dataset. Initially, we experimented on the original dataset with 1087 features, and their results have been discussed in the Subsect. 4.1, Adaboost outperforms with all 1087 features. Six feature selection algorithms have been used to reduce the features to 30, which is shown in Fig. 2. After feature selection, the experiments have been performed with the above algorithms (Adaboost, KNN, Neural Networks, Decision Tree, and Random forest), and the results are discussed in Subsect. 4.2. Random Forest outperforms all the supervised machine learning approaches over the dataset with 30 features. Local outlier factor has been applied on the dataset with 30 features to cluster the dataset into inliers and outliers. Then C-Means

	Info. gain	Gain ratio	Gini	χ^2	ReliefF	FCBF
minor_image_version	0.325	0.314	0.121	4004.081	0.000	0.775
minor_operating_system_version	0.319	0.297	0.123	3632.130	0.000	0.000
major_operating_system_version	0.253	0.137	0.092	1144.571	0.115	0.000
minor_subsystem_version	0.239	0.170	0.103	469.058	0.038	0.346
major_subsystem_version	0.220	0.131	0.086	973.310	0.080	0.000
size_of_stack_reserve	0.219	0.214	0.065	505.853	0.016	0.000
major_image_version	0.219	0.140	0.062	3225.851	0.000	0.000
minor_linker_version	0.178	0.105	0.053	6.897	0.038	0.000
dll_characteristics	0.166	0.112	0.044	1426.753	0.318	0.000
major_linker_version	0.162	0.083	0.040	1189.308	0.010	0.000
CheckSum	0.128	0.072	0.027	342.933	-0.000	0.000
characteristics	0.106	0.057	0.026	596.623	0.220	0.000
compile_date	0.095	0.048	0.024	11.722	0.067	0.000
pushf	0.085	0.043	0.020	0.582	0.001	0.000
size_of_stack_commit	0.079	0.058	0.022	71.890	0.002	0.000
number_of_sections.1	0.072	0.036	0.020	24.854	0.013	0.000
number_of_IAT_entires.1	0.070	0.036	0.012	393.288	0.033	0.000
number_of_IAT_entires	0.070	0.036	0.012	393.288	0.033	0.000
not	0.067	0.034	0.015	15.441	0.001	0.000
files_operations	0.064	0.042	0.010	474.915	0.000	0.069
.text:	0.061	0.062	0.009	101.579	0.056	0.000
count_dll_loaded	0.054	0.038	0.008	409.358	0.017	0.000
SizeOfHeaders.1	0.054	0.043	0.009	114.133	0.083	0.000
size_of_headers	0.054	0.043	0.009	114.133	0.083	0.000
SizeOfHeaders	0.054	0.043	0.009	114.133	0.083	0.000
count_file_opened	0.052	0.038	0.008	349.667	0.001	0.000
int	0.049	0.025	0.010	247.525	0.002	0.000
nop	0.046	0.023	0.010	261.173	-0.001	0.000
shr	0.044	0.022	0.010	0.257	0.004	0.000
ret	0.041	0.020	0.008	6.770	0.003	0.000

Fig. 2. Summary of feature selection methods on malware dataset

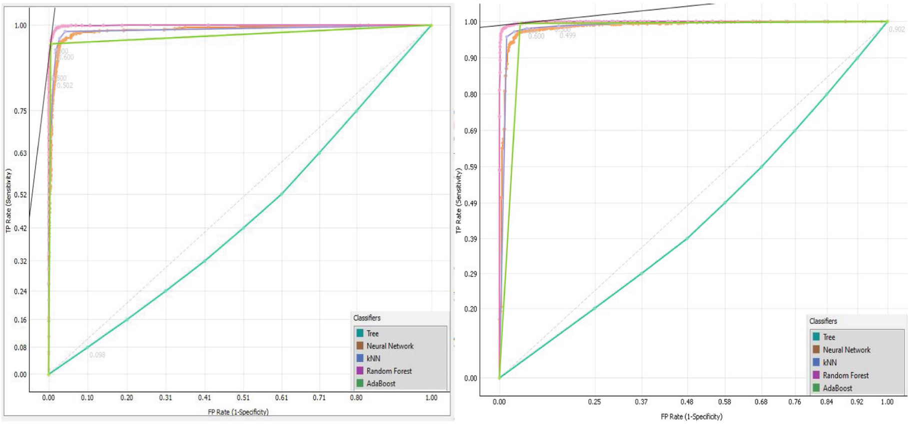
algorithm is used on inlier data. Since, after feature selection, the Random Forest outperforms. Therefore the Random Forest method is used as the supervised approach to label the two clusters formed by the C-Means algorithm. In Subsect. 4.3, we have discussed the result of an outlier, c-means clustering, and Random forest on the dataset with 30 features.

4.1 Initial Results

The supervised methods, namely Adaboost, Decision Tree, K-Nearest Neighbor, Neural Network, and Random Forest, are applied to the original dataset. The confusion matrices during the training process is shown in Fig. 4a, Fig. 4b, Fig. 4c, Fig. 4d, and Fig. 4e respectively. As per the confusion matrices, the Adaboost method outperforms and improves training processes with minimal Type-I and Type-II training errors. The ROC curve generated using these methods for class 0, and class 1 is presented in Fig. 3a and Fig. 3b respectively.

4.2 Results After Feature Selection

Here, six feature selection techniques have been used to reduce the features from 1087 to 30; by averaging the most relevant feature ranking as shown in Fig. 2,



(a) Cluster 1 with label 0 (b) Cluster 1 with label 1

Fig. 3. Combined ROC of classifiers on malware dataset

we have performed the experiments using the same techniques as in Subsect. 4.1. The confusion matrices obtained from Adaboost, Decision tree, KNN, Neural Network and Random Forest are shown in Fig. 5a, Fig. 5b, Fig. 5c, Fig. 5d, and Fig. 5e respectively. Here, we found that the performance of all algorithms except the decision tree is improving after feature selection. Among all the algorithms used, Random forest outperforms in execution time and detection accuracy. The Comparative results of the supervised methods using malware dataset are shown in Fig. 3.

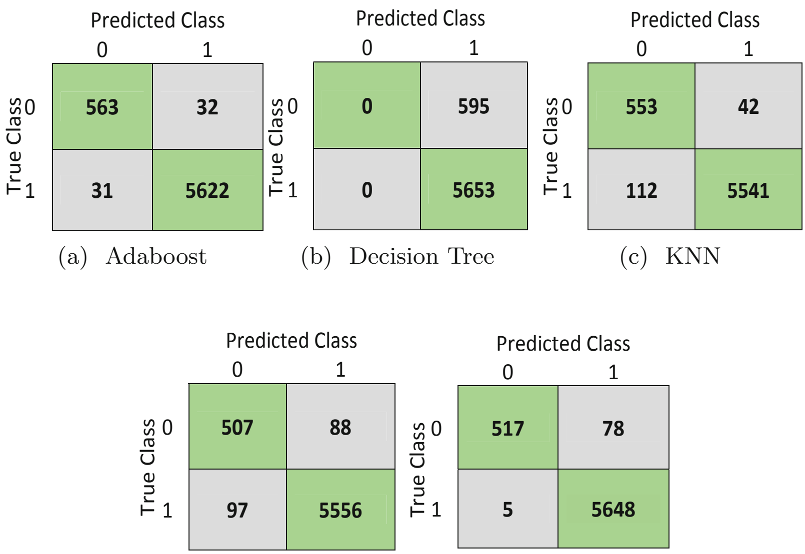
After Feature, again the supervised methods applied on the reduced data. The result is given in Table 3.

Table 3. After feature selection evaluation results

Model	AUC	CA	F1	Precision	Recall
KNN	0.988	0.985	0.985	0.985	0.985
Decision Tree	0.444	0.905	0.860	0.819	0.905
Random Forest	1.000	0.996	0.996	0.996	0.996
Neural Network	0.984	0.967	0.967	0.967	0.967
Adaboost	0.977	0.992	0.992	0.992	0.992

4.3 Results of the Proposed Model

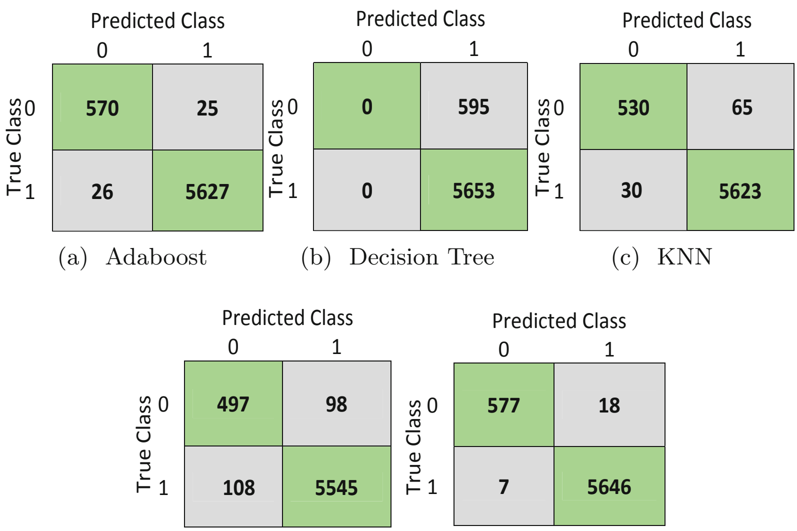
In this experiment, a total of 30 features are considered for predictive analysis after feature analysis. The local outlier factor is used to separate the dataset into inliers and outliers. Then, C-Means clustering algorithms are applied to the



(a) Adaboost (b) Decision Tree (c) KNN

(d) Neural Network (e) Random Forest

Fig. 4. Confusion metrics of the models before feature selection

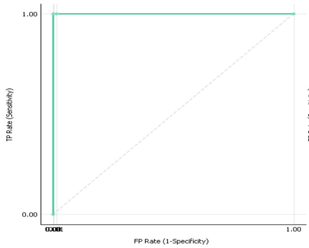


(a) Adaboost (b) Decision Tree (c) KNN

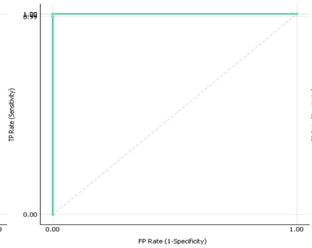
(d) Neural Network (e) Random Forest

Fig. 5. Confusion metrics of the models after feature selection

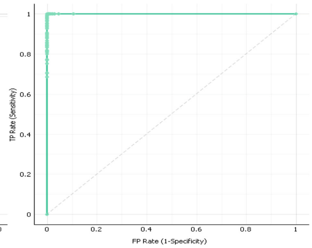
inliers to form two clusters. Then the Random forest approach labels the three clusters element as benign and malicious, as shown in Fig. 3. The confusion matrices proposed model for cluster 1, cluster 2 and cluster 3 are shown in



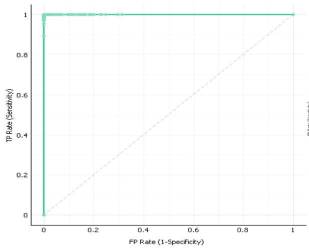
(a) Cluster 1 with label 0



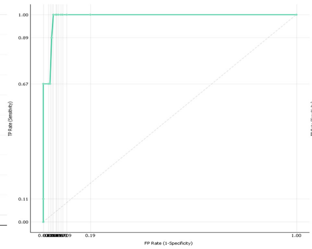
(b) Cluster 1 with label 1



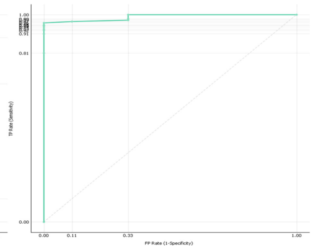
(c) Cluster 2 with label 0



(d) Cluster 2 with label 1

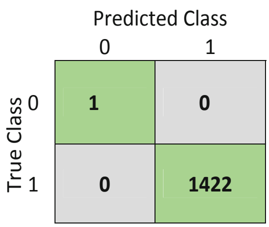


(e) Cluster 3 with label 0

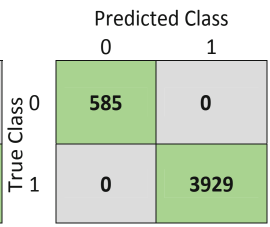


(f) Cluster 3 with label 1

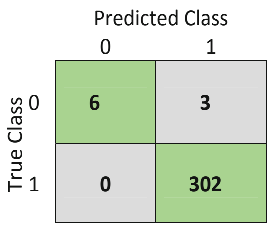
Fig. 6. ROC of the proposed model with different clusters



(a) Cluster 1



(b) Cluster 2



(c) Cluster 3

Fig. 7. Confusion metrics of the proposed model on different clusters

Fig. 7a, Fig. 7b and Fig. 7c as there are 3 clusters benign, malicious and outlier. The results of cluster 1 and cluster 2 don't have type I or type II errors. Cluster 3 contains minimal type I error but doesn't have type II error. The ROC graphs for cluster 1 for benign and attack are shown in Fig. 6a and Fig. 6b. The ROC graphs for cluster 2 for benign and attack are shown in Fig. 6c and Fig. 6d and ROC graphs for cluster 3 are shown in Fig. 6e and Fig. 6f. From the ROC curves, it can be clearly observe that the ROC curves for cluster 1 and cluster 2 are touching the top left corner, but it slightly deviates in case of cluster 3. The reason behind this is, the proposed approach is achieved a better classification result in case of Cluster 1 and Cluster 2 but slightly less in case of Cluster 3. Overall, the proposed model is classified the threat classes more efficiently with a minimal error rate.

Table 4. Cluster-wise performance metrics of proposed model

Cluster	AUC	CA	F1	Precision	Recall
1	1.000	1.000	1.000	1.000	1.000
2	1.000	1.000	1.000	1.000	1.000
3	0. 989	0. 990	0. 989	0. 990	0. 990

The detection accuracy along with other performance assessment metrics of the three Clusters is shown in the Table 4.

5 Conclusion

Malware is a massive threat to the systems in the digital world. Its effects can't be avoided but can be tried to minimize. As malware tools evolve to falsify the detection engine, it is challenging to detect and countermeasure such malicious efforts. In this study, the model combines outlier, clustering, and supervised machine learning-based detection approaches that can detect such malware signature variations. Various feature analysis approaches are used to analyze attack patterns and relevant features. As a result, out of 1087 features, we have successfully reduced them to 30 attributes. Empirically, we have tested the proposed method using the malware dataset; the result is quite impressive to detect such malicious instances from the dataset.

In our future works, we will analyze other malware datasets and focus on how to improve the algorithm/tune the hyper-parameters using optimization techniques.

References

1. Malware Dataset (2021). https://archive.ics.uci.edu/ml/datasets/Malware+static+and+dynamic+features+VxHeaven+and+Virus+Total. Accessed 30 Sept 2021
2. Ahmadi, M., Ulyanov, D., Semenov, S., Trofimov, M., Giacinto, G.: Novel feature extraction, selection and fusion for effective malware family classification. In: Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy, pp. 183–194 (2016)
3. Ahmed, Y.A., Koçer, B., Huda, S., Al-rimy, B.A.S., Hassan, M.M.: A system call refinement-based enhanced minimum redundancy maximum relevance method for ransomware early detection. J. Netw. Comput. Appl. **167**, 102753 (2020)
4. Alam, M.S., Vuong, S.T.: Random forest classification for detecting android malware. In: 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, pp. 663–669. IEEE (2013)
5. Alzubi, J., Nayyar, A., Kumar, A.: Machine learning from theory to algorithms: an overview. J. Phys.: Conf. Ser. **1142**, 012012 (2018)

6. Anderson, B., Quist, D., Neil, J., Storlie, C., Lane, T.: Graph-based malware detection using dynamic analysis. J. Comput. Virol. **7**(4), 247–258 (2011)
7. Bahtiyar, Ş, Yaman, M.B., Altınığne, C.Y.: A multi-dimensional machine learning approach to predict advanced malware. Comput. Netw. **160**, 118–129 (2019)
8. Breunig, M.M., Kriegel, H.P., Ng, R.T., Sander, J.: LOF: identifying density-based local outliers. In: Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data, pp. 93–104 (2000)
9. Darem, A., Abawajy, J., Makkar, A., Alhashmi, A., Alanazi, S.: Visualization and deep-learning-based malware variant detection using opcode-level features. Future Gener. Comput. Syst. **125**, 314–323 (2021)
10. Han, W., Xue, J., Wang, Y., Liu, Z., Kong, Z.: Malinsight: a systematic profiling based malware detection framework. J. Netw. Comput. Appl. **125**, 236–250 (2019)
11. Imtiaz, S.I., ur Rehman, S., Javed, A.R., Jalil, Z., Liu, X., Alnumay, W.S.: DeepAMD: detection and identification of android malware using high-efficient deep artificial neural network. Future Gener. Comput. Syst. **115**, 844–856 (2021)
12. Jain, A., Nayyar, A.: Machine learning and its applicability in networking. In: New Age Analytics, pp. 57–79. Apple Academic Press (2020)
13. Mimura, M., Ito, R.: Applying NLP techniques to malware detection in a practical environment. Int. J. Inf. Secur. 1–13 (2021)
14. Rezaei, T., Manavi, F., Hamzeh, A.: A PE header-based method for malware detection using clustering and deep embedding techniques. J. Inf. Secur. Appl. **60**, 102876 (2021)
15. Sahu, S.K., Jena, S.K.: A study of K-means and C-means clustering algorithms for intrusion detection product development. Int. J. Innov. Manag. Technol. **5**, 207–213 (2014)
16. Sahu, S.K., Katiyar, A., Kumari, K.M., Kumar, G., Mohapatra, D.P.: An SVM-based ensemble approach for intrusion detection. Int. J. Inf. Technol. Web Eng. (IJITWE) **14**(1), 66–84 (2019)
17. Samantray, O.P., Tripathy, S.N.: A knowledge-domain analyser for malware classification. In: 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA), pp. 1–7. IEEE (2020)
18. Samriya, J.K., Kumar, N.: A novel intrusion detection system using hybrid clustering-optimization approach in cloud computing. Mater. Today: Proc. (2020)
19. Singh, P., Krishnamoorthy, S., Nayyar, A., Luhach, A.K., Kaur, A.: Soft-computing-based false alarm reduction for hierarchical data of intrusion detection system. Int. J. Distrib. Sens. Netw. **15**(10), 1550147719883132 (2019)
20. Taheri, R., Ghahramani, M., Javidan, R., Shojafar, M., Pooranian, Z., Conti, M.: Similarity-based android malware detection using hamming distance of static binary features. Future Gener. Comput. Syst. **105**, 230–247 (2020)

Futuristic Approach for Intelligent Cognitive Radio Using Different Machine Learning Algorithms

Megha Motta[1(✉)], Partha Sarathy Banerjee[2], and Deepak Sharma[1]

[1] Department of Electronics and Communication Engineering, Jaypee University of Engineering and Technology, Guna, India
motta.megha1@gmail.com, deepakforu23@rediffmail.com
[2] Department of Computer Science Engineering, Jaypee University of Engineering and Technology, Guna, India
partha1010@gmail.com

Abstract. As the utilization of spectrum is increasing rapidly with the increase of wireless devices Cognitive radio (CR) is a novel approach introduced by FCC which provide enhancement in the utilization of available spectrum. It can be done with the help of smart radio devices. It senses the presence of primary users (PUs) in order to use the spectrum more efficiently in their absence. Secondary Users (SUs) plays the role of smart radios for sensing the radio environment. Machine learning (ML) is serving as one of the most important factor to facilitate intelligent CR networks. It not only enhances the performance but also gives much more accurate results. There is an ever growing interest for using the algorithm of machine learning in Cognitive Radios. Various learning models that can be applicable for CR networks are demonstrated in this paper. The author recapitulates the method stepwise and design a learning-based cooperative secondary network, by giving emphasizes on factors that lay an impression on detection performance. Recent learning techniques are also highlighted in this paper with their applications in cognitive radio. Author also tries to shown a relationship between cognitive radio and Software defined radios.

Keywords: Cognitive radio · Machine learning · Supervised learning · Unsupervised learning · Cooperative secondary network · Software defined radios

1 Introduction

Government holds the authority of licensing the spectrum of radio frequencies to the users for the communication of signals. According to the Fixed Spectrum Access (FSA) policy fixed channels are assigned to licensed users which are also acknowledged as primary users (PUs) for limited use. PUs are the only eligible users to access the assigned spectrum. On the hand, the recent studies also show that maximum portion of licensed spectrum practices less utilization i.e, Oftenely, it was noticed that the spectrum was not being utilized by the PUs also and was found ideal. As a solution to this problem

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 464–476, 2023.
https://doi.org/10.1007/978-3-031-13150-9_37

Dynamic Spectrum Access (DSA) was introduced this lays an idea of utilizing spectrum in much more efficient manner. According to DSA in ideal condition when primary users (PUs) are not using the spectrum then spectrum can be used by the unlicensed or secondary users (SUs). However the priority will always be given to the primary users [1].

Cognitive Radio emerges as a pioneering technique to increase the efficiency of the allocated spectrum. Currently, steps are now being taken to enhance the efficiency of cognitive radio networks. Technologies are encountered now a days that enhances the utilization of time with respect of frequency and space or either permit secondary users to work simultaneously with primary users in the same spectrum without creating any interference. Cognitive radio networks (CRN) are classified under three main categories: the underlay, the overlay and the interweave models. In the underlay networks, the licensed users and secondary users access the spectrum band simultaneously at a condition of setting some minimum value of interference that will not be exceeded. Overlay model can be well explained as licensed users and secondary users may access the channel in parallel order but secondary users have to assist the licensed users. Last but not the least in case of an interweave model, secondary users perform the function of spectrum sensing effectively and can use the spectrum only and only if PUs are not using it [2].

2 Cooperative Spectrum Sensing

This type of sensing takes place when a cluster of sensors or network of CRs performs the function of spectrum sensing continuously to detect the presence of PUs. Under the condition of fading as well as noise cooperative spectrum sensing also helps in enhancing their sensing performances. It plays a major role in reducing the time involved in sensing and helps to detect the presence of hidden PUs. There are different categories of Cooperative spectrum sensing depending upon the approach CRs use to share their data in the network. They are further classified on the basis of the alignment and type of sensors. If the alignment is operated by central hub then it is known as Centralized approach. For the alignment of sensors where each sensor is individually responsible for their decision is known as distributed approach. Rest two alignment are considered on the basis of type of sensors they are using for same type of sensors it is called as same sensor and if different type of sensor is used then it is called as different sensor. In this article we will consider cooperative sensing with centralized approach [3].

3 Centralized Approach for Cooperative Sensing

In centralized cooperative sensing, there is a centralized hub known as fusion center (FC) that manages the sensing process by opting the required frequency band, a control channel requests for separate results of sensing from individual CR sensors. All the signals received after sensing are combined to make a final decision on the status of primary user (whether present or absent). As a last step, of spectrum sensing the final decision is taken by the FC by evaluating the sensing results and also determines the availability of the spectrum for SUs. This result is also broadcasted to all the neighboring CRs (see Fig. 1).

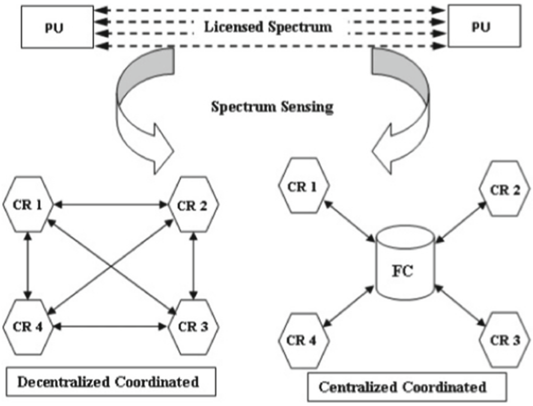


Fig. 1. Cooperative detection model

4 Blending of Machine Learning with CRN

Machine Learning (ML) is a technology which works on the concept of human mind and tries to understand the impressions or trends with the help of Artificial Intelligence. Based on the present and previous facts ML helps cognitive users to apply the theory of self-adaptation and self managing Intelligent CR will get much more accurate results with better generalized functionality rather than the standard cognitive radios. It may lead radio environment patterns with inaccurate and incomplete results [4].

Considering the above scenario we have integrated the role of learning in cognitive radio networks. In this paper, we will be defining some steps which are involved for establishing learning based cooperative CR network. Classification of different algorithms under supervised and unsupervised learning paradigms based on the data analysis will be demonstrated in cooperative CR networks.

5 Establishing Intelligent Cognitive Network

In cognitive network, the SUs perform the spectrum sensing technique to detect the presence of PUs. There are various spectrum sensing techniques used by the SUs. Some of them are Energy detector, Matched filter and cyclostationary feature as shown in Table 1. Depending upon the context and the requirements of CR systems the sensing technique to be used is decided. Among all the methods available for spectrum sensing energy detection is one of the most basic and efficient ways to perform the task of spectrum sensing. Energy detector works on the principle of collecting samples accurately, combing them and then estimates level of energy present in the spectrum. The information of estimated level of energy is send to fusion centre by SUs. By applying different fusion rules at the fusion centre (FC) the presence of PUs can be decided by the current channel occupancy state (COS) in cooperative spectrum sensing [5].

Following are some major steps which needs to be fulfilled for designing ML enabled cooperative CR network. Figure 2 demonstrates the steps involved in the process. First step of establishing the stable model is to train the module. The training as well as

Table 1. Comparison of spectrum sensing methods

Sensing Methods	Advantages	Disadvantages
Energy Detection	No prior knowledge of the signal is required, is less complex	Vulnerable to noise uncertainty
Matched Filter	Optimum Performance	Requires the prior knowledge of the signal consumes high power and is complex in implementation
Cyclostationary feature	Vigorous to interference and noise uncertainty	Takes much time in observation, Highly complex, vulnerable to sampling clock offsets

classification of modules can be done simultaneously to make system work in much more efficient manner. This is only possible because the learning process is modular.

During this phase learning-based FC is fed with data of different energy levels. It maps the energy level of the radio environment with the COS of PUs. In CR networks based on learning techniques the performance of detection is affected by the quality of training data. Therefore, it is very important that the data gathered by FC must précised, appropriate and adequate. It is not required to have the prior information regarding the COS and SNR of the system. FC will be able to perform the detection of PU once the training phase of learning–based CR is completed. Topology of the network also doesn't affect the detection performance. The most important role played in training and learned CR network is the type of data used. We will be considering Labeled data and unlabelled data sets. When the features of data set are explained and tagged with one or more classified results then such type of data is called as labeled data set. Whereas, in case of unlabeled data set we only know the features and the data set available is not been tagged with any labels mentioning characteristics or any classifications of the result. The size of data set used for training acts as a main factor for obtaining the accurate detection results. [4].

As mentioned earlier in this article data sets plays very important role in intelligent CR. An inadequate data set can lead to under-fitted learning model and if the data provided is too long it goes to over-fitting learning model. In both the cases detection performance gets affected. However, it can be improved in under-fitted model but in case of over-fitting it implies the negative impact on overall detection performance.

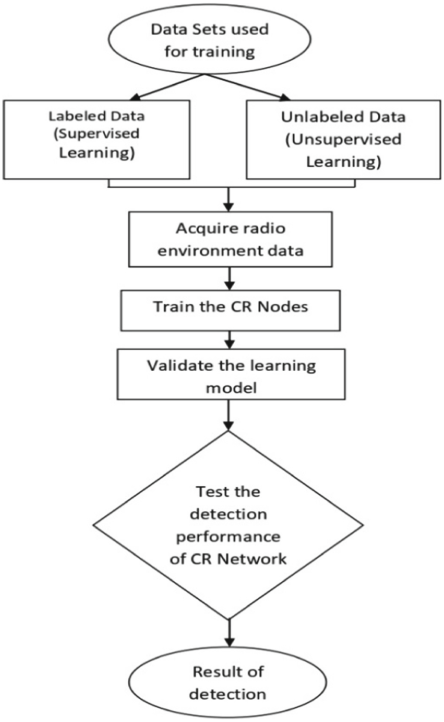


Fig. 2. Step by step process of implementation of ML in cooperative CR networks

6 Amalgamation of Machine Learning with Smart Radio

Practicing ML in CR networks is highly recommendable now days. Functioning like feature classification and clustering can be very well conducted that too in a controlled manner. Data set (Labeled or unlabelled) used by the system model decides the type of learning techniques which is to be executed in CR network. Machine learning algorithms used for cooperative CR networks can be classified as: Supervised learning, unsupervised learning and Reinforcement learning (RL).

7 CR Network Enabled with Supervised Learning

In case of supervised learning the most important factor is to feed the system with labeled data, i.e. "basic reality "should be known to the classification pattern. It is mandatory, for CR secondary networks to have designated energy levels with their respective COS at the FC as the labeled data to map and find the outcomes. Its relevance's in CR networks is very important for getting better accuracy of detection of SUs. Learning algorithm used for supervised learning techniques are: The Support Vector Machine (SVM), The Naive Baye's Classifier, Decission Tree (DT) and Linear Regression (LR).

7.1 Support Vector Machine (SVM)

It is one of the most frequently exercised algorithms because of the strength it has towards the high dimensional data and noise. Support vector machine increases the dimensionality of the data if there is increase in SUs for cooperative CRN. This is the reason which makes it most suitable to perform the task. Over-fitting problem is least expected in this algorithm for small data sets [6].

7.2 Naïve BAye's Classifier

Naive Baye's Classifier works on the concept of conditional probability to determine the chance of any event to take place which is been implemented from the principle of Bayes' theorem.

It is this algorithm which introduced the concept of "Naïve" theory which states that the elements of the data are not dependent on each other thus also named as "Independent feature model" [7]. Above hypothesis would work for the energy levels at each SU who are mutually independent in cooperative secondary networks.

7.3 Decision Tree (DT)

This approach works on the principle of classification of trees where class labels are being represented with the help of leaf. DT also considers the features like interactions and dependences. In DT, internal node plays most vital role for making decisions as they are responsible for dividing the data into subsets. Representation of leaf nodes depends on trees in case of classification trees they are represented as class labels and in case of regression trees it is represented as real numbers [8].

7.4 Linear Regression

This approach works on the basic rule of designing a liner combination of various features in different time dimensions such as time, space, frequency and threshold. This capability leads the usage of algorithm to be mostly used step wise for modeling. It is observed that computational time for evaluating the response of the model is directly proportional to the number of frequency bins involved. If frequency bins increases computational time will also be increased [9].

8 Unsupervised Learning in Cooperative CR Network

Unsupervised learning algorithm is conceptualized on the basis of unlabelled data which allows the identification of the patterns of data sets that are neither classified nor labeled in the system. Clustering of data and compression of data are the two main key factors responsible for using this algorithm. There is a negative aspect of unsupervised learning algorithm over supervised learning as it is not aware of the ground reality; the performance of unsupervised learning gets inferior to the supervised learning.

8.1 The Gaussian Mixture Model (GMM)

GMM algorithm is based on the concept of clustering and is designed on the basis of certain distribution model. Combination of different mixing coefficients with K multivariate Gaussian distributions is considered in it. The number of clusters is dependent on the number of combinations given by the data set. This implies that the features mentioned in the given data set and the number of variables corresponding to multivariate Gaussian distribution is dependent on each other. The parameters of the multivariate Gaussian distribution which belongs to cluster is defined by the secondary network and is termed as "Channel Available". The Log-likelihood is created by one or two clusters and then is calculated by GMM. The threshold is predefined on the basis of the difference in likelihood. Regarding the assimilation of data some work has been incorporated by the authors in [14–17].

9 Reinforcement Learning in Cooperative CR Network

The reinforcement Learning (RL) algorithm is based on the idea of finding the optimal action policy. It imitates the learning processes in the mind by means of trial and error. By continuous interaction with the environment it also helps in enhancing the long term reward. Q-Learning technique is the most commonly used RL algorithm [10].

9.1 Q-Learning

In Q-learning approach a model is designed with Q-table which consists of Q-values as elements. For each random state–action Q-value works as a long term reward (discounted accumulative reward) which designates the impact of the action on the state. Iterative method takes place in a continuous manner for updating the Q-value of individual state action pair till optimal action reaches the maximum Q-value which is selected for executing. By considering the reasonable hardware of configuration and delays in this algorithm we can easily obtain the best results for detecting the spectrum in ideal condition for wideband spectrum. To enhance the transmitted power of cognitive radio users and to get accurate results distributed Q-learning algorithm is established. It's main role is to maximize the signal interference pulse noise ratio (SINR) at secondary receivers whereas meeting the primary protection constraint [11, 12].

10 Current Upcoming Learning Techniques in CRN

Many AI and ML based techniques are evolved now a day's which has emphasized the function of learning in cognitive radios. AI based advance techniques such as fuzzy logic, genetic algorithm, neural networks, game theory, case –based reasoning, multi-agent systems and artificial bee colony algorithms also play a vital role in enhancing the performance index of cognitive radios [13].

10.1 Fuzzy Logic

The fuzzy logic set theory was introduced in 1965 to explain and design improbability, elusiveness using analytical and experimental models. The outcomes of fuzzy logic are now not only bounded by two options (True or False) as mentioned in earlier classical sets. Now, in case of fuzzy element it also has a degree of association which is compatible with the set and its contradictions. It facilitates the system with many beneficial outcomes in situations where a decision is to be generated using rules of if-then and taking fuzzy values as an input. It also has an ability to give a decision by forecasting the consequences in the condition of uncertainty. It is with the help of fuzzy logic only we also learn to generalize and adapt the new situation with learning from past experiences. This theory of fuzzy logic is applied in CR for calculation various aspects in the domain of allocating the bandwidth, availability of spectrum for the usage of SUs, to resolve the issues caused due to interference. Researchers have also been conducted their studies on power management with minimizing the effect of interference and enhancing the quality of service [18, 19].

10.2 Genetic Algorithms (GA)

It was introduced in 1958 by the work of Friedberg, which laid the foundation of FORTRAN programs. The building block of this technique works on the principle of making suitable sequences of small alterations in the programming of machine code and then generates a new code that has enhanced outcome in terms of performance to accomplish any particular assignment. Genetic Algorithm has many applications in the domain of wireless communications and especially when it comes to cognitive radios. In CR it plays a vital role in spectrum utilization in optimized manner, decision making by FC on the presence or absence of SUs. GA has also provided a solution to various problems that occur in CR [20, 21].

10.3 Neural Networks

This approach was introduced in 1943 and was conceptualized on the concept of central nervous system of human brain. Artificial Neural Network forms nodes which are similar neurons sometimes also called as processing units which are connected together to form a network. It gets information from all the neighboring nodes and delivers an outcome depending on its weight and activation functions. These weights also characterized as the connecting strengths among neurons. To achieve the learning process the weights are adjusted till the outcome received from the network is approximately equal to the desired output. Artificial Neural Network (ANNs) was introduced as a key to resolve the issues of inefficient usage of spectrum in current communication system by replacing the scheme utilized by existing frequency allocation system. Therefore, ANNs proved as a remedial for enhancing the utilization of spectrum by installing the algorithm at SUs end separately and predict the sensing probabilities [22, 23].

10.4 Game Theory

Game theory was originated in 1713 by James Waldegrave. It gives the concept of decision making in the condition where a number of participants have to make selection that also affects the performance of other participants. Every individual make a decision of this action which is based on the history of actions preferred by other individuals in previous rounds of the game. In the game of cognitive networks CRs plays the role of players. Setting the RF parameters of transmitting power and performing the selection of channels plays the role of actions in game theory. Now, on the basis of observations conducted by environment parameters like availability and quality of the channel, occurring of interference in the channel action will be taken by cognitive radio networks. Thus, all the CR nodes will learn from their previous actions, also monitors the actions of other CR and then modify their actions consequently [24, 25].

10.5 Case-Based Reasoning (CBR)

CBR laid the concept of analyzing previous problems and finding solutions to resolve the existing problem falling under same circumstances. This is being done by maintaining the database of previous problems with their solutions and the situations in which they have occur. Solution of the new or existing problem is found by mapping the current problem with the same type of previous problem from the memory of the database and find a solution. This type of technique is useful for designing a spectrum allocation model and identifying a channel used by the SU as a problem statement. It plays a vital role in proper channel management and also to increase the efficiency of the system [26, 27].

10.6 Multi-agent Systems (MAS)

Multi-agent systems are intelligent elements which are aware of its surroundings, capabilities of its skills and they communicate in an independent pattern. They are enclosed with several relations among themselves. This model mainly works in problem solving the environment of virtual world. This concept has introduced a novel technique in dealing with the problem of handoff in CR. It allows CR nodes to analyze their environment and toggle the spectrum to archive the excellent condition for communication of signals through MAS. It considers the spectrum band as environment and CR terminals, PUs as agents. MAS is also useful for sharing for spectrum in CRN. They install agents on all primary as well as secondary users and perform the task of spectrum sharing when SUs tends to use the spectrum [28, 29].

10.7 Artificial Bee Colony (ABC)

Artificial bee colony was introduced in 2005 which was conceptualized on the smart activity performed by honey bees. This implies the benefits of memory with numerous characters conducting local search with a resolution of advance mechanism. The working pattern of bee model works as per the name given. It mainly consists of three assemblies of bees namely: employee bees, looker and scouts. They all work together with an aim to find the position of the best resources of food. The task of finding the source of nectar is conducted by employee bees with a condition if the amount of nectar found on a new source is higher than the old one in memory, they will memorize the new location and forget the old one. The same methodology is followed to find the solution of a problem in optimized manner and here the amount of nectar resembles the quality of the solution. This concept of ABC is applied in cognitive radio for the spectrum allocation, relay selection and power allocation of transmitting signals [30].

11 Software Define Radios (SDR) and its Relation with Cognitive Radios

The purpose of introducing cognitive radio was to enhance the spectrum utilization by adapting the various radio parameters like power, frequency, modulation and bandwidth that changes as per the requirements of the network or situation. SDR provides very flexible radio functionality without any use of analog circuits. Thus, cognitive radios are designed with SDR. We can also say that SDR is the most enabling technology for CR that are aware of their environment, internal state and location. They adjust its working to obtain the designated results. The basic model of SDR consists of cognitive engine, SDR and various other supporting functionalities to perform various operations of cognitive radio. The optimizing or the function of controlling of SDR when input parameters are sensed or learned from the radio environment is done by cognitive engine. It is much aware of the capabilities of the radios and their hardware resources too. Thus, it can be said that the SDR is built around software based on digital signal processing enriched with software tunable radio frequency components that are capable of performing functions with various bandwidths over a wide range of frequencies.

12 Challenges and Future Directions

There are various challenges and obstacles which takes place when machine learning algorithm is combined with CR. But, the best part is that by applying the algorithm of machine learning we find much more accurate results and the overall performance of CR networks also enhances. Although, still there are some points that need to be taken care of while designing the learning-based CR systems. Some of them are mentioned below:

12.1 Acquiring Training Data

Many times the data used for training is obtained with the help of theoretical models and software simulation. This leads to sometimes in accurate collection of data. The performance quality of learning based models is strongly affected by the quality of training data. The biggest challenge for secondary network is to get fed by the original data which labeled and also follow supervised learning technique for accurate results.

12.2 Learning Technique

Decision making and Feature classification are the two most common learning problems that may take place in CR networks. Feature classification problem arises in spectrum sensing domain and decision making takes place in power control as well as in sensing policies. To reduce the risk of various learning problems and get much more accurate results of high-caliber it is mandatory that CR system adapts the most accurate learning model.

There is a lot scope to enhance the performance of learning base techniques in CR systems. In this article we have studied the models based on supervised learning (SL), unsupervised learning (USL) and reinforcement learning (RL). An effort should be made to investigate the use of Semi-Supervised learning. This approach may be designed by combing the labeled and unlabelled data. For getting better results labeled data can be kept in minority and major emphasis to be given on unlabelled data.

12.3 Commercialization of Spectrum

We all know this that spectrum resources are purely owned by government which leads towards as an obstacle in commercialization and development area of a spectrum. Some work can be done to establish some compatibility standards and technologies with the government to enhance the use of spectrum in commercialization.

13 Conclusion

CR networks are considered to be the most innovative method to use the spectrum in most opportunistic manner without any interference to the PUs. On the other hand machine learning in AI is the most upcoming and accurate technology to get accurate results. In this paper we have studied and tried to explain the blend of different machine learning techniques with CR networks. We have summarized the various learning algorithm based on the type of data set they acquire for execution. It also gives an explanation about the CR nodes which developed from standard cognitive to intelligent cognitive with the help of learning techniques. This article also covers the techniques used by CR node for learning and organizing observations which are collected by radio environment with the help of feature classification and clustering algorithm. Moreover, a future scope for establishing a new learning model combing the supervised and unsupervised learning algorithm can lead to new heights of accuracy may also be designed. A brief review of upcoming trends involved in cognitive with learning techniques is also provided with a small introduction of software defined radios.

References

1. FCC: Spectrum policy task force report, Federal Communications Commission, Tech. Rep. 02–155 (Nov 2002)
2. Ali, A., Hamouda, W.: Advances on spectrum sensing for cognitive radio networks: theory and applications. IEEE Commun. Surveys Tutorials **19**(2), 1277–1304 (Second Quarter 2017)

3. Unnikrishnan, J., Veeravalli, V.: Cooperative sensing for primary detection in cognitive radio. IEEE Journal on Selected Areas in Signal Processing **2**(1), 18–27 (2008)
4. Zhang, K., et al.: Artificial intelligence inspired transmission scheduling in cognitive vehicular communications and networks. IEEE Internet of Things J. **6**(2), 1987–1997 (2019). Apr.
5. Zhang, W., Letaief, K.B.: Cooperative communications for cognitive radio networks. Proc. IEEE **97**, 878–893 (2009). May
6. Hsu, C.-W., Lin, C.-J.: A comparison of methods for multiclass support vector machines. IEEE Trans. Neural Networks **13**(2), 415–425 (2002)
7. Azmat, F., Chen, Y., Stocks, N.: Analysis of spectrum occupancy using machine learning algorithms. IEEE Trans. Vehicular Technology **65**(9), 6853 (Sep. 2016)
8. Rokach, L., Maimon, O.: Decision Trees, Data Mining and Knowledge Discovery Handbook, 2nd ed., pp. 1285. Springer Publisher (2010)
9. Willkomm, D., Machiraju, S., Bolot, J., Wolisz, A.: Primary users in cellular networks: a large-scale measurement study. In: Proc. DySPAN' 08, pp. 1–11 (2008)
10. Sutton, R.S., et al.: Introduction to Reinforcement Learning. MIT press, vol. 135 (1998)
11. Li, S.K., Jayaweera, M., Bkassiny, Ghosh, C.: Learning-aided sub-band selection algorithms for spectrum sensing in wide-band cognitive radios. IEEE Trans. Wireless Commun. **13**(4), 2012–2024 (Apr. 2014)
12. Van Den Biggelaar, O., Dricot, J.-M., De Doncker, P., Horlin, F.: Sensing time and power allocation for cognitive radios using distributed q-learning. EURASIP J. Wireless Commun. Netw. **2012**(1), 138 (2012). Apr.
13. Qin, Z., et al.: 20 Years of evolution from cognitive to intelligent communications. IEEE Trans. Cognitive Communications and Networking **6**(1), 6–20 (2020)
14. Banerjee, P.S., Chakraborty, B., Tripathi, D., Gupta, H., Kumar, S.S.: A information retrieval based on question and answering and NER for unstructured information without using SQL. Wireless Pers. Commun. **108**(3), 1909–1931 (2019). https://doi.org/10.1007/s11277-019-06501-z
15. Banerjee, P.S., Chakraborty, B., Anand, U., Upadhyay, H.: Trainable framework for information extraction, structuring and summarization of unstructured data, using modified NER. Wireless Pers. Commun. **117**(2), 769–807 (2020). https://doi.org/10.1007/s11277-020-07896-w
16. Banerjee, P.S., Ghosh, A., Gupta, A., Chakraborty, B.: Natural Language Information Extraction Through Non-Factoid Question and Answering System (NLIEQA Non-Factoid). In: Hassanien, A.E., Bhatnagar, R., Darwish, A. (eds.) AMLTA 2020. AISC, vol. 1141, pp. 105–117. Springer, Singapore (2021). https://doi.org/10.1007/978-981-15-3383-9_10
17. NLP for Clinical Data Analysis: Handling the Unstructured Clinical Information, Partha Sarathy Banerjee, Jaya Banerjee (National Institute of Technology, Durgapur, India)Source Title: Handbook of Research on Advancements of Artificial Intelligence in Healthcare Engineering. https://doi.org/10.4018/978-1-7998-2120-5.ch018
18. Kaur, P., Uddin, M., Khosla, A.: Proceedings of the Eighth International Conference on ICT and Knowledge Engineering. Fuzzy based adaptive bandwidth allocation scheme in cognitive radio networks. Bangkok, Thailand (2010)
19. Matinmikko, M., Ser Del, J., Rauma, T., Mustonen, M.: Fuzzy-logic based framework for spectrum availability assessment in cognitive radio systems. IEEE J. Selected Areas Commun. **31**(11), 1136–1159 (2013)
20. Russell, S.J., Norvig, P.: Artificial Intelligence AModern Approach. Pearson Education Limited, London, United Kingdom (2014)
21. Kantardzic, M.: Data Mining: Concepts, Models, Methods, and Algorithms. John Wiley and Sons, Hoboken, New Jersey, USA (2003)
22. Rojas, R.: Neural Networks A Systematic Introduction. Springer, Berlin Heigelberg, Germany (1996)

23. Tan, X., Huang, H., Ma, L.: Proceedings of the IEEE TENCON Spring Conference. Frquency allocation with artificial neural networks in cognitive radio system. Sydney, Australia (2013)
24. Bellhouse, D.: The problem of Waldegrave. Electronic J. History Probability Stat. **3**(2), 112 (2007)
25. Han, Z., Niyato, D., Saad, W., Basar, T.: A Hj?rungnes, Game Theory in Wireless and Comunication Networks: Theory, Models, and Applications. Cambridge University Press, New York, USA (2012)
26. Xu, L.D.: Case based reasoning. IEEE Potentials **13**(5), 10–13 (1994)
27. Kolodner, J.: Case-Based Reasoning. Morgan Kaufmann, California, USA (1993)
28. Ferber, J.: Multi-Agent System: An Introduction to Distributed Artificial Intelligence. Addison Wesley Longman, Harlow, United Kingdom (1999)
29. Trigui, E., Esseghir, M., Merghem-Boulahia, L.: Proceedings of the 5th International Conference on New Technologies, Mobility and Security.Multi-agent systems negotiation approach for handoff in mobile cognitive radio networks. Istanbul, Turkey (2012)
30. Rout, M., Majhi, B., Mohapatra, U.M., Mahapatra, R.: Proceedings of theWorld Congress on Information and Communication Technologies. An artificial bee colony algorithm based efficient prediction model for stock market indices. Trivandrum, India (2012)

Novel Techniques for Analysing Satellite Imagery Data

Uttam Banik(✉) and Lalit Garg

Department of Information and Communication Technology, University of Malta, Msida MSD 2080, Malta
rtruttam@gmail.com, lalit.garg@um.edu.mt

Abstract. With the rapid development of space technology, numerous applications are being developed utilising satellite imagery data, including environmental monitoring, meteorology and map making, mapping and monitoring the Earth's resources ecosystems and observing various particles in space. The satellite data can be analysed with the help of machine learning and artificial intelligence. Satellite data deliver the signal for information about the surface and surrounding changes in a location on the Earth. The satellite image quality of the target surface depends on many factors, including atmospheric circumstances, the direction of lighting source, scattering of the target and path view of the surface arena. All performance of different observatory technologies depends on whether the data is gathering through a passive or an active remote sensing method. The limitation of satellite images is their very low spatial a temporal resolution, making it challenging to use them for many practical applications. This research proposes to review the literature to critically analyse existing approaches to improve the resolution of satellite images. A novel technique will be developed and evaluated based on the fusion of satellite imagery data collection from various satellites to improve a target surface's spatial and temporal resolution.

Keywords: Digital image processing · Satellite image data · Remote sensing · Spatial resolution · Edge detection · Image enhancement

1 Introduction

A satellite is a simulated structure that deploys in orbit to explore the planets for numerous changes like the weather, climate, geography, monitoring network, and broadcasting applications. A satellite image provides a pleasant description of what is occurring at every location on the Earth, exclusively over the tropical oceans. In land, agriculture, geology, forestry, biodiversity, regional planning, education and warfare can make a vital prediction [1]. Satellite remote sensing image provides an effective way to collect critical information of respective areas. The process can be divided into image acquisition, image restoration, image enhancement and information extraction. Modern satellite image data processing is done entirely by digital satellite techniques [2]. Image quality measurement has become vital for image processing applications [3]. Developing and

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 477–484, 2023.
https://doi.org/10.1007/978-3-031-13150-9_38

implementing the enhancement techniques, that are providing the acceptable informations and the ideas about the hyperspectral image. However, satellite image processing is extremely complex due to the large dimensions of the satellite images [4]. In general, satellite images comprise a low brightness level—the importance of image enhancement to protect the information details without the loss of any information.

2 Aims and Objectives

Enhancing the image in visual perception is not only the motive of these techniques. Enhancement means simply identifying the real and the virtual objects [5]. These objects are visible in satellite imagery but sometimes do not appear due to shadow. When solar radiation hits a target surface, it may be transmitted, absorbed or reflected in wavelengths. The complexity of the satellite images in terms of edges, contours and textures paves the way towards the importance of general feature extraction [6]. By adopting below mentioned techniques suitable for the application, the final image processing outcome can be modified to get the required result. The conversion of data to information involves a lot of processing. The pre-processing is required to highlight the hidden details in the image and quality in the presence of known or unknown degradations and noises.

3 Proposed Approaches

To begin the implementation process, we need a satellite image dataset for appropriate image enhancement. We got it from the satellite service provider Copernicus open access hub satellite imagery data set source. We are exploring this hypothesis research with the help of the Copernicus Sentinel-2 satellite imagery data set that belongs to Maltese Island S2B_MSIL2A_20191129T095249_N0213_R079_T33SVV_20191201T153719.SAFE for implementation. After getting the images, we moved forward to the next enhancement phase to implement the image via Matlab R2020b tool kits. Here an actual procedure was achieved to manipulate the image enhancement techniques. For implementation, we have used the row satellite image of RGB format (image.jpg, image.png, image.tiff) for the colour enhancement methodology. By using the imread command, let's read a JPEG image named image1.JPG and store it in an array named I.

I = imread ('image1. JPG');

Now, we can call imshow to display them from the stored image I.

This displayed image is showing in Fig. 1, the portion of Maltese Island (Malta and Gozo). Some features in the image are (i) the Mediterranean Sea around Maltese Island (ii) the Small white patches in the image are clouds.

We can check the stored image memory by entering the whos command to see the below properties of the image I memory.

Name	Size	Bytes	Class
I	512 × 512 × 3	786432	unit8

Fig. 1. Original row image for enhancement

To see the distribution intensities of image1.JPG in its current state, a histogram can be created by calling the imhist function so that the histogram does not overwrite the display of the image in the current figure window. Image enhancement processing methods have been taken under the systematic step-by-step arrangement such as (i) Histogram equalisation of spread the intensities distribution process, (ii) Image contour Image analysis, (iii) Process of spatial resolution techniques, (iv) Image edge detection methods and (v) Image enhancement process classification. After the analysing, these methods then evaluated the approaches of the proper resulting system.

3.1 Histogram Equalisation Analysis

In the initial step, the histogram intensity is calculated for a better observation as a graphical representation. In this dataset, histogram analysis shows the statistical frequency of data distribution values over the full range of image I.

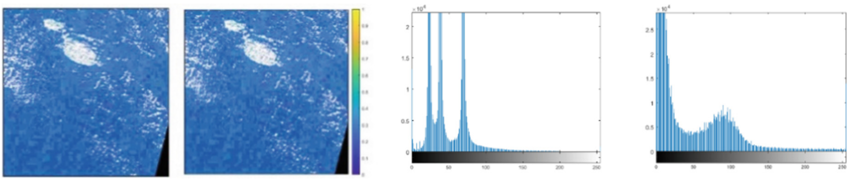


Fig. 2. Histogram equilisation analysis

Figure 2 is summarising the visual histogram intensities of the image range. The distribution of a continuous numeric variable by measuring the frequency at which certain values appeared in the image. Understanding the distribution of data is an important step in this data exploration process.

3.2 Contours Analysis

Contour detection in image enhancement processing that classify and segment the analysis to split the image into several parts. It is quite easy to detect edges using local image analysis techniques. But the detection of continuous contours is more complicated and needs a global analysis of the image. The contours are mainly used for shape analysis, object detection and recognition, by using imcontour command to display a contour dataset plot of the image. Here, image contrast is showing every contour plot of different colour shapes. These three separate images indicate each contour of the satellite image, including the contours of each cloud. This example displays a contour plot shown in Fig. 3.

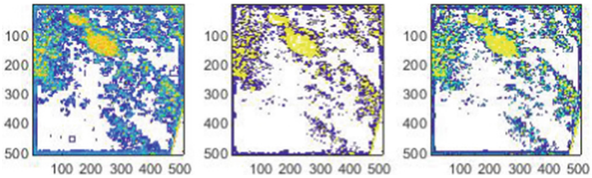


Fig. 3. Image contour plot system

3.3 Spatial Resolution Analysis

Spatial resolution corresponds to the elementary size of the ground surface measured by the different instruments of an embedded sensor are being observed strongly on the altitude of the platform [8]. Satellite sensors store information about objects as a grid, and the pixel's size depends on the sensor type [9]. A lower resolution usually coincides with a higher repetition rate, meaning that the satellite investigates the same area within a short interval. On the other hand, high-resolution data is mainly used for smaller areas of the Earth's surface can reduce the repeat rates and monitor the desired areas edges are shown in Fig. 4.

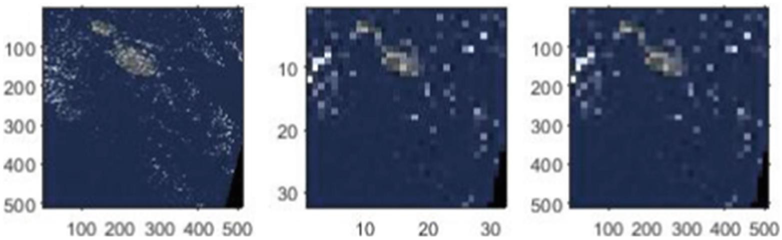


Fig. 4. Spatial image resolution referencing objects

3.4 Edge Detection Analysis

Analysing of the satellite image, the most commonly used platform is edge detection [7]. Diversity of edge detection techniques such as Sobel, Prewitt and Canny methods have been used. Hence, the present research work has been focused on the comparative study and implementation of various classic edge detection techniques of desired object boundaries. The example below illustrates the power of the edge detector. The result of applying an edge detector to a satellite image may lead to a set of connected curves that indicate the boundaries of objects image1.JPG. Therefore, filtering information may be regarded as less relevant while preserving the important structural properties of the image. However, it is not always possible to obtain such ideal edges from real-life satellite complexity.

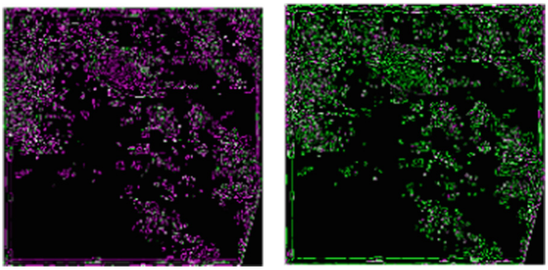


Fig. 5. Edge detection impairment method (a) Sobel and Canny; (b) Canny and Prewitt

The edge detection impairment subsystem skips a configurable number of valid pixels at the beginning of the simulation. The result would be as in the lower half of the timing diagram that impairs the visual pixels of the image. We can see that skipping low valid pixels are impaired in the images in Fig. 5. The first one is impairment of Sobel and canny edge detection impairment valid pixels on the marked lines. The second image is the valid pixel on the given line marked are associated with the canny and Prewitt method. Moreover, the edge impairment subsystem introduces two different cycles of image edge detection systems.

4 Enhancement Analysis

Satellite image enhancements are used to make it easier for visual interpretation and understanding of imagery. The image processing toolbox supports a range of standard image processing operations for analysing and enhancing images[10]. It is important to obtain pixel values and statistics of the satellite image to improve the signal-to-noise ratio and modify the colours or intensities shown in Fig. 6. For example, image1.JPG is a low contrast image. The histogram of image1.JPG indicates that there are very few values above 80. If the data values are remapped to fill the entire intensity range [0, 255], one can increase the image's contrast. This kind of adjustment can be achieved with the imadjust function and the histeq function already explained. The general syntax of imadjust is J = imadjust(I, [low_in high_in], [low_out high_out]).

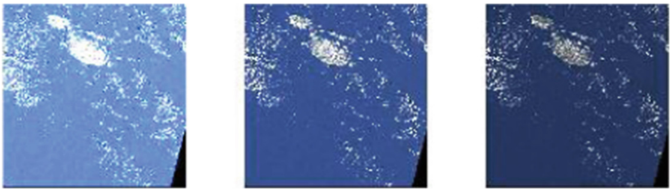


Fig. 6. Image enhancement process

Where low_in and high_in are the intensities in the input image which are mapped to low_out and high_out in the output image is shown in Fig. 7. For example, the code below performs the adjustment described above.

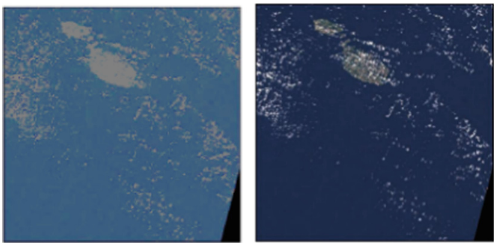


Fig. 7. Image Enhancement-Intensity Adjustment

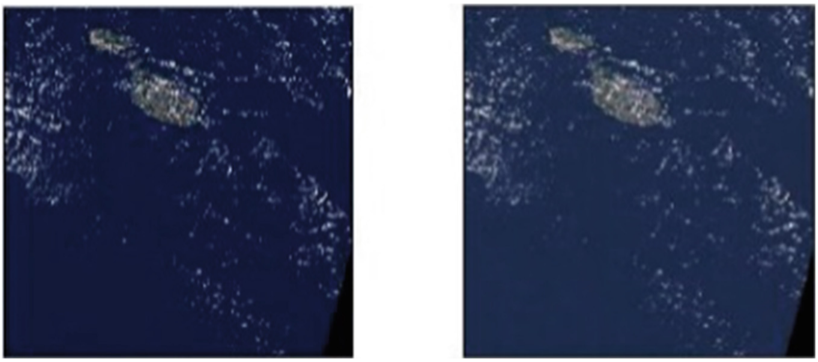


Fig. 8. Image enhancement process comparison

The first vector intensity to imadjust [0.0 0.2] specifies the low and high intensity values of the input image. The second vector [0.0 1.0] specifies the scale over which we want to map them. The intensity value ranges 0.0 in the input image and 0.5 in the output image, where another value range 0.0 to 1.0 in the output image is shown in Fig. 8. The intensity must be specifying the value between 0 and 1, regardless of class I is in uint8 multiplied by 255 to determine the actual values to use. The techniques for satellite image enhancement are contrast enhancement, density slicing and edge enhancement images.

5 Discussion

After getting the above-mentioned analysing processes, we compared them with the original satellite image for a better enhancement view. We visualised the resulting of the image enhancement filter is smoother than the original row image. This used method is quite different from the multiple satellite sensing reflectance platforms such as the radiometric process. This is also different from observing the subject at different times from Earth-orbiting satellites with short intervals and repetitive coverage. This involves temporal effects of the change detection technique. In this work, we analysed single satellite remote sensing for image enhancement. After long observation work, we proposed our desired result in Fig. 8. It is visually understandable and easy to explain that the image enhancement procedure followed sequential methods to equalise the different methodology in contrast stretching. It used a good constant value for satellite image enhancement, and it will create a good value for further enhancement.

6 Conclusion

In our working area of image enhancement, the resolution of the original row images is not the only problem. We had to face different equivalent geographical issues such as weather, cloud, fog and sunlight. That's why we found similar images with minor variations during observation. In the end, we have visualised and examined the attribute due to the specific need of the image analyst. Identifying the real object and the virtual object from the image is the actual purpose of our image enhancement. We tried to cover most of the techniques used to enhance the image quality and its attributes. In future, this work can be continued for further research-oriented work.

References

1. Sharma, L., Sengupta, S., Kumar, B.: an improved technique for enhancement of satellite image. J. Phys. Conf. Ser. **1714** (2021) 012051 (2021). https://doi.org/10.1088/1742-6596/1714/1/012051
2. Harichandana, M., Sowmya, V., Sajithvariyar, V.V., Sivanpillai, R. Comparison of image enhancement techniques for rapid processing of post flood images. In: ASPRS 2020 Annual Conference Virtual Technical Program, 22–26 June 2020
3. Ahuja, S.N., Biday, S.: A survey of satellite image enhancement techniques. IJAIR, **2**(8) (2018). ISSN: 2278-7844
4. Shukla, S.A., Khairnar, J., Mandawkar, U.: A survey on satellite image enhancement. J. Compos. Theory **XIII**(II) (2020). ISSN: 0731-6755
5. Ablin, R., Helen Sulochana, C., Prabin, G.: An investigation in satellite images based on image enhancement techniques. Eur. J. Remote Sens. (2019)
6. Pandey, P., Dewangan, K.K.: Satellite image enhancement techniques- a-comparative study. In: International Conference on Energy, Communication, Data Analytics and Soft Computing (2017)
7. Fawwaz, I., Zarlis, M., Rahmat, R.F.: The edge detection enhancement on satellite image using bilateral filter. In: 10th International Conference Numerical Analysis in Engineering (2018) https://doi.org/10.1088/1757-899X/308/1/012052

8. Psomiadis, E., Dalezios, N.R.: The role of spatial and spectral resolution on the effectiveness of satellite-based vegetation indices. Remote Sens. Agric. Ecosyst. Hydrol. XVIII (2016)
9. Traore, B.B., Kamsu-Foguem, B., Tangara, F.: Data mining techniques on satellite images for discovery of risk areas. Expert Syst. Appl. **72**, 443–456 (2017)
10. Khanduri, N., Akhtar, S., Vashisht, S., Gupta, S.: An enhancement to satellite image processing resolution. Amity J. Comput. Sci. (AJCS) **4**(1) (2020). ISSN: 2456-6616

Identification of Hotspot of Rape Cases in NCT of Delhi: A Data Science Perspective

G. Venkata Manish[1], Simran[1], Jitendra Kumar[1], and Dilip Kumar Choubey[2](✉)

[1] School of Advanced Sciences, Vellore Institute of Technology, Vellore, Tamil Nadu, India
jitendra.kumar@vit.ac.in

[2] Department of Computer Science and Engineering, Indian Institute of Information Technology Bhagalpur, Bihar, India
dkchoubey.cse@iiitbh.ac.in

Abstract. Human history endorsed evidence of violence against women in different forms. Offense against women made an appearance in the early stages, and it is continuing. The present research based on an inferential methodology using scan statistics. It is one of the most extensively used statistical methods as one of the most popular emerging data science techniques in the study of events like crime. Moral degradation in human values, narrow-mindedness, growing intolerance, lack of value-based education, illiteracy, and unemployment are some of the critical factors, that is likely to be held responsible for offenders to perpetrate criminal activities that could lead to such a heinous and shameful crime event. The research is conducted based on the secondary data available on the data portal, gathered from different government sources. The geographical unit under the study is based on various crime zones adjusted to and embed into the revenue district of NCT of Delhi. The p-value obtained from the log-likelihood ratio for each crime district taken as the basis of identification and segregation of hotspot. The software used for computation is M.S. Excel, MS Solver, R-Studio, and SaTScan. The current work considered to be of great importance in the optimization of resources needed for crime control, monitoring, and surveillance to avoid such events in any form in future planning. The term optimization is used for maximal utilization of available scarce resources like installation of cameras, number of police deployments, distribution of various sophisticated policing equipment's etc. to an extent of best possible measures to curb the menace effectively. Presently policing resources per person in NCT of Delhi is very much scarce and Delhi can be rated as very poor on that scale. For example, even in 2021 the estimated number of sanctioned strengths of Delhi Police is 83,762, means there are only 27 police sanctioned (not deployed) per ten thousand of the population. The actual number of deployed police per ten thousand populations may be further less. Similarly, we can cite an example of available CCTV cameras for surveillance estimated in the year 2021 is 1.32 lakh which comes to almost four CCTV for ten thousand person and even many of them are nonfunctional and defectives due to poor operational and maintenance reasons. Hence the problem of optimum utilization of resources is of prime importance. As such the relevance of the present work is aiming at societal interest and also enables our stressed policing bodies to execute an effective planning, is likely to be appreciated.

Keywords: Hotspots · Inferential · Scan statistics · Log-likelihood ratio · p-value

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 485–496, 2023.
https://doi.org/10.1007/978-3-031-13150-9_39

1 Introduction

The abduction of women is a serious crime that has a significant impact on the country's development. National Crime Records Bureau (NCRB) statistic [5] shows that Rajasthan, Madhya Pradesh and Delhi (the Capital of India) record the highest number of cases of rape. Delhi, being the nerve of India, needs more attention to control its growing rape cases as it leaves a lifelong remark on the victim. Due to the rise in the number of rape cases, the law enforcement bureau is persisting in looking for new approaches to analyze crime data and identify the locations with dense clusters of rape cases. The hotspot cluster analysis helps to determine the districts having a high intensity of happening of crime in the future. Using the outcome of the analysis, people can choose a better place to live, and it will help police forces create alertness, take preventions, and optimize the efficient use of human resources and available resources. There is a necessity to study the factors influencing the increment of the number of rape cases. Population density, area of the district, employment, literacy, and sex ratio are critical parameters to consider and analyze the relationship between the considered factors and the number of rape cases. The result from this study will establish some new measures to think about how literacy, unemployment, and sex ratio play a vital role in the growth rate of rape cases, and hence, it will help to reform the policies and education system. Besides, the model helps in predicting the count of cases with a unit change in factors involved in a particular study. The prime objectives of this research article are:

- To do descriptive analysis on cases of rape in NCT of Delhi between 2005 & 2015
- Ranking of Revenue districts in NCT of Delhi concerning consistency in crime (rape) happened.
- Develop & fit the regression model to explain the possibility of rape cases for some demographic factors.
- To identify the hotspot of cases of rape in NCT of Delhi.

The proposed approach in the article has been supported [15] with the earlier works. It is very important to mention that several algorithms implemented and used tools referenced through various articles and text references [16–28].

The rest of the article organized as follows: Introduction has been given in Sect. 1, Related Work stated in Sect. 2, Methodology has been stated in Sect. 3, Analysis and Results has been described in Sect. 4, and Conclusions has been committed to Sect. 5.

2 Related Work

Suri & Khan (2013) [1] found that most convicts were known to the victim. Kedia (2016) [2] explained how GIS could be used for crime mapping instead of using old traditional systems. Sukhija et al., (2017) [3] identified primary hotspots in state of Haryana, India. Venkatesh Nayak (2014) [4] performed statistical analysis on various the states of India. Chainey (2008) [5] identified if the certainty of one crime type is equally as accurate as another type of crime. They have also performed an analysis that measures the differences in the ability of hotspot mapping techniques for predicting future spatial crime patterns.

The area under the study is Camden and Islington in Central/North London. The result shows that Kernel density estimation is the best hotspot mapping technique among the commonly used technique for the identification of hotspots in the near future.

Sivaranjani et al., (2015) [6] designed a Geographic Information System for crime mapping. They used a radial basis and triangular with a linear interpolation method to map the hotspots and evaluated the precision comparison between different types of crimes involved under the study.

Nath (2006) [7] used a clustering algorithm to model crime detection. The proposed system used a geospatial plot to design crime clusters for significant attributes contributing to a crime pattern.

Rufus (2014) [8] states that globalization has led to a steady increase in the rate of employment of women. However, it has also led to many evils such as gender discrimination, physical and mental harassment, and more specifically, sexual harassment at the workplace.

Rawat (2015) [9] states that the national capital Delhi state has an explosion in rape cases, it has increased from 7.3% (in 2011) to 18.7% (in 2013) even after some legal progress with new laws enforcements. In 2013 Delhi has been recorded among top three highest rates of rape cases prevailed in India.

Orrenius and Coronado (2017) [10] states that they found evidence of a positive and significant correlation between the volume of apprehensions of illegal immigrants and the incidence of violent crime which made the border areas as the hotter safer stop for the crime.

Malleson and Andresen (2015) [11] used Spatio-temporal clustering to find hotspots in crime, spatial scan statistics are designed to detect significant clusters of events by moving a circular window of varying radius across a dataset and recording those circles that exhibit a statistically significant number of events.

Jangir et al., (2021) [12], Choubey et al., (2021) [13], (2016) [14] have used similar data science and machine learning algorithms for the identifications and predictions of medical diabetes. Kumar, J. (2014) [15] had done extensive work in hotspot detection and identification of criminal events in NCT of Delhi but his work was generic in nature not so specialized on rape cases. Various empirical theories have been discussed implicitly in multiple text references [16–18]. Recently, Bhatia, U. et al. (2022) [19], have used somewhat similar but not the same ideation in his work on drowsiness image detection using computer vision. The idea conceived through the review of many published articles, text and references like comparative analysis of classification methods [24], performance evaluation of classification methods [25], rule-based diagnosis system [26] and classification techniques and diagnosis for diabetes [27, 28] are found to be of great help in accomplishment of the present work.

3 Methodology

The consistency of crime occurring in a specific district, the relationship between the various demographic dimensions with the rate of rape cases and identifying hotspot can be analyzed using the below-mentioned techniques based on the dataset:

In this study, the districts of NCT of Delhi considered as per the 2011 census data. The crime district of Delhi converted into the revenue districts as shown in Table 1. The number of cases in the Outer crime district formed after 2011 divided into the part of Northeast and West Delhi.

Table 1. Revenue districts of Delhi

District	2015	2014	2013	2012	2011	2010	2009	2008	2007	2006	2005
Central	85	91	71	31	16	20	28	30	22	17	20
East	243	236	210	90	55	47	52	73	73	61	59
New Delhi	22	20	19	5	2	16	6	3	7	6	6
North	51	63	53	14	11	7	19	20	33	22	22
North East	250	244	183	78	69	51	47	32	89	93	106
North West	332	311	232	98	95	75	75	89	112	169	190
South	573	562	393	186	140	139	101	98	83	87	87
South West	226	250	194	87	69	54	52	38	51	79	72
West	440	386	273	112	109	96	83	83	124	88	94

A. **Descriptive Analysis:** It summarizes the characteristics of the data. To find out the most consistent crime happening revenue district in NCT of Delhi to rape cases over the period 2005–15, coefficient of variance is used, where

$$C.V = \left(\frac{\sigma}{\mu}\right) * 100 \tag{1}$$

The least C.V. valued district will be the most consistent crime happening Revenue district.

B. **Multiple Linear Regression Model:** The model predicts the number of rape cases likely to happen shortly to the unit change in the independent factors. Multiple Linear Regression model can fit as:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \ldots + \beta_k X_k + \in \tag{2}$$

Y is a dependent variable, X_1, X_2 ....Xk, are k independent variables that influence the response variable Y, in the model and $\in$ is the error component that explains the factors beyond control of this model or we may say that whose effects are not being reflected on Y.

C. **Analysis of Variance (ANOVA):**

The ANOVA technique used to analyze the variation of rape cases across time in the district of NCT Delhi. The hypothesis formulated as:
Null Hypothesis: It is a general statement which states that nothing changed in the situation or there is $H0$ denotes no significant difference occurred.
Alternative Hypothesis: The statements with a significant change in any of the parameters involved in the study.

D. **Finding hotspots using SaTScan:**

SaTScan is an opensource software to inspect the data in consideration of time, space, or both. The primary goal is to determine the clusters of hotspots (locations having a high intensity of happening of crime in the future). The software uses the Bernoulli and Poisson based model to analyze spatial crime data.
If C is the number of cases conferred on a map with n different zones, then the hypothesis is formulated as:
Null Hypothesis: The number of events for each region follows the Poisson distribution. The scandal cluster occurs by chance.
Alternative Hypothesis: There exist significant clusters on the map.
Under the assumption of Poisson model, the log-likelihood ratio [6] defined as:

$$L(x) = (\frac{C_x}{\mu_x})^{C_x}(\frac{C - C_x}{C - \mu_x})^{C-C_x} \quad (3)$$

where, C = Number of cases in x and μx = the adjusted average number of cases within x. The region with the maximum likelihood creates the most likely cluster.

4 Analysis and Results

Based on the data following summary tables are obtained:

1. **Consistency in crime:**
   On using the statistical measure called the coefficient of variance, the ranks obtained as:

Table 2. Computed consistency ranking

District	C.V	Rank
North West	58.33	1
North	65.73	2
North East	68.48	3
East	72.27	4
South West	75.56	5
Central	72.79	6
New Delhi	73.21	7
West	76.51	8
South	86.25	9

As per the Table 2, Northwest district of NCT Delhi is the most consistent district in the occurrence of rape cases. North Delhi and North East are secondary and tertiary consistent districts (Fig. 1).

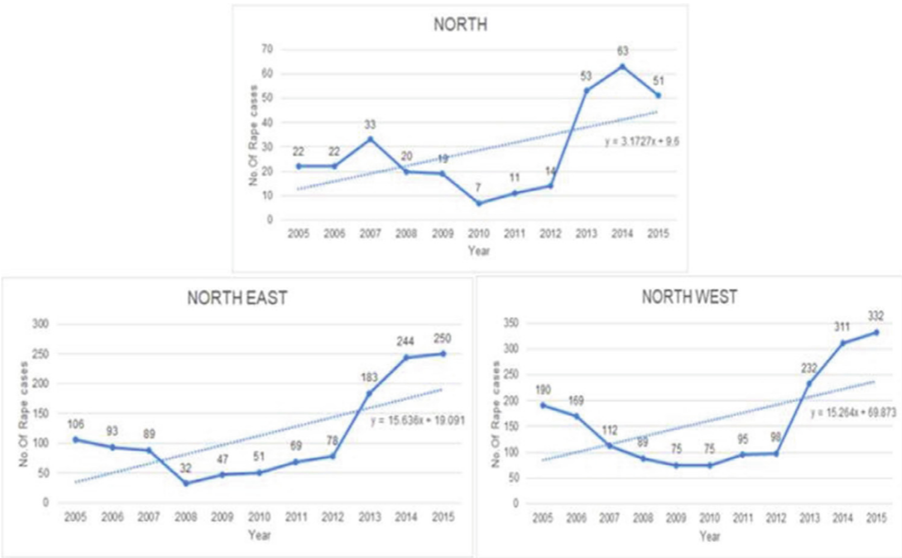


Fig. 1. Time series graph of the top three consistent revenue district to cases of rape

2. **Multiple Linear Regression model:** The mean no. of cases is calculated by using no. of cases registered in the period 2005–15.

The regression line draws to predict the average number of rape cases with a unit change in factors like population density, literacy rate, sex ratio, and the number of workers.

$$Y = 857.3 + 0.00210X_1 + 0.0002833X_2 + 11.6X_3 - 0.1834X_4$$

where, Y = No. of rape cases, X_1 = Population Density, X_2 = No. of Workers, X_3 = Literacy Rate, X_4 = Sex Ratio, $\in$ = Others factor not included in this study (Fig. 2).

```
Coefficients:
             Estimate Std. Error t value Pr(>|t|)
(Intercept) -8.573e+02  2.952e+03  -0.290    0.786
b            2.101e-03  6.003e-03   0.350    0.744
c            2.833e-04  9.449e-05   2.999    0.040 *
d            1.116e+01  1.721e+01   0.649    0.552
e           -1.834e-01  2.932e+00  -0.063    0.953
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 82.75 on 4 degrees of freedom
Multiple R-squared:  0.7383,    Adjusted R-squared:  0.4766
F-statistic: 2.821 on 4 and 4 DF,  p-value: 0.1696
```

Fig. 2. Snapshot of summary of the regression model

Based on the adjusted R-squared value, we conclude that the study's factors contribute 47% variation in the number of rape cases (Table 3).
Analysis of Variance (ANOVA):

Table 3. Revenue district of NCT of Delhi from year 2011 to 2015

District	2015	2014	2013	2012	2010
North West	332	311	232	96	95
North	51	63	53	74	11
North East	250	244	183	78	69
East	243	236	210	90	55
South West	226	250	194	87	69
Central	85	91	71	31	16
New Delhi	22	20	19	5	2

(*continued*)

Table 3. (*continued*)

District	2015	2014	2013	2012	2010
West	440	386	273	112	109
South	573	562	393	186	140

As per Table 4, shown below, a two way ANOVA technique can use, to estimate and reduce the variances emerging out of regression effects in the model, where two variables involved are year and district. We set the null hypothesis and alternative hypothesis as follows:
$H_0 : \mu_{2011} = \mu_{2012} = \mu_{2013} = \mu_{2014} = \mu_{2015}$ H_1: At least one of the μ_i is not equal, where, μ_i = mean value of rape cases of the ith year. This is a simple versus composite hypothesis and the level of significance chosen for the study is by default $\alpha = 0.05$. Table 4 consists of summarized details produced by ANOVA methods.

Table 4. Analysis of variance (ANOVA)

Sources of Variation	df	SS	MSS	F-Ratio	p-Value	F critical
Rows	8	523272.2	65409.02	16.10076	0.000000315	2.244396
Columns	4	275368.2	68842.06	16.94582	0.0000149	2.668437
Errors	32	129999.4	4062.481			

Since the F value is higher than the critical value, we reject the null hypothesis. Also, the p values are statistically significant in favour of rejecting the null hypothesis. We can infer that the change of the effect of time over the cases registered in different districts of NCT Delhi is significant in regard to rising figure of rape cases in NCT of Delhi. It's a worrisome situation.
Hotspots using SaTScan software: The following summary table has obtained Based on the dataset on the number of incidents of rape cases from the period 2013–15:

Table 5 consists of the summary of the relative risk in the primary clusters from the period 2013–2015.

Table 5. Summary of relative risk in the primary clusters from the period 2013–2015

	2013	2014	2015
Primary Cluster	North	South	West
	North West	South West	North West
	North East	East	South West
Relative Risk	2.59	2.98	2.99
LLR (Log Likelihood Ratio)	154.683902	305.334086	317.030288
p-Value	<0.00000000000000001	<0.00000000000000001	<0.00000000000000001

Figures 3, 4 and 5 illustrates the primary clusters for the year2015, 2014 and 2013.

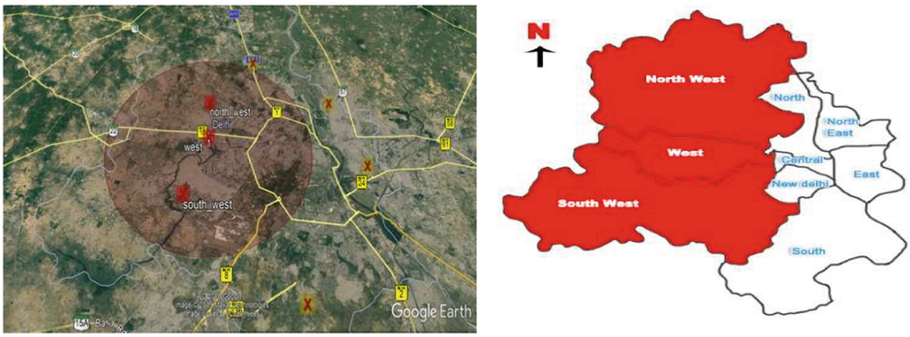


Fig. 3. Primary clusters for the year 2015

Fig. 4. Primary clusters for the year 2014

By using the SaTScan software, it has observed that the hotspots are shifting every year in a cyclic pattern, which indicates that the effect of patrolling and alertness of

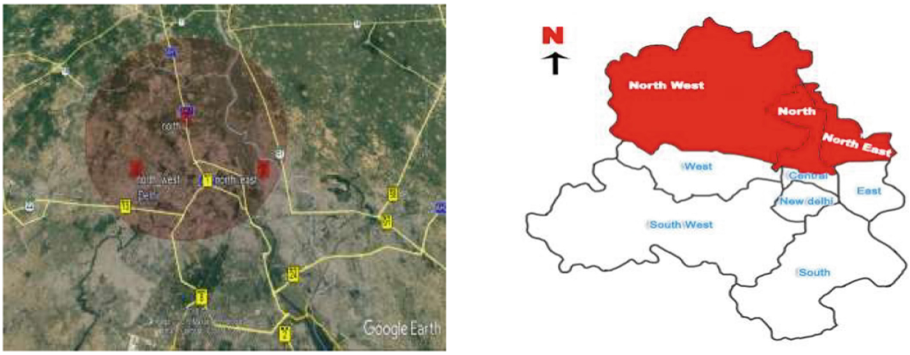


Fig. 5. Primary clusters for the year 2013

police forces in particular districts compel offenders and illegal migrants to move to another district. From the summary table, we found that North West and the southwest district of NCT Delhi are major primary hotspots with a high likelihood of happening in rape cases. Also, the relative risk in the happening of rape cases is increasing in the border area of NCT Delhi from the year 2013–15.

5 Conclusion

We propose The Descriptive study indicates that North West, North, and North East districts of NCT Delhi are more consistent in happening of rape cases. As per output generated through the SaTScan, North West and South West are the significant clusters. Further, it observed that the increase in population density, number of workers, and literacy rate cause inflation in the number of rape cases. These results have been supported with the earlier work done. These observations give a new intuition to rethink that raising the literacy rate with education and morals is more important. With the rise in sex ratio, the count of rape cases will fall, which reveals that gender equality can bring down the number of rape cases. Also, the change of the effect of time over cases of rape found to be significant. It is important to mention that the various methods and tools implemented in the present work has been thoroughly read and cautiously & meticulously examined before being used for theoretical and computational analysis. The future work that basically provides further scope of the present work should be focus on characterization of the hotspot regions and it must be investigated thoroughly to establish a best possible fit for the cause-and-effect analysis stochastic and simulation model to combat such shameful menace. One should look forward for the best fit model so that all elements of uncertainties could easily be analyzed and assessed properly to make the life of the people of our national capital more and more safe, progressive and joyful.

The limitations of this work may be:

a. The demographic information used to draw from the 2001 and 2011 census data.
b. Complete data regarding Crime Districts of NCT Delhi is not available.

c. The revenue districts considered are based on the 2011 census instead of present revenue districts formed after 2011.
d. Micro level dataset not available.

Glossaries: Primary cluster, NCT, GIS, most likely cluster, coefficient of determination, $R^2 and adjusted R^2$, Analysis of Variance (ANOVA), degrees of freedom, F ratio, Sum of Squares (SS), Mean Sum of Squares (MSS), Relative Risk, Log Likelihood Ratio (LLR), level of significance (α), p-value.

References

1. Suri, S., Khan, S.: An analytical study of rape in Delhi. Int. J. Edu. Psychol. Res. **2**(3), 60–68 (2013)
2. Kedia, P.: Crime mapping and analysis using GIS. Int. Inst. Info. Technol. **1**(1), 1–15 (2016)
3. Sukhija, K., Singh, S.N., Kumar, J.: Spatial visualization approach for detecting criminal hotspots: An analysis of total cognizable crimes in the state of Haryana. In: 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), pp. 1060–1066. IEEE (2017 May)
4. Nayak, V.: Preliminary Analysis of Some Statistics relating to the Offence of Rape as Reported by the National Crime Records Bureau for the Period 2001–2013, CHRI, New Delhi (2014)
5. Chainey, S., Tompson, L., Uhlig, S.: The utility of hotspot mapping for predicting spatial patterns of crime. Secur. J. **21**(1), 4–28 (2008)
6. Sivaranjani, S., Sivakumari, S.: GIS based crime hotspot mapping and analysis using radial base function (RBF) and interpolation method. Int. J. Remote Sensing and Geoscience **4**(5), 43–49 (2015)
7. Nath, S.V.: Crime pattern detection using data mining. In: 2006 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology Workshops, pp. 41–44. IEEE (2006 December)
8. Rufus, D.: Victims of sexual harassment at the workplace a comparative study in the organized and unorganized sectors of Tirunelveli district (2014)
9. Rawat, R., Masthanaiah, T.: Explosion of rape cases in India: a study of last one decade. Int. J. Curr. Res. **7**(7), 17976–17984 (2015)
10. Orrenius, P.M., Coronado, R.: The effect of illegal immigration and border enforcement on crime rates along the US-Mexico border (2017)
11. Malleson, N., Andresen, M.A.: Spatio-temporal crime hotspots and the ambient population. Crime Sci. **4**(1), 1–8 (2015). https://doi.org/10.1186/s40163-015-0023-8
12. Jangir, S.K., Joshi, N., Kumar, M., Choubey, D.K., Singh, S., Verma, M.: Functional link convolutional neural network for the classification of diabetes mellitus. Int. J. Numeri. Methods in Biomedical Engineering, e3496 (2021)
13. Choubey, D.K., Tripathi, S., Kumar, P., Shukla, V., Dhandhania, V.K.: Classification of Diabetes by Kernel based SVM with PSO. Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science), 14(4), 1242–1255 (2021)
14. Choubey, D.K., Paul, S.: GA_MLP NN: a hybrid intelligent system for diabetes disease diagnosis. Int. J. Intell. Sys. Appli. **8**(1), 49 (2016)
15. Kumar, J.: Some Contribution to Scan Statistics and Their Applications. Doctoral thesis, Department of Statistics, Patna University, Patna (2014)
16. Anderson, N.H., Titterington, D.M.: Some methods for investigating spatial clustering with epidemiological applications. J. R. Stat. Soc. A. Stat. Soc. **160**(1), 87–105 (1997)

17. Alm, S.E.: Approximation and simulation of the distributions of scan statistics for Poisson processes in higher dimensions. Extremes **1**(1), 111–126 (1998)
18. Kulldorff, M., Rand, K., Gherman, G., Williams, G., DeFrancesco, D., SaTScan, V.1.: Software for the spatial and space-time scan statistics. SaTScan. National Cancer Institute, Bethesda, MD (1998)
19. Bhatia, U., Tshering, Kumar, J., Choubey, D.K.: Drowsiness image detection using computer vision. In: Sharma, T.K., Ahn, C.W., Vesma, O.P., Panigarhi, B.K. (eds.) Soft Computing: Theories and Applications. Advances in Intelligent Systems and Compting, 1380(1), pp. 667-683. Springer, Singapore (2022)
20. Hajela, G., Chawla, M., Rasool, A.: A clustering based hotspot identification approach for crime prediction. Procedia Computer Science **167**, 1462–1470 (2020)
21. Anselin, L., Cohen, J., Cook, D., Gorr, W., Tita, G.: Spatial analyses of crime. Criminal justice **4**(2), 213–262 (2000)
22. Andresen, M.A.: Crime measures and the spatial analysis of criminal activity. Br. J. Criminol. **46**(2), 258–285 (2006)
23. Anselin, L., Griffiths, E., Tita, G.: Crime mapping and hot spot analysis. In: Environmental criminology and crime analysis, pp. 119–138. Willan (2013)
24. Choubey, D.K., Kumar, M., Shukla, V., Tripathi, S., Dhandhania, V.K.: Comparative analysis of classification methods with PCA and LDA for diabetes. Curr. Diabetes Rev. **16**(8), 833–850 (2020)
25. Choubey, D.K., Kumar, P., Tripathi, S., Kumar, S.: Performance evaluation of classification methods with PCA and PSO for diabetes. Network Modeling Analysis in Health Informatics and Bioinformatics **9**(1), 1–30 (2019). https://doi.org/10.1007/s13721-019-0210-8
26. Choubey, D.K., Paul, S., Dhandhenia, V.K.: Rule based diagnosis system for diabetes. An International Journal of Medical Sciences **28**(12), 5196–5208 (2017)
27. Choubey, D.K., Paul, S.: GA_RBF NN: a classification system for diabetes. Int. J. Biomed. Eng. Technol. **23**(1), 71–93 (2017)
28. Choubey, D.K., Paul, S.: Classification techniques for diagnosis of diabetes: a review. Int. J. Biomed. Eng. Technol. **21**(1), 15–39 (2016)

Survey on Fruit Classification Using Deep Learning Techniques

Surya Petluru and Pradeep Singh(✉)

National Institute of Technology, Raipur, India
psingh.cs@nitrr.ac.in

Abstract. Fruit classification is one of the important tasks in both agricultural and industrial fields. A fruit classification model can help a farmer in classifying his products according to size, shape, or even weight. Artificial intelligence is growing day by day and proper machine learning models are being developed for fruit classifications. Due to the ability of automatic robust feature extraction from images, deep Learning (DL) has variety of applications. Hence, the use of Deep Learning (DL) techniques specially CNN based architectures with the ability to perform object identification based on multiple features like color, shape, and object have gained attention for fruit classification. In this paper, we have studied some of the initial fruit classification models and deep learning models that are currently used in agricultural and industrial applications.

Keywords: Artificial intelligence · Image segmentation · Deep learning

1 Introduction

Smart farming is very important in tackling several problems of agriculture like productivity, food security, the impact of climate changes, and sustainability. Since the population around the globe keeps increasing every day, food production needs to take a big boost. Along with increasing the scale of production, it is very important to keep the balance of the ecosystem intact using more eco-friendly methods of farming.

To address the challenges possessed in agriculture, complex and unpredictable ecosystems need to be understood in a better way. Measuring, monitoring, and analysing several physical aspects continuously helps to achieve the solution to the challenges of agriculture. The deployment of new technologies for small-scale agricultural needs and largescale observation of ecosystems around the globe will help in performing tasks and decision making by a situation, context, and awareness on the local environment.

The classical Machine Learning (ML) models are being applied in several fields. There are several advancements made in the field of image processing and introducing a new era of machine learning called deep learning in agricultural fields. In order to reduce the rising food demands and for increasing the scale of productivity, agricultural products must be monitored all the time and is only possible by new emerging technologies [1]. Artificial intelligence methods such as ML and DL models are used for various purposes in the field of agriculture. Among the techniques that are being used, DL has given better

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 497–505, 2023.
https://doi.org/10.1007/978-3-031-13150-9_40

outputs compared to other techniques because of its ability to perform feature extraction effectively.

Precise classification of several kinds of species of fruits is one of the rising topics in computer science research. It was very important not only because of its application in academic research but also for its application in industries. Several industrial applications can be built on DL classification techniques. One such application can help the cashiers identify the species of fruits bought by the customers and can be helpful to determine the exact price for the fruits.

The deep learning model of the classification problem also can be implemented as a mobile application. This developed application can help patients or people with some long-term health problems in deciding whether the fruit satisfies the diet requirements of the patient. These models help in identifying the fruit types and matches them with its list of contents and providing advice to the patient. On the contrary, fruit classification models which are based on computer vision is still a difficult challenge because following reasons.

1. There is so much similarity in colour, texture, and shape of several species of fruits.
2. A single class of fruit has an extreme variation among several aspects like the maturity of the fruit and the form in which fruit has been presented.

Further, this paper discusses the initial fruit classification models, Deep learning, fruit classification using the Deep Learning with their results and the challenges of fruit classification.

2 Initial Classification Models

Many researchers have tackled the challenge of fruit detection such as works done by [2–4], but the necessity of building a fast, reliable fruit classification system is still challenging [5]. This problem keeps persisting because of its high variation in fruit appearance including shape, colour, texture, and size. Furthermore, fruits are brought abstracted partially and they are subjected to continuous changes in shadows of fruits which makes it a difficult task to perform [6].

The works presented in this section address the challenges possessed by the fruit image segmentation problem. Wang et al., [7] developed apple fruit detection to predict the amount of yield. The system developed by the authors is based on colour differences and different reflective patterns. A segmentation approach for sweet peppers has been proposed in [8]. They performed experiments on raw data and normalized indices, also used the entropy of texture features. These experiments are performed in a glasshouse environment that is highly controlled manually. However, this model is not accurate enough to perform the task.

Hung et al., [9] proposed a technique for almond segmentation with the help of conditional random fields. The authors proposed a method for a five-class segmentation technique in which the features are extracted with the help of a Sparse Encoder (SAE). Then these features were used in a CR framework and the results of this model were better than the previous works. However, they performed the segmentation very impressively but fails to do object detection. This model is also suitable only for very few levels of occlusion.

Yamamoto et al., [3] proposed tomato detection and used colour and shape attributes to train Classification and Regression Trees (CART).

Most of these studies have been performed a near-accurate fruit classification in a controlled environment. Hence, the challenge of performing a fruit classification in a highly complex environment is still unsolved. The reason for this is the variability rate of fruits is very high in these environments. Although for selected images, the performance is high still it cannot handle the variable-rate deployed in real farm environments. Hence, Deep Learning techniques are explored. DL has the ability to perform classification in very complex situations and it gives a better result than classical classification techniques.

3 Deep Learning

Deep Learning (DL) is an extension of traditional machine learning. The concept of DL adds more complexity and depth to the machine learning models along with transforming the data with the help of several functions which will represent the data in a new hierarchical model with several levels of abstraction [8]. DL allows feature learning which is a great addition to the traditional methods. Feature Learning is a concept of extracting automatic features from raw data, where the composition of lower-level features is combined to get the higher levels.

The complex DL models can reduce the error rate for regression problems and accuracy can be increased hugely compared to ML models. DL models have several components like gates, pooling, and fully connected layers, convolutions, activation functions, etc.

DL models have a very large hierarchical design and have a good learning capacity which makes them perform predictions very well and these DL models are flexible and adaptable for a much complex problem. DL has gained its popularity for dealing with video and image-based data but DL models can be applied to any kind of data like speech, natural language processing continuous data such as weather prediction data [10], chemical components of soil [11], and population data [12].

Deep learning uses the concept of neural networks to perform classification and regression problems. CNNs are the most widely used network to perform image classification problems because of having lesser parameters than other networks [13]. Within the CNN, there are several kinds of layers like convolutional layers, pooling layers, fully connected layers etc.

The basic architecture of a fruit classification model using CNNs has been provided in Fig. 1. The deep learning method performs certain pre-processing techniques to get better results from the dataset. Pre-processing involves several techniques like data augmentation [14], Wavelet Transform [15], S-transform [16], etc. The function of convolutional layers is to determine the output of neurons that are connected to the local regions. The output of neurons is calculated by doing the scalar product of the weights and region of input layer. Every convolutional network in a CNN is followed by a pooling layer. Hence, multiple convolutional layers have multiple pooling layers. The function of pooling layer is to down-sample the spatial dimensionality of the input layers. This helps in further reducing the number of parameters of the deep learning model [17]. The convolutional layers along with pooling layers are used for feature extraction for the given input image. The output of the convolution or pooling layer is flattened and fed into one or more fully connected layers. The fully connected layers classify the images based on the feature extraction done by the convolution or pooling layers.

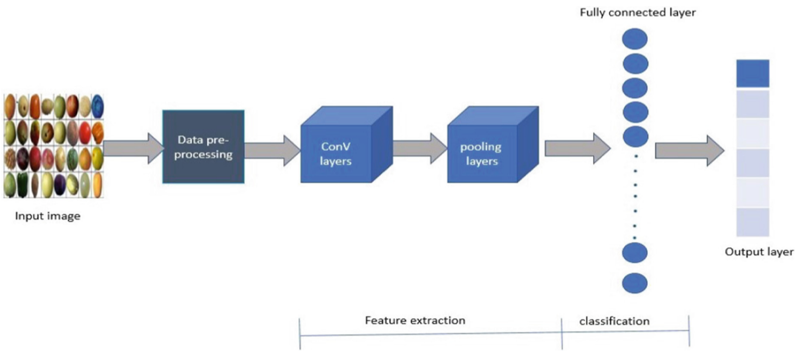


Fig. 1. CNN architecture for image classification

4 Fruit Classification Systems

This section discusses various fruit classification models based on deep learning which are used in agricultural or industrial purposes.

4.1 Deep Learning and Computer Vision for Estimating Date Fruits Type, Maturity Level, and Weight

Faisal et al., [18] has discussed three types of date fruit classification systems. i)Date Type Estimation System [DTES] ii) Date Maturity Estimation System [DMES] and iii) Date Weight Estimation System [DWES]. This paper uses deep learning techniques along with computer vision for the purpose of estimating the type, maturity, and weight. The technique uses a date fruit dataset which is collected and processed by the centre of robotics research [19]. This dataset consists of 8079 images separated into two different types. Type-1 is used for type and maturity estimation whereas the type-2 dataset is used for weight estimation.

They used four DL models namely ResNet, VGG-19, Inception-V3, and NASNet. These four DL techniques are used for both type and maturity estimation of date fruit. For the weight estimation of the fruit, the authors have used Support Vector Machine (SVM). DTES has achieved a maximum accuracy of 99.175% whereas DMES has got 99.058% for the dataset. The maximum accuracy of the DWES system is 84.27% which is achieved by using an SVM-linear system.

4.2 Monitoring the Change Process of Banana Freshness by GoogLeNet

In the year 2020, Jiangong et al., [20] proposed a paper that monitors the ripening process of a banana. In the proposed model, the dataset consists of images of 103 bananas of two types. These bananas are stored for 11 days at constant room temperature and images are taken from a constant position.

The proposed method uses a GoogLeNet architecture proposed by Szegedy [21] which is a prominent CNN and deep learning model. For training the model, GooogLeNet was used because it is far superior model for the identification of vegetables and fruits. For classification purposes, the average pooling layer was used instead of the fully connected layer. The proposed model achieved an accuracy of 98.92% in identifying the freshness of bananas.

4.3 Olive-Fruit Variety Classification by Means of Image Processing and Convolutional Neural Networks

Juam et al., [22] have proposed a model for olive fruit classification by using techniques of image processing and CNNs. The dataset used consists of 2800 images of olive fruits 400 of each 7 types [23]. In 2800 images, 1750 are used for training the model and 1050 are used for validation.

Initially, in the image pre-processing phase, olive images which are generated are converted into binary images using the methodology proposed by [23]. Once the images are binarized, images are converted into a new image of square shape with a width and height of 501 * 501. For training, the CNN, pre-trained image model of ImageNet [24] along with Transfer learning [25] are used for training. In the proposed method, maximum accuracy of 95.91% has been achieved by using Inception-ResnetV2 architecture.

4.4 Automatic Fruit Classification Using Deep Learning for Industrial Applications

Hossain et al., [26] proposed an automatic classification model for industrial applications. The model proposed uses two datasets that are publicly available. Dataset 1 contains 2633 clear fruit images collected from [27]. Dataset 2 contains 5946 images of 10 types of fruits. Dataset 2 consists of complex images.

The proposed model for industrial application has two different DL architectures. The first model is a lightweight model with 6 CNN layers. The second model is a pre-trained deep learning model of VGG-16. The accuracy achieved by these two models are 99.49% and 99.75% respectively on dataset1. The accuracy achieved on dataset2 is 85.43% and 96.75% respectively.

4.5 Pure-CNN: A Framework for Fruit Images Classification

Asis et al., [28] have proposed a paper for fruit image classification of multiple fruits. They used a Pure Convolutional Neural Network (PCNN) model for classification purposes. This model uses a minimum number of pooling layers. The proposed method also involves the Global Average Pooling (GAP) layer for reducing the overfitting problems.

The model has been tested on fruit-360 [29]. The dataset in which 41322 images are used for training, 9744 images for validating the working of the model, and 4133 images for testing the model. Hence, a total of 55244 images are used for building the model. The experiments have shown that the proposed PCNN+GAP model has given better accuracy than a CNN with a fully connected layer.

4.6 A Fruit Detection Algorithm Based on R-FCN in Natural Scene

Liu et al., [30] have proposed a fruit detection technique for a natural scene. This paper aims at improving the precision and efficiency of a computer vision system for robotic picks. The proposed deep learning technique combines two techniques like regional suggestion network and a full convolutional layer for better performance. This technique performs pixel-level feature extraction in the initial layers of the CNN. The model was tested on a publicly available COCO dataset [31] and within the dataset apple, orange and banana are taken as objects of the experiment. Table 1 shows the summary of various machine learning approaches used for fruit classification task.

Table 1. Summary of ML/DL approaches for fruit classification

Dataset	Fruit type	Image type	Model	Accuracy
Faisal et al., [19]	Date fruit	RGB images	ResNet – DTES and DMES SVM – DWES	DTES-99.175% DMES-99.058% DWES-84.27%
Jiangong et al., [20]	Banana	RGB images 224 * 224 * 3	GoogleNet model	98.92%
Juam et al., [22]	Oliver	RGB images 227 * 227 * 3	Inception-ResnetV2 architecture	95.91%
Hossain et al., [26, 27]	Multiple fruits	RGB images	(i) Light architecture model ii) VGG-16	99.49% and 85.43% 99.75% and 96.75%
Asis et al., [28]	Multiple fruits	RGB images 100 * 100	PCNN architecture + global average pooling layer	98.88%
Liu et al., [31]	Apple, Orange, Banana	RGB images 640 * 480	RPN + fully convolutional network	Apple: 97.66% Orange: 96.50% Banana: 82.30%

5 Challenges of Fruit Classification

Object classification in fruits is considered as an inherently more complex task than other object classifications. A crucial set of sensory and feature characteristics are also present in fruits. The major challenges of fruit classification are:

5.1 Appropriate Sensor

In fruit classification, selecting an appropriate sensor for data acquisition is one of the key challenges. Sensors which range from black & white cameras to sensors such as tactile and acoustic sensors are used for fruit classification. However, every sensor is not suitable for all applications. As mentioned in [32], Acoustic and tactile sensors are very less suitable for fruit classification. These sensors need either physical contact or excitation of the fruit for classification purposes. Visual sensors are highly sensitive to several factors like illumination conditions and background environment [33]. There are much more complex factors like scale, rotation, refraction, reflection, and translation.

5.2 Feature Selection and Representation

Features of an object are the physical characteristics that can distinguish it from other objects. There are several features for fruit such as shape, color, texture, and size. These features together combined can be used for effective classification. Fruits generally have various inter and intraclass similarities as well as variations between them. The interclass variations are the major changes i.e., color, texture, and shape variations. However, intraclass variations are very subtle and difficult to differentiate i.e., various kinds of mangoes which will have only slight feature variations.

An ideal feature selection technique will deal with inter and intraclass feature classification [34]. However, the computer representation of selected features is another challenge. Researchers have shown that effective fruit classification cannot be done based on a single feature [35].

5.3 Machine Vision Approach

In machine vision approaches, a set of machine learning algorithms are used for the purpose of classification of images. The algorithms used for classification can be categorized in many ways, one usual categorization is an artificial neural network based and handcrafted. The task of selecting a proper algorithm is always difficult and most crucial but is even more crucial in the case of fruits.

6 Conclusion

Deep Learning is a very powerful version of machine learning or artificial intelligence. In this paper, a survey has been done on the fruit classification techniques in industrial and agriculture applications. As it is evident for the literature that classical machine learning & vision algorithms are not performing satisfactorily to cope with numerous classes and multi-feature nature of fruits. The current research with deep learning technique is a step toward development of efficient fruit classification model. A comprehensive study of the deep learning techniques used for fruit classification is performed. The study also explores the possibilities and challenges for fruit classification. Deep Learning has given a boost for fruit image classification and can be utilized more effectively in the food industry.

References

1. Goncharov, P., Ososkov, G., Nechaevskiy, A., Uzhinskiy, A., Nestsiarenia, I.: Disease detection on the plant leaves by deep learning. In: Kryzhanovsky, B., Dunin-Barkowski, W., Redko, V., Tiumentsev, Y. (eds.) Neuroinformatics 2018. SCI, vol. 799, pp. 151–159. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-01328-8_16
2. Nuske, S., Wilshusen, K., Achar, S., Yoder, L., Singh, S.: Automated visual yield estimation in vineyards. J. Field Robot. 837–860 (2014). https://doi.org/10.1002/rob.21541
3. Yamamoto, K., Guo, W., Yoshioka, Y., Ninomiya, S.: On plant detection of intact tomato fruits using image analysis and machine learning methods. Sensors (Switzerland) **14**, 12191–12206 (2014). https://doi.org/10.3390/s140712191
4. Nuske, S., Achar, S., Bates, T., Narasimhan, S., Singh, S.: Yield estimation in vineyards by visual grape detection. Presented at the Dec 6 (2011). https://doi.org/10.1109/iros.2011.6095069
5. Kapach, K., Barnea, E., Mairon, R., Edan, Y., Ben-Shahar, O.: Computer vision for fruit harvesting robots – state of the art and challenges ahead. Int. J. Comput. Vis. Robot. **3**, 4–34 (2012). https://doi.org/10.1504/IJCVR.2012.046419
6. Song, Y., Glasbey, C.A., Horgan, G.W., Polder, G., Dieleman, J.A., van der Heijden, G.W.A.M.: Automatic fruit recognition and counting from multiple images. Biosyst. Eng. **118**, 203–215 (2014). https://doi.org/10.1016/j.biosystemseng.2013.12.008
7. Wang, Q., Nuske, S., Bergerman, M., Singh, S.: Automated Crop Yield Estimation for Apple Orchards (2013)
8. Bac, C.W.: Improving obstacle awareness for robotic harvesting of sweet-pepper (2015)
9. Hung, C., Nieto, J., Taylor, Z., Underwood, J., Sukkarieh, S.: Orchard fruit segmentation using multi-spectral feature learning. In: IEEE International Conference on Intelligent Robots and Systems, pp. 5314–5320 (2013). https://doi.org/10.1109/IROS.2013.6697125
10. Sehgal, G., Gupta, B., Paneri, K., Singh, K., Sharma, G., Shroff, G.: Crop Planning using Stochastic Visual Optimization (2017)
11. Song, X., Zhang, G., Liu, F., Li, D., Zhao, Y., Yang, J.: Modeling spatio-temporal distribution of soil moisture by deep learning-based cellular automata model. J. Arid. Land **8**(5), 734–748 (2016). https://doi.org/10.1007/s40333-016-0049-0
12. Demmers, T.G.M., Cao, Y., Gauss, S., Lowe, J.C., Parsons, D.J., Wathes, C.M.: Neural predictive control of broiler chicken growth. In: IFAC Proceedings Volumes (IFAC-PapersOnline), pp. 311–316. IFAC Secretariat (2010). https://doi.org/10.3182/20100707-3-BE-2012.0061
13. Albawi, S., Mohammed, T.A., Al-Zawi, S.: Understanding of a convolutional neural network. In: Proceedings of 2017 International Conference on Engineering and Technology, ICET 2017, pp. 1–6. Institute of Electrical and Electronics Engineers Inc. (2018). https://doi.org/10.1109/ICEngTechnol.2017.8308186
14. Shorten, C., Khoshgoftaar, T.M.: A survey on image data augmentation for deep learning. J. Big Data **6**(1), 1–48 (2019). https://doi.org/10.1186/s40537-019-0197-0
15. Qiao, W., Tian, W., Tian, Y., Yang, Q., Wang, Y., Zhang, J.: The forecasting of PM2.5 using a hybrid model based on wavelet transform and an improved deep learning algorithm. IEEE Access **7**, 142814–142825 (2019). https://doi.org/10.1109/ACCESS.2019.2944755
16. Guo, F., Wang, P., Wang, Y., Ren, P., Zhang, Y.: Research on improved S transform for the feature extraction of power quality disturbance signal. IEEE Access **8**, 137910–137917 (2020). https://doi.org/10.1109/ACCESS.2020.3012291
17. O'Shea, K., Nash, R.: An Introduction to Convolutional Neural Networks (2015)
18. Faisal, M., Albogamy, F., Elgibreen, H., Algabri, M., Alqershi, F.A.: Deep learning and computer vision for estimating date fruits type, maturity level, and weight. IEEE Access **8**, 206770–206782 (2020). https://doi.org/10.1109/ACCESS.2020.3037948

19. Hamdi Altaheri, M.A.M.F.G.M.: Date fruit dataset for automated harvesting and visual yield estimation. IEEE Dataport
20. Ni, J., Gao, J., Deng, L., Han, Z.: Monitoring the change process of banana freshness by GoogLeNet. IEEE Access (2020). https://doi.org/10.1109/ACCESS.2020.3045394
21. Szegedy, C., et al.: Going Deeper with Convolutions (2014)
22. Ponce, J.M., Aquino, A., Andújar, J.M.: Olive-fruit variety classification by means of image processing and convolutional neural networks. IEEE Access **7**, 147629 (2019). https://doi.org/10.1109/ACCESS.2019.2947160
23. Ponce, J.M., Aquino, A., Millan, B., Andujar, J.M.: Automatic counting and individual size and mass estimation of olive-fruits through computer vision techniques. IEEE Access **7**, 59451–59465 (2019). https://doi.org/10.1109/ACCESS.2019.2915169
24. Deng, J., Dong, W., Socher, R., Li, L.-J., Kai, L., Li, F.-F.: ImageNet: a large-scale hierarchical image database. Presented at the 1 Mar 2010. https://doi.org/10.1109/cvpr.2009.5206848
25. Shin, H.C., et al.: Deep convolutional neural networks for computer-aided detection: CNN architectures, dataset characteristics and transfer learning. IEEE Trans. Med. Imag. **35**, 1285–1298 (2016). https://doi.org/10.1109/TMI.2016.2528162
26. Shamim Hossain, M., Al-Hammadi, M., Muhammad, G.: Automatic fruit classification using deep learning for industrial applications. IEEE Trans. Ind. Informatics. **15**, 1027–1034 (2019). https://doi.org/10.1109/TII.2018.2875149
27. Rocha, A., Hauagge, D.C., Wainer, J., Goldenstein, S.: Automatic fruit and vegetable classification from images
28. Kausar, A., Sharif, M., Park, J., Shin, D.R.: Pure-CNN: a framework for fruit images classification. In: Proceedings – 2018 International Conference on Computational Science and Computational Intelligence, CSCI 2018, pp. 404–408. Institute of Electrical and Electronics Engineers Inc. (2018). https://doi.org/10.1109/CSCI46756.2018.00082
29. Oltean, M.: Fruits 360 dataset
30. Liu, J., Zhao, M., Guo, X.: A fruit detection algorithm based on R-FCN in natural scene . In: Chinese Control and Decision Conference (CCDC) (2020)
31. Lin, T.-Y., et al.: Microsoft COCO: Common Objects in Context
32. Liu, H., Yu, Y., Sun, F., Gu, J.: Visual-tactile fusion for object recognition. IEEE Trans. Autom. Sci. Eng. **14**, 996–1008 (2017). https://doi.org/10.1109/TASE.2016.2549552
33. Dong, C.Z., Celik, O., Catbas, F.N., Obrien, E., Taylor, S.: A robust vision-based method for displacement measurement under adverse environmental factors using spatio-temporal context learning and Taylor approximation. Sensors (Switzerland) **19** (2019). https://doi.org/10.3390/s19143197
34. Zhou, H., Guo, J., Wang, Y., Zhao, M.: A feature selection approach based on interclass and intraclass relative contributions of terms. Comput. Intell. Neurosci. **2016** (2016). https://doi.org/10.1155/2016/1715780
35. Bhargava, A., Bansal, A.: Fruits and vegetables quality evaluation using computer vision: a review (2021). https://doi.org/10.1016/j.jksuci.2018.06.002

Digital Twin in Industry 4.0 A Real-Time Virtual Replica of Objects Improves Digital Health Monitoring System

Prabhanjan Chaudhari(✉), Chaitali Gangane, and Akshay Lahe

Saraswati College, Shegaon, India
prabhanjan1111@gmail.com

Abstract. Digital twin is the most popular notion in Industry 4.0 which assists to improve the performance by the deployment of a real-time virtual replica of objects. Digital twin will detect the issues more accurately and predict the outcomes to improve the result and decision support system. Now near all the hospitals and clinical pharmacies expanding the use of digital twin for the well-being of patients and the effects of drugs on patients' health. In healthcare, the digital twin acts as a lifelong rich data record of human health combined with Artificial intelligence and big data analysis models that will catechize the information to find treatment methods to various clinical questionnaires. Digital twin provides a deep understanding of a patient's health like what is the patient's medical condition and history? How is that responding to drugs? How does a patient reply to medical therapy? At the same time, it is very easy to provide the decision support system to doctor about the therapy which will help him to diagnose the disease. In this paper we are trying to elaborate the use of Digital Twin in medical sector industries based on IoT and Artificial Intelligence. Also, here we want to do the propaganda of Digital Twin enabling technologies and scope of open research for healthcare.

Keywords: Digital twin. Artificial intelligence · Internet of Things (IoT) · Big data analysis · Healthcare · Industrial Internet of Things (IIoT) · Precision modeling · Computational modeling

1 Introduction

The concept of a digital twin isn't new. With the help of support from enhaced data analytics and Internet of things (IoT), Digital Twin is mostly implemented concept in the current industries which can optimize the performance of businesses by developing and deploying real-time virtual replicas of physical objects and detecting issues and predict solutions more accurately which helps to build better products. Digital twin is not only used in Industry 4.0 but now its use is widely accepted in the Healthcare industry too as a powerful digital tool. Also, use of SDN and IoMT, term together called SD-IoMT, improves IoT system in respect of the network management and security capabilities [14].

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 506–517, 2023.
https://doi.org/10.1007/978-3-031-13150-9_41

2 Definitions of Digital Twin

There are various definitions available for Digital Twin but these definitions are having some misconceptions. This paper will clear these definitions properly by maintaining a close watch on different misconceptions which have identified Digital Twins wrongly.

The idea of digital twin was proposed around the 2000s formally for the manufacturing sector [1] spoken as digital replicas of physical objects. The National Aeronautical Space Administration (NASA) used Digital Twin technology for astronautics and aerospace. It had been utilized by NASA and they released their research in 2012 which describes Digital Twin as Virtual Factory Replicas to achieve manufacturing excellence. This has set a new benchmark for defining Digital Twins.

Digital twins can also be explained as essential link between real object and digital version of that object which is using data from multitude of sensors continuously. Data is coming from various sensors which are on physical objects in real world and this data is mapped to a certain representation of virtual objects.

(a) According to NASA, It is nothing but a simulation which is integrated on Multiphysics & multiscale level of the as-built systems which perfectly utilizes available data from sensors, physical models, fleet history, etc. to replicate lifetime of its real twin"[2] .
(b) As Digital twin adapts continuously to operational changes, it can be considered as de facto living model of physical system which can support huge knowledge and data collected online and can predict long run of physical counterpart [3].
(c) Digital representation of physical assets/assembly of integrated simulation is said to be digital twin which can repair data. This digital representation have data information collected from various sources among the merchandise life cycle which is updated continuously. It can be visualized using tools and can predict present as well as future conditions in operational and design environments which helps in stronger decision making [4].
(d) El Saddik has defined Digital Twins as "Digital replications of living further as non-living entities that enable data to be seamlessly transmitted between the physical and virtual worlds." Digital Twins can be further used for observing, understanding and optimizing various methods of all physical objects and also for providing continuous feedback to humans which can be used to increase quality of human life and its well-being [5].

3 Defining Digital Twin in Healthcare

Digital twin act as a digital representation for the physical objects or services in the healthcare sector which provides monitoring and evolution with very less close contact with the patients. In addition to that, this can give a security-aware testing environment which tests various impacts on system in the view of changes.

Health record of patient which has patient's private health data of his lifetime can be used with latest technologies of AI, IoT and big data models which can in turn give answers to various clinical and medical questions by analyzing the data. This can be achieved through digital twin. In Healthcare domain, Digital twin can provide improvements in many sections and strengthen pre-planning operations. Certain medical risks can be reduced and accurate therapy can be formed based on patient's historical data. Clinical environment workflow can be improved by the use of Digital twin technology which can pinpoint inefficiencies and make suggestions on what modifications to make to overcome those inefficiencies like decreasing waiting time of patient and developing strategical methods of testing tools for effective use.

Digital twin can be referred as virtual representation of a physical entity such as a patient, anatomical structure, or hospital environment. Problems can be predicted as if and when they have occurred with the time to implement necessary changes by changing the reality with system dynamics with the machine, process, or living body. This will give a refined solution by reducing the risk which is also important in healthcare. Smart machines can help humans to accurately predict things, collecting and communicating data. This will help to identify any inefficiencies and problems quickly which in turn reduce time required, money spend, and lives can be saved. Digital twin plays an active role in both Hospital design and Patient Care Units.

The following Fig. 1 shows the application of virtual human organs developed by Siemens healthineers for disease detection and therapy.

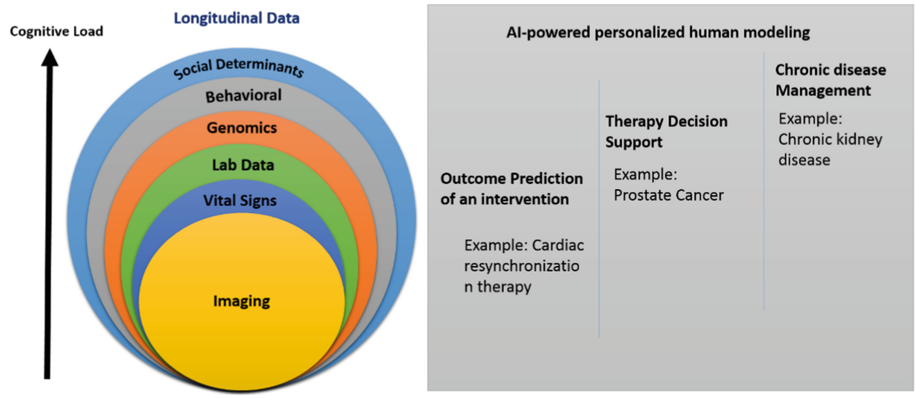


Fig. 1. Digital twin defined by siemens healthiness

4 A Brief History of Digital Twin

The basic core concept of digital twin remains constant even if the terminology of it has been changing overtime. The idea is based on the concept that an entity can be created on its own from digital information construct of a physical object or system and this information is known as "TWIN" of actual physical system itself which contains real information and which is connected to that physical system through its entire lifeline.

The concept of digital twin emerged in 2002 among industries after the presentation of the University of Michigan for the formation of the Product Lifecycle Management

(PLM) center. Figure 2 given below depicts the conceptual ideal of PLM represented by Dr. Michael Grieves which describes all components of Digital Twin which includes Real space, Virtual space and connection link which carries data from real space to virtual one and Information from virtual to real space. Multiple virtual sub-spaces are shown in the figure [6].

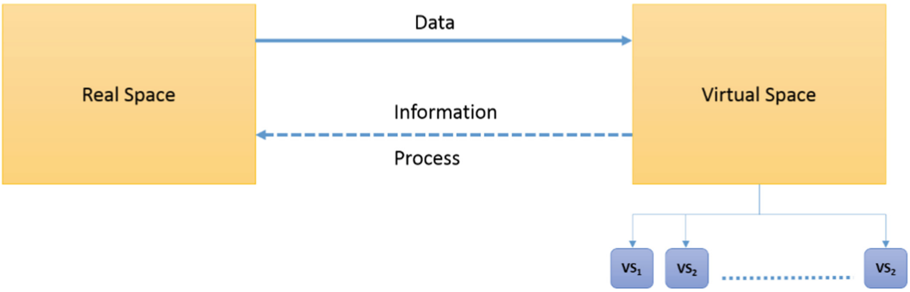


Fig. 2. Conceptual ideal for PLM

This concept was later extended perfectly in virtual sense in driving Innovative and Learn Products through PLM (Grieves 2011). In this the concept is still referred to as Information Mirroring Model [6].

The Digital Twin was adopted as the basis for astronautics and aerospace domains. While NASA was using the technology for building roadmaps and drafting various proposals for space exploration programs, this concept was put forth for next-gen fighter aircraft operations as well as for vehicles used by NASA with various challenges and implementation strategies of as-builts [7].

Where NASA needs to make two identical spacecraft. The aircraft left on earth is named a twin and is employed to reflect the status/condition of the spacecraft in action. During the flight preparation, the spacecraft referred to as the twins are widely utilized in training. During the mission, the twins were wont to simulate the space model on the bottom, and it can accurately reflect and predict the status of the spacecraft in operation the maximum amount possible, to assist the astronauts in orbit to form the foremost correct decision in emergencies (Fig. 3).

From this concept, the manufacturing industry started the use of digital twin to replicate the physical assets to make the footprint of products with the help of IoT, IIOT, and AI. Then the digital thread concept comes into account with digital twin which delivers correct information to right place at correct time [8]. The concept of digital thread is used in digital manufacturing and cyber-physical systems which is pivoting point in Industry 4.0 and intelligent manufacturing [9].

Digital twin's concept can be extended to various technologies and that is why likely to disrupt many industry sectors along with manufacturing. This will help in improved, optimized functions of physical entities by providing seamless data transmission of data between virtual and physical world. Then the evolution of digital twins came towards healthcare and well-being with smart digital technologies such as IoT, sensors, AI, ML with interrogating the patient's healthcare.

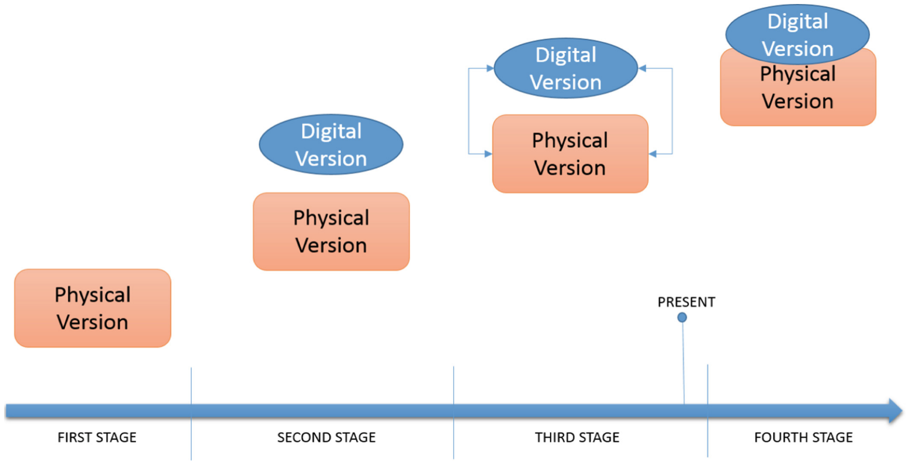


Fig. 3. Stages in digital twin

When digital twins combined with AI algorithms, it can be used to make intelligent predictions and smart decisions making. Various applications in healthcare domain do not include the physical appearance of patients but are treated as ongoing treatment and it is a key role of such systems (Fig. 4).

5 Working of Digital Twin

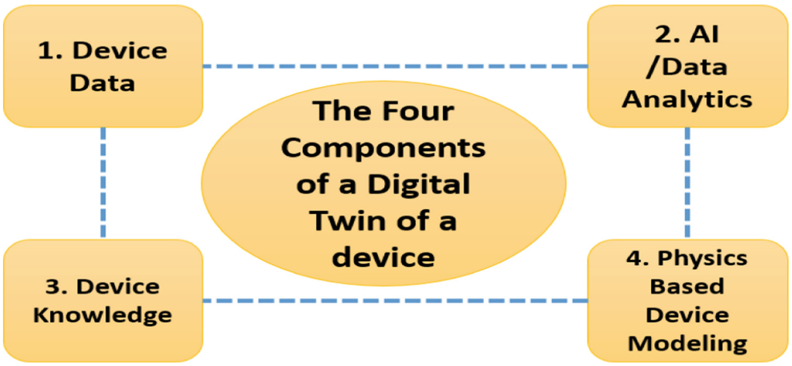


Fig. 4. Four components of digital twin

Sometimes, a digital twin is considered as a computer virus that makes use of real world information to make simulations which will give predictions on how a process will perform in future. In such scenarios, it can integrate various technologies like web of things, IIoT 4.0, AI, etc. and analytical tools which reinforces the output. To increase service efficiency ERP-IoT traffic flow entries on network devices called scheduler can be used [13].

Due to emergence of machine learning techniques and other advanced technologies like big data handling tools, virtual space models has become like a glue which can combine various tools and improve performance. In brief, it can be said that the concept drives the improvement in strategic technology then provide failure preventions in physical objects and implements monitoring then predicts future and test processes/services.

The developers who created digital twins made sure that feedback from various sensors which gather data from real world should be received by virtual computer model so that it will be easy to monitor what is happening in real-time in turn giving opportunities to collect insights and foresights into the problem which will help to improve performance. A digital twin can be often as complex or as simple as the application need depending on amounts of information and knowledge which determines how model will simulates (Fig. 5).

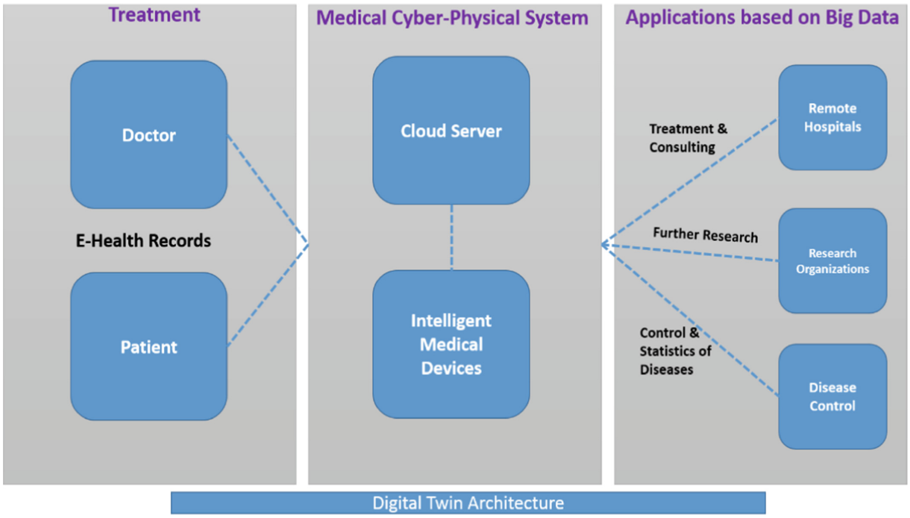


Fig. 5. Digital twin architecture

While digital twin creation of a physical system, it first collects and optimizes data from variety of data sources which includes multiple domains like physical, manufacturing, analytical datasets, operational data and data from sensors.

Various types of sensors and wearable are being used which can be helpful in conveying various aspects of its operating condition to human experts like doctors who has their domain knowledge and can make decisions and deduce conclusions about certain therapy on particular patients. A digital twin takes the past data from machines to implement its digital model. Then Analytical tools are used on the implemented model such as environmental conditions or analytics required for interactions with other devices to detect issues and the life cycle of the real twin. The twin then determines the actual body response of the patient towards the drugs given and helps in optimizing the long-term monitoring and decision support system by analyzing the conditions of human organs. The digital twin updates itself with the new interactive data collected from real-time status and working conditions or location with the help of technological support from fields such as IoT, Machine Learning, AI and Analytical tools with spatial network graphs which gathers entire relevant data and mapping it onto virtual-physical model. Various analytical models can be applied to this to obtain performance characteristics of physical assets.

The Fig. 6 shows Clinical environment workflow with completely equipped digital twin model combined with individual representation as well as population representation which can efficiently make decisions in clinical environment [10].

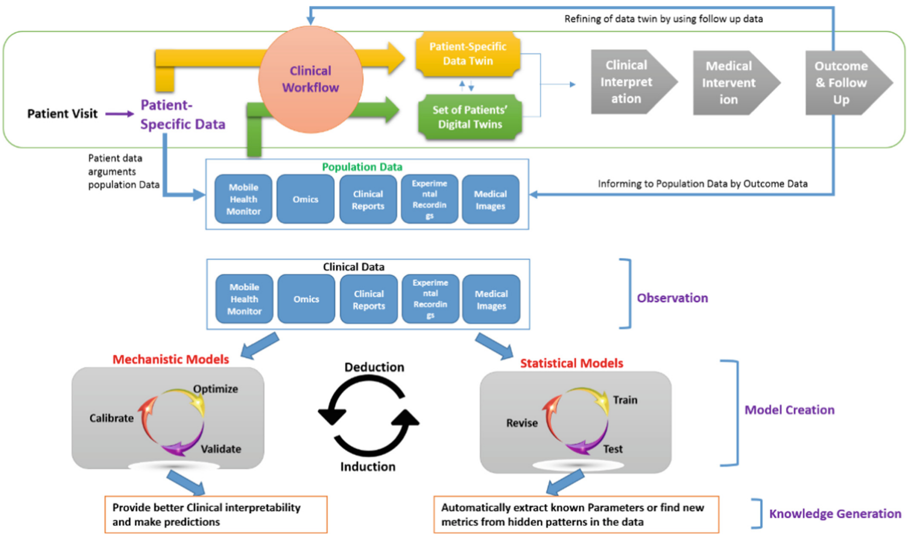


Fig. 6. Developed digital twin with clinical workflow

Data collected from previous patients and their study i.e. historical data of clinic can be categorized as population data. When we create mechanistic model to validate, calibrate and optimize population data or create statistical models to train, test and revive population data, we also create a digital twin which is based on population data. Current patient data with the help of these models are analyzed and integrated into it which gives patient's digital twin (Yellow). Now the interaction of these digital twins provide us with important insight which can be used in risk assessment, optimization, predictions, decision makings, etc. Then these insights and foresights are gets clinically analyzed and interpreted with the help of historically traditional data, the results will help in the process of decision making and therapy process of the patient. The results of this can be populated to entire data and to refine the follow up data [10].

The twin is suggested to be used with certain prototype which can give feedback about the patients' health or can even act as a prototype to give decision support by analyzing the patients' health with the help of sensors and AI support.

6 Applications of Digital Twin

7

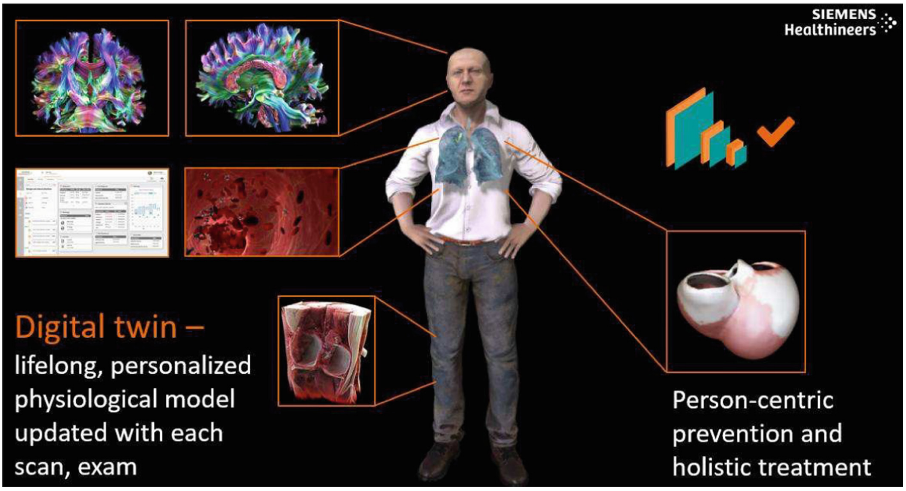


Fig. 7. Digital Twin defined for human organs by siemens healthineers

The real world application of digital twin implementation is depicted in above Fig. 7 for the human cardiology defined by Siemens healthineers using AI. It assists medical experts in devising much more accurate diagnosis of effect of medicines on the body of the patients. This technology can also be used for predicting decisions by calculating risks in epidemiology data which can track down typical infection (Fig. 8).

Digital twin will shift the current treatment selection decision based on the patient's state to an optimized state of patients tomorrow [10] and it would be a key part of the P4- Medicine – predictive, preventive, personalized, and participative. Digital twin will be an essential piece to move from one treatment that fits all to personalized medicine.

A. **Diagnosis and treatment decision support with software as a medical device:**
The patient's digital twin is accessed from different health record resources like imaging records, in-person measurement, laboratory results and genetics which assist during diagnosis. The patient model will define status of the patient's health which is captured from clinical history and parameters that are missing will be defined with statistical models [10].

B. **Patient monitoring with wearables:**
Small and more comfortable wearable sensors will be used to collect real-time data to digital twin clouds. With an understanding of disease progression and data collected from wearables like biometric, behavioral, emotional, cognitive, psychological we can build the model that detects the symptoms at an early stage which will help the doctors to diagnose the cure before getting ill and doctors be able to detect the effect of treatment on patient's health. There are many resources of data

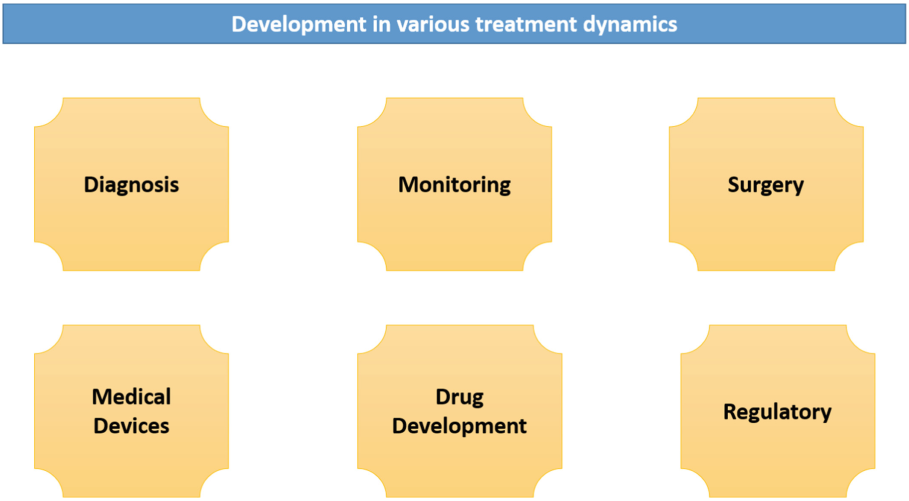


Fig. 8. Development in various treatment dynamics.

that can feed our digital twin to minimize the risk factor like medical records, lab test reports, pharmacy data and disease management [11].

C. **Drug development and dosage optimization- in silico clinical trials:**

We can conclude among huge number of drugs as which drug is best with the use of digital twin and which is best suitable for certain case. After creating a digital representation of real patients with different phenotypes that share some common symptoms, we can test new potential drugs and conclude which one has more success rate among them. Improving the first shoot will reduce the number of clinical trials necessary. In silico clinical trial will shed light on processes that take years to be observed in vivo or assess the risk of rare cases where a randomized clinical study would need thousands of patients to observe just a few of such cases [12].

D. **Regulatory decision making:**

Since 2016, both US and European parliaments have started to include modeling and simulation of evidence in the regulatory process of biomedical products [12]. In fact, FDA has committed to transform digital evidence into a valuable regulatory kit as it is beneficial while saving cost required at the time of medical devices evaluation. With this, some of the companies have started demonstrating the safety and effectiveness of medical devices and pharmaceutical products [12].

7 Advantages of Digital Twin in Healthcare

With modern world technologies like AI, IoT, Big Data, it is observed that there is huge disruption in various digital trends in all emerging sectors. Digital twin completely grasps the real world- changing condition and analyzes how to respond to these changes so as to improve functionality of operations and applying modifications. The twin technologies have presently been accepted in various domains like smart cities, automotive, retails, sales, oil & gas, Aerospace and Healthcare.

The effects are at a high extent in these given areas. Especially in healthcare, where data from IoT, digital twin technology is going to play an essential role in reforming the health and medical sector.

i. **Patient Monitoring:**

Healthy person may ignore the little symptoms but the digital twin keeps the track of the person's health records, cross-checks it against patterns and trends of previous encounters and analyzes if there is any signs of a particular disease. After complete analysis of a particular patient's data health record and using virtualization to represent it, it can reveal new information or standards for being healthy.

By the use of adaptive and diagnostic analytical methods and tools, Virtual patient data can give more accurate results along with updated data collection. With use of various modern technologies and tools along with digital twin, we can help many doctors in remote monitoring of patient with better access to healthcare services and giving assurance to their life and family.

ii. **Cost saving:**

There is significant cost saving in a hospital environment after we implement digital twin technology to help doctors diagnose a disease which also reduces patient's health risks. Initial cost of implementation of the technology and tools is high but as it serves patient better and saves cost in long run along with huge growth to hospitals, it is being implemented. This will help the organization in managing their workforce and inventories more effectively. Predicting emergencies like cardiopulmonary and respiratory arrest can be done with the help of digital twin in turn support hospitals with better service and healthcare costs.

iii. **Personalized Healthcare:**

We can have virtual twin of a hospital which will give admin and healthcare experts robust and real-time analysis of incoming and outgoing of patients by assigning them a proper schedules and managing their appointments. It can monitor exact amount of consumption of resources and do automatic maintenance and inventory management. With the assistant of digital twin, the doctors can take care of individual cases more effectively which results in better output. The "digital heart twin" developed by Siemens Healthcare Company using AI, assists the healthcare experts in making much more accurate predictions of how the medicine affects the patient's body. This technology can be used to predict risk factor which can be found after analyzing the data to track any particular infection.

iv. **Therapy Decision Support:**

The digital twin can assist doctors to determine correct therapy for particular patients. For example, prostate cancer treatment can have multiple options lined up from surgery to radiation therapy to less invasive therapy like hormone therapy. A digital twin will refer to all patients' medical history, lab results and genetic data combined with a prostate cancer model to ensure optimal decision making regarding patient treatment.

Conclusion

The concept of digital twin is an emerging technology which is having its applications in various sectors like manufacturing, construction, smart cities and healthcare. There are so many applications of digital twin in manufacturing but this concept still needs research in the field of healthcare. This paper defined the application of digital twin in healthcare with the support of AI, Big data analysis, IoT for accessing the data of patients from historical medical records. Digital twin provides the comparison between health and disease and gives the sharp idea about therapy versus enhancement and it will provide physical well- being parameters that would refer. Digital twin also has the potential to impact a person's identity based on the patterns in data. It can simulate what is happening inside real patient body and make it easier to collect foresight and predict occurrence of diseases after analyzing historical data of the patient and current situation such as location, time, activity and daily life routine. Using smart algorithms, we could deduce the real twin's pattern of stressful situations, emotional changes and send feedback to reduce anger, sadness based on the performance of favorite activities the real twin performs.

Future Scope

The proposed concepts can be extended in various sectors of healthcare with recent healthcare information systems and digital health records which is being widely used. Healthcare data being very sensitive, the security and privacy aspects of method's use can be researched further in healthcare domain as it is very important to monitor health issues. It will be very interesting and for the welfare of society to find out the implementation of Digital Twin to measure the Happiness factors of a particular group of persons and suggest the factors to improve the Happiness level of society and it will be the future of IoT.

References

1. Grieves, M.: Digital twin: manufacturing excellence through virtual factory replication. White Paper, NASA (2014)
2. Glaessgen, E., Stargel, D.: The digital twin paradigm for future NASA and U.S. Air Force Vehicles. In: 53rd AIAA Structures, Structural Dynamics and Materials Conference. American Institute of Aeronautics and Astronautics, Honolulu, Hawaii (Apr 2012)
3. Liu, Z., Meyendorf, N., Mrad, N.: The role of data fusion in predictive maintenance using digital twin. In: Annual Review of Progress in Quantitative Nondestructive Evaluation, Provo, Utah, USA, pp. 020023 (2018)
4. Vrabic, R., Erkoyuncu, J.A., Butala, P., Roy, R.: Digital twins: Understanding the added value of integrated models for through-life engineering services. Procedia Manufacturing **16**, 139–146 (2018)
5. El Saddik, A.: Digital twins: the convergence of multimedia technologies. IEEE Multimedia **25**(2), 87–92 (2018)
6. Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems (Excerpt) by Dr. Michael Grieves and John Vickers
7. Tuegel, E.J., Ingraffea, A.R., Eason, T.G., Spottswood, S.M.: Reengineering aircraft structural life prediction using a digital twin. Int. J. Aerosp. Eng. **2011**, 1–14 (2011). https://doi.org/10.1155/2011/154798

8. Leiva, C.: What is the digital thread?. [online] Available: https://www.ibaset.com/blog/what-is-the-digital-thread/ (Oct 2018)
9. Vachálek, J., Bartalský, L., Rovny, O., Šišmišová, D., Morhč, M., Lokšík, M.: The digital twin of an industrial production line within the industry 4.0 concept. Proc. PC, pp. 258–262 (2017)
10. Corral-Acero, J., et al.: The 'Digital Twin' to enable the vision of precision cardiology. Eur. Heart J. **41**(48), 4556–4564 (2020). https://doi.org/10.1093/eurheartj/ehaa159
11. Schwartz, S.M., Wildenhaus, K., Bucher, A., Byrd, B.: Digital twins and the emerging science of self: implications for digital health experience design and "Small" data. Front. Comput. Sci. (2020)
12. Pappalardo, F., Russo, G., Tshinanu, F.M., Viceconti, M.: In silico clinical trials: concepts and early adoptions. Brief. Bioinform. **20**(5), 1699–1708 (2019). https://doi.org/10.1093/bib/bby043
13. Sahoo, K.S., et al.: Demand–supply-based economic model for resource provisioning in industrial IoT traffic. IEEE Internet Things J. **9**(13), 10529–10538 (2022). https://doi.org/10.1109/JIOT.2021.3122255
14. Sahoo, K.S., Puthal, D.: SDN-assisted DDoS defense framework for the Internet of multimedia things. ACM Trans. Multimedia Comput. Commun. Appl. **16**(3s), 1–18 (2021). https://doi.org/10.1145/3394956

Cyber Security Intruder Detection Using Deep Learning Approach

Tariqul Islam, Md. Mosfikur Rahman(✉), Md. Ismail Jabiullah, and Mohd. Saifuzzaman(✉)

Daffodil International University, Dhaka, Bangladesh
{tariqul15-2250,drismail.cse,saifuzzaman.cse}@diu.edu.bd

Abstract. Intrusion detection systems (IDS) are among the most promising approaches for securing data and networks; through the years, numerous categorization algorithms have been utilized in IDS. In recent years, as the alarming increase in computer connectivity and the substantial number of applications associated with computer technology have increased, the challenge of cyber security is constantly rising. A proper system of protection for numerous cyber-attacks is also required. This is how incoherence and attacks in a computer network are detected and IDS developed, which could play a possible role in cyber security. The authors used the CICIDS2017 dataset to meet this objective. It is the 2017 set of the Canadian Cyber Security Institute. The authors propose an IDS based on the deep learning technique to increase safety. The purpose was to use a neural network classifier to predict the network and web attacks.

Keywords: Cyber security · Artificial intelligence · Deep learning · Cyberattack · Intrusion detection system

1 Introduction

The number of applications that stream services to their consumers has expanded dramatically in recent years. Because the apps run on the service provider's cloud servers rather than the local terminal, this service requires the user terminal's minimum installation and computational resources [1]. Many organizations have begun to establish their streaming services, seeing the clear benefit of delivering better service to clients who have no high-end equipment access. "On the other side, the large network-level interchange of data cloud servers to local users raises the assault area. Anonymous may apply several tactics, such as DDoS, port scan, and penetration to steal crucial data and render services unavailable to users" [1]. A significant issue that has to be addressed in order to avoid these invasions is the creation of reliable and effective IDS for cyber security. Systems of intrusion detection are ancient ideas; P. Anderson characterized an IDS as a program that explores informs management for suspicious activity or system regulatory breaches [2]. Intrusion detection systems most traditionally rely on the attack signature database of experts to operate in conjunction with the predetermined software judgment criteria for intrusion detection [3]. The author argued that it's simple to design and Understand

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 518–530, 2023.
https://doi.org/10.1007/978-3-031-13150-9_42

IDS-based signature if unusual target behavior is known to be network performance. However, cyber-attacks have gotten increasingly corrupted in recent years, particularly assaults on systems that store or manipulate sensitive information [4]. Without frequent updates, the expertly built attack database will rapidly become obsolete. Another key problem with intrusion detection systems based on signatures is that these systems are not wide enough to recognize new attacks with signatures in the signatory database. Briefly, large overhead storage for the attack signature database comprises signatures of all known attacks that make it hard to build or distribute. Furthermore, It may be computationally costly to compare incoming data flow with fingerprints in the data collection. "The Architecture of ANN is typical to predict and classify. ANN has various characteristics which make it particularly effective for network intrusion detection" [5]. For starters, ANN excels with a great variety of input properties in non-linear modeling data, for instance, network packets. Secondly, the future propagation of the ANN or forecasts is quick once trained. If the IDS model is aligned with network traffic, this is crucial to network performance. ANN is trained to provide an overall solution to one job using a vast dataset. Traditional intrusion-detection systems based on signatures, on the other hand, identify intrusions using manually set and comprehensible criteria. The ANN technology is strongly mathematical by using a stochastic gradient descent strategy to convey the mistake [6, 7]. ANN's training phase, no predetermined rules are necessary. This means that developers do not need to be cyber security professionals to train ANN-based intrusion detection systems. Moreover, as ANN-based IDS decision-making algorithms are generalized by all known attacks, upcoming attacks with comparable characteristics can be recognized in relation to existing attacks. On the other hand, they will miss creative assaults due to a lack of information about their distinctive signatures. "This article presents an IDS based on the Convolutional Neural Network architecture. Unlike other previously recommended CNN IDS which focus on a class or a subset of classes" [8–10], it is good to identify unique and well-known methods of attack on the dataset in multiclass classification. Moreover, compared with the advanced, multiclass-based CNN IDS like that of Potluri for classifying the dataset of UNSW-NB15 [11].

2 Review Works

In [12] categorized several IDS models according to approaches for detection. The IDS uses statistically driven ways to construct a distribution model for innocuous traffic and recognizes low likelihood events of possible attacks. On the other side, a knowledge base is developed which reflects the large traffic profile used by knowledge-based approaches. Each activity that differs from the conventional form is therefore designated as an invasion. Finally, machine-learning algorithms are used for intrusion detection systems. These employ huge quantities of data to model some components of any kind of attack and then to categorize traffic according to the knowledgeable characteristics. "A data collection survey is also available for intrusion detection systems. Some of the public data sets were explored including Knowledge Discovery Databases (KDD) Cup'99, CAIDA, Network Security Laboratory-KDD (NSLKDD), and CICIDS2017, and feature selection and kind of computer assaults were also reported in the comparative analysis of these IDS datasets. Finally, the authors provided classification findings for the selected datasets, based on their past study. Their model which mixes a neural network with a payload classifier with a Multilayer Perceptron (MLP) obtained an exactness of 95% at CICIDS2017" [1]. "Several database development techniques were offered to boost the performance of the model in the detection of current network intrusions in order to attain a useable multiclass classification accuracy. The CICIDS 2017, semi-controlled K-means method was developed by Yonghao Gu et al. for the detection of DDoS attacks" [13]. In addition, they have established a hybrid selection strategy, which did not use unlogical characteristics as input to the model, in order to prevent a 'dimensionality curse. The features accessible are added to your functional selection algorithm. Before the algorithm outputs, chosen characteristics are handled, including data normalization, ranking, and feature finding. Finally, the feature selection technique achieved a rate of detection is 96.50% and 30.5% false positive rate. Deep learning practices like neuronal networks, due to their potential to generalize more sophisticated task data patterns, have become more successful solutions for categorization problems in recent years. The authors of [14] "examined anomaly analyzes of the intrusion detection by means of K-Nearest Neighbors and Deep Neural Network (KNN) and the Deep Neural Network (DNN). CICIDS2017 was utilized as the database for model performance simulations in the study. They concluded that DNN was significantly higher than close neighbors. Their DNN, for the instance, is 96,427% accurate, which is considerably more than 90,913% for the closest neighbors. In addition, the overall calculation time of the two models was investigated." "The 110(s) CPU time of the DNN is below 130(s), which shows that it has a shorter overhead time than nearest k neighbors. DNN's overhead time is below that of 130(s). The study on deep learning models for cyber security within IoT (IoT) networks is being continued by Monika Roopak, Gui Yun Tian, and Jonathon Chambers" [8]. "A hybrid LSTM and CNN model employing DDoS samples from the 2017 CICIDS evaluates the performance of MLP, Long Short term Memory (LSTM), CNN. The model LSTM reached 98.44% accuracy, followed by the 98.14% precision CNN and the 97.41% precise hybrid model. The MLP model finally reached a precision of 88.47% in its simulation. The authors also compared the results to various approaches to machine learning. After a simulation, all the deep learning models assessed, with the exception of MLP, have outperformed machine learning models like SVM, Bavaria, and Random Forest. In order to evaluate the performance of Naive Bayes, SVM, and C NN-based classifier have used the CICIDS2017 dataset" [9]. The study focused on the binary classification performance of the model in the dataset for each attack class. The raw data set for the CICIDS2017 was utilized to train the models which include various network activity subdatasets all day long. Each sub-data set comprised mainly of just 13 attack categories and was trained and tested by the authors. The CNN-based IDS proposed in [10]. The authors are using deep learning approaches to construct a 2018 CICIDS dataset CNN model that contained but had a higher sample size with the same characteristics as 2017 CICIDS. The study models have been trained and evaluated using CICIDS2018 sub-datasets covering a sub-set of network traffic categories. Consequently, the models were simulated instead of all at once for a multiclass classification for some classes in the data set. Another deep learning model, which is common when time series of data are employed as input, is that of CNN-basic IDS that can be bigger than the recurring neural network. The proposed CDN model has obtained 96.77% accuracy of the CICIDS

2018 sub-dataset in the benign and DoS samples. In this research, however, the RNN model tested attained an accuracy of 82.84% in the same dataset, which was far lower than the CNN model. A new hierarchical IDS based on Decision Tree and rules based models was introduced in this study [15]. CICIDS2017 was also used as a data set to examine the performance of the model. The proposed model combines the first stage Reduced Error Pruning Tree (REP Tree) and JRip. In order to classify traffic as malicious or benign, the input properties of the data set are used as input. In order to get the final classification result, a Forest PA classifier then uses the output of the two classifiers in the first stage, coupled with input features of the initial data set [16]. Their concept has been successful in virtually every traffic class at CICIDS2017. They also tested the performance of their recommended model with 11 renowned classifications to demonstrate its classification capability. They had the lowest false alarm rate on benign road traffic, overtaking the other 12 classification models in 7 assault categories. Due to its good overall classification performance, this model is competitive in CICIDS2017. Therefore, for the evaluation of the proposed model performance, in the findings component of this survey, the recommended IDS model was compared to its unique hierarchical IDS. Traffic records may be retrieved rapidly and network problems can be detected utilizing technology. Traditional network analysis, IDS and malicious activities have limited recognition and reaction capability in dynamic and long-term series [17]. Canadian researchers offer an IDS for the detection of intrusion in the network based on the Convolutions Neural Network. Nine other known classifiers were compared to the proposed model [1]. Botnets are one of the most severe cyber security concerns every day for organizations. This article constitutes a detailed evaluation that thoroughly explores the botnet problem. It describes all possible techniques of detecting botnet [18].

3 Research Methodology

The authors are using the most recent Intrusion Detection Evaluation Dataset (CICIDS2017) [19]. This is more of a proof of the concept for the usage of FFBP neural network classifiers in IDSs than a final working product. The dataset contains network traffic data during regular traffic and execution of different attacks. The authors need standard Python ML tools such as modeling goal Pandas, Scikit learn, TensorFlow 2.0, and Keras. Pipeline Main part of the ML pipeline is the neural network classifier built with TensorFlow 2.0. Data is contained in 8 different CSV files, each having additional attack data at other times. So the first thing the authors must do is merge all the data from files into one Pandas DataFrame. They are reading all the CSV files into data, frames and putting those DFs into one list. Next, the authors show the number of rows and columns for each table. The authors already established that all tables have the same number of columns. That is why the authors loop over all given tables and compare them to all others combining all tables into one dataset. This is possible since all tables have the same columns, as the authors checked. By checking the shape of the dataset, the authors can confirm that concatenation has been successful.

3.1 Data Analysis

Some general info about the dataset. It contains roughly 2.5 million records across 79 columns. Data consists of mostly int64 and float64 types, except three attributes of the 'object' type. First of all, the authors determined the kinds of attacks they want to use in the dataset. These attack types are DoS DDoS and Port Scan. The authors created a CSV file from the dataset covering these three attack traffic and BENIGN traffic. Reading the data from the dataset file, combining DoS attacks, reducing the noise, finding NaN values, and assigning the column average, making the data type int64 and float64. The dataset contains network traffic data during different attacks, represented with values like port numbers, IP addresses, packet lengths, SYN/ACK/FIN flag counts, packet size, and others. Further examination reveals that the dataset contains 15 labels, "including BENIGN, DDoS, PortScan, Bot, Infiltration, Web Attack Brute Force, Web Attack XSS, Web Attack SQL Injection, DoS Hulk, DoS GoldenEye, Heartbleed, FTPPatator, SSHPatator, DoS Slowloris, DoS Slowhttptest, Labels represent network/web attacks and BENIGN" state which is the network traffic during a typical business day. Most records in the dataset are of DDos and DOS Hulk attacks. This might pose a problem later in model training, considering minimal data for most attacks. This information will significantly influence model selection.

3.2 Preprocessing and Data Cleaning

At this stage, from Fig. 1, the authors just clean the code containing data. The authors go through renaming columns, removing NaN and non-finite values (-inf, inf) to get the data ready for visualization and model training. Removing whitespaces in column names. Then the authors can see that the 'Label' column contains some weird characters. The following snippet uses regular expressions to replace quirky characters with Dundas. Replacing 'Label' column values with new readable values. Checking if there are any NULL values in the dataset and which column/s contain NULL values. And also how many NULL values this column contains. Next, removing all NULL values, removing rows that have NULL values. Additional attacks Check if the number of rows that have been eliminated is equal to the Null value number. Considering that only 334 rows contain NULL values in the entire dataset, which makes about 0.01%, the authors can safely remove all NULL rows without spoiling the data. Subsequent checking if all values are finite. Checking what column/s contain non-finite values and how many non-finite values each column contains. Same as before, since there is a small number of non-finite values, the authors can safely remove them from the dataset without spoiling the dataset. Replacing infinite values with NaN values. The authors can see that now the authors have Nan values again. Bringing the Labels back into the dataset before deleting Nan rows and removing new NaN values. Converting the final version of the data to CSV format, saving a cleaned dataset.

3.3 Data Visualization

By now, the authors know the dataset has 78 features and is split into 15 categories (14 attacks and 1 "normal" state). The next step is to try and visualize what the dataset

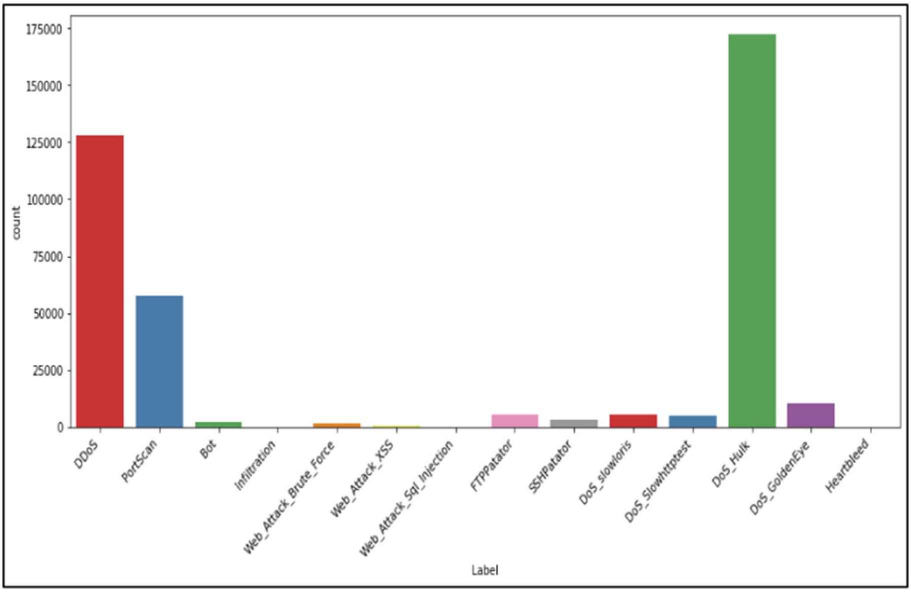


Fig. 1. Feature importance

looks like in feature space. To do this, the authors will employ the principal component analysis (PCA) to decrease dimensionality before passing the reduced dataset to t-SNE (t - Distributed Stochastic Neighbor Entities) for visual representation in 2D space. The authors are going to pick 10.000 random rows from the dataset for visualization purposes. Setting the random seed for reproducibility of results. Performing the principal component analysis. With just 19 components, the variance ratio remains 99%, which is excellent. Then just computing t-SNE. From Fig. 2, the authors can see the distribution of data in 2D space. Attacks are not spatially well separated from a normal state. Clusters of seizures can hardly be seen. Instead, they are found in the same place as the “normal state” data points. This insight leads us to conclude that the ML model will probably have some issues with this kind of data. ML models will have to be chosen with this in mind.

3.4 Data Preparation

Final data, preparation steps are taken before the authors use the data for model training and testing. The following few steps process for scaling the data into the size adequate for the ML algorithm. Splitting the dataset into features and labels. For mounting and scaling the data, the author’s RobustScaler class uses form Scikit Learn. RobustScaler is used to preserve outliers in the data. Checking if scaling has been successful. Label encoding is done when the dataset contains categorical values (ex. 0–5, A/B/C, 55+). Turn absolute values into numerical values by replacing data categories with integers starting with 0. No need to do previous operations. To convert this into numerical values, the authors will use the ‘LabelEncoder’ class from Scikit Learn. Labels have been replaced with integers.

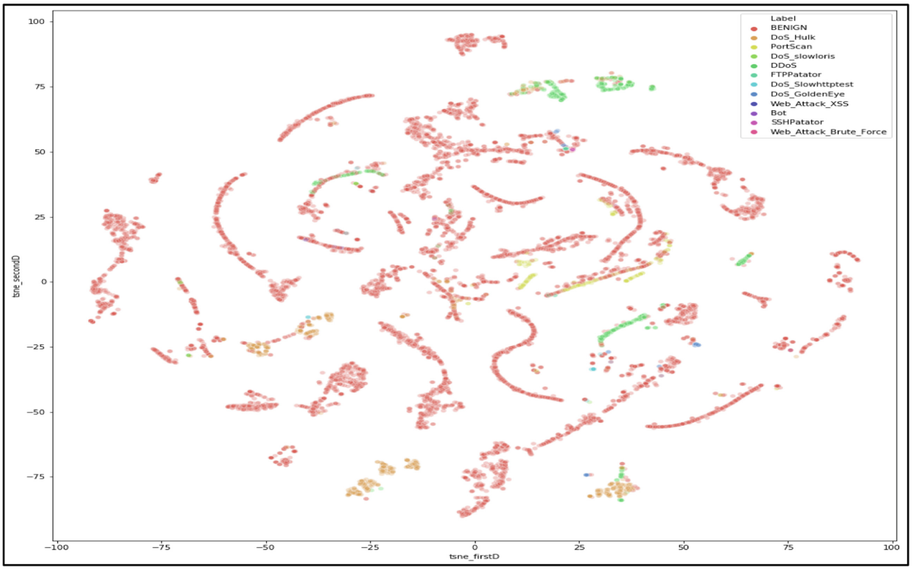


Fig. 2. Feature implementation visualization

Splitting the data into training and testing sets is the final stage in data preparation. For this, a Scikit Learn function does all the splitting for us. This step is essential so the authors can have representative data for evaluating the author's model. Both train and test samples should contain similar data variance. The next step is to split training and testing data. For this, the authors will use Scikit Learn's training test splitting function.

4 Proposed System

For completing all steps, the authors chose to use a neural network. Specifically, the multilayer perceptron, more specifically, feedforward neural network multiclass classifier with the "backpropagation algorithm". NN will be used to classify 14 different attacks and one normal state. The author's TensorFlow Sequential model consists of three layers. There are three layers: one visible, one concealed, and one output. The input layer has 78 neurons, one for each feature. The hidden layer has 67 neurons, and this number calculated by the formula [1] 2/3 the number of input neurons + several output neurons. The output layer has 15 neurons, one for each class the authors predict. For activation functions, the authors used standard procedures for multiclass classification tasks - ReLu for the hidden layer and "softmax function" for the output layer. Figure 3 shows the entire proposed system.

The authors use the Dropout parameter set to 0.2 for randomly shutting off 20% of neurons in each learning iteration. This technique is used for decreasing overfitting, thereby increasing network accuracy. For learning rate optimization, the authors used Adam optimizer. The loss function used is sparse categorical cross-entropy, which is standard for multiclass classification problems. In the next cell, the author set up training

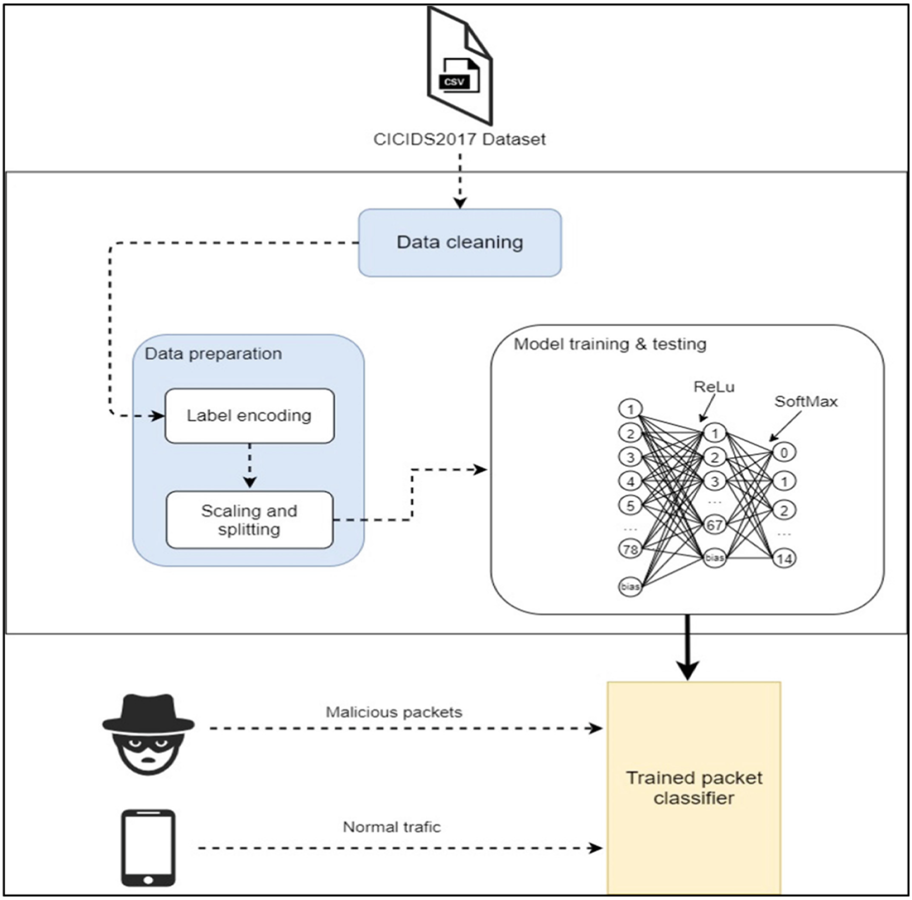


Fig. 3. Proposed system architecture

logs for the TensorBoard and some TensorBoard callbacks. TensorBoard - a callback that logs training data. EarlyStopping - a callback that monitors the ‘loss (function)’ metric, and if the loss function does not get better in the successive ten iterations, callback stops the training and restores the network with best weights up until that iteration. TF callback that sets up TensorBoard with training logs. TF callback that contains training when the best value of the validation loss function is reached. It also restores weights from the best training iteration. The authors can see that activity stopped after 18 out of 100 epochs due to the loss function metric not changing much in the previous ten epochs; after training, the authors evaluated model accuracy and found model predicts attacks with 91.2% accuracy. Apply algorithms in pairs (DoS, BENIGN), (DDoS, BENIGN) (PortScan, BENIGN); Creation of Train and Test datasets for all data frames. First, the authors created data frames by taking rows with specific Labels from the existing database. Creation and apply algorithms for the data frame with DoS and BENIGN. Accuracy is defined in the Table 1, 2 as the percent of positive observations properly predicted to total expected positive observations. The F1-Score is also the weighted Precision and Recall average. We got 99% precision and recall via Random Forest, Decision Tree, and Neural Network techniques. Finally, we attain a high F1-score and a 99% accuracy rate.

Table 1. Classification report with DoS and BENIGN

Algorithms	Precision	Recall	F1-Score	Accuracy
Random Forest	0.9993	0.9993	0.9993	0.9993
Decision Tree	0.9996	0.9996	0.9996	0.9996
Neural Network	0.9949	0.9949	0.9949	0.9949

Table 2. Confusion matrix with DoS and BENIGN

<table>
<tr><th>Algorithms</th><th colspan="2">Predict</th><th></th></tr>
<tr><td rowspan="2">Random Forest</td><td>188634</td><td>92</td><td rowspan="6">Actual</td></tr>
<tr><td>88</td><td>58301</td></tr>
<tr><td rowspan="2">Decision Tree</td><td>188662</td><td>47</td></tr>
<tr><td>60</td><td>58346</td></tr>
<tr><td rowspan="2">Neural Network</td><td>187949</td><td>483</td></tr>
<tr><td>773</td><td>57910</td></tr>
</table>

Creation and apply algorithms for data frame with DDoS and BENIGN. In the Table 3, accuracy is defined as the proportion of correctly predicted positive observations to the total expected positive observations. Furthermore, F1-Score is the weighted average of Precision and Recall. Precision for Random Forest, Decision Tree, and Neural Network algorithms is 99%, and recall is 99%. Finally, we acquire an excellent score, F1-Score, and Accuracy of 99% (Table 4).

Table 3. Classification report with DDoS and BENIGN

Algorithms	Precision	Recall	F1-Score	Accuracy
Random Forest	0.9999	0.9999	0.9999	0.9999
Decision Tree	0.9999	0.9999	0.9999	0.9999
Neural Network	0.9992	0.9992	0.9992	0.9992

Creation and apply algorithms for the data frame with PortScan and BENIGN. Accuracy is defined in this table as the percent of positive observations properly predicted to total expected positive observations. The F1-Score is also the weighted Precision and

Table 4. Confusion matrix with DDoS and BENIGN

Algorithms	Predict		
Random Forest	188719	12	Actual
	3	38395	
Decision Tree	188701	11	
	21	38396	
Neural Network	188600	53	
	122	38354	

Recall average. We got 99% precision and recall via Random Forest, Decision Tree, and Neural Network techniques. Finally, we attain a high F1-score and a 99% accuracy rate (Tables 5 and 6).

Table 5. Classification report with PortScan and BENIGN

Algorithms	Precision	Recall	F1-Score	Accuracy
Random Forest	1.0000	1.0000	1.0000	1.0000
Decision Tree	0.9999	0.9999	0.9999	0.9999
Neural Network	0.9954	0.9954	0.9954	0.9954

Table 6. Confusion matrix with PortScan and BENIGN

Algorithms	Predict		
Random Forest	188722	5	Actual
	0	27241	
Decision Tree	188715	7	
	7	27239	
Neural Network	188226	501	
	496	26745	

Creation and apply algorithms for the data frame with Normal and Abnormal. Accuracy is defined in this table as the percent of positive observations properly predicted to total expected positive observations. The F1-Score is also the weighted Precision and Recall average. We got 99% precision and recall via Random Forest, Decision Tree, and Neural Network techniques. Finally, we attain a high F1-score and a 99% accuracy rate (Tables 7 and 8).

Tagging attack traffic as abnormal and creating the data frame by labeling the BENIGN traffic as Normal. The author completed the CSVs of the datasets and designed

Table 7. Classification report with normal and abnormal

Algorithms	Precision	Recall	F1-Score	Accuracy
Random Forest	0.9995	0.9995	0.9995	0.9995
Decision Tree	0.9996	0.9996	0.9996	0.9996
Neural Network	0.9920	0.9920	0.9920	0.9920

Table 8. Confusion matrix with normal and abnormal

Algorithms	Predict		
Random Forest	123980	88	Actual
	65	188635	
Decision Tree	123984	77	
	61	188646	
Neural Network	122989	1456	
	1056	187267	

them to use in KNIME. Therefore, all accuracy is based on an understanding and standard of the purport of three algorithms in the below table (Table 9).

Table 9. Accuracy table for Random Forest, Decision Tree, K-nearest neighbors, ANN

Algorithms	Precision	Recall	F1-Score	Accuracy
Random Forest	0.9993	0.9999	1.0000	0.9995
Decision Tree	0.9996	0.9999	0.9999	0.9996
KNN	0.9949	0.9992	0.9954	0.9920
ANN	0.7636	0.8307	0.8738	0.6034

Random Forest, Decision Tree, k-nearest neighbors have the best accuracy among the tables, giving better execution. Partition of the dataset into isolated segments like the preparation dataset is 70%, and for testing, it is 30%. This work is the proposed store-up AI method for examination attack, in which the authors can discover in the tables that the proposed methodology is showing up with 99% precision. Currently, only 79 attack insurance features are available. Later on, the authors will try all features and achieve the best accuracy. Using Random Forest returns a segment importance grid that may be will not pick parts. This framework is dreary to find information that is low and continuously exact.

5 Comparative Analysis

The CICIDS2017 dataset [17] used in this research is harder for a classifier, as the dataset is more resilient and contains more attack types. This is a problem for a classifier (59% and 55% more than the UNSW-NB 15 dataset, respectively). This research article is constructed such that it contains a brief overview of some existing research into cyber security deep learning applications. In order to illustrate design decisions of the proposed model's custom training and testing data sets, the CICIDS2017 database is evaluated during the model design phase. The CNN, a profound learning model on which the suggested IDS is based, is architecture and mathematics. The proposed parameter and IDS architecture are finally provided. In order to perform validation and comparison, this model was evaluated against existing benchmarks in the simulation results section. Nevertheless, in [15] this study revealed a "new hierarchical IDS based on Decision Tree and Rules-based models. They used CICIDS2017 as a dataset to evaluate the performance of their model. The proposed model combines the first stage Reduced Error Pruning Tree (REP Tree) and JRip". In order to classify traffic as malicious or benign, the input properties of the data set are used as input. In addition, in order to get the end result of classification, a Forest PA Classifier employs the input features of the first dataset in the first step. Their concept has been successful in virtually every traffic class at CICIDS2017. Furthermore, to confirm the classification capacity of the authors, their proposal model was compared with 11 well-known classifications in this study. Their model had the lowest false alarm for benign transport, outperforming all other 12-classifier models in seven attack types. The overall performance of this model for the CICIDS2017 classification is competitive. As a consequence, the proposed IDS model was compared to their unique hierarchical IDS in the outcome phase of the research to evaluate the performance of the proposed model.

6 Conclusion and Future Work

This research aims to model a neural network classifier that can predict 14 network/web attacks and regular traffic with 91% accuracy. This model is proof of the concept that a feedforward neural network with a backpropagation algorithm can be used for classifying attacks in anomaly-based intrusion detection systems. The authors propose a couple of solutions for improving model accuracy. Feature engineering and feature selection can probably improve the accuracy of this model. Picking the features that have the most influence on the model. Regarding this model, the authors propose tuning the hyper-model parameters. Changing the hidden layer activation function, early stopping callback, dropout, optimizer, and loss function should increase accuracy to some extent. Another way, albeit more complicated and resource-intensive, to develop the optimum neural network design for this particular job, apply a genetic algorithm. Finally, the authors propose the usage of some other ML algorithms. Moreover, the following section includes an analysis of ML algorithms such as Random Forest, Decision Tree, k-nearest neighbors, and ANN state. Here Random Forest and Decision Tree give the most optimization accuracy. Random forest classifiers have been used in intrusion detection systems for a while now. Alternatively, the authors found some sources using auto encoders for detection.

References

1. Ho, S., Al Jufout, S., Dajani, K., Mozumdar, M.: A novel intrusion detection model for detecting known and innovative cyberattacks using convolutional neural networks. IEEE Open J. Comput. Soc. **2**, 14–25 (2021)
2. Anderson, J.P.: Computer security threat monitoring and surveillance. Technical Report, James P. Anderson Company (1980)
3. Lee, W., et al.: Realtime data mining-based intrusion detection. In: Proceedings DARPA Information Survivability Conference and Exposition II. DISCEX 2001, vol. 1, pp. 89–100. IEEE (June 2001)
4. Jyothsna, V.V.R.P.V., Prasad, R., Prasad, K.M.: A review of anomaly-based intrusion detection systems. Int. J. Comput. Appl. **28**(7), 26–35 (2011)
5. Ciaburro, G., Venkateswaran, B.: Neural Networks with R: Smart Models Using CNN, RNN, Deep Learning, and Artificial Intelligence Principles. Packt Publishing Ltd., UK (2017)
6. Kiefer, J., Wolfowitz, J.: Stochastic estimation of the maximum of a regression function. Ann. Math. Stat. **23**(3), 462–466 (1952)
7. Bottou, L., Curtis, F.E., Nocedal, J.: Optimization methods for large-scale machine learning. SIAM Rev. **60**(2), 223–311 (2018)
8. Roopak, M., Tian, G.Y., Chambers, J.: Deep learning models for cyber security in IoT networks. In: 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0452–0457. IEEE (January 2019)
9. Yeom, S., Kim, K.: Detail analysis on machine learning-based malicious network traffic classification (2019)
10. Kim, J., Shin, Y., Choi, E.: An intrusion detection model based on a convolutional neural network. J. Multimedia Inf. Syst. **6**(4), 165–172 (2019)
11. Moustafa, N., Slay, J.: The UNSW-NB15 data set description. Unsw. ADFA. edu. au. (2016). https://www.unsw.adfa.edu.au/unswcanberracyber/cybersecurity/ADFANB15-Datasets/. Accessed 10 May 2021
12. Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J.: Survey of intrusion detection systems: techniques, datasets, and challenges. Cyber Secur. **2**(1), 1–22 (2019)
13. Gu, Y., Li, K., Guo, Z., Wang, Y.: Semi-supervised k-means DDoS detection method using hybrid feature selection algorithm. IEEE Access **7**, 64351–64365 (2019)
14. Atefi, K., Hashim, H., Kassim, M.: Anomaly analysis for the classification purpose of the intrusion detection system with K-nearest neighbors and deep neural network. In: 2019 IEEE 7th Conference on Systems, Process and Control (ICSPC), pp. 269–274. IEEE (December 2019)
15. Ahmim, A., Maglaras, L., Ferrag, M.A., Derdour, M., Janicke, H.: A novel hierarchical intrusion detection system based on decision trees and rules-based models. In: 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), pp. 228–233. IEEE (May 2019)
16. Kingma, D.P., Ba, J.: Adam: a method for stochastic optimization. arXiv preprint arXiv:1412.6980 (2014)
17. Tian, X., et al.: IntruDTS: interactive visual analysis system for intrusion detection in time series. In: 2020 IEEE International Conference on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom). IEEE (2020)
18. Shetu, S.F., Saifuzzaman, M., Moon, N.N., Nur, F.N.: A survey of botnet in cyber security. In: 2019 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT), pp. 174–177 (2019). https://doi.org/10.1109/ICCT46177.2019.8969048
19. Intrusion Detection Evaluation Dataset. https://www.unb.ca/cic/datasets/ids-2017. Accessed 18 May 2021

Android Malware Detection Using Ensemble Feature Learning

Siddhartha Suman Rout[1(✉)], Lalit Kumar Vashishtha[1], Kakali Chatterjee[2], and Jitendra Kumar Rout[3]

[1] KIIT Deemed to be University, Bhubaneswar, Odisha, India
siddhartharout285@gmail.com, vashishthafcs@kiit.ac.in
[2] National Institute of Technology, Patna, Patna, India
kakali@nitp.ac.in
[3] National Institute of Technology, Raipur, Raipur, India
jkrout.cs@nitrr.ac.in

Abstract. The ransomware threat is no longer limited to personal computers; it is gradually growing to include smartphones. For monetary gain, the attackers target smartphone devices to steal personal information from consumers. Existing methods concentrate on collecting static or dynamic data from mobile apps and using machine learning algorithms to construct mobile malware, detection models. A significant number of static or dynamic features may be extracted. As a result, the data has a lot of different aspects. In this paper, combining six well-known classification models, we have used the ensemble learning meta-classifier for stacking using cross-validation to classify the malware. The study finds that the stacking ensemble approach performs better than any single model on average classification performance.

Keywords: Meta-classifier · Ensemble learning · Semi-supervised · Malicious · Android OS system · Static analysis · Benign application

1 Introduction

There is an issue that consumers are confronting as the number of individuals using smartphones powered by the Android operating system grows. Malware attacks on Android cell phones are becoming more common by the day. Due to this, users are experiencing numerous issues, and people must learn how to secure their phones from such intrusions. Furthermore, security software is rarely installed on any android smartphone. Even individuals who install it may have difficulty detecting malware [10]. Because of the high number of consumers and the massive amount of essential information obtained through these devices, these characteristics may make the Android platform more tempting to cyber criminals [4]. According to estimates from the AV-Test Institute, 350,000 additional malware elements get discovered daily [3]. The bulk of security flaws in the android platform are caused by third-party applications being installed. The

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 531–539, 2023.
https://doi.org/10.1007/978-3-031-13150-9_43

security of android devices has been addressed, including presentation judgments, malware findings, and investigation [13]. Detecting Android malware has recently received much attention; dynamic analysis and static analysis are the two main categories. The former refers to acquiring dynamic behavior aspects of applications while executing them in actual devices rather than in a test environment. However, discovering malicious activities is usually very time-consuming, and specific damaging actions may be lost in a narrow scope. As a result, dynamic analysis is ineffective at detecting malware across many applications [21]. At the same time, Static analysis is a method of analyzing a questionable file without running it. An initial analysis strategy includes obtaining relevant information from the suspect binary to decide how to classify or analyze it and where to focus. The static analysis flow to approach a sample of malware: (1) Identifying the file type - Target OS, architecture, and format (dll, exe).(2) Identifying the malware- Generating a hash to see if anyone else has analyzed the malware as a unique identifier. Using the hash to see if anyone else has analyzed the malware. (3) Strings- strings give the idea/glimpse of the functioning of the malware. (4) Packing Obfuscation- obfuscated packing are the techniques used to prevent detection. It helps reveal additional information.(5) PE headers- The PE header reveals much information on the malware functionality. The Android OS includes a module that authorizes the permissions requested by Android applications and grants them if no security policy violations occur. Android authorizations are divided into four levels of assurance, which are discussed in further depth in the sections that follow [13,16].

Many studies have been undertaken on detecting malware and resolving the issue with Android smartphones. The malware analysis techniques consist of static and dynamic analysis in which the malware samples applications are categorized as benign and malware [8]. Further, the static analysis is done to recognize the pattern and the signature of the application. However, the malware has bypassed the signature-based techniques, simply changing the small code without changing its semantics. The machine learning approach uses reverse engineering methods by obtaining the file containing benign and malicious files in APK format, which the Android OS uses to transfer and execute code on devices [8]. An APK contains an app's raw data, which can be examined to extract Android ransomware features. The contribution of this paper includes:

(1) An ensemble feature learning technique which uses six-different classifiers to classify the meta-classifier for cross-validation to classify the malware.
(2) The performance of the meta-classifier is evaluated using the AUC graph and AUROC curve graph. The meta-classifier accuracy results are improved in comparison to the single classifier on different data sets.

The remaining of this work is arranged as follows: The related work is discussed in Sect. 2. The classification technique is explained in Sect. 3.The results and discussion are compared in the Sect. 4 Finally, in Sect. 5 the conclusion and the future work are explored.

2 Related Work

Android application analysis can be classified as static [18], dynamic [19], and hybrid methods [7]. The main objective of dynamic analysis methods [7] is to extract real-time data from programs and use it to detect threats.

Apel et al. [5] suggested a dynamic analytic technique to improve malware sample grouping for distance measurement. Their method can produce satisfactory results. However, its lengthy evaluating time (over 2 min) can make it difficult for large-scale malware classification. Static analysis techniques [18] make use of specific data from the analyzed application, like the AndroiManifest.xml file or some special API calls. Rieck et al. [6] created an automatic malware classification method in which a classifier classifies samples using anti-virus software. In addition to the syntactic-based technique, Faruki et al. [9] created a malware detection method based on an improbable feature signature database of known malicious application. Despite their impressive results, their method may not be suitable for big data processing, and they may be unable to detect the most recent malware. With 58 features, Yerima et al. [20] used Bayesian classification to characterize App's kind. 1000 malware samples from 49 families and 1000 benign samples were included in the training set. They improved their work much more by combining the static technique and ensemble machine learning. API calls, commands, and permissions were among the 179 features collected from APPs. They used various methods to test 6863 Apps. (2925 malware and 3938 benign samples), including naive Bayes, simple logistic, and random tree. The findings of the trial revealed a detection rate of up to 97%–99%. The above papers use supervised and unsupervised methods to analyze the malware in the android data sets. So, for malware analysis, we used an ensemble approach and semi-supervised learning in this research (Tables 1 and 2).

Table 1. Supervised learning methods

Ref.	Data set	Approach/Classification algorithm	Accuracy
Elayan et al. [8]	CIC, Mal2017	GRU	98.2%
Syrris et al. [16]	Derbin	SVM BNB	0.998% 0.974%
Wang et al. [17]	Not Given	C4.5	97.89%
Hamid et al. [12]	Virus Total Malgenome	K-means	98.12% 74.7%
Frenklach et al. [11]	VTAz (Virus total)	KNN, RF	0.987%

Table 2. Unsupervised learning methods

Ref.	Data set	Approach/Classification algorithm	Accuracy
Liu et al. [14]			Increased By
	OmniDroid	SRBM	6.2%
	CIC2019		6.9%
	CIC2020		15.4%
Imtiaz et al. [13]	CIC2019	Deep AMD	93.4%
	MAL2019		
Martin et al. [15]	OmniDroid	AndroPyTool	0.897%

3 Classification Technique

This section discussed the meta-classifier used for feature learning and the data sets that are used in the experiments.

3.1 Data Set

The DefenceDroid, Drebin data sets are used in the experiment. In the Table 3 the sample size and features are discussed.

Table 3. Data sets, number of samples and its features

Data set		Features	Samples
DefenceDroid [1]	API	10,000	
	Permission	1490	5975 Bengin/6000 malware
	Recivers	593	5975 Bengin/6000 malware
	Services	855	5975 Bengin/6000 malware
Drebin [2]	Permission	215	9476 Bengin/5555 malware

3.2 Stacking

Stacking is a technique that uses a meta-classifier to merge different classification models. Instead of using the traditional stacking technique, the StackingCV-Classifier prepares the input data for the level-2 classifier using cross-validation (implemented as Stacking Classifier). In a typical stacking technique, the first-level classifiers are fitted to the same training set used to generate the inputs for the second-level classifier, which might result in overfitting. The StackingCV-Classifier, on the other hand, uses cross-validation: the data set is divided into k folds, and k-1 folds are used to fit the first-level classifier in k successive rounds; The first-level classifiers are applied to the first subset that was not utilized for model fitting in the previous iteration in each round. The generated predictions are then stacked and fed into the second-level classifier as input data. The first-level classifiers are fitted to the complete data set after the StackingCVClassifier has been trained, as seen in Fig. 1.

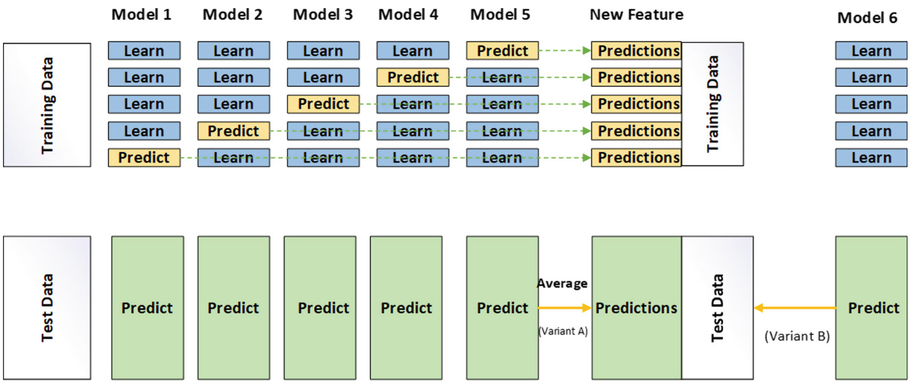


Fig. 1. Stacking ensemble learning

Predictions on the test set are made using this model. For a simple stacked ensemble, here's a step-by-step breakdown:

Algorithm 1: Ensemble learning: Stacking

Input: Data for the training $D = \{x_i, y_i\}_{i=1}^{m}$ $(x_i \ \epsilon \ \mathbb{R}^n, \ y_i \ \epsilon \ Y)$
Output: Best Optimized meta-classifier scl

```
/* Learn First Level Base-Model                                   */
```

for $t \leftarrow$ *1 to* T **do**
  $learn\, a\, base\, classifier\, h_i \ for\ the\ training\ data\ D$
end for

```
/* create a new data set from D                                   */
```

for $i \leftarrow 1$ *to* M **do**
  $Create\, the\, new\, data\, set\, that\, contain$
  $(x_i^{`}, \ y_i) \ where \ x_i \ = \ \{ \ h_1 \ (x_i), \ h_2 \ (x_i).....h_n \ (x_i) \ \}$
end for

```
/* Learn second level meta-model                                  */
```

$Model\ that\ learns\ how\ to\ combine\ the\ base\ models'\ predictions\ in\ the\ most\ effective\ way.$
return $H(x) \ = (\ h^{`}(h_1(x) \ . \ h_2(x).... \ h_T(x) \ )$

The classifiers do not make any hyperparameter optimization in this stacking approach. Random Forest, Decision Tree, CatBoost, Light Gradient Boosting

Machine, ExtraTrees, and Multilayer Perceptron are used in Level 0 to build a stacking cross-validation classifier with a meta-classifier. Only the classifier available in the scikit-learn, only the 5 most promising classifiers were taken to speed up the learning process. Ensemble learning works best when the base models are not correlated. For instance, the model can be trained in linear models, decision trees, and neural nets on different data sets or features.

4 Results and Discussion

The search for the optimum hyperparameter, In this case the search is only for meta-model but other hyperparameters can also be searched. Choosing the best hyperparameter for the 1st level model, that can fit for the predictions on a new data just like any other model.

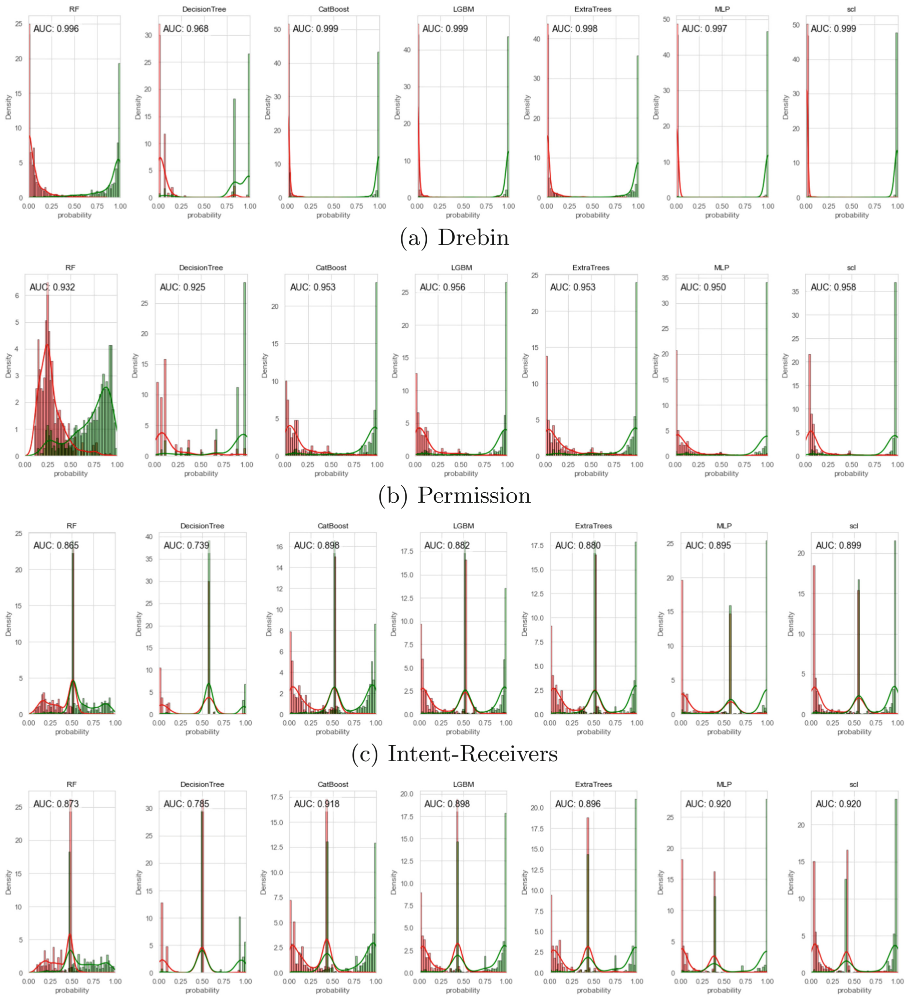
The stacking ensemble is first fitted to all available data, and then the SCL classifier function is used to create new predictions on new data. Running the search for optimum hyperparameter reports the performance of each model. This includes the performance of each base model, then the stacking ensemble.

Table 4. Optimum hyperparameters on Drebin Data set for meta-classifier

Classifier	Hyperparameter accuracy	Meta best parameter search
Random Forest	0.987 ± 0.00	$meta\_classifier\_{C}$: 0.001
Decision Tree	0.988 ± 0.00	$meta\_classifier\_{C}$: 0.01
CatBoost	0.988 ± 0.00	$meta\_classifier\_{C}$: 0.1
LGBM	0.988 ± 0.00	$meta\_classifier\_{C}$: 1
ExtraTrees	0.988 ± 0.00	$meta\_classifier\_{C}$: 10
MLP	0.988 ± 0.00	$meta\_classifier\_{C}$: 10
	Best parameters:	$meta\_classifier\_{C}$: 1
	Accuracy: 0.98794	

Table 5. Optimum hyperparameters on DefenceDroid data set for meta-classifier

Classifier	Hyperparameter accuracy	Meta best parameter search
Random Forest	0.910 ± 0.00	$meta\_classifier\_{C}$: 0.001
Decision Tree	0.911 ± 0.00	$meta\_classifier\_{C}$: 0.01
CatBoost	0.913 ± 0.00	$meta\_classifier\_{C}$: 0.1
LGBM	0.913 ± 0.00	$meta\_classifier\_{C}$: 1
ExtraTrees	0.913 ± 0.00	$meta\_classifier\_{C}$: 10
MLP	0.913 ± 0.00	$meta\_classifier\_{C}$: 10
	Best parameters	$meta\_classifier\_{C}$: 1
	Accuracy: 0.91336	



(a) Drebin

(b) Permission

(c) Intent-Receivers

(d) Intent-Services

Fig. 2. AUC results of different classifiers on DefenceDroid, Drebin data sets

The results may vary given the stochastic nature of the algorithm or evaluation procedure, or differences in numerical precision.

In this case, we can see that the stacking ensemble appears to perform better than any single model on average, achieving an accuracy of about 98.79% and 91.33% (Table 4).

Plotting a prediction distribution of AUC model (Fig. 2) will help in studying the accuracy of each single classifier. The model helps in ensemble machine learning strategy that discovers the most efficient way to combine predictions from multiple high-performing machine learning models (Table 5).

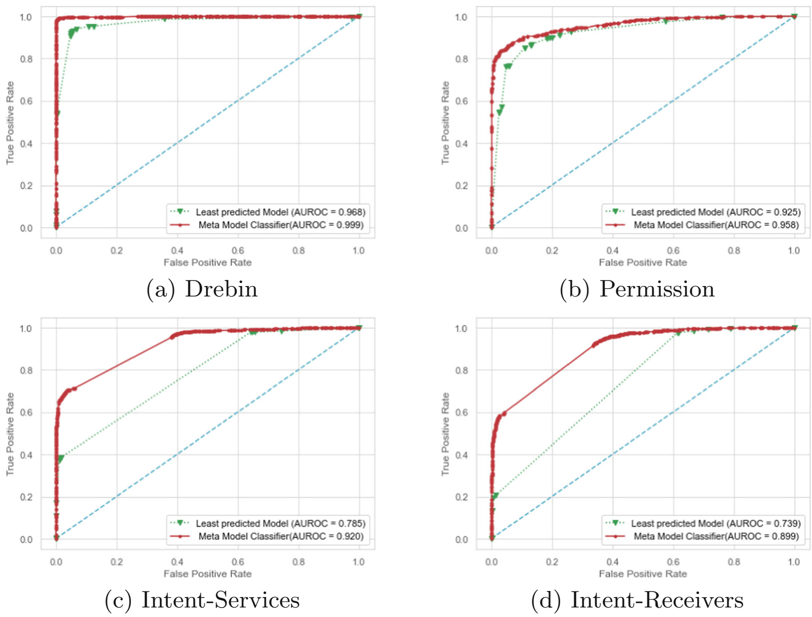


Fig. 3. AUROC score of Drebin, DefenceDroid data sets with Meta model classifier

5 Conclusion and Future Work

The study presents a ensemble feature learning method for detecting Android malware applications. It is based on Stacking, an ensemble feature-based learning technique applied in unsupervised mobile malware to reduce data dimensionality. It improves classifier performance by introducing the optimal meta-classifier concept to reduce resource usage and improve classifier performance (Fig. 3).

Before learning the features under each feature subspace, a clustering method is employed to search for a good classifier across the complete feature set, and the best meta classifier is utilized to learn the features. In the study, we find the stacking ensemble technique performs better than the single classifiers model, achieving an accuracy of about 96.72% in the case of the DefenceDroid data set, and for Drebin, it is 98.79%. The performance for some data sets is not that accurate as the more classifiers are used to predict, the more data leakage occurs. In the future, we plan to work on boosting algorithms that help meta-classifier predict more accurately and work on other ensemble approaches discussed in the literature that can help in classification performance.

References

1. Defencedroid dataset. https://github.com/DefenseDroid/DefenseDroid. Accessed 04 Sept 2021
2. Drebin dataset. https://www.sec.cs.tu-bs.de/~danarp/drebin/download.html. Accessed 16 Sept 2021

3. Malware | AV-test report. https://www.av-test.org/de/statistiken/malware/. Accessed 12 Oct 2021
4. Almin, S.B., Chatterjee, M.: A novel approach to detect android malware. Proc. Comput. Sci. **45**, 407–417 (2015)
5. Apel, M., Meier, M.: Generalizing behavioral signatures for detecting unknown malware variants and early warning. PIK-Praxis Informationsverarbeitung Kommunikation **35**(1), 17–24 (2012)
6. Arp, D., Spreitzenbarth, M., Hubner, M., Gascon, H., Rieck, K., Siemens, C.: DREBIN: effective and explainable detection of android malware in your pocket. In: NDSS, vol. 14, pp. 23–26 (2014)
7. D'Angelo, G., Ficco, M., Palmieri, F.: Malware detection in mobile environments based on autoencoders and API-images. J. Parallel Distrib. Comput. **137**, 26–33 (2020)
8. Elayan, O.N., Mustafa, A.M.: Android malware detection using deep learning. Proc. Comput. Sci. **184**, 847–852 (2021)
9. Faruki, P., Laxmi, V., Gaur, M.S., Vinod, P.: Behavioural detection with API call-grams to identify malicious PE files. In: SECURIT, pp. 85–91 (2012)
10. Fedler, R., Kulicke, M., Schütte, J.: An antivirus API for android malware recognition. In: 2013 8th International Conference on Malicious and Unwanted Software: "The Americas" (MALWARE), pp. 77–84. IEEE (2013)
11. Frenklach, T., Cohen, D., Shabtai, A., Puzis, R.: Android malware detection via an app similarity graph. Comput. Secur. **109**, 102386 (2021)
12. Hamid, I.R.A., Khalid, N.S., Abdullah, N.A., Ab Rahman, N.H., Wen, C.C.: Android malware classification using k-means clustering algorithm. In: IOP Conference Series: Materials Science and Engineering, vol. 226, p. 012105. IOP Publishing (2017)
13. Imtiaz, S.I., ur Rehman, S., Javed, A.R., Jalil, Z., Liu, X., Alnumay, W.S.: DeepAMD: detection and identification of android malware using high-efficient deep artificial neural network. Future Gener. Comput. Syst. **115**, 844–856 (2021)
14. Liu, Z., Wang, R., Japkowicz, N., Tang, D., Zhang, W., Zhao, J.: Research on unsupervised feature learning for android malware detection based on restricted boltzmann machines. Futur. Gener. Comput. Syst. **120**, 91–108 (2021)
15. Martín, A., Lara-Cabrera, R., Camacho, D.: Android malware detection through hybrid features fusion and ensemble classifiers: the andropytool framework and the omnidroid dataset. Inf. Fusion **52**, 128–142 (2019)
16. Syrris, V., Geneiatakis, D.: On machine learning effectiveness for malware detection in android OS using static analysis data. J. Inf. Secur. Appl. **59**, 102794 (2021)
17. Wang, S., Chen, Z., Yan, Q., Yang, B., Peng, L., Jia, Z.: A mobile malware detection method using behavior features in network traffic. J. Netw. Comput. Appl. **133**, 15–25 (2019)
18. Yen, Y.S., Sun, H.M.: An android mutation malware detection based on deep learning using visualization of importance from codes. Microelectron. Reliab. **93**, 109–114 (2019)
19. Yerima, S.Y., Sezer, S.: DroidFusion: a novel multilevel classifier fusion approach for android malware detection. IEEE Trans. Cybern. **49**(2), 453–466 (2018)
20. Yerima, S.Y., Sezer, S., McWilliams, G.: Analysis of Bayesian classification-based approaches for android malware detection. IET Inf. Secur. **8**(1), 25–36 (2013)
21. Zhang, Y., Ren, W., Zhu, T., Ren, Y.: SaaS: a situational awareness and analysis system for massive android malware detection. Futur. Gener. Comput. Syst. **95**, 548–559 (2019)

Multiclass-Based Support Vector Machine for Parkinson's Disease Detection on Speech Data

Bali Devi[1(✉)], Sumit Srivastava[2], and Vivek Kumar Verma[2]

[1] Computer Science and Engineering, Manipal University Jaipur, Jaipur, Rajasthan, India
baligupta03@gmail.com

[2] Information Technology, Manipal University Jaipur, Jaipur, Rajasthan, India

Abstract. Overview: Parkinson's disease is a central nervous system neurodegenerative condition that impairs the ability to manage certain bodily activities. Parkinson's symptoms begin gradually and worsen with time due to dopamine's supply to the motor system. It is well established that vocal difficulties associated with illnesses may be assessed for early Parkinson's disease identification.

Objective: The primary objective of this project is to develop a categorization system for the typical symptoms of Parkinson's disease to aid in early identification.

Methods: All features were examined and chosen to utilize feature selection algorithms to categorize subjects into four groups based on their UPDRS (Unified Parkinson's disease Rating Scale) score. SVM, LR, GNB, K-Nearest Neighbor's (KNN), and Random Forest (RF) were some of the machine learning classifiers that we used to make predictions.

Results: SVM had the highest classification accuracy of 89% when combined with PCA for Parkinson's disease identification.

Keywords: Classification · Parkinson's disease · Machine learning · Supervised learning · Neurodegenerative disorder

1 Introduction

Parkinson's disease is a disease of the central nervous system that makes it hard to control someone's actions [28]. Starting slowly, Parkinson's symptoms get worse over time because there is a lot of dopamine in the motor system but not enough of it. [1] It is thought that vocal problems can be used to detect Parkinson's disease at an early stage. Little et al. [2] have shown the measurement of the Parkinson's disease patients from healthy ones by utilizing the dysphonia indicators. Parkinson's disease cannot be cured; however, treatment after diagnosis can allay symptoms significantly. So, it is essential to diagnose Parkinson's disease patients at the early stage [3]. In [4], the Parkinson's disease diagnosis is conducted using empirical tests and invasive techniques, but the results are less effective, and the accuracy is not satisfactory. Using machine learning algorithms diagnosis will better understand Parkinson's disease [5]. SVM, LR, and KNN have been

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 540–557, 2023.
https://doi.org/10.1007/978-3-031-13150-9_44

applied, but this can be improved by applying more algorithms for accurate Parkinson's disease detection [6]. A new method, Random Forest, consists of Haar wavelets used as a projection filter and integrated with logistic regression [7, 27]. The fuzzy KNN method upon voice measurements was developed [8]. The hybrid intelligent system is proposed [9] to detect PD. Unsupervised methods were also used for Parkinson's disease detection [10]. The accuracy is high, but the number of features extracted increased the computational time even though they used few features [11, 12]. The features obtained are voice-based and more accessible than the MRI-based [13, 14]. The main goal of this paper is to make it easier to detect Parkinson's disease (PD) at an early stage by putting together a list of things that make each person different. Each one of the features was looked at and chosen by feature selection algorithms to put people into one of four groups based on their UPDRS scores. Dataset, Methodology, Results & Discussion, and conclusionare all covered in Sects. 2 through 5 in this article. Table 1 presents the literature reviewed and key points.

2 Literature Review

A deep learning model, machine learning and ensemble learning methods were used by Wu Wang et al. [24]. They used these methods to analyse clinical data, imaging, and biomarker biomarker data. They were good at detecting things because they were able to get a 96.45% accuracy rate. There was 95% accuracy on the training database and 100% accuracy on the testing database when all dataset features were used. This is called linear discriminant analysis (LDA). People who work at the phone number [6] have used three supervised algorithms to improve the detection of Parkinson's disease. With three types of handwriting records, the author got an accuracy rate of 100% with recall for SVM and an accuracy rate of 40% with precision for KNN. People who worked on smartphone phonation used speech data to look for signs of Parkinson's disease. Jefferson S. et al. [11] used speech data to look for signs of Parkinson's. Accuracy was 94.55% and 92.94%, respectively, with the best feature set. AUC was 87.84%, and EER was 19.01 and 14.15, when phonation and speech were used together. Techniques for extracting linear and nonlinear features, principal component feature (PCA), and nonlinear PCA used by Benba et al. [25] on voice dataset with an accuracy of 87.5% using SVM. Cai, Zhennao [26] worked on Parkinson's illness diagnostic system based on an enhanced fuzzy KNN approach for chaotic bacterial foraging optimization. Robust methods are used to predict Parkinson's disease by Indrajit Mandal et al. [7] on a voice dataset with 100% accuracy for Linear LR with train and test samples. Using the corrected t-test, the accuracy of 96.75% with additive LR. Measurement of the Parkinson's disease patients from healthy ones by utilizing the dysphonia indicators and applied Support vector machine in Little, M.A at el. [2] used the SVM approach to get 91.4% accuracy on voice samples.

3 Dataset

This study used a dataset from The Patient Voice Analysis [15]. The research collected data from 620 participants and 779 paired voice recordings, with some persons participating more than once. Each person was asked to phonemes and held the long vowel

/a/ at their level. We grouped classes into four based on their UPDRS score: healthy controls, early, moderate, and advanced stages of Parkinson's disease. Each class has 109 healthy individuals, 332 early-stage individuals, 250 intermediate-stage individuals, and 49 advanced-stage individuals.

Key Contribution
The key contributions of our work are as follows:

- To address the early PD (Parkinson's disease) detection and diagnosis by categorizing distinguishing features.
- All features were examined and chosen using feature selection algorithms to categorize subjects into four groups based on their UPDRS (Unified Parkinson's disease Rating Scale) scores.

4 Methodology and Implement

Data Pre-processing
After collecting the data, we will conduct several experiments to check any missing values. Missing values were removed, and get_dummies () have been used to convert the categorical variable into an indicator variable. RPDE (Recurrence period density entropy) is used to determine the periodicity of a signal [16]. PDA (Parkinson's disease with Anxiety) is a method used for power-law scaling autocorrelations known as non-stationary, introduced a stationary signal for overcoming the scaling techniques [17, 21]. PPE (Pitch period entropy) is a common symptom of Parkinson's disease people [18], a measure of dysphonia robust to much uncontrollable stable pitch in voice frequency [2, 29].

Principal Component Analysis
All the parameters do not show the presence of Parkinson's disease and cannot be distinguished for healthy. So relevant features need to be identified [19]. In this work, we will apply principal component analysis (PCA). The objective of PCA is to reduce the dimensionality of the data to a smaller dimensionality to optimize the variance. Prior voice data analyses have shown that the dimensionality reduction approach produces positive results [20]. The "key" to a PCA is the eigenvectors and eigenvalues of a covariance matrix. The eigenvectors define the new feature space's directions. The eigenvalues will determine the variance of each data point along the new axis. The covariance matrix is one whose elements each indicate the covariance between two features. It is calculated using Eq. 1.

$$\mathbf{Cov}\,(\mathbf{X}, \mathbf{Y}) = \sum (\mathbf{xi} - \overline{\mathbf{x}})\,(\mathbf{yi} - \overline{\mathbf{y}})\,\mathbf{N} - 1 \tag{1}$$

Support Vector Machine
This is a common way to solve problems that need Supervised Learning in both Classification and Regression. The Support Vector Machine, or SVM, can help you do this.

Machine Learning is, however, where it is mostly used. It is used to solve problems with classifying things. Find a line or boundary to divide n-dimensional space into classes so that new data points can be classified in the future. A hyperplane is a mathematical term for this optimum decision boundary [22, 23]. The SVM algorithm determines the hyperplane's extreme points/vectors. Support vectors are used to describe these extreme situations, and the technique is called a Support Vector Machine. Consider the following illustration, which illustrates two different categories divided by a decision boundary or hyperplane (Fig. 1).

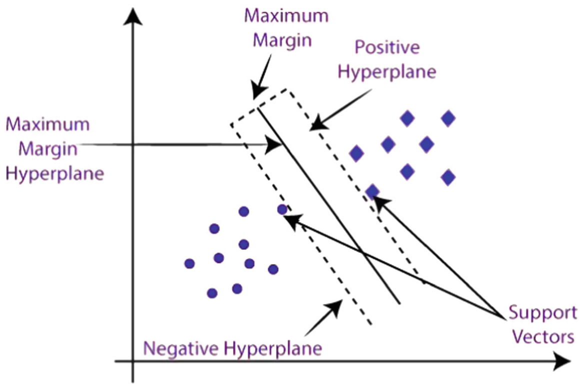


Fig. 1. SVM classification with the hyperplane

Table 1 describes different features with dataset descriptions, including type, format, units, and values. It is also described according to sex with different age groups.

Table 1. Voice data attributes description [15]

Field	Description	Type, format/units/values
call_timestamp	Date and time IVR voice call initiated	string, YYYY/MM/DD HH:MM: SS UTC +0000
recording_duration	Length of recording captured by IVR system	integer, seconds
callref	Unique reference number for voice recording	integer
audio_duration	Length of audio captured by IVR system during call	real, seconds
voice_indexstart	Starting audio sample index at which voicing is detected, if at all	integer, samples

(*continued*)

Table 1. (*continued*)

Field	Description	Type, format/units/values
voice_indexend	Ending audio sample index at which voicing is detected, it at all	integer, samples
voice_code	Quality of voice recording: 'ok' – (part of) recording usable, 'bad' – recording unusable (no features extracted)	string, 'ok'/'bad'
voice_usable_duration	Length of usable voicing detected	real, seconds
feature01	Median F0	real, Hz
feature02	Mean absolute F0 time derivative	real, Hz^2
feature03	The median absolute F0 time derivative	real, Hz^2
feature04	Mean absolute value of time derivative of RMS power	real, Hz
feature05	The median absolute value of time derivative of RMS power	real, Hz
feature06-feature19	Median cepstral coefficients 0–12 for entire voice recording	13 x real
feature20-feature32	Mean absolute time derivative of cepstral coefficients 0–12 across entire voice recording	13 x real
feature33	Recurrence period density entropy (RPDE) Hnorm	real
feature34	Detrended fluctuation analysis (DFA) scaling parameter alpha	real
feature35	Modified pitch period entropy (PPE)	real
feature36	Relative spectral power 0–500 Hz	real
feature37	Relative spectral power 500–1 kHz	real
feature38	Relative spectral power 1 kHz–2 kHz	real
feature39	Relative spectral power 2 kHz–4 kHz	real

(*continued*)

Table 1. (*continued*)

Field	Description	Type, format/units/values
user_id_hashed	Hashed PatientsLikeMe user ID	string
pvi_created_at	Date and time at which PatientsLikeMe collected unique reference number for call	string, YYYY-MM-DD HH:MM: SS. d
current_age	Age of participant when the call was recorded	integer, years
Sex	**Sex of participant**	**String, 'M'/'F'/empty**
years_since_first_symptom	Years since the first Parkinson's symptoms detected by the participant	integer, years
pdrs_date	Reference date at which PDRS (Parkinson's disease rating scale) applies	string, YYYY-MM-DD
pdrs_reported_at	Date and time at which PatientsLikeMe collected PDRS	string, YYYY-MM-DD HH:MM: SS. d
days_from_pvi_to_pdrs	Number of days elapsed between PDRS reference date (pdrs_date) and unique call reference number collected (pvi_created_at)	integer, days
pdrs_score	The scaled sum of all PDRS entries Q1-Q17 below	integer, 0–68
memory	PDRS Q1	integer, 0–4
hallucinations	PDRS Q2	integer, 0–4
mood	PDRS Q3	integer, 0–4
motivation	PDRS Q4	integer, 0–4
speech	PDRS Q5	integer, 0–4
saliva	PDRS Q6	integer, 0–4
swallowing	PDRS Q7	integer, 0–4
handwriting	PDRS Q8	integer, 0–4
cutting_food	PDRS Q9	integer, 0–4
dressing	PDRS Q10	integer, 0–4
hygiene	PDRS Q11	integer, 0–4
turning_in_bed	PDRS Q12	integer, 0–4
falling	PDRS Q13	integer, 0–4

(*continued*)

Table 1. (*continued*)

Field	Description	Type, format/units/values
freezing	PDRS Q14	integer, 0–4
walking	PDRS Q15	integer, 0–4
tremors	PDRS Q16	integer, 0–4
numbness	PDRS Q17	integer, 0–4
hoehn_yahr	Hoehn and Yahr stage at the time of reporting PDRS	integer, 1–5
on_treatment_id	Whether participant was 'on' vs. 'off' medication when PDRS was reported	string, 'true'/'false'
calls_per_user	Number of calls made by this user	integer

There are four parts to the Unified Parkinson's Disease Rating Scale, and they are: (UPDRS). 0 means there are no problems, 1 means there are some problems, 2 means there are some mild problems, 3 means there are some moderate problems, and 4 means there are some very bad problems (Table 2).

Table 2. PLM-PVA PDRS/Hoehn & Yahr (H&Y) staging system [15]

Field	Value	Descriptive value
Memory	0, 1, 2, 3, 4	0 - 'There are no memory difficulties.' 1 - 'Mild memory issues; I am often forgetful and recall events only in fragments.' 2 - 'Due to moderate memory issues, I sometimes get disoriented and may become easily confused.' 3 'Severe memory issues mean that I often forget what day it is or where I am.' 4 - 'I have serious memory issues; I often lose track of where I am or what day it is; I have a tough time making choices or resolving problems.'
Hallucinations	0, 1, 2, 3, 4	0 - 'I never see things that other people cannot see ('hallucinations').' 1 - 'I have really vivid dreams.' 2 - 'At times, I see things that other people cannot see, but I know they are not real.' 3 - 'Occasionally, I see things that are unseen to others and believe them to be real.' 4 - 'I often see things that are unseen to others and feel they are genuine.'

(*continued*)

Table 2. (*continued*)

Field	Value	Descriptive value
Mood	0, 1, 2, 3, 4	0 - 'I do not suffer from prolonged sadness.' 1 - 'I sometimes experience sadness that lasts longer than typical, i.e., more than a few days or a week.' 2 - 'I sometimes get depressed for more than a week at a time.' 3 - 'I have prolonged spells of sadness during which I lose weight, am unable to sleep, and have a bad appetite.' 4 - 'I experience prolonged sadness and have suicidal thoughts.'
Motivation	0, 1, 2, 3, 4	0 - 'My motivation is about average.' 1 - 'I have become more docile and less forceful.' 2 - 'I've lost some initiative and am becoming less interested in activities.' 3 - 'I've lost some initiative and am bored with my regular routine.' 4 - 'I am a recluse who initiates little action.'
Speech	0, 1, 2, 3, 4	0 - 'No, my tone of voice has not altered.' 1 - 'Yes, my speech has altered, but other people understand me well.' 2 - 'Yes, my tone of voice has altered somewhat, and I sometimes have to repeat myself to be understood.' 3 - 'Yes, my manner of speaking has evolved enough, and I often have to repeat myself to be understood.' 4 - 'Indeed, my manner of speaking has evolved to the point that others have difficulties understanding me or do not comprehend me at all.'
Saliva	0, 1, 2, 3, 4	0 - 'I have not noticed that my saliva is excessive or that I drool.' 'Yes, I have noticed a little increase in salivation and sometimes slobber on my pillow at night.' 2 - 'Yes, I sometimes have an excess of saliva and drool throughout the day.' 3 - 'Yes, I create an excessive quantity of saliva and drool often during the day.' 4 - 'Yes; I drool so often that I am always carrying a handkerchief.'
Swallowing	0, 1, 2, 3, 4	0 - 'No; I do not have any difficulty eating or choking.' 1 - 'Yes, I sometimes have difficulty swallowing.' 2 - 'Yes, I sometimes have difficulty eating and choking.' 3 - 'Yes, I do have swallowing problems and need soft food to consume.' 4 - 'Yes, I have difficulty swallowing and need nasogastric intubation or a gastrostomy

(*continued*)

Table 2. (*continued*)

Field	Value	Descriptive value
Handwriting	0, 1, 2, 3, 4	0 - 'I have not observed any modifications in my writing style.' 'Yes, my handwriting is a little slower, and my letter construction is a little smaller.' 2 - 'Yes, my handwriting has slowed somewhat, and my letter structure has shrunk, but everything I write is understandable.' 3 - 'Yes, my handwriting has significantly changed, and certain words are unintelligible.' 4 - 'Yes, my handwriting has degenerated to the point that most of the words are unintelligible.'
cutting_food	0, 1, 2, 3, 4	0 - 'No; I do not slow down my meal preparation and have no difficulty handling my utensils.' 1 - 'Yes; I am somewhat slower and clumsier than I was before, but I am still capable of eating alone.' 2 - 'Yes, I am slower and clumsier than I was before, and I need help cutting some items.' 3 - 'Even if someone has to slice my food, I am still able to eat alone.' 4 - 'I need nourishment because I am unable to do it on my own.'
Dressing	0, 1, 2, 3, 4	0 - 'No; I have no difficulty getting dressed and am no slower than I was before.' 1 - 'Yes; I dress more slowly - but with minimal assistance.' 2 - 'Yes, I dress more slowly and sometimes need assistance buttoning my pants, tying my shoes, or slipping my arm through the sleeves.' 3 - 'Yes, I need significant assistance to dress - yet I am still capable of doing certain tasks myself.' 4 - 'I am required to be clothed by another person.'
Hygiene	0, 1, 2, 3, 4	0 - 'No; I do not have any difficulty eating or choking.' 1 - 'Yes, I sometimes have difficulty swallowing.' 2 - 'Yes, I sometimes have difficulty eating and choking.' 3 - 'Yes, I do have swallowing problems and need soft food to consume.' 4 - 'Yes, I have difficulty swallowing and need nasogastric intubation or a gastrostomy
Turning_in_bed	0, 1, 2, 3, 4	0 - 'My motivation is about average.' 1 - 'I have become more docile and less forceful.' 2 - 'I've lost some initiative and am becoming less interested in activities.' 3 - 'I've lost some initiative and am bored with my regular routine.' 4 - 'I am a recluse who initiates little action.'

(*continued*)

Table 2. (*continued*)

Field	Value	Descriptive value
Falling	0, 1, 2, 3, 4	0 - 'I have not observed any modifications in my writing style.' 'Yes, my handwriting is a little slower and my letter construction is a little smaller.' 2 - 'Yes, my handwriting has slowed somewhat, and my letter structure has shrunk, but everything I write is understandable.' 3 - 'Yes, my handwriting has significantly changed, and certain words are unintelligible.' 4 - 'Yes, my handwriting has degenerated to the point that most of the words are unintelligible.'
Freezing	0, 1, 2, 3, 4	0 - 'I have not encountered freezing.' 1 - 'On rare instances, I have experienced cold while walking. Or sometimes, when I begin walking, I suffer hypothermia.' 2 - 'Yes, I do suffer freezing on occasion.' 3 - 'Yes; I regularly get hypothermia while walking and have fallen as a result.' 4 - 'Yes; I regularly get hypothermia when walking and have fallen as a result
Walking	0, 1, 2, 3, 4	0 - 'No, my gait and arm movement have remained the same.' 1 - 'Yes, my walking style has altered, but this is not an issue.' 2 - 'Yes, I have some trouble walking, but I do not need assistance.' 3 - 'Yes, I have significant difficulties walking and need assistance.' 4 - 'I am unable to walk alone or with assistance.'
Tremors	0, 1, 2, 3, 4	1 - 'No, I have no obvious tremors.' 2 - 'Yes; on occasion, I do experience obvious tremors.' 3 - 'Yes, I have little tremors that cause me discomfort.' 4 - 'Yes, I have severe tremors that impair my ability to do some things.' 5 - 'Yes, I suffer from severe tremors that impair the bulk of my activities.'
Numbness	0, 1, 2, 3, 4	1 - 'No, I do not experience numbness, tingling, or specific pain as a result of my Parkinson's disease.' 2 - 'On occasion, I do have numbness, tingling, or localised pain as a result of my Parkinson's disease.' 3 - 'Yes; I have numbness - tingling - or pain on a frequent basis, which I attribute to my Parkinson's disease.' 4 - 'Yes, I often have unpleasant symptoms connected with Parkinson's disease.' 5 - 'Yes, I am in extreme pain because of my Parkinson's disease.'

(*continued*)

Table 2. (*continued*)

Field	Value	Descriptive value
hoehn_yahr	1, 2, 3, 4, 5	1 - One-sided symptoms 2 - Both sides exhibit symptoms 3 - Balance and walking difficulties 4 - Struggle to stand and walk 5 - Is incapable of standing or walking independently

Model Selection

Following PCA, model selection is a critical stage in developing the Machine Learning Model used to decide the computations. It entails selecting the optimal Machine Learning Models. Beyond model performance, accuracy, available resources, and maintainability are essential considerations when undertaking model selection. Additionally, the AUC – ROC curve has been incorporated. Evaluation is conducted using metrics such as recall, precision, and the f1-measure. Figure 2 illustrates the experimental flow chart.

$$\text{Accuracy} = (\text{TP} + \text{TN})/(\text{TP} + \text{FP} + \text{TN} + \text{FN})$$
$$\text{Recall} = \text{TP}/(\text{TP} + \text{FN})$$
$$\text{Precision} = \text{TP}/(\text{TP} + \text{FP})$$
$$\text{F1} = 2 * (\text{Recall} * \text{Precision})/(\text{Recall} + \text{Precision})$$

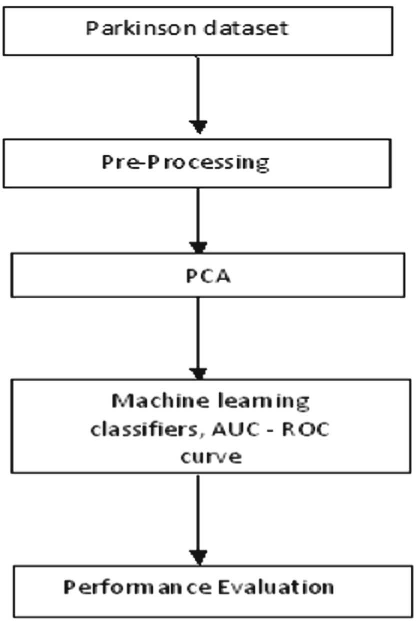


Fig. 2. Experimental flow chart

5 Results and Discussion

Support Vector Machine (SVM)

Table 3 represents the SVM classification results and selected PCA = 5, with 89% overall accuracy. Figure 3 represents the accuracy matrix for the classes. Figure 4 represents the ROC curve for the classes with AUC scores. In this model, Confusion matrix table:

- Advanced class: There are 4 correctly classified; 2 are misclassified and considered as an intermediate class.
- Early class: There are 60 correctly classified; 5 are misclassified (2 as healthy class, and 3 as intermediate class).
- Healthy class: There are 18 correctly classified; 6 are misclassified and considered as an early class.
- Intermediate class: There are 49 correctly classified; 4 are misclassified and considered as an early class.

Table 3. Confusion matrix table for SVM

	Advanced	Early	Healthy	Intermediate
Advanced	4	0	0	2
Early	0	60	2	3
Healthy	0	6	18	0
Intermediate	0	4	0	49

	precision	recall	f1-score	support
advanced	1.00	0.67	0.80	6
early	0.86	0.92	0.89	65
healthy	0.90	0.75	0.82	24
intermediate	0.91	0.92	0.92	53
accuracy			0.89	148
macro avg	0.92	0.82	0.86	148
weighted avg	0.89	0.89	0.88	148

Fig. 3. Accuracy matrix for SVM

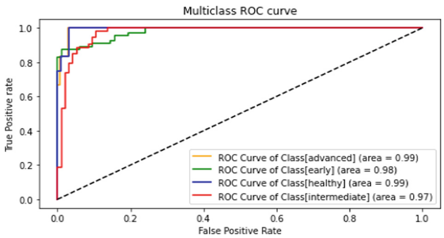


Fig. 4. ROC curve for SVM

Logistic Regression (LR)

Table 4 represents the results obtained using Logistic regression (LR) classification and selected PCA = 5, with 87% overall accuracy. Figure 5 represents the accuracy matrix for the classes. Figure 6 represents the ROC curve for the classes with AUC scores. In this model, Confusion matrix table:

- Advanced class: There are 4 correctly classified; 2 are misclassified and considered as an intermediate class.

- Early class: There are 59 correctly classified; 6 are misclassified (4 as healthy class, and 2 as intermediate class).
- Healthy class: There are 20 correctly classified; 4 are misclassified and considered as an early class.
- Intermediate class: There are 46 were correctly classified, 7 are misclassified (1 as advanced class, and 6 as early class).

Table 4. Confusion matrix table for LR

	advanced	early	healthy	intermediate
advanced	4	0	0	2
early	0	59	4	2
healthy	0	4	20	0
intermediate	1	6	0	46

	precision	recall	f1-score	support
advanced	0.80	0.67	0.73	6
early	0.86	0.91	0.88	65
healthy	0.83	0.83	0.83	24
intermediate	0.92	0.87	0.89	53
accuracy			0.87	148
macro avg	0.85	0.82	0.83	148
weighted avg	0.87	0.87	0.87	148

Fig. 5. Accuracy matrix for LR

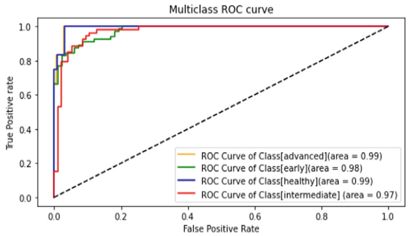


Fig. 6. ROC curve for LR

Gaussian Naïve Bayes (GNB)

Table 5 represents the Gaussian Naïve Bayes (GNB) classification results and selected PCA = 5, with 80% overall accuracy. Figure 7 represents the accuracy matrix for the classes. Figure 8 represents the ROC curve for the classes with AUC scores. In this model, Confusion matrix table:

- Advanced class: There are 4 correctly classified; 2 are misclassified and considered as an intermediate class.
- Early class: There are 62 correctly classified; 3 are misclassified and considered as an intermediate class.
- Healthy class: There are 14 correctly classified; 10 are misclassified and considered as an early class.
- Intermediate class: There are 39 correctly classified; 14 are misclassified and considered as an early class.

K-Nearest NEighbour's (KNN)

Table 6 represents the KNN classification results with k = 4 and selected PCA = 5, with 76% overall accuracy. Figure 9 represents the accuracy matrix for the classes. Figure 10 represents the ROC curve for the classes with AUC scores. In this model, Confusion matrix table:

Table 5. Confusion matrix table for GNB

	advanced	early	healthy	intermediate
advanced	4	0	0	2
early	0	62	0	3
healthy	0	10	14	0
intermediate	0	14	0	39

	precision	recall	f1-score	support
advanced	1.00	0.67	0.80	6
early	0.72	0.95	0.82	65
healthy	1.00	0.58	0.74	24
intermediate	0.89	0.74	0.80	53
accuracy			0.80	148
macro avg	0.90	0.73	0.79	148
weighted avg	0.84	0.80	0.80	148

Fig. 7. Accuracy matrix for GNB

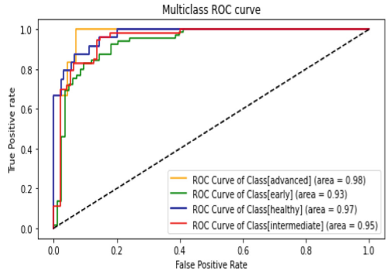


Fig. 8. ROC curve for GNB

- Advanced class: There are 4 correctly classified; 2 are misclassified and considered as an intermediate class.
- Early class: There are 60 correctly classified; 5 are misclassified and considered as a healthy class.
- Healthy class: There are 10 correctly classified; 14 are misclassified and considered as an early class.
- Intermediate class: There are 38 correctly classified; 15 are misclassified (2 as advanced class, and 13 as early class).

Table 6. Confusion matrix table for KNN

	advanced	early	healthy	intermediate
advanced	4	0	0	2
early	0	60	5	0
healthy	0	14	10	0
intermediate	2	13	0	38

Random Forest (RF)

Table 7 represents the results obtained using Random Forest (RF) classification and selected PCA = 5, with 82% overall accuracy. Figure 11 represents the accuracy matrix for the classes. Figure 12 represents the ROC curve for the classes with AUC scores. In this model, Confusion matrix table:

- Advanced class: There are 4 correctly classified; 2 are misclassified and considered as an intermediate class.

	precision	recall	f1-score	support
advanced	0.67	0.67	0.67	6
early	0.69	0.92	0.79	65
healthy	0.67	0.42	0.51	24
intermediate	0.95	0.72	0.82	53
accuracy			0.76	148
macro avg	0.74	0.68	0.70	148
weighted avg	0.78	0.76	0.75	148

Fig. 9. Accuracy matric for KNN

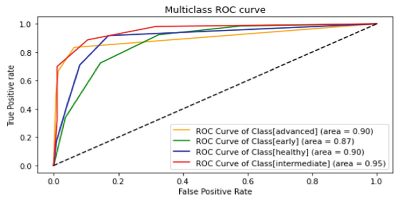


Fig. 10. ROC curve for KNN

- Early class: There are 60 correctly classified; 5 are misclassified (4 as healthy class, and 1 as intermediate class).
- Healthy class: There are 16 correctly classified; 8 are misclassified and considered as an early class.
- Intermediate class: There are 42 that were correctly classified; 11 are misclassified (1 as advanced class, and 10 as early class).

Table 7. Confusion matrix table for RF

	advanced	early	healthy	intermediate
advanced	4	0	0	2
early	0	60	4	1
healthy	0	8	16	0
intermediate	1	10	0	42

	precision	recall	f1-score	support
advanced	0.80	0.67	0.73	6
early	0.77	0.92	0.84	65
healthy	0.80	0.67	0.73	24
intermediate	0.93	0.79	0.86	53
accuracy			0.82	148
macro avg	0.83	0.76	0.79	148
weighted avg	0.83	0.82	0.82	148

Fig. 11. Accuracy matrix for RF

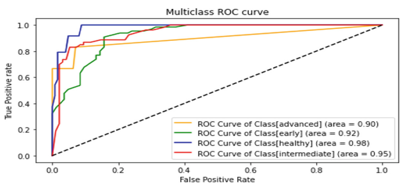


Fig. 12. ROC curve for RF

We can say that SVM has shown the best performance with 89% overall accuracy from all the performance measurements.

Result Analysis of all Classifiers

Table 8 represents a comparative analysis between all machine learning models to get accurate results.

Table 8. Comparative analysis between all machine learning models

Model	Accuracy
Support vector machine	89%
Logistic regression	87%
Gaussian naïve bayes	80%
K-nearest neighbors	81%
Random forest	82%

6 Conclusion

By putting together, a list of things that each person has that make them unique, this paper aims to make it easier to spot Parkinson's disease (PD) early. Each feature was looked at and chosen by algorithms that used them to group people into four groups based on their UPDRS scores. We used various machine learning methods in conjunction with PCA to identify Parkinson's illness using the multi-classification dataset. SVM performed the best, with an overall accuracy of 89%, while KNN performed the poorest, 76%. This multi-classification dataset can distinguish a person's stage based on the UPDRS score. This will be helpful for the medication purpose. In the future, we intend to implement Deep Learning algorithms and their alternative algorithm to improve the accuracy and detection model also tried some balancing techniques in the following study to avoid imbalance issues.

Acknowledgments. I am pleased to express my heartfelt gratitude to the Department of Information Technology and Computer Science and Engineering, School of Computing and Information Technology, Manipal University Jaipur, Jaipur, Rajasthan, India, for providing the research platform on which the extensive analytical process could be carried out. We are also thankful to Patient Voice Analysis Study: Synapse ID-syn2321745 for providing the dataset and making this available for research.

References

1. Harel, B., Cannizzaro, M., Snyder, P.J.: Variability in fundamental frequency during speech in prodromal and incipient Parkinson's disease: a longitudinal case study. Brain Cogn. **56**(1), 24–29 (2004)
2. Little, M.A., et al.: Suitability of dysphonia measurements for telemonitoring of Parkinson's disease. IEEE Trans. Biomed. Eng. **56**(4), 1015–1022 (2009)
3. Singh, N., Pillay, V., Choonara, Y.E.: Advances in the treatment of Parkinson's disease. Prog. Neurobiol. **81**(1), 29–44 (2007)
4. Parkinson's Disease: National clinical guideline for diagnosis and management in primary and secondary care. Nat. Collaborating Centre Chronic Conditions, London, U.K. (2006)
5. Sriram, T.V.S., Rao, M.V., Narayana, G.V.S., Kaladhar, D.S.V.G.K., Vital, T.P.R.: Intelligent Parkinson disease prediction using machine learning algorithms. Int. J. Eng. Innov. Technol. (IJEIT) **3**(3) (Sep 2013)

6. Shamrat, F.M.J.M., Asaduzzaman, M., Rahman, A.K.M.S., Tusher, R.T.H., Tasnim, Z.: A comparative analysis of Parkinson disease prediction using machine learning approaches. Int. J. Sci. Technol. Res. **8**(11) (Nov 2019)
7. Mandal, I., Sairam, N.: New machine-learning algorithms for prediction of Parkinson's disease. Int. J. Syst. Sci. (Jul 2012)
8. Cai, Z., et al.: An intelligent Parkinson's disease diagnostic system based on a chaotic bacterial foraging optimization enhanced fuzzy KNN approach (Jun 2018)
9. Ali, L., Zhu, C., IEEE Fellow, Zhang, Z., Liu, Y., IEEE Senior Member: Automated detection of parkinson's disease based on multiple types of sustained phonations using linear discriminant analysis and genetically optimized neural network. IEEE J. Transl. Eng. Health Med. (2019)
10. Nilashi, M., Ibrahim, O., Ahmadi, H., Shahmoradi, L., Farahmand, M.: A hybrid intelligent system for the prediction of Parkinson's Disease progression using machine learning techniques. Biocybern. Biomed. Eng. **38**(1), 1–15 (2018)
11. Almeida, J.S., et al.: Detecting Parkinson's disease with sustained phonation and speech signals using machine learning techniques. Pattern Recognit. Lett. **125**, 55–62 (2019). https://doi.org/10.1016/j.patrec.2019.04.005
12. Wang, Y., Wang, A.N., Ai, Q., Sun, H.J.: An adaptive kernel- based weighted extreme learning machine approach for effective detection of Parkinson's disease. Biomed Signal Process Control **38**, 400–410 (2017)
13. Singh, G., Vadera, M., Samavedham, L., Lim, E.C.H.: Machine learning-based framework for multiclass diagnosis of neurodegenerative diseases: a study on Parkinson's Disease. IFAC-Papers OnLine **49**(7), 990–995 (2016)
14. Pahuja, G., Nagabhushan, T.N.: A Novel GA-ELM approach for Parkinson's disease detection using brain structural T1-weighted MRI data. In: 2016 Second International Conference on Cognitive Computing and Information Processing (2016)
15. Patient Voice Analysis (PVA) Synapse ID: [syn2321745] https://www.synapse.org
16. Kantz, H., Schreiber, T.: Nonlinear Time Series Analysis. Cambridge University Press (2010). https://doi.org/10.1017/CBO9780511755798
17. Little, M.A., McSharry, P.E., Roberts, S.J., Costello, D.A.E., Moroz, I.M.: Exploiting nonlinear recurrence and fractal scaling properties for voice disorder detection. Biomed. Eng. Online **6**(1), 23 (2007). https://doi.org/10.1186/1475-925X-6-23
18. Cnockaert, L., et al.: Low frequency vocal modulations in vowels produced by Parkinsonian subjects. Speech Commun. **50**, 288–300 (2008)
19. Ferchichi, S.E., et al.: Feature selection using an SVM learning machines. In: Proceedings of the 422 3rd International Conference on Signals, Circuits and Systems (SCS 2009), pp. 1–6 (2009)
20. Benba, A., Jilbab, A., Hammouch, A.: Voice assessments for detecting patients with Parkinson's diseases using PCA and NPCA. Int. J. Speech Technol. **19**(4), 743–754 (2016). https://doi.org/10.1007/s10772-016-9367-z
21. Devi, B., Srivastava, S., Verma, V.K.: Predictive analysis of Alzheimer's disease based on wrapper approach using SVM and KNN. In: Senjyu, T., Mahalle, P.N., Perumal, T., Joshi, A. (eds.) ICTIS 2020. SIST, vol. 196, pp. 707–715. Springer, Singapore (2021). https://doi.org/10.1007/978-981-15-7062-9_71
22. Shankar, V.G., Sisodia, D.S., Chandrakar, P.: DataAutism: an early detection framework of autism in infants using data science. In: Sharma, N., Chakrabarti, A., Balas, V.E. (eds.) Data Management, Analytics and Innovation. AISC, vol. 1016, pp. 167–178. Springer, Singapore (2020). https://doi.org/10.1007/978-981-13-9364-8_13
23. Goel, V., Jangir, V., Shankar, V.G.: DataCan: robust approach for genome cancer data analysis. In: Sharma, N., Chakrabarti, A., Balas, V.E. (eds.) Data Management, Analytics and

Innovation. AISC, vol. 1016, pp. 153–166. Springer, Singapore (2020). https://doi.org/10.1007/978-981-13-9364-8_12

24. Wang, W., Lee, J., Harrou, F., Sun, Y.: Early detection of Parkinson's disease using deep learning and machine learning. IEEE Access **8**, 147635–147646 (2020). https://doi.org/10.1109/ACCESS.2020.3016062
25. Benba, A., Jilbab, A., Hammouch, A.: Detecting multiple system atrophy, Parkinson and other neurological disorders using voice analysis. Int. J. Speech Technol. **20**(2), 281–288 (2017). https://doi.org/10.1007/s10772-017-9404-6
26. Cai, Z., et al.: An intelligent Parkinson's disease diagnostic system based on a chaotic bacterial foraging optimization enhanced fuzzy KNN approach. Comput. Math. Methods Med. **2018**, 1–24 (2018). https://doi.org/10.1155/2018/2396952
27. Devi, B., Shankar, V.G., Srivastava, S., Srivastava, D.K.: AnaBus: a proposed sampling retrieval model for business and historical data analytics. In: Sharma, N., Chakrabarti, A., Balas, V.E. (eds.) Data Management, Analytics and Innovation. AISC, vol. 1016, pp. 179–187. Springer, Singapore (2020). https://doi.org/10.1007/978-981-13-9364-8_14
28. Shankar, V.G., Sisodia, D.S., Chandrakar, P.: A novel discriminant feature selection–based mutual information extraction from MR brain images for Alzheimer's stages detection and prediction. Int. J. Imaging Syst. Technol. **32**(4), 1172–1191 (2021). https://doi.org/10.1002/ima.22685
29. Shankar, V.G., Devi, B., Sachdeva, U., Harsola, H.: Real-time human body tracking system for posture and movement using skeleton-based segmentation. In: Sharma, D.K., Son, L.H., Sharma, R., Cengiz, K. (eds.) Micro-Electronics and Telecommunication Engineering. LNNS, vol. 179, pp. 499–510. Springer, Singapore (2021). https://doi.org/10.1007/978-981-33-4687-1_48

Automated Journalism Based on Sports Analysis

Eeshan Nanekar(✉), Siddhant Nalawade, Zenden Castelino, and Smita Rukhande

Information Technology, Fr. Conceicao Rodrigues Institute of Technology, Mumbai, India
eeshann20001@gmail.com

Abstract. Despite increasing amounts of data and ever improving natural language techniques, work on automated journalism is still relatively scarce. Reporting news requires significant amount of time and effort of the journalists and they need more domain knowledge as well. If this editorial process is automated, more working time of journalists can be reduced considerably while they can spend more on in depth reporting. Overall, this recent development is sure to grow, as it provides the industry with more accurate, up-to-date, and effortless reporting.

Automated journalism is rising in the news world, especially in sports coverage where structured data is abundant and readily available. Algorithms churn out full length articles in masses and practically instantaneously, using big data, and this bloat the sheer volume of articles available to news readers. Noting the importance of perceived credibility and readability in sports news articles in particular, as well as the pertinence of text objectivity and by lines in automated journalism, an experiment was developed to understand how these factors interact.

Automatically generated text can also be easily customized to reflect preferences that are particular to players' style and level of experience of the viewers.

1 Introduction

Automated journalism is becoming more prevalent due to the availability of data feeds, the demand for news on mobile devices, and advancements in algorithms. Advances in Natural Language Generation (NLG) and data-to-text tools have found relative success outside various sporting events. In automated journalism, also known as algorithmic journalism or robot journalism, news articles are generated by computer programs. Through artificial intelligence (AI) software, stories are produced automatically by machines rather than human reporters. These programs interpret, organize, and present data in human-readable ways. Typically, the process involves an algorithm that scans large amounts of provided data, selects from an assortment of pre-programmed article structures, orders key points, and inserts details such as names, places, amounts, rankings, statistics, and figures. The output can also be customized to fit a certain voice, tone, or style.

Sports works well for automated journalism since sports stats are numbers-based. These data can be structured in a way which makes automated articles easy to write. Automated journalism requires data in a machine-readable format, like a spreadsheet.

Today, there is a need to report on a lot of football matches and, many of them, are played at the same time. A significant amount of human resources and working time

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 558–564, 2023.
https://doi.org/10.1007/978-3-031-13150-9_45

would be needed for journalists to watch every match that they have to make a report. Due to the abundant availability of information that is stored in databases, journalists are able to make a report based just that information. However, if this process was automated it would save a lot of working time of journalists. As a result, journalists would have more time for In-depth reporting. There is a wide requirement for news to get produced within a short period after a sports match. Publishing news article is a manual process and needs journalists with domain and language competencies. Most of the time it is not possible for sport journalists to focus on in-depth reporting due to time and cost constraints. Therefore, an automated process is required which would be efficient and cost effective. As a solution, we present an Automated News Generation System and demonstrate the suitability and utilization of a template based natural language generation system. Advantages of the proposed system are:

Huge amount of data is analyzed and scanned quickly and efficiently
Grammatical and human errors are reduced significantly
Journalists can focus more on reporting of news, interviews and background research
Saves significant amount of time for journalists to write and share content
Same data can be used to tell stories from different angles and narratives in multiple languages.
Stories can be personalized based on user's demands. They are more unique and precise.

2 Literature Review

2.1 Related Work

2.1.1 Natural Language Generation

Natural language generation (NLG) is a sub-branch of artificial intelligence that generates textual explanations, comparisons and summaries of business data in a human-like way. It combines contextualized narratives with analytical output to express the most important and interesting concepts that lie within data in a universally consumable language that is relevant and timely.

2.1.2 Phases of NLG

Content determination: Deciding what information to mention in the text.

Document structuring: Overall organization of the information to convey. For example, deciding to describe the areas with high pollen levels first, instead of the areas with low pollen levels.

Aggregation: Merging of similar sentences to improve readability and naturalness.

Lexical choice: Putting words to the concepts.

Referring expression generation: Creating referring expressions that identify objects and regions.

Realization: Creating the actual text, which should be correct according to the rules of syntax, morphology, and orthography.

2.1.3 Applications of NLG in Journalism

Natural Language Generation in journalism has been making waves for the past few years. In 2018, a Natural Language Generating AI named Tobi was responsible for reporting on the results of Swiss referendums for 2,222 municipalities. Similarly, in 2017, Press Association won a £621,000 grant to start producing automated regional news. They partnered up with Urbs Media and are working towards producing up to 30,000 local news stories every month. This is currently the major strength of Automated Journalism – the ability to produce huge quantities of news stories out of structured data. The current limitations, however, are fairly obvious. There is no conscious writer behind these articles, but rather a series of templates and decision trees. It is in fact difficult in many cases to justify the descriptor "AI" when it comes to these kinds of techniques and software, or perhaps we just give too much credit because of the grandiose associations of the word AI. This is changing as more advanced machine learning and NLG technologies begin to surface. What it takes to make a machine write, or talk, like a human is becoming clearer, and it may not be so long until AI journalists are producing more than just templates and statistics. Moving forward, however, will require a fundamentally different approach.

Automated Insights ("Ai") is an American-based technology company that specializes in natural language generation (NLG) software that turns big data into readable narratives. Automated Insights produced 300 million pieces of content in 2013,which Mashable reported was greater than the output of all major media companies combined. In 2014, the company's software generated one billion stories. In 2016, Automated Insights produced over 1.5 billion pieces of content. In October 2015, Automated Insights released their Wordsmith software for beta testing to allow organizations access to natural language generation technology as a SaaS offering.The company has since commercialized the natural language generation platform called Wordsmith, with customers including Yahoo, Associated Press, and Tableau.

Automated Insights provides natural language generation (NLG) technology in the form of their Wordsmith platform. Natural language generation is a software process that automatically turns data into human-friendly prose. Normally, structured data is fed into NLG software and run through a narrative template, producing content that reads as if a human writer created it. The technology is used mostly in instances that require a routine, large-scale production of content in which each narrative is similarly structured. Automated Insights (Ai) generates personalized recaps and previews for Yahoo Sports Fantasy Football.

Wordsmith, which is a product of Automated Insights, is the world's first public natural language generation (NLG) engine. Wordsmith allows users to generate human-sounding narratives from data. The platform makes it easy to produce millions of personalized reports, articles, and narratives in the time it takes to write just one. Wordsmith helps companies in data-driven industries, including financial services, e-commerce, real estate, business intelligence, media and many others, achieve content scale, efficiency and personalization.

This platform uses natural language generation to transform fantasy football data into draft reports, match previews, and match recaps. The platform generates millions of stories each week of the season, essentially giving every fantasy owner a personalized sports reporter writing about their team.

2.1.4 Existing System

The GoalGetter system is a Data-to-Speech system which generates spoken soccer reports (in Dutch) on the basis of tabular data. The system takes as input data about a soccer match that are derived from a Teletext. The output of the system is a spoken, natural language report conveying the main events of the match described on the Teletext page, GoalGetter was developed on the basis of D2S, a generic system for the creation of Data-to Speech systems. It consists of two modules, the Language Generation Module (LGM), and the Speech Generation Module (SGM). The LGM takes data as input.and • produces enriched text, i.e., text which is annotated with prosodic markers indicating pitch accents and international boundaries. This text is sent as input to the SGM, which turns it into a speech signal [5].

GameRecapper is a template based system which generates summaries of football matches in Portuguese where the structure input data is game sheets taken from www.zerozero.ptwebsite.In order to make summaries of game reports, D2T template-based system similar to the text generation module of the GoalGetter system is used [4].

The GameRecapper system generates Portuguese summaries of football matches. The data which forms the input of GameRecapper is retrieved from an API developed by www.zerozero.pt that transforms the information of a certain game on their webpage into a JSON tree structure. It is then converted into a JSON tree structure since it allows a logical hierarchy and ordering of information. JSON was chosen over XML since JSON doesn't require templates such as XSLT for transformation and it is more readable [4].

PASS is a data-to-text system that generates Dutch soccer reports from match statistics. This system is based on templates, and generates football reports in Dutch, starting from match statistics. For each match, two reports are produced, one for the supporters of each club that played the match; the aim is generating a report that uses tailored emotional language, e.g. ex-pressing disappointment for the loss or excitement for the victory. The templates were manually created, starting from an "affective soccer corpus, that is, summaries of the matches as published by the opposing teams, in which the emotional investment is clear. The reports generated by PASS are composed of a title, summarizing the final result, a general introduction that gives information about the opponents or the team expectations, a summary of the game course and its events, and a final debriefing with the outcome for the team [3].

3 Architecture and Methodology

The system will be based on two phases: Statistical modelling and Text generation using NLP and NLG. Initial process will involve use of statistical models to calculate and learn win percentages, game scores, key players involved and highlights from the game. The system will then make use of decision trees to select an appropriate narrative, which will determine the main components of the game story, enabling the system to put them together in a cohesive manner. Stories can be generated from point of view of either team. The stories will be more dynamic and compelling. Use of complex game related algorithms will prioritize journalism.

Figure 1 depicts the main architecture design for the proposed system in this research. According to the architecture, the generation module is mainly based on the traditional pipeline architecture [5]. As shown, the input generator works as a separate module since the text generation process only interests on the final input. This final input needs to be in a proper standard structure and in this case, it would be a json format. This json tree would characterize the basic information about a selected match. The domain data, paragraph and sentence templates are another source of input to generator module. This domain data module contains different information that helps to generate the final output. For example, it would contain the information about the teams. The coach of the team, the players who are not playing for the given match from the team, fresh players of the team are some of the information about teams. Sentence and paragraph templates are one of the main inputs to generator module. There are several similar templates which would be used according to the instance. The generator module will choose the correct template [5]. Variation in the final output depends on the sentence templates choices that are made. Templates are divided in to groups according to some criteria such as where to be used in the final output [5].

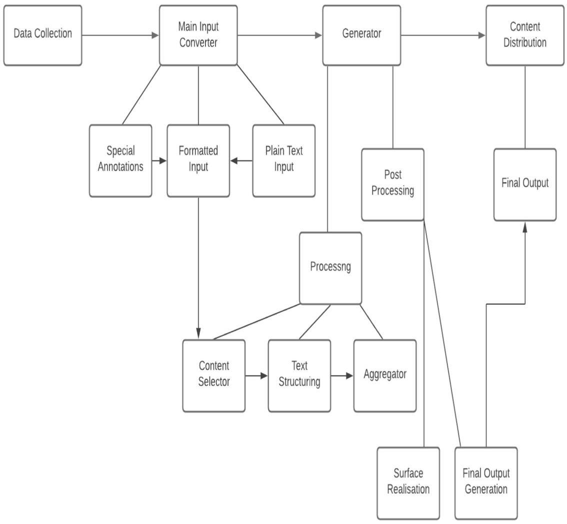


Fig. 1. Architecture diagram

The platform allows user to view latest match statistics, player and team comparisons and team schedule. In addition, the platform will allow registered users to publish articles and news stories.The game statistics will be scraped from various websites. Data about the match (for example, final result and statistics for each team, who scored and when, who was given a card by the referee),the two teams, their players, the referee and the venue (such as location, name of stadium and number of attendees) will be collected from these websites. The system involves use of statistical models to calculate and learn win percentages, game scores, key players involved and highlights from the game. Template selection will select the templates to be used among the possible templates, privileging those that are more descriptive of the match event System will make use of decision trees to select an appropriate narrative, which will determine the main components of the game story, enabling the system to put them together in a cohesive manner. Stories can be generated from point of view of either team. The stories will be more dynamic and compelling.The output of this module will be the final summary generated on the given domain.

4 Conclusion

AI journalism and automated journalism are shaking up the industry, and are bringing about changes within the profession. As we move into a networked society, software will continue to supplement journalists and provide a helping hand for media companies. They will work together to do a better job and maximize limited resources by automating processes, carrying out routine work, providing a presence across multiple locations, and conducting data research – all while cutting costs and increasing profit margin for media companies.

Algorithmic journalism may be spreading out more because of its speed and its power to deal with huge amounts of data, which will provide deeper, more specific, and also immediately available information, which can benefit society, as long as ethical rules are followed and necessary measures are taken, such as checking the input, output, and models regularly to eliminate ethical concerns, such as violations of transparency, verification, privacy, bias, etc. [6]. Moreover, automation may call for human skills, such as judgment, curiosity, and scepticism, so that we can continue to access succinct, comprehensive, and accurate news. The effects of automation on sports journalism do not exist in isolation. The effects of automated journalism have to be seen in relation to existing journalistic norms, practices, and values. Only then, can it qualify as a home run for sports news [6].

References

1. Leppanen, L., Munezero, M., Granroth-Wilding, M., Toivonen, H.: Data-Driven News Generation for Automated Journalism. Department of Computer Science, University of Helsinki, Helsinki, Finland, 10th International Natural Language Generation conference, Spain, September 4–7 (2017)
2. Robertson, J., Kirman, B.: Automatic Generation of text for Match Recaps using Esport Caster Commentaries. 1Weavr, Arena Research Cluster (ARC), University of York, York, UK, 2DC Labs, Arena Research Cluster (ARC), University of York, York, UK (2020)
3. Gatti, L., van der Lee, C.: Template-based multilingual football reports generation using Wikidata as a knowledge base. University of Twente, Enschede, The Netherlands, International Natural Language Generation Conference, The Netherlands, November 5–8 (2018)
4. Automatic Generation of Sports News João Pinto Barbosa Machado Aires DISSERTATION Mestrado Integrado em Engenharia Eletrotécnica e de Computadores Supervisor: Prof. Sérgio Sobral Nunes June 27 (2016)

5. Gunasiri, D.Y., Jayaratne, K.L.: Automated Cricket News Generation using Natural Language Generation. University of Colombo School of Computing, European Journal of Computer Science and Information Technology (2019 December)
6. Dalgali, A., Crowston, K.: Algorithmic Journalism and Its Impacts on Work. Syracuse University, USA, Woodstock'18, June, 2018, El Paso, Texas USA
7. Dörr, K.N.: Mapping the field of Algorithmic Journalism. University of Zurich, Switzerland (2016)
8. Gatt, A., Krahmer, E.: Survey of the State of the Art in Natural Language Generation: Core tasks, applications and evaluation. Journal of Artificial Intelligence Research (2018)

Brain Hemorrhage Detection Using Deep Learning: Convolutional Neural Network

Nipun R. Navadia[1](✉), Gurleen Kaur[1], and Harshit Bhardwaj[2]

[1] Dronacharya Group of Institution, Greater Noida, Uttar Pradesh, India
nipunn2011@gmail.com
[2] MIET, Greater Noida, Uttar Pradesh, India

Abstract. A brain haemorrhage is a form of stroke that occurs when a blood vessel in the brain bursts, producing bleeding in the surrounding tissues. The accurate assessment of malady and the excavation of robust and reliable measurements for sick people to define the morphological brain changes as the recovery developments are made possible by the ability to diagnose brain haemorrhage, which is primarily done through the investigation of a CT scan. Even though much research has indeed been accomplished on medical image segmentation, there's still some potential for more studies in the context of brain haemorrhage prognosis considering the low accuracy of prevailing techniques and algorithms, programming uncertainty of developed approaches, preposterousness in the real world, and a dearth of many other advancements that could make the process quite impactful and beneficial. Furthermore, many of the current techniques only target the identification of a small number of brain haemorrhage subtypes. In this paper, we are focusing on the application of convolution neural networks, which is a deep learning technique to detect brain haemorrhage, and we found that the classification accuracy of the model is 89.9% .

Keywords: Brain hemorrhage · Deep learning · Convolutional neural network

1 Introduction

Since the brain is such an intricate, delicate, and dominating organ of the body, it governs all of the body's activities [1]. Furthermore, even a little brain damage has a significant impact on the body. The brain is most likely hidden from clear sight by the protective skull. The brain can be protected from injuries via the skull, which is likely to stymie research into its usefulness. The bleeding might have negative effects on the brain by altering its normal function and structure [2]. Whenever blood vessels and aberrant cells in the brain are arranged, it typically stems from a malfunction, leading to brain haemorrhage, and the regular functioning of the brain is also harmed. The most common cause of death from solid tumour cancer in humans is brain haemorrhage.

Pathologic calcification in the human body is defined as the accumulation of calcium salts in necrotic tissue as well as the increase of calcified materials in local injuries [3].

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 565–570, 2023.
https://doi.org/10.1007/978-3-031-13150-9_46

The calcification is often shown as a high-density Hounsfield unit, comprising magnesium, calcium, phosphorus, potassium, zinc, and silicon throughout CT scans. CT scanning, as opposed to regular MRI, is more effective in detecting intracranial calcifications because it is based on the X-ray acoustic impedance.

In the unfortunate incident of traumatic brain injury, computed tomography (CT) is perhaps the most frequently utilised diagnostic imaging technology to determine the degree of brain bleeding. The identification of bleeding after a TBI is particularly time-sensitive since even a few seconds of delay might prove fatal. Traditional approaches include radiologists visually inspecting the hematoma and manually calculating the thickness of the midline displacement and hematoma. The whole operation takes a long time and necessitates the presence of skilled radiologists at all times. As a result, computerised haemorrhage detection techniques that can provide quick inference while also being precise to the standard of radiologists have the chance to save countless lives. The purpose of this study is to discuss the use of convolutional neural networks, a kind of deep learning technology, in the detection of brain haemorrhage. The model has a classification accuracy of 89.9%, according to our findings. The purpose of this study is to discuss the use of convolutional neural networks, a kind of deep learning technology, in the detection of brain haemorrhage. The model has a classification accuracy of 89.9%, according to our findings.

2 Related Work

Academic institutions as well as other research facilities across the globe began performing research on merging this medical knowledge with something like a computer-assisted system as technology improved in areas like AI technology, computer vision, deep learning, and genetic engineering, among other areas. Thus, significant research has been done in the last 30 years on brain background subtraction using MR and CT scan pictures, in addition to identifying brain haemorrhages.

The authors employed a region-expanding and thresholding approach to analyse brain segmentation using CT data, as stated in [4]. Authors in [5] employed the Fuzzy C Means Method [FCM] to segment brain MRI scans, whereas [6] used Bayesian classification to detect the distribution of various materials in MRI volumetric datasets of the brain. For the first time, the authors of [7] were able to suggest EM segmentation for MR brain pictures. As previously described in [8], the classic FCM employed in [5] was extended to reflect the quality of the MR image acquisition process, while a multi-resolution simulated annealing for brain image processing was performed the same year. We decided to look into the idea of utilising a different strategy since we believed some of the algorithms were too sophisticated and had the problems described in the preceding section.

Beginning in the year 2000, there were several techniques for brain picture classification for the diagnosis and classification of haemorrhages and strokes. A typical strategy that employs active contours was utilised in [9], and the writers in [10] offered a summary of the studies on MR brain feature extraction the following year. Several approaches for classification and assessment of tumours were developed, including manual, user-assisted by medical specialists, and completely automated systems [9], while

Liu et al. developed a common approach that used fuzzy interconnectivity and anticipation. [11] goes into further detail on this. Alternative Fuzzy C-means [AFCM] were used for medical image segmentation in [12]. Several scientists [8] discovered another reliable approach to image segmentation using a genetic algorithm for brain tumour segmentation using CT images in the past two years.

The authors have developed a 34-layer CNN architecture that accurately identifies arrhythmias from echocardiography data [14]. A viable real-world method for computerised cardiac delineation was recently proposed by the authors in [15]. Another study found that 3D neuron regeneration from electron microscopic brain pictures had superhuman accuracy [16].

Numerous attention techniques have been used in the past to direct the neural network's attention to important elements [17]. Hard and soft attention are two types of attention processes that exist today. By sampling the visuals, hard attention approaches and moves focus from one portion of the image to another [18]. Soft attention approaches, on the other hand, use probabilistic attention maps to concentrate on particular aspects more than others [19], such as those associated with a certain job [17] or various sized objects [20].

3 Experiment and Dataset

3.1 Experiment Setup

The test was run on a Macbook Pro running macOS Big Sur 11.6, with a Quad-Core Intel i5 CPU running at 2.4 GHz and 8 GB of 2133 MHz LPDDR3 RAM. The code was written in Python and used important machine learning packages.

For performing the experiment we are using CQ500 dataset. It consists of 491 scan images along with 193.317 slices. Total 205 images are of haemorrhage and remaining are showing normal state.

3.2 Implementation

For the experiment we are using Convolutional Neural Network. The Convolutional Neural Network (CNN) is an architecture that specialises in analysing matrix precision. 1-D matrix data with periodic intervals, pictures, and 2-D data with pixel matrices are the most prevalent examples. The arithmetical convolution procedure that the framework utilises inside its processing gives this sort of network its name. Convolution, in basic terms, is the action of combining two functions with a real value parameter, which is treated as:

$$s(t) = (x * w)(t) \tag{1}$$

The first parameter (x) is referred to as the input, whereas the second argument (w) is referred to as the kernel. Typically, the result is referred to as a feature map. Convolution's main purpose is to extract features from input photos.

A convolutional neural network is often separated into three stages: first, convolutional layers with ReLU (rectified linear unit) activation, and second, a pooling layer for

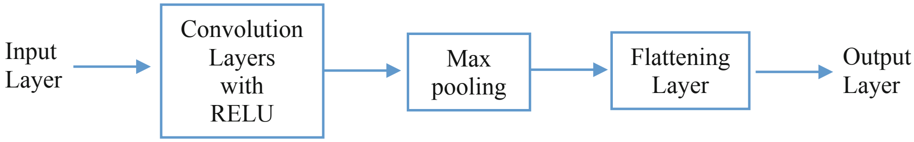


Fig. 1. Convolutional neural network architecture used for experiment

size reduction, typically max-pooling. Finally, a flatten layer is used before a completely connected layer is used to classify the features maps (Fig. 1).

We have trained the neural network with a batch sizes number of epochs but we found that batch size of 10 for 100 epochs using CQ500 dataset.

4 Result Analysis

We have trained convolutional neural network with a batch size of 10 for 100 epochs and we have acquired 89.9% accuracy. From Fig. 2 we can see that the accuracy changed with the number of epochs and quite fluctuated but at the end it was found that at 100 epochs it showed better true positive results.

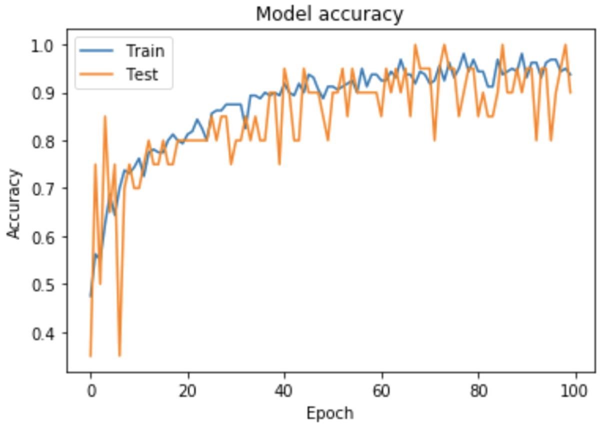


Fig. 2. Scatter plot showing relationship between the total cases and total deaths predicted

In Fig. 3 we can see the actual and predated values for some random images taken after testing the model. We had partition dataset in 70 to 30 ratio where 70% data was used to train the model and 30% data was used to test the model.

We find that there were few false positive and false negative results also.

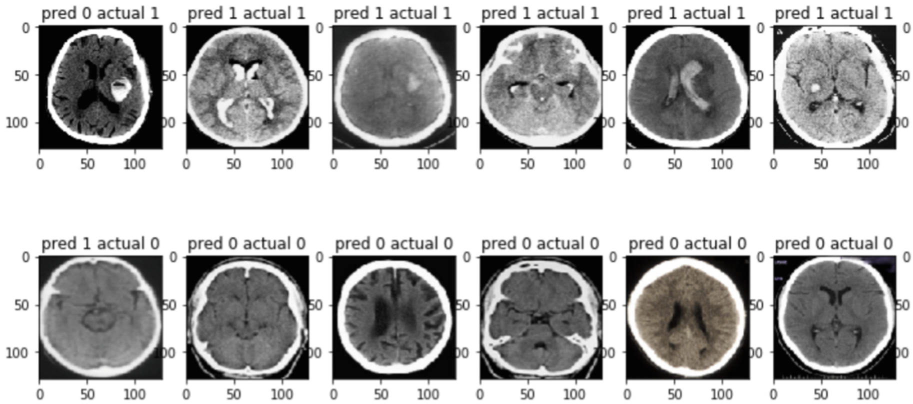


Fig. 3. This figure shows the result comparing actual and predicted values.

5 Conclusion

A lot of studies on haemorrhage identification have been conducted. Some of the research tried to identify several of the three aberrant structures in brain images: micro calcifications, haemorrhage, or both. Some techniques are based on whether the brain lesions are classified as calcification or haemorrhage. Conventional brain photogrammetry experienced problems caused by human operatives' lack of expertise, but it was also hampered by weariness and other life form variables. We explored that the Convolutional Neural Network can be one of the most effective way to detect the brain haemorrhage. We found that our model showed 89.9% accurate detection along with true positives.

It is indeed important to keep in mind that, even though suggested technique gives impressive outcomes in automated haemorrhage identification with increased precision than radiologists, there really are a slew of other potentially serious brain disorders that the offered deep learning model is ignorant of. As a result, further work in the area of numerous abnormalities identification from brain CT images is assured. As a result, the proposed method should not be construed as a viable substitute for real radiologists on the job.

The suggested deep learning algorithm shows promise as a tool for rapid detection in an exigency. Nevertheless, the approach has only been evaluated on a small sample size, and its real-world effectiveness is currently being investigated.

References

1. Arif, M., Abdullah, N.A., Phalianakote, S.K., Ramli, N., Elahi, M.: Maximizing information of multimodality brain image fusion using curvelet transform with genetic algorithm. In: 2014 International Conference on Computer Assisted System in Health (CASH). IEEE, pp. 45–51 (2014)
2. Vishnuvarthanan, G., Pallikonda Rajasekaran, M., Subbaraj, P., Vishnuvarthanan, A.: An unsupervised learning method with a clustering approach for tumor identification and tissue segmentation in magnetic resonance brain images. Appl. Soft Comput. **38**, 190–212 (2016)

3. Singh, S., Deep Gupta, R.S., Anand, V.K.: Nonsubsampled shearlet based CT and MR medical image fusion using biologically inspired spiking neural network. Biomed. Signal Process. Control **18**, 91–101 (2015). https://doi.org/10.1016/j.bspc.2014.11.009
4. Ganesan, R., Radhakrishnan, S.: Segmentation of computed tomography brain images using genetic algorithm. Int. J. Soft Comput. **4**(4), 157–161 (2009)
5. Li, C.L., Goldgof, D.B., Hall, L.O.: Knowledge-based classification and tissue labeling of MR images of human brain. IEEE Trans. Med. Imaging **12**, 740–750 (1993)
6. Laidlaw, D., Fleischer, K., Barr, A.: Partial-volume Bayesian classification of material mixtures in MR volume data using voxel histograms. IEEE Trans. Med. Imaging **17**, 74–86 (1998)
7. Wells, W.M., Grimson, W.E.L., Kikinis, R., Jolesz, F.A.: Adaptive segmentation of MRI data. IEEE Trans. Med. Imaging **15**(4), 429–442 (1996)
8. Loncaric, S., Majcenica, Z.: Multiresolution simulated annealing for brain image analysis. Medical Imaging 1999: Image Processing, vol. **3661**, pp. 1139–1146 (1997). Accessed 15 Aug 2010
9. Prastawa, M., et al.: A brain tumor segmentation framework based on outlier detection. Med. Image Anal. **8**, p275-283 (2003)
10. Cuadra, M.B., Cuisenaire, O., Meuli, R., Thiran, J.P.: Automatic segmentation of internal structures of the brain in MR images using a tandem of affine and non-rigid registration of an anatomical brain atlas. In: Proceedings 2001 International Conference on Image Processing (Cat. No. 01CH37205), vol. 3. IEEE, pp. 1083–1086 (2001, October)
11. Mohamed, R.: Comparative study of edge detection algorithms applying on the grayscale noisy image using morphological filter. GVIP J. **6**(4), 17–23 (2006)
12. Liu et al.: Hemorrhage slices detection in brain CT images. In: 19th International Conference on Pattern Recognition, 2008 (ICPR 2008), pp. 1–4. IEEE, Tampa, FL, 23 January 2009 (2009)
13. Loncaric, M.: Quantitative intracerebral brain hemorrhage analysis (1997)
14. Rajpurkar, P., Hannun, A.Y., Haghpanahi, M., Bourn, C., Ng, A.Y.: Cardiologist-Level Arrhythmia Detection with Convolutional Neural Networks (2017)
15. Lieman-Sifry, J., Le, M., Lau, F., Sall, S., Golden, D.: FastVentricle: cardiac segmentation with ENet. CoRR, vol. abs/1704.04296 (2017)
16. Lee, K., Zung, J., Li, P., Jain, V., Sebastian Seung, H.: Superhuman accuracy on the SNEMI3D connectomics challenge. CoRR, vol. abs/1706.00120 (2017)
17. Chen, K., Wang, J., Chen, L.-C., Gao, H., Xu, W., Nevatia, R.: ABC-CNN: an attention based convolutional neural network for visual question answering. CoRR (2015)
18. Ba, J., Mnih, V., Kavukcuoglu, K.: Multiple object recognition with visual attention. CoRR, vol. abs/1412.7755 (2014)
19. Zagoruyko, S., Komodakis, N.: Paying more attention to attention: improving the performance of convolutional neural networks via attention transfer. CoRR (2016)
20. Chen, L.-C., Yang, Y., Wang, J., Xu, W., Yuille, A.L.: Attention to Scale: Scale-aware Semantic Image Segmentation (2015)

An Approach for Theft Detection and Alerting System

B. C. Manujakshi[1](✉), K. B. Ramesh[2], Lalit Garg[3], and T. M. Shashidhar[4]

[1] Department of Computer Science and Engineering, Presidency University, Bengaluru, Karnataka, India
manujakshibc@gmail.com
[2] Department of Electronics and Instrumentation Engineering, RV College of Engineering, Bengaluru, Karnataka, India
[3] Department of Computer Information Systems, University of Malta, Msida, Malta
[4] Department of Computer Science and Engineering, Acharya Institute of Technology, Bengaluru, Karnataka, India

Abstract. Today there is a high rate of theft everywhere. Detecting the theft earlier is in high demand. The system which exists is popular using only using CCTV. But now a day's lots of systems are available with many advanced algorithms. It makes the process more efficient. The proposed research work discusses face recognition and also weapon detection if the thieves brought weapons. In this system, a mobile application telegram is used. The image processing system is also used to implement the application. Wi-Fi module is used to send a photo of a person if he stands near the door. If an unknown person image is detected, then a buzzer will be triggered as an alarm, and then the owner can check the camera in the telegram application. The problems of the existing systems are the intruder can be identified after the theft. The human, along with the weapon, is also not detected in the existing approaches. The work carried out in this paper detect the unknown person and design a cost-effective and more efficient system to identify the theft in real-time and send the immediate notification of the theft to the owner for further action.

Keywords: Rasberry Pi · Twillo · Weapon detection · Alerting face detection · Convolution Neural Network · HAAR Cascade algorithm

1 Introduction

In the modern era, due to the evolution of technology, there are many changes in the world. Day by day, the internet is playing a vital role in everyone's life. In this direction, many technologies are invented. This paper provides a better approach to using the recent techniques and provides the precise solution with a new design with a high level of security and notification on time. The internet of things allows connecting various devices like real-world objects using the internet. This helps to exchange the data among the objects. This system helps to provide better safety and security to the system. It interfaces the components like Raspberry Pi and sends alert messages if an unknown person tries to

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 571–578, 2023.
https://doi.org/10.1007/978-3-031-13150-9_47

enter the house. It is associated with weapon detection if an unknown person is identified with a weapon. Then the siren sound is activated, and an alert message will be sent to the owner. The scope of the work is to use the embedded system and provide the high-level security composed to the product existing in the market. The work is limited to household users. The work elaborates on the various domain knowledge. This system avoids the illegal entry of a person and provides high-level security. The work recognises the familiar faces and weapons for the proposed system. A similar type of work is carried in [8], where the driver identification is made through several steps like preprocessing, feature generation and real-time classification. CNN approaches are adopted to identify the theft. The different approaches and algorithms involved in determining the features are explained in [9]. Detecting the third party or the intruder near the door is a tedious task. In [12], authors have discussed the approaches for detecting the face and the facial expressions using the Haar cascade classifier.

1.1 The Objectives of This Work

- Design of the anti-theft security system with high efficiency, low cost and easy to operate.
- Face recognition for security.
- Alarming and alerting system.
- Notification to the owner.

2 Experimental Work

The system involves various hardware and software implementation, the discussion of the components. The hardware used in the system design is described below.

2.1 Raspberry Pi

Raspberry Pi has a 1.5 GHz 64 big quad-core ARM cortex –A-72 processor. It has 1 GB of RAM memory. This Raspberry Pi is associated with a full-sized Ethernet port, two USB 3.0 ports, two USB 2.0 ports, and two micro HDMI ports.

2.2 Pi Camera

Raspberry pi camera module is a five megapixel best designed with add on for Rasberry Pi. It has a fixed focus lens. The camera is supported with the latest version of Raspbian.

2.3 DC Motor

DC Motor is used to perform any mechanical movement that is caused by AC or DC electric motor.

3 Software Requirements

The Raspberry Pi's system resembles the normal operating system. There is a menu bar, web browser, file manager, and also it has desktop shortcuts. This OS provides faster performance for the majority of the applications. Applications use the performances through advanced instructions.

3.1 Python IDE

The Python language is an easy to learn and more efficient programming language. Data structures are the high level, simple and effective approach of object-oriented programming like python. Python is dynamic typing together with its interpreted nature. The python can be easily extended with new functions and data types.

3.2 Open CV

The Open CV as a programming library is used in real-time computer vision. Its binding is done with python, Java and Mat Lab. This open CV runs on many platforms. It can be used for facial recognition gesture recognition. The OpenCV is an authentic application for detecting faces [1].

4 Face Recognition

Many researchers have worked in the field of image recognition. A lot of contributions have been made in the area of the image processing domain. Deep learning comes as the category of neural network that takes the metadata as an input. It will process this data in several layers of the non-linear transformation and compute the output classification [10]. Different approaches are studied to carry out the proposed work.

4.1 Haar Cascade

The Haar cascade classifier is used to analyse the pixels in the image into squares by function. This uses the integral image concepts which are used to compute the features. In [11], the author discusses the usage of Haar cascade classifier to detect the human presence on the thermal images. In this paper, Haar cascade uses the ADA boost learning algorithm. Every small number of features will be considered to give an efficient result. Then we use the cascading technique to detect the face in an image. The Haar uses the features on the images and finds it easier to find the edges or the lines in the image [2]. The AdaBoost algorithm is an efficient algorithm in machine learning. This is referred to as an adaptive boosting algorithm. The weights will be reassigned to the instances. The higher weights are incorrectly classified instances. The boosting will reduce the bias and the variance for supervised learning. The learners will grow sequentially in the adaBoosting algorithm.

4.2 Feature Extraction

The Haar cascade uses the machine learning technique. In this method, a function is trained from positive and negative images. This algorithm uses feature extraction. The Haar feature is similar to the sub-window. It is discarded if it fails in any of the stages.

5 Convolutional Neural Network

The convolution neural network is used to analyse the visual image. Object detection is the commonly used algorithm for machine vision. It is used to get faster and accurate outputs. There is an increase in the data. This increase in data leads to rich information for training the data object classifiers. The CNN gives excellent performance when we work on the image data [3]. CNN is the rapidly developing field of machine learning. The CNN involves the multi-layer perceptron used to recognise the two-dimensional shapes [6].

Object detection algorithms are famous for detecting objects. The images need to be preprocessed and passed through the deep convolution network to obtain or extract the distinguishing features. Every layer results in a matrix. It is the result of the mathematical operation performed on the matrix. The sliding window approach is used for each segment of the image. It will check if there is any frame containing an object. In the neural network, we can add a layer to detect automatically. This is possible if more training examples are taken for implementation. The convolution neural network is essential for deep learning algorithms, like face recognition or object detection. The convolution neural network architecture is shown in Fig. 1.

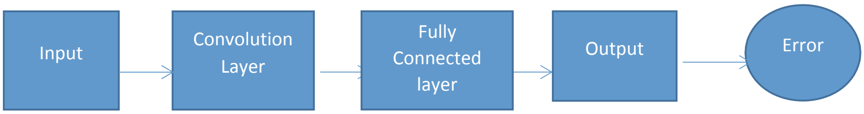


Fig. 1. Convolution neural network architecture

In [7], the CNN large size image recognition needs to be done then a small size local data will be collected from the training sample. Some features are learned from these samples from the small sample, and they will be used as filters with the original image for CNN operation. In the convolution technique, we divide the entire image into small equal parts. These parts are called tiles. Each of these tiles is traversed through the small neural network, and the result is saved into an array. An array is high dimensional. So it can be used to reduce it to a lower dimension using downsampling. Every array is processed in a square grid, and it will be stored in an output array. The process we call a max pooling. Each matrix will be extracted from the max pooling will have an array of numbers.

The convolution is mathematically represented with the asterisk * sign. The input image is represented as X, and the filter will be f then the expression could be defined as,

$$Z = X * f$$

It can be given to get a feature vector with only a single column of numbers. This array will be passed into a neural network with a fully connected layer. The above steps will be repeated in different combinations to get the complex networks. In this way, it helps to learn more features when the number of convolution layers increases. The goal of the process is to reduce into simple features which help to distinguish the images.

6 System Design

An anti-theft system requires the hardware and software part to perform the functionality. The mobile applications capture the photo and send it to the owner with the telegram. The owner has a provision to control the locker with on and off operations. This will be done with the help of the mobile application. The OpenCV is used to implement the image processing algorithm. This OpenCV is compatible to run raspberry pi. The hardware components used to implement the work is raspberry pi 3 model B, solenoid electric door locker, keypad, 1620 LCD, ultrasonic sensor module and the buzzer. The raspberry pi will take the responsibility to process the complete workload. The sensor detects a person if he comes near the door, and then the trigger will activate the camera to capture the person's face, and it compares with the database. If the camera detects the stranger, it will notify the owner with the telegram via Wi-Fi. Immediately an alert message will be given with the buzzer. If the person image is matched with the database, then the password needs to be given to unlock the door.

6.1 Process of the System

Raspberry Pi
The raspberry pi is the main component that runs all the components. The main.py. led_vkey.js, lockstcheck.py and telegrambot.py are the codes that run on the raspberry pi. The main.py is a function to control the locker. The telegrambot.py is used to allow the communication between the telegram and raspberry pi. For the door access records, we can use lockstcheck.py to know locked and unlocked structures.

Telegram
The telegram helps the application to capture the photo. This controls the locker to be available in on and off status. The command "C". Command "S" can be used to start the live cam. To end the cam, use the command stop. The shutdown and Rbt are the commands used to turn off the system and reboot the system. The telegram is the best customer end application used to securely transmit the information through the layers of IoT architecture [4].

Raspbian Operating System
It is necessary to install the operating system called Raspbian to work with the Raspberry Pi. Fig. 2 is the home page of the Rasbian operating System. Once the operating system is installed, the Raspberry Pi will be booted. It will have the system configuration. We can change the system password, update the settings, set the hostname, and create a new

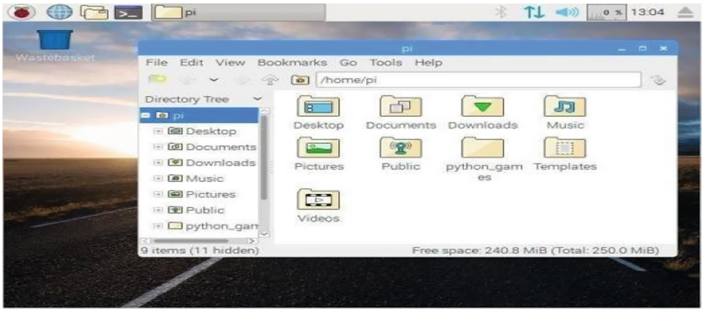


Fig. 2. Rasbian operating system

user. Raspberry pi needs to be connected via the internet. The fixed IP address will be assigned with Raspberry Pi.

VNC Viewer

The VNC viewer enables the VNC server by selecting the Menu, preferences, Rasberry Pi configuration, Interfaces. After that, select enabled for VNC. It will open the VNC server. Once the top right corner menu is clicked, select the licensing and sign in to the VNC account. The file option on the top left will be clicked to establish the new connection. The IP address in the VNC server should be given, then click on OK. It will enable the VNC viewer, as shown in Fig. 3. Raspberry Pi can be connected by double-clicking the connection. Once all the above connections are established, username and password will be given, and VNC set up will be completed [5].

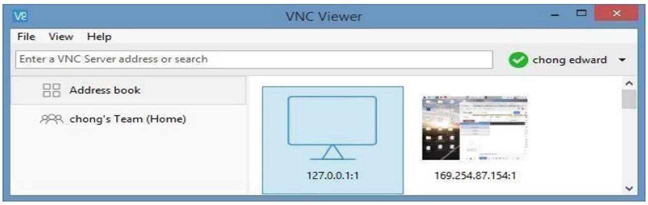


Fig. 3. VNC viewer

Experimental Results

The work is carried out using all the components mentioned above. The experimental results are shown in Fig. 4, Fig. 5, Fig. 6, Fig. 7 and Fig. 8.

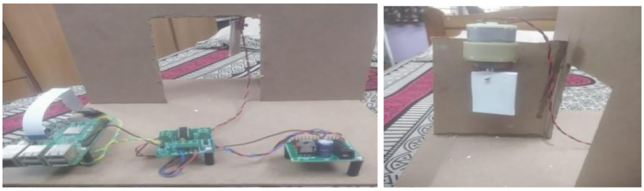


Fig. 4. Experimental setup

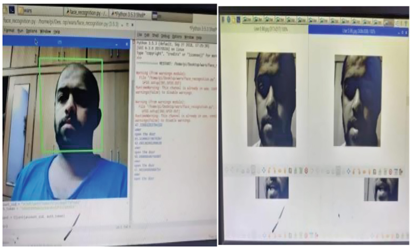


Fig. 5. Face detection of a known person

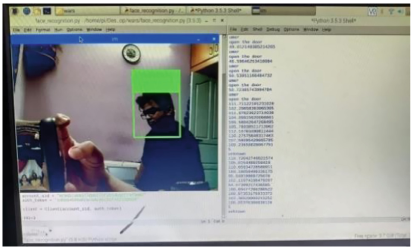


Fig. 6. Face detection of unknown person

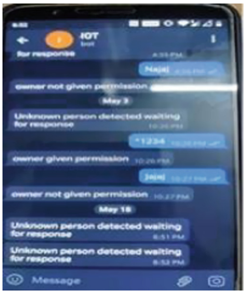


Fig. 7. Unknown person Identified message

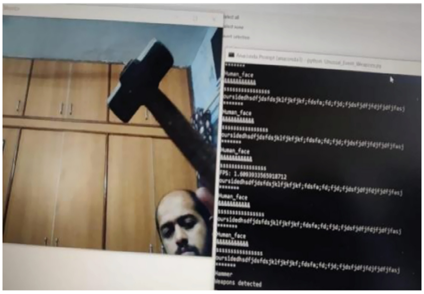


Fig. 8. Unknown person with weapon detection

Conclusion

This "Theft detection and alerting system" can be implemented in many places as security cameras are used almost everywhere today. With the perks of detecting face and weapon, this system is more efficient and is more reliable as the owner will be notified in real-time, bringing down the risk of theft. There are still a few drawbacks that can be upgraded in the system and make it a fully functioning system that can be used in the real world to deal with home security threats. The project's main aim is to design an alert and anti-theftsystem that is both cost-effective and efficient to use. The system is designed to detect the face, recognise the insider and stranger, and allow the owner to give authentication to allow people not in the database. Appropriate hardware and software are used as they are the crucial component to perform the task. Therefore, the prototype designed detectsthe face and weapon, which can be very helpful in security.

References

1. Naveenkumar, M., Vadivel, A.: OpenCV for computer vision applications. In: Proceedings of National Conference on Big Data and Cloud Computing (NCBDC'15) (20 Mar 2015)
2. https://towardsdatascience.com/face-detection-with-haar-cascade-727f68dafd08
3. Albawi, S., Mohammed, T.A., AlZ, S.: Understanding of a convolutional neural network. International Conference on Engineering and Technology (ICET) **2017**, 1–6 (2017). https://doi.org/10.1109/ICEngTechnol.2017.8308186
4. Anvekar, R.G., Banakar, R.M.: IoT application development: home security system. IEEE Technological Innovations in ICT for Agriculture and Rural Development (TIAR) **2017**, 68–72 (2017). https://doi.org/10.1109/TIAR.2017.8273688
5. https://magpi.raspberrypi.org/articles/vnc-raspberry-pi
6. Wang, Y., Ke, W., Wan, P.: A method of ultrasonic image recognition for thyroid papillary carcinoma based on deep convolution neural network. NeuroQuantology **16**(5), 757–768 (2018). https://doi.org/10.14704/nq.2018.16.5.1306
7. Al-Saffar, A.A.M., Tao, H., Talab, M.A.: Review of deep convolution neural network in image classification. In: 2017 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications
8. Abu-gellban, H., Nguyen, L., Moghadasi, M., Pan, Z., Jin, F.: LiveDI: An Anti-theft Model Based on Driving Behavior. IH&MMSec '20, June 22–24, Denver, CO, USA (2020)
9. Rere, L.M.R., Fanany, M.I., Arymurthy, A.M.: Metaheuristic algorithms for convolution neural network. Comput. Intell. Neurosci. **2016**, 1–13 (2016). https://doi.org/10.1155/2016/1537325
10. Traore, B.B., Kamsu-Foguem, B., Tangara, F.: Deep convolution neural network for image recognition. Ecological Informatics **48**, 257–268 (2018). https://doi.org/10.1016/j.ecoinf.2018.10.002
11. Setjo, C.H., Achmad, B., Faridah: Thermal image human detection using Haar-cascade classifier. In: 2017 7th International Annual Engineering Seminar (InAES), pp. 1–6 (2017). https://doi.org/10.1109/INAES.2017.8068554
12. Gangopadhyay, I., Chatterjee, A., Das, I.: Face detection and expression recognition using haar cascade classifier and fisherface algorithm. In: Bhattacharyya, S., Pal, S.K., Pan, I., Das, A. (eds.) Recent Trends in Signal and Image Processing: Proceedings of ISSIP 2018, pp. 1–11. Springer Singapore, Singapore (2019). https://doi.org/10.1007/978-981-13-6783-0_1

Author Index

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 579–580, 2023.
https://doi.org/10.1007/978-3-031-13150-9