Check for updates

Fuzzified Deep Learning based Forgery Detection of Signatures in the Healthcare Mission Records

ISHU PRIYA, Dr B R Ambedkar National Institute of Technology, India
NISHA CHAURASIA, Dr B R Ambedkar National Institute of Technology, India
ASHUTOSH KUMAR SINGH, Birla Institute of Technology and Science, India
NAKUL MEHTA, Dr B R Ambedkar National Institute of Technology, India
ABHISHEK SINGH KILAK, Engineering College Bikaner, India
AHMED ALKHAYYAT, College of Technical Engineering, The Islamic University, Iraq

In an era subjected to digital solutions, handwritten signatures continue playing a crucial role in identity verification and document authentication. These signatures, a form of bio-metric verification, are unique to every individual, serving as a primitive method for confirming identity and ensuring security of an individual. Signatures, apart from being a means of personal authentication, are often considered a cornerstone in the validation of critical documents and processes, especially within the healthcare sector. In healthcare missions, particularly in the regions that are underdeveloped, hand-written records persist as the primary mode of documentation. The credibility of these handwritten documents hinges on the authenticity of the accompanying signatures, making signature verification a paramount safeguard for the integrity and security of medical information. Nonetheless, traditional offline methods of signature identification can be time-consuming and inefficient, particularly while dealing with a massive volume of documents. This arises the evident need for automated signature verification systems. Our research introduces an innovative signature verification system which synthesizes the strengths of fuzzy logic and CNN (Convolutional Neural Networks) to deliver precise and efficient signature verification. Leveraging the capabilities of Fuzzy Logic for feature representation and CNNs for discriminative learning, our proposed hybrid model offers a compelling solution. Through rigorous training, spanning a mere 28 epochs, our hybrid model exhibits remarkable performance by attaining a training accuracy of 91.29% and a test accuracy of 88.47%, underscoring its robust generalization capacity. In an era of evolving security requirements and the persistent relevance of handwritten signatures, our research links the disparity between tradition and modernity.

Additional Key Words and Phrases: Machine Learning, Deep Learning, Neural Network, Convolutional Neural Network, Fuzzy Logic, Offline Signature, Handwritten Signature, Healthcare Records

1 INTRODUCTION

In recent times, offline signature forgery detection has drawn a lot of attention of researchers. Hand-written signatures are a crucial component of identity verification and document confirmation in the healthcare sector. Under the healthcare missions, the database is maintained by making entries for each treatment where signature is the most critical aspect of verifying the treatment offered. However, it is also the most forged entry while uploading / maintaining the records. In underlying facts, the system in practice for detecting forgery should be

Authors' addresses: Ishu Priya, ishup.cs.21@nitj.ac.in, Dr B R Ambedkar National Institute of Technology, Jalandhar, Punjab, India, 144011; Nisha Chaurasia, chaurasian@nitj.ac.in, Dr B R Ambedkar National Institute of Technology, Jalandhar, Punjab, India, 144011; Ashutosh Kumar Singh, ashutoshsingh24@pm.me, Birla Institute of Technology and Science, Pilani Campus, Vidya Vihar , Rajasthan, India; Nakul Mehta, nakulm.it.20@nitj.ac.in, Dr B R Ambedkar National Institute of Technology, Jalandhar, Punjab, India, 144011; Abhishek Singh Kilak, abhishekkilak@gmail.com, Engineering College Bikaner, Bikaner, Rajasthan, India, 334004; Ahmed Alkhayyat, ahmedalkhayyat85@iunajaf.edu.iq, College of Technical Engineering, The Islamic University, Najaf, Iraq.

Publication rights licensed to ACM. ACM acknowledges that this contribution was authored or co-authored by an employee, contractor or affiliate of a national government. As such, the Government retains a nonexclusive, royalty-free right to publish or reproduce this article, or to allow others to do so, for Government purposes only.
© 2024 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM 2375-4699/2024/1-ART
https://doi.org/10.1145/3641818

Just Accepted

able to discern signatures from signed papers and verify them. But there are numerous difficulties on the horizon. One of the primary concerns in signature-related processes is the prevalence of low-quality signature images. Apart from this, it may be a difficult task to verify a cropped signature as it may contain immaterial background context from the document. Besides, some fake signatures closely resemble the real ones, making verification a harder problem to deal with.

By affirming the signature on a variety of medical documents, such as prescriptions, consent forms, and other legal documents, the suggested system seeks to assure the legitimacy and confidentiality of medical information. To achieve high accuracy in signature verification, a combination of multiple methods can be employed. Our methodology takes into account the amalgamation of fuzzy logic and CNN model considering the benefits offered by these techniques. The fuzzy logic-based solution accounts for variations in the data while taking into consideration the imprecise nature of handwritten signatures. Based on the trained dataset, the CNN model applies a deep learning approach in order to extract features and categorize the signature as real or fraudulent.

1.1 Need for an Automated Signature Verifier

On many different kinds of documents, like legal documents, bank cheques, medical prescriptions, etc., handwritten signatures can be spotted. Given the large number of these documents, which is still growing day-by-day, an automated system for signature verification is preferred which needs to be highly dependable and accurate. An automated signature verifier can be substantially important in healthcare organizations to improve the efficiency and security of healthcare documents. Jungpil Shin and Tomomi Kikuchi [43] worked on proposing an algorithm to build a signature verifier using fuzzy set theory.

1.2 Role of a Deep Neural Network

Since, it is a well-known fact that ANNs do not work efficiently on image data as it requires the 2D images to be converted into 1D space, which is a difficult task for ANN to perform, hence, Convolutional Neural Networks (CNNs) are the best suitable method for image classification problems [52]. The image pooling property of CNN adds to its functionality enabling it to scrutinize images more easily than ANN. Thus, the proposed system makes use of a CNN classifier which is discussed in the upcoming sections.

1.3 Role of a Fuzzy Logic System

In general, fuzzy logic is nothing more than a set of rules. Fuzzy sets comprise vague or imprecise data [49]. A fuzzy logic system tells the degree of truth instead of the actual truth which in the simplest terms means that a fuzzy logic defines that a statement may or may not be true. Because of these perks of fuzzy logic, many researchers have worked on studying the application of fuzzy logic systems in the field of hand-written image recognition [15].

Fig. 1 depicts the basic difference between crisp (boolean) logic and fuzzy logic.

In brief, to comment on why there is a need to explore fuzzy logic when we already have the concept of crisp (boolean) logic is because fuzzy logic does not require explicit inputs to work on as these systems are capable of incorporating imprecise data [36], which is not applicable in case of crisp system. One of the main advantages of using fuzzy logic in signature verification is its ability to extract features that are robust to variations in the signature such as size, rotation, and slant.

Although NN is a well-capable classifier, the vitality of infusing fuzzy logic with NN offers a unique advantage. A fuzzy logic system is heavily dependent on the generation of rules and membership functions to yield output. But to generate these rules, domain expertise is required, which might not always be available. Hence, to deal with this limitation of the fuzzy classifier, a neural network (NN) can be trained which can then be used to

Just Accepted

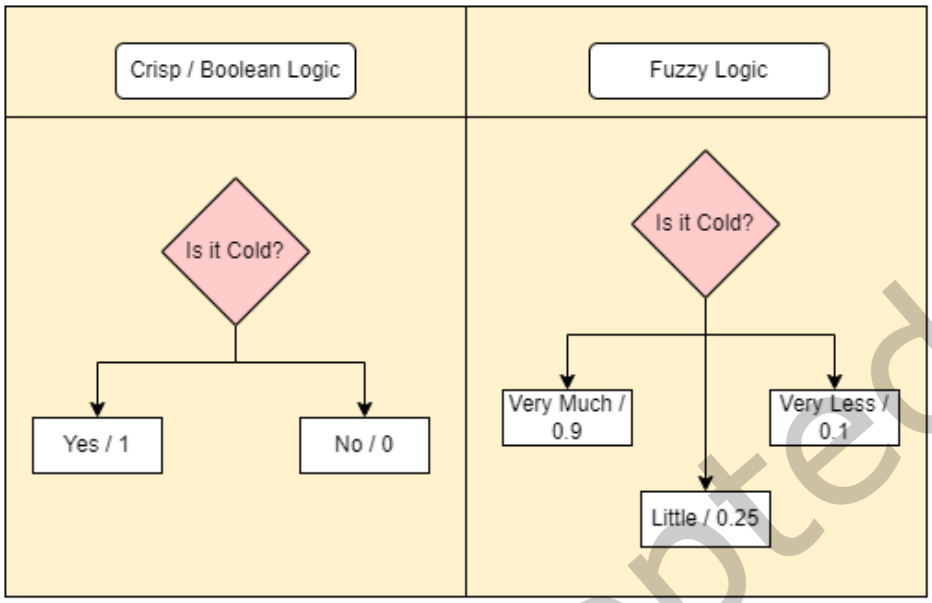


Fig. 1. Boolean Logic v/s Fuzzy Logic

generate these rules [25] [42]. Several researchers conducted detailed surveys of work done so far in this domain by making use of NNs and fuzzy logic-based systems, thus, helping them get better insights into their research [32] [9] [22]. These surveys also helped the researchers to strengthen their much valuable contributions by helping others to readily understand the ongoing trends in this domain.

2 MOTIVATION OF OUR RESEARCH

This section elucidates the core motivations and significance underlying our research endeavors majorly focused on signature verification through the amalgamation of Fuzzy Logic and CNN, within the intricate realm of the healthcare sector. Understanding the rationale for this research is crucial for discerning the potential impact and relevance of our work. These pivotal aspects have been thoughtfully visualized in the diagram presented in Fig. 2, enhancing the clarity of our research's context and impact.

2.1 Enhanced Security

- **Access Control**: Healthcare organizations handle vast amount of sensitive patient data, making it imperative to safeguard this information from unauthorized access and potential breaches. Thus, this drove the key motivation behind our research in this field to enhance the security and access control in healthcare institutions. Signature verification not only offers a robust and non-invasive method for verifying the identity of healthcare professionals, but also ensures that only authorized personnel gain access to patient records.
- **Prevention of Unauthorized Access**: Another key aspect to be considered lies in prevention of unauthorized access. Unauthorized access to patient records can lead to identity theft, privacy breaches, and misuse

Just Accepted

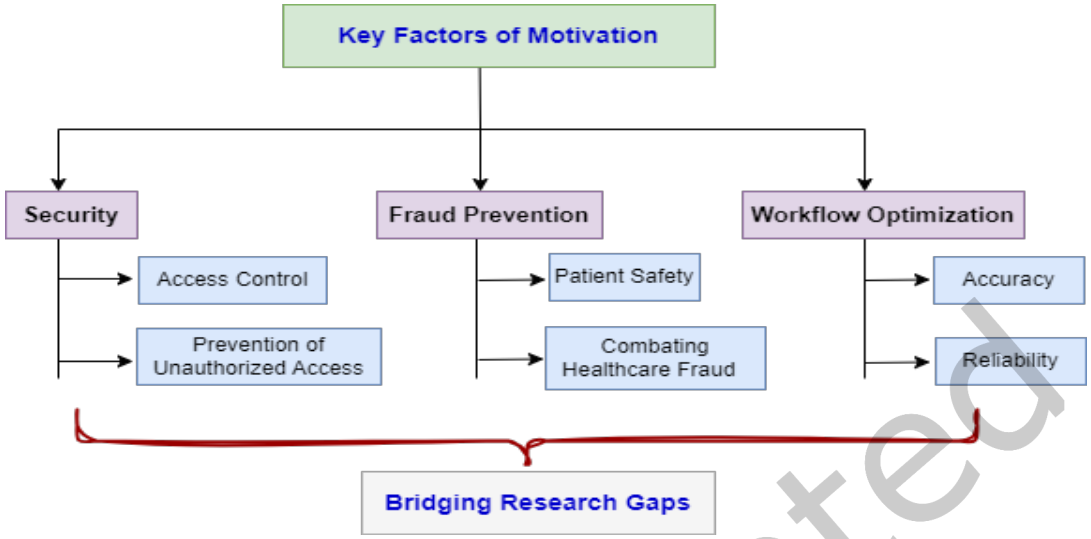


Fig. 2. Motivation behind our Research

of sensitive medical information. By implementing an effective signature verification system, we aim to prevent unauthorized access, safeguarding patient confidentiality, and privacy.

2.2 Fraud Prevention

- **Patient safety**: Patient safety is paramount in healthcare settings. Accurate signature verification ensures that only authorized healthcare providers access patient records, reducing the risk of medical errors and enhancing patient safety.
- **Combating Healthcare Fraud**: Healthcare fraud is a global issue with significant financial implications, costing billions of dollars annually. Our research seeks to address this concern by deploying signature verification as a tool to validate signatures on critical documents such as insurance claims, prescriptions, and medical records. This can help in reducing fraudulent activities within the healthcare sector.

2.3 Workflow Optimization

- **Accuracy**: The healthcare industry faces increasing administrative burdens. Our research endeavors to streamline administrative workflows by automating signature verification processes. This automation can lead to improved efficiency and reduced administrative overhead, allowing healthcare professionals to allocate more time and resources to patient care.
- **Reliability**: Fuzzy logic, in conjunction with CNN, offers a promising approach for signature verification. Fuzzy Logic accommodates the inherent variability and uncertainty in human signatures, while CNN can extract intricate features from signature images, resulting in high accuracy and reliability in the verification process.

Bridging Research Gaps: Overall, our research bridges a potential gap in the existing literature by applying advanced technologies like CNN and Fuzzy Logic to the domain of signature verification in healthcare. This interdisciplinary approach contributes to the advancement of both signature verification methods and healthcare technology.

Just Accepted

In conclusion, this section has outlined the motivations and significance of our research on signature verification using Fuzzy Logic and CNN in the healthcare sector. By addressing security, fraud prevention, workflow optimization, and legal compliance, our research aims to make valuable contributions to the healthcare industry, enhancing patient safety and data security.

3 KEY CONTRIBUTIONS OF OUR RESEARCH

An illustrative overview of the key advancements emanating from our extensive research efforts conducted in the domain of healthcare record signature verification has been presented in Fig. 3.

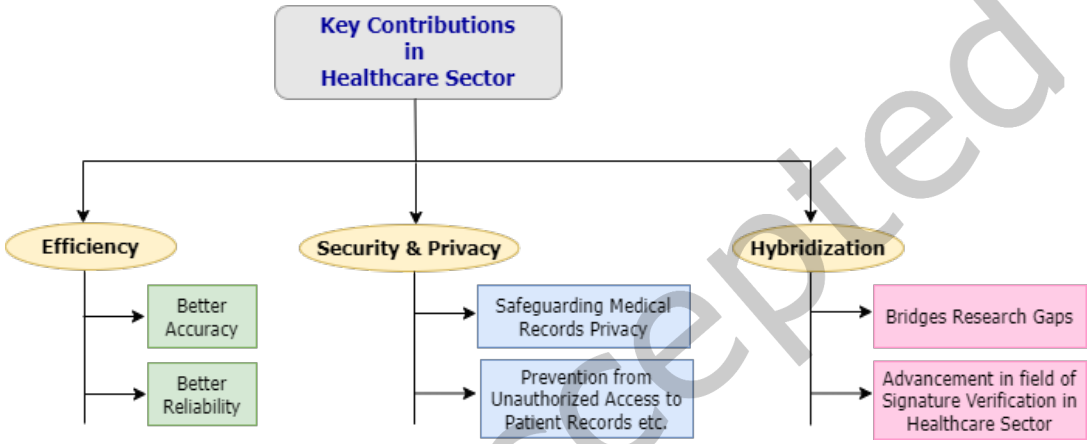


Fig. 3. Key Contributions of our Research

Just Accepted

- This paper commences by conducting an extensive literature review of the already established techniques of signature verification, critically evaluating their strengths and limitations. This examination pinpoints the areas that require enhancement, laying the groundwork for the paper's forthcoming creative developments.
- Moreover, our research bridges existing gaps in the literature by applying advanced technologies, such as CNN and fuzzy logic, to the specific context of healthcare signature verification. This interdisciplinary approach not only advances the field of signature verification but also opens doors to broader applications requiring authentication and access control.
- Our research significantly contributes to the healthcare sector by introducing a novel approach to signature verification. By combining Fuzzy Logic and CNN, we have developed an innovative method that enhances the accuracy and reliability of signature verification processes. This contribution is particularly valuable in the healthcare sector, where precision and security are paramount.
- Furthermore, our work addresses the pressing need for enhanced security measures in healthcare institutions. We provide a solution that helps prevent unauthorized access to patient records and sensitive information. This not only safeguards patient privacy but also aligns with the stringent data security requirements.
- Patient safety, a paramount concern, benefits from our work as we ensure that only authorized personnel access patient records. This reduces the risk of medical errors and ensures that crucial decisions regarding patient care are made by the right individuals.

4 REVIEW OF LITERATURE

Signature verification is a widely researched topic, and the use of fuzzy logic & neural networks has shown promising results in matters of model performance. The literature survey done in this section aims to review existing research on signature verification using various methodologies, majorly focusing on the applications of Fuzzy Logic and NNs, and identifying strengths, limitations, and potential areas for future research.

Fig. 4 presents the key areas that have been explored in the literature survey to investigate the working of various categories and methodologies employed in healthcare missions' signature verification.

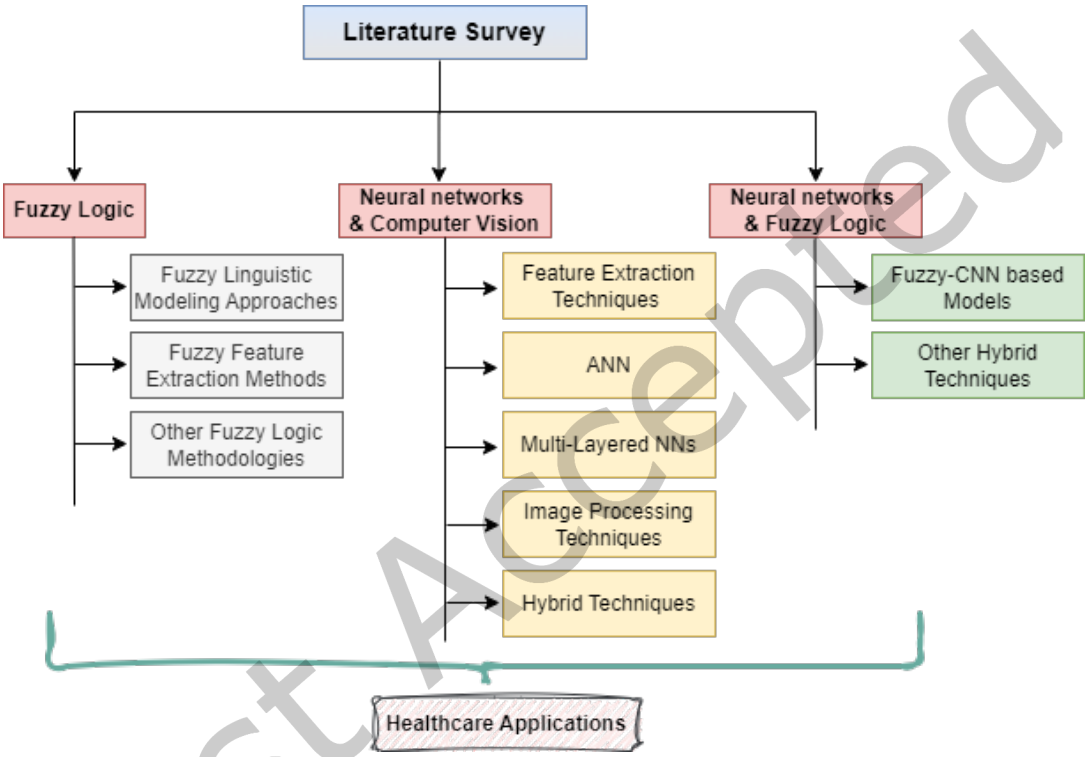


Fig. 4. Categorization of Literature Survey

Just Accepted

4.1 Healthcare Sector

Qi Chen et al [10] presented a post-processing approach to enhance the accuracy of doctor's hand-writing recognition in the medical field. The approach involves several steps. Firstly, the handwriting is recognized using an optical character recognition (OCR) system. Then, the recognized text is processed using a medical knowledge base to correct errors and improve the accuracy of the recognition. With a digital pen, nine different medical instances presented by the doctor were noted along with some medical descriptions of the patients. This data was given as input to the model. The conducted experiment yielded an accuracy of Best Confidence to be 82% and that of post-processing, 87%. Thus, showing that the post-processing approach yielded better results.

Lovely Joy Fajardo et al [14] presented a study on cursive handwriting of doctors using the deep CRNN methodology. In this study, two models were assessed, CRNN with model-based normalization scheme being

preferred as compared to CRNN alone. The validation accuracy being 72% for validation set that was taken from the remaining 540 prescription picture photos, this study was able to obtain a training accuracy rate of 76% and effectively integrate the model developed in a mobile application. OpenCV python and Tensorflow was used to build the model. Validation of the mobile application was done a second time with 48 examples of researchers' hand-writing that were taken. Of the 48 photos, 17 were properly identified, giving a 35% validation accuracy. Also, the conducted study had certain limitations which were left to be tackled in the future endeavors.

A mobile app having the ability to scan and interpret handwritten medication names, and subsequently generate legible digital text representation of the medication and its dosage, Esraa Hassan et al [20] suggested a system in this study that offers a solution for both the chemist and the patient. Using some preprocessing techniques, like image subtraction, noise reduction etc., the system recognises names of the medications and their dosages for the obtained data set. Next, pre-processed images will go through certain processing, have features extracted using CNN, and then, in the post-processing phase, a low-accuracy OCR approach will be applied to the drugs to determine their names by assessing the results with the dataset that contains all medicines. The suggested method was evaluated utilizing several real-world scenarios and demonstrated a (CNN) model accuracy of 70%. Also, scope for further research was left undiscovered.

Prescriptions written by doctors by hand are frequently regarded as being unreadable. Medical terminology uncertainty can have catastrophic effects. Thus, Riya Patil et al [34] worked together to propose a technique to recognise medication names written in a doctor's handwriting. With the assistance of several doctors, a corpus of 600 photographs was created. For the same, a comprehensive list of 50 medications was employed. CRNN-CTC model recognition was carried out with 93.3% accuracy. Edit distance procedures were further developed and examined in order to address faults created in the detected text. A fuzzy matching block that outputs the right term was added to the model in order to enhance the incorrect predictions made by it.

Seerat Rani et al [39] highlighted the significance of patient record keeping medical treatment & diagnosis emphasizing need for accurate as well as reliable prescription writing. The authors proposed an innovative solution in the form of an online system which allows doctors in writing prescriptions on a tablet by making use of a stylus. The system utilizes medicine recognition software and signature verification technology to enhance accuracy of prescription reading and interpretation, thus minimizing the risk of error. The proposed system collects a range of information about the prescription, including the coordinates of pen, time, and pen-up/down features, which are used to identify and verify the doctor's handwriting. A dataset of 24 medicine names collected from two users was used to test the system, and the outcomes drawn showed that the SVM classifier yielded accuracies ranging from 38.5% to 84% for 9 users. These findings indicate that the proposed system possesses the capabilities to significantly enhance the accuracy & reliability of prescription writing and interpretation, ultimately enhancing patient safety and well-being.

Dinuka Kulathunga et al [27] presented research that aims at improving the accuracy of extracting the medication information from handwritten medical prescriptions and reduce the risk of misreading errors. To achieve this goal, the researchers developed an image recognition system that utilizes OCR and NER techniques to draw out medical information out of the uploaded prescription images. This system works by converting the image into an unstructured textual data through OCR & segmentation, and next using NER to break down the medical data into various fields. The approach was tested and compared with existing solutions, and the outcomes yielded that the system attained better accuracy levels due to its domain-specific approach. The system achieved a 64-70% level of accuracy in recognizing doctors' hand-writing and a 95-98% level of accuracy in categorizing medical information from prescription formats.

Dr. E. Kamalanaban et al [13] proposed a solution to the problems with reading doctor's prescriptions, named Medicine Box, a hybrid of a mobile application and a smart medicine box. CNN was used to identify handwritten drug names and generate digital text that is readable. To match partial texts with the appropriate medicine name. Tensorflow was used as the ML library along with a Custom Repository to pair text with the appropriate drug

Just Accepted

name, thus helping the layman as well as the pharmacists to easily understand the doctor's prescription. To sequence handwriting, the IAM dataset was used. Patches of text were passed to the NN to make it acquainted with the doctor's writing style. The text was cropped and patches were formed using a simple generator function in python. LSTM from RNN was used to make predictions of the next character in images. CNN was built using keras with Tensorflow, the activation functions being ReLU and Softmax. Android platform was used for conversion of smart applications.

Roger Achkar et al [2] proposed a methodology to develop a model built up using ANN that works on recognition of handwritten medical prescriptions in English. Deep CRNN was used to train the supervised system, segmentation of input images was performed and classification was done into 64 different (predefined) characters. The model was implemented using python. The results were recorded using a log file. 203 epochs were required to finish the training. Several modifications were performed to improve the results. 50 prescriptions in total were used for testing, and 45 of the findings were accurate (with a 10% inaccuracy). The model yielded quite promising results with an accuracy of 95%. Also, scope for implementing the project as a mobile application was left for future endeavors to make it accessible on a larger scale.

Neha Nayak et al [33] worked on developing an application to aid identification of descriptions and names of the medicines prescribed using OCR, machine learning and image recognition. The application holds significant potential in benefiting patients and pharmacists alike by addressing the issue of handwritten prescription misinterpretation. The mobile app was built using android studio and ML model was implemented using python to accurately identify the medical prescriptions. The dataset was collected from various resources such as Kaggle & UCI. Transformer model was used for text recognition. To enable seamless integration "django" was used for backend, and to store & manage the data "firebase" was used.

W.R.A.D Wijewardena [47] proposed a neural network based system to facilitate character recognition and knowledge-based matching to correctly identify medical prescriptions. The authors proposed a CNN model for feature extraction of handwritten character images amalgamated with RNN (LSTM) for accurate identification of these characters. The authors worked on IAM dataset to develop the model. The Connectionist Temporal Clasification algorithm is used to decode the RNN generated output matrix into final text. To retrieve the most relevant drug name matching algorithm is used to compare perceived words against Knowledge base. Also, the segmentation of the prescription image lines was done using Adobe Photoshop CC 2015. The model yielded 63.10% accuracy.

Table 1 summarizes the techniques utilized for signature forgery detection in Healthcare Sector.

4.2 Fuzzy Logic

Yan Solihin et al [45] proposed an image enhancement method to extract handwritten images from a document by making use of fuzzy logic. This method was put forward to refine the pre-processing of handwritten documents. It suggests fuzzy-based if-then rules which are mainly put-up onto two fuzzy sets thus resulting in improved efficiency and accuracy. The researchers applied the if-then fuzzy rules based on an assumption that foreground (hand-writing) and the background can be separated on the basis of their intensities. The membership functions used for the same are represented in Eq. (1) and Eq. (2).

Membership function used for "Foreground":

$$\mu_f(x) = \begin{cases} 1, & \text{if } 0 \le x < A \\ \frac{(C-x)}{(C-A)}, & \text{if } A \le x < C \\ 0, & \text{if } C \le x < 255 \end{cases} \tag{1}$$

Just Accepted

Table 1. Techniques used in Healthcare Sector

Ref.	Year	Methodology	Findings
[10]	2010	Image Segmentation, Character Recognition using Lipi Toolkit, Image Restoration	The authors successfully proposed in the model that post-processing method helps increasing the accuracy for handwriting recognition.
[13]	2018	CNN, LSTM, (RNN), TensorFlow Lite Converter, Native Development Kit	The model returns readable digital text from doctor's prescription.
[2]	2019	ANN, Deep CRNN, RNN (LSTM), Image Segmentation, OCR	The researchers proposed a CRNN system to recognise text words from doctors' prescriptions which yielded remarking results.
[14]	2019	Deep CRNN, Image Processing, Connectionist and Temporal Classification, BLTSM, token-passing algorithm & beam search	Testing accuracy = 72% for first set, Validation accuracy for second set = 35%.
[27]	2020	OCR, Image Segmentation, NER (NLP), spell correction mechanism, Otsu's binarization	The model gave 64-70% accuracy for doctor's handwriting recognition and also depicted promising results for categorization of medical information.
[20]	2021	CNN, Optical Character Recognition, Image Processing	Training accuracy = 73%, Testing accuracy = 50%.
[47]	2021	CNN, RNN (LSTM), Matching algorithm, Adobe Photoshop CC 2015, CT Classification	The proposed system gave an accuracy of 63.10% also leaving scope for further research.
[34]	2022	CRNN, Connectionist-Temporal classification, Damerau-Levenshtein distance, Fuzzy Logic (matching)	The research yielded that DL distance matching, being the most appropriate method, provides a robust methodology in recognizing medicine names.
[39]	2022	SVM classifier, Naive Bayes, Gradient Boosted, Decision Tree, KNIME analytics for analysis	The model gave an accuracy of 84% for SVM classifier, 59% for NB, 57% for Decision Tree, 51% for gradient boosted.
[33]	2023	Image recognition, ML, OCR, android studio, python, django, firebase	The app facilitated a digital version of medical prescriptions which is legible and easy to read for both pharmacists & patients.

Just Accepted

Here, in Eq. (1),
$\mu_f(x)$ represents the membership function for foreground.
A and C represent the two intensity values.

Membership function used for "Background":

$$\mu_b(x) = \begin{cases} 0, & \text{if } 0 \leq x < A \\ \frac{(x-A)}{(C-A)}, & \text{if } A \leq x < C \\ 1, & \text{if } C \leq x < 255 \end{cases} \tag{2}$$

Here, in Eq. (2),
$\mu_b(x)$ represents the membership function for background.
A and C represent the two intensity values.

Similarly, M Hanmandlu et al [17] worked on formulating a research method recognized as the box method in the field of feature extraction so as to recognize handwritten characters. The dataset chosen for conducting the experiment was CEDAR CDROMI. The feature recognition was performed using back-propagation (BPNN) and fuzzy logic, yielding a 100% recognition rate.
Y. Alginahi et al [4] used a novel set of fuzzy-descriptive features to process optical code, implemented using the cross-correlation for character classification. The cross-correlation coefficient ρ is represented using the

following formula as mentioned in Eq. (3):

$$\rho_{ab} = \frac{\sum_{i=1}^{n}(a_i - \bar{a})(b_i - \bar{b})}{\sqrt{\sum_{i=1}^{n}(a_i - \bar{a})^2 \sum_{i=1}^{n}(b_i - \bar{b})^2}} \tag{3}$$

Here, in Eq. (3):
$\bar{a}$ depicts the mean of $a_i's$ prototype feature vector,
$\bar{b}$ depicts the mean of $b_i's$ feature vector for the characters which are under recognition
The study was conducted using MICR codes placed at bottom of bank cheques. The results drawn showed that it was feasible to attain 100% recall for the training patterns and apart from this, 100% recognition rate for warped and skewed patterns was also achieved.
Taking into consideration the power that fuzzy logic offers, M. Soleymani Baghshah et al [44] proposed a novel fuzzy-based methodology to recognize Persian hand-written characters. Fuzzy linguistic modeling approach was used to accomplish the character parameters representation and these features were used to rule out the token shapes. The model yielded a 95% recognition rate. Elaheh Dehghani and Mohsen Ebrahimi Moghaddam [12] worked on Persian Signature dataset and SUBCORPUS-100-MCYT to mount a verification system for online signatures using global information and ANFIS model. Mohammed Zeki Khedher and Dr. Ghayda Al-Talib [24]. also worked on handwriting recognition for Arabic sub-words using fuzzy logic. Membership functions were generated to recognize these patterns using feature extraction.
G.E.M.D.C. Bandara et al [7] came forward to develop a portable, efficient, and relatively short algorithm so as to replicate human intellect targeting hand-written alphanumeric characters. It took into account fuzzy feature extraction methods to examine the uncertainties and vagueness of handwritten characters and concluded that the given method outperformed the traditional methodologies by yielding better results. Similarly, K.B.M.R. Batuwita and G.E.M.D.C. Bandara [8] together worked on developing a fuzzy-based numeric character recognition system. The authors binarized and skeletonized the input character images and then performed isolation and segmentation on the characters individually.

In our continued effort to provide a comprehensive overview of fuzzy logic in this field, a few more related papers have been enlisted in table 2.

However, the work done in the studied papers enlisted appreciable results but to handle other promising works, the study of other relevant fields is required that aided in signature verification. In addition to fuzzy logic, there are several other techniques used in the area of hand-written image classification which are discussed in the upcoming sub-sections.

4.3 Neural Networks and Computer Vision

Image classification is a common application of Neural Networks (NNs) and Image processing. Over the years, significant amount of research has been done in this domain and many researchers have applied Machine Learning (ML), Deep Learning (DL), image processing, and various other techniques for hand-written image classification. Some of these techniques used have been discussed in this section.

Tai-Ping Zhang et al [53] proposed a method of feature extraction by making use of rotation-invariant curvature sequences of signature envelope. This method depicted both the changes in pattern and the smoothness of the envelope generally used by human experts to perform signature verification. To annihilate the shift effect, polygon matching technique was used. The database was created by collecting signatures from 80 writers. The AER (average error rate) came out to be 17.17%.

Neural Networks have proved to be one of the most efficient methods for signature verification. K. V. Lakshmi and Seema Nayak [29] came together to work upon proposing one such verifier for signature authentication by

Just Accepted

Table 2. Applications of Fuzzy Logic in Signature Verification

Ref.	Year	Methodology	Findings
[31]	1995	Fuzzy Linguistic Rules, Fuzzy Feature Extraction, Fuzzy Logic, Aggregation Operators	Built a robust multi-level system for handwriting recognition.
[18]	2001	Takagi-Sugeno Model, Angle Feature, Distance Feature, Fuzzy Logic	The proposed TS model approach gave satisfactory results with angle feature approach and this model could be applied for both signature verification and forgery detection.
[51]	2003	Fuzzy Modeling, TS Model, Exponential Membership Function, Fuzzy Logic	Built an innovative approach for signature verification using TS model, giving promising results.
[19]	2005	Fuzzy Logic, TS Model, Fuzzy Set, Box Approach, Structural Parameters	Derived two TS models and ruled out that TS model having multiple rules works better than TS model with single rule for signature forgery detection.
[21]	2013	Fuzzy Logic in Image Matching, Fuzzy Set Theory	The author proposed an image matching algorithm using Fuzzy Logic, leaving wide scope of further research.

Just Accepted

building a multi-layered NN. The pre-rpocessing was done using "im toolkit" to design the verification model. The data used to train the model is captured using an acquisition device (camera) and then converted to numeric data. Around 200 images were collected in total. The extracted features were fed to the NN as input. Simulation was performed using the nntool from MATLAB.

Similarly, Md. Iqbal Quraishi et al [37] presented an ANN model to build an automated signature verifier by considering the frequency and spatial domain methodologies for transformation. Once the RoI was drawn out, Log Polar & Ripplet-II Transformation methods and Fractal Dimension were employed for descriptor extraction. HP Scanjet G3110 scanner was used for signature scanning from the signature under consideration. A feed-forward NN which also requires back-propagation is used in the decision-making phase. The model accuracy came out to be around 96.15% which was comparatively better than the systems proposed by several other researchers.

N. Aqili et al [5] presented an algorithm based on point pattern matching to verify online signatures. The DTW algorithm was applied to draw correspondence between 2 signals. The study was carried out using the ATVS-SSig DB 1 database. The RMS was evaluated to obtain the points between two signatures that are most likely similar.

Rajib Ghosh et al [16] attempted at proposing a method that recognizes bank cheque hand-written text. It was divided into 4 stages: cropping, segmentation, feature extraction using GLCM and HOG methods, and isolated character recognition with the help of SVM classifier. The dataset used for the model was self-generated from 100 people. The method proposed gave an accuracy of 89.73%.

Nivedita Yadav et al [48] worked on Devanagari handwritten scripts to explore the capabilities of employing inequitable primitives comprising words to detect skilled forgeries. SFS was combined with k-NN to select distinct primitives, HOG was used for object detection, and RBF-SVM for recognition purposes. The handwritten dataset was collected by several people who contributed by giving samples of their natural handwriting and the forgery dataset was collected from other authors who imitated these handwritten scripts. The model showed promising results by successfully detecting forgery using artificial tremorous strokes in fraudulent documents.

Furthermore, a summary of other relevant research conducted in this field has been compiled in the form of a table in table 3.

Table 3. Comparison of other NNs and Image Processing Techniques

Ref.	Year	Methodology	Findings
[40]	2012	Presented a survey on several techniques such as NNs, Hidden Markov Model, Fuzzy Logic, preprocessing techniques for feature extraction etc.	Concluded that NNs and HMM were better options from implementation perspective.
[32]	2013	Presented the signature modality outputs in terms of likelihood ratio and reported ICDAR2013 competitions result	Signature verifiers gave satisfactory performance on various datasets whereas writer identifiers couldn't perform well.
[28]	2013	Image Processing, 2-layer Feed Forward Neural Network, Error Back Propagation Algorithm	The model gave 82.66% of correct classification rate.
[36]	2014	Artificial Neural Network, Fuzzy Logic, MATLAB	The model gave satisfactory results but still requires certain improvements.
[6]	2014	GMM was used for training the model and Euclidean Distance was calculated to define the acceptance range between the signatures.	The model yielded fast output and had minimal storage requirements and gave better performance.
[38]	2016	Applied Harris Corner Detector, feature descriptor was calculated using the SIFT operator.	The proposed system outperformed the other methodologies used.
[9]	2018	Put-forth the work done so far on handwritten signatures WT, Discrete Radon, FT and other methods.	The experiments conducted yielded that DWT was the most effective technique in this case.
[23]	2018	Local Binary Pattern method was used for feature extraction, and k-NN for classification.	The model worked more accurately on writer dependent method for verifying signatures.
[52]	2020	Proposed a CNN model for handwriting pattern recognition, a regression algorithm used was Softmax.	The proposed system gave better accuracy and speed also providing high recognition rate on handwritten digits.

Just Accepted

4.4 Neural Networks and Fuzzy Logic

Since, NNs have shown its efficiency in the forged signature detection, the combination of NNs and Fuzzy logic is expected more significant. The following subsection consider the papers that cover both as a combination. In terms of verifying healthcare signatures entry, both fuzzy logic and neural networks offer advantages and disadvantages. NNs can be very efficient at identifying various patterns in complex data, however a large (significant) amount of data is required to train them. Also, NNs may not always be able to explain how they actually arrived at a decision. On the other hand, fuzzy logic can deal with uncertainty and ambiguities but may need more fine-tuning and domain-specific expertise to be effective. Overall, both techniques can be applied in combination to create a robust signature verification system to verify clinical (healthcare) data entry signatures that can detect and prevent forgery. Some of such methodologies that have been worked upon over the years by several researchers have been summarized in table 4.

Table 4. Comparison of Neuro-Fuzzy Techniques

Ref.	Year	Methodology	Findings
[46]	2022	Comparison of VGG16, VGG19 and ResNet50 on SigComp2009 data and some raw input	VGG19 outperformed the other two models.
[54]	2022	Hybrid DualFuzzy CNN, Probabilistic hesitant fuzzy elements	Optimized algorithm, helps relax the requirements of input, gives better performances.
[3]	2021	Image classification, CNN, Keras, RMSprop optimizer	The conducted experimental results depicted that the suggested CNN model worked more efficiently as compared to other methodologies in the domain.
[35]	2020	CNN, Crest-Trough method, Harris Corner Detection and SURF for forgery classification	The authors proposed a cost-effective system which also gave encouraging performance results.
[11]	2020	Sequence-to-Sequence implementation, LSTM on IAM dataset, CNN, Contour Detection	The system gave better accuracy than using traditional CNN without contours.
[41]	2020	Adaptive fuzzy network-based CNN for classification and image segmentation, Transfer Learning	Adaptive fuzzy network-based CNN for classification and image segmentation, Transfer Learning.
[49]	2019	Deep Neuro-Fuzzy network, TSK fuzzy model, SIMO rule based system image classification.	Contributed that deep structures when combined with fuzzy systems can be used in image analysis.
[50]	2019	Fuzzy logic using CNN having a single layer, Gaussian Membership function, Type-1 fuzzy set.	Introduced a novel pooling method to facilitate dimension reduction so as to overcome loss of information; better accuracy.
[25]	2018	VGG net model, fuzzy based logic system, ANN for classification	The hybrid model gave an accuracy of 70.8% which is better than traditional CNN.
[22]	2017	Reviewed the research work done by various other researchers on Handwritten character recognition	The survey reported that the most widely used character pattern is that of Hindi language.

From the above cited papers, it can be ruled out that the use of both Fuzzy Logic and NNs serve the need of the hour. Hence, the proposed work makes use of these techniques for determination of forged signatures in healthcare databases. The upcoming sections discuss about the work contributions addressing specific to healthcare sector.

Fig. 5 gives a statistical representation of the number of papers reviewed to conduct the literature survey that have been published over the years in this field. Over the years, various methodologies have been applied for image classification as well as pattern recognition which range from machine learning to fuzzy systems such as SVM, k-NN, ANN, CNN, RNN, Fuzzy Logic, Wavelet Transform along with many other regression and classification algorithms. Fig. 6 showcases a pie chart facilitating a general overview of the statistical information regarding the algorithms that have been utilized in this domain and have been covered in this paper.

5 PROPOSED METHODOLOGY

Decision Making is a crucial component of our day-to-day lives. In some circumstances, it becomes a tricky task to figure out if a particular assertion is true or not. Given the ambiguity, fuzzy logic plays a key role as it can be applied in these circumstances to provide flexibility in reasoning. Also, taking into consideration the amount of work that has been done on CNN, it can be inferred that CNN is considered to be the state-of-the-art technique for image and pattern recognition. The integrated approach we have proposed, encompasses the advantages of both fuzzy logic and CNN that ensures robust decision-making as well as accurate pattern recognition, making it highly suitable for applications in signature verification especially in context of healthcare sector and beyond.
Our methodology proposes a hybrid model combining benefits of both a fuzzy logic as well as CNN model. In the proposed methodology, Fuzzy c-Means Clustering method is applied to the signature image first to extract the

Just Accepted

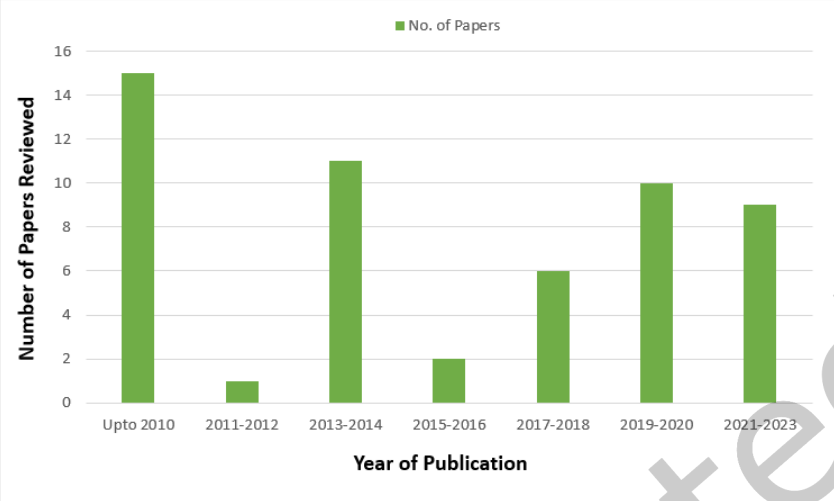


Fig. 5. Number of Papers Reviewed Year-Wise

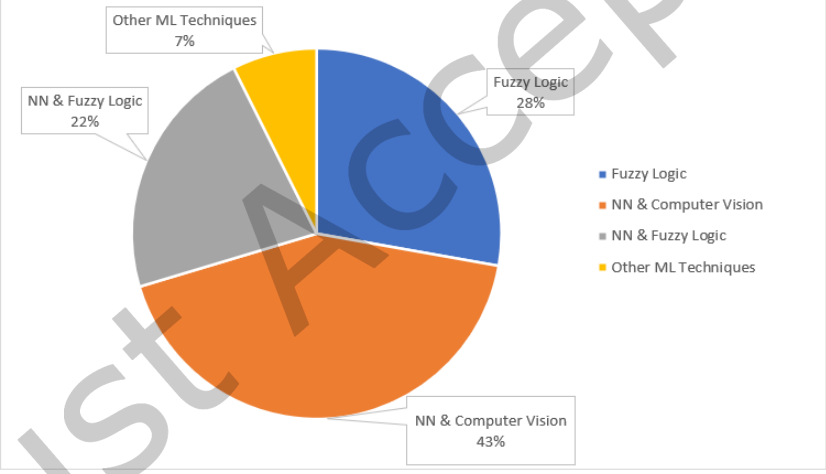


Fig. 6. Analysis of various methodologies discussed in this paper

Region of Interest (ROI), which contains the signature. This extracted ROI is then inputted into a CNN model, which learns distinctive features or traits of the signature. Then the CNN model yields the final decision indicating whether the provided signature image is real or forged.
The proposed architecture to build the model has been depicted in Fig. 7.

The overall work performed for the proposed forged healthcare signature detection can be understood from Algorithm 1.

Just Accepted

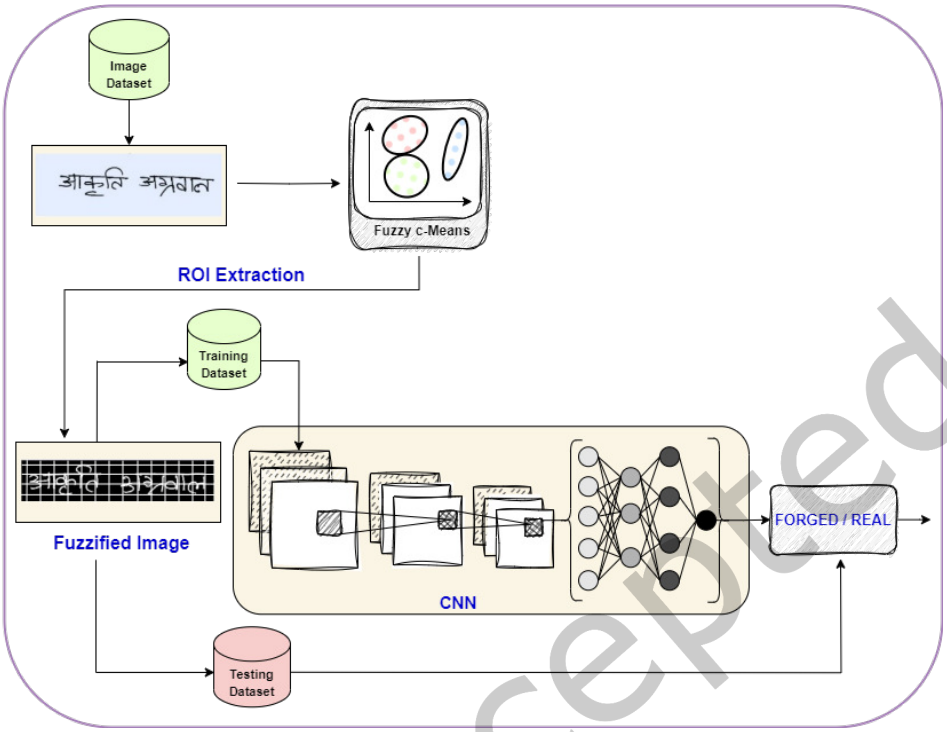


Fig. 7. Proposed Architecture

Algorithm 1 outlines the training procedure to build the hybrid model for healthcare signature verification. We have broken down the algorithm below step-by-step to provide a detailed explanation for the same.

- **Initialization** (Step 1-2):
  - *num_epoch*: Number of training epochs.
  - B: contains Batches of fuzzified images and labels.
  - η: Learning Rate.
- **Training Loop** (Step 3-16):
  - The algorithm utilizes a training loop that runs for a specified number of epochs *num_epoch*
  - Inside each epoch, the training data is divided into batches B, and the model is updated based on these batches.
- **Batch Processing** (Step 4-15):
  - For each batch in B, the following steps are performed:
    - **Data Preparation** (Step 5):
      - X_i represents a batch of input images, and Y_i represents their corresponding labels.
    - **Initialization for Weight Updates** (Step 6):
      - $\Delta\delta w_i$ is initialized to 0 for all weight updates δw_i in the model's weights.
    - **Forward Pass** (Step 7):
      - The model ('*model*') takes the batch of input images X_i and produces predictions $\hat{Y}_i$
    - **Loss Calculation** (Step 8):

Just Accepted

Algorithm 1 Algorithm for the Proposed Architecture

1: Initialize num_epoch, B, η
2: B contains batches of fuzzified images and labels
3: **for** each round $e \in$ num_epoch **do**
4: **for** each batch $b \in B$ **do**
5: $X_i, Y_i \leftarrow$ batch($X_i$image, $Y_i$label)
6: Initialize $\Delta\delta w_i$ to 0, $\forall \delta w_i \in w_i$
7: $\hat{Y}_i \leftarrow$ model(X_i)
8: $l \leftarrow -\frac{1}{n}(Y_i \cdot \log(\hat{Y}_i)) + (1 - Y_i) \cdot \log(1 - \hat{Y}_i)$
9: $g_{t,i} \leftarrow \Delta\theta_t J(\theta_t, l)$
10: $m_t \leftarrow B_1 m_{t-1} + (1 - B_1) g_t$
11: $v_t \leftarrow B_2 v_{t-1} + (1 - B_2) g_t^2$
12: $\hat{m}_t \leftarrow \frac{m_t}{1 - B_1^t}$
13: $\hat{v}_t \leftarrow \frac{v_t}{1 - B_2^t}$
14: $\theta_{t+1} \leftarrow \theta_t - \frac{\eta}{\sqrt{v_t} + \epsilon}$
15: **end for**
16: **end for**

  - The loss l is calculated using a BCE (Binary Cross-Entropy) loss function. It measures the discrepancy between the predicted values $\hat{Y}_i$ and the true labels Y_i
 * **Gradient Computation** (Step 9):
  - The gradient of the loss with respect to the model's parameters, denoted as $g_{t,i}$, is computed. This gradient guides the weight updates.
 * **Momentum Updates** (Step 10-13):
  - A variation of the Adam optimizer is employed by the algorithm for weight updates.
  - It calculates m_t and v_t, which are moving averages of the gradient and squared gradient, respectively.
  - m_t and v_t are bias-corrected to $\hat{m}_t$ and $\hat{v}_t$.
  - These values are used to update the model's parameters in the next step.
 * **Weight Updates** (Step 14):
  - The model's parameters θ_{t+1} are updated using the calculated gradients and momentum terms. The learning rate η and epsilon ϵ are used to control the update step.
- The training loop continues for the specified number of epochs (*num_epoch*), processing batches of data and updating the model's parameters iteratively.

The model was executed by following a series of well-defined steps, each of which contributed to the overall implementation and building of the hybrid model for healthcare signature verification. These steps are described below in detail.

5.1 Preprocessing:

The signature images in the dataset undergo preprocessing to eliminate any noise or unwanted artifacts. This involves procedures such as normalization, image enhancement, and image segmentation.

The input images for the model have a size of 224x224 pixels. Prior to feeding the images into the model, we performed image normalization utilizing mean and standard deviation values of [0.485, 0.456, 0.406] and [0.229, 0.224, 0.225], respectively.

Just Accepted

5.2 ROI Extraction:

FCM clustering is applied to the preprocessed signature image to extract the region of interest (ROI), which contains the signature. FCM serves as a pivotal methodology in signature verification by efficiently segmenting the image pixels on the taking the intensity values into account. The clustering algorithm groups pixels (based on their intensity values) and allocates each pixel a degree of membership to different clusters, rather than a singular one. The pixels in the ROI are chosen based on their membership degree to the cluster that corresponds to the signature pixels. Following that, the ROI is extracted from the signature image.

This degree of membership signifies the likelihood of a pixel belonging to a particular cluster. For signature extraction, clusters are typically configured to differentiate signature pixels from background or noise. By applying a threshold or membership degree criterion, pixels with a strong affiliation to the cluster corresponding to the signature are selected, effectively isolating the signature from its surroundings. The resulting ROI is subsequently extracted, encompassing the signature itself while excluding superfluous background elements and noise. This ROI constitutes a crucial element for ensuing signature verification procedures, ensuring a focused and accurate analysis of the signature's authenticity.

The fuzzy c-means clustering algorithm calculates the pixel-wise membership on the input image, and returns a segmented image.

The FCM is implemented according to the following steps as depicted in Fig. 8.

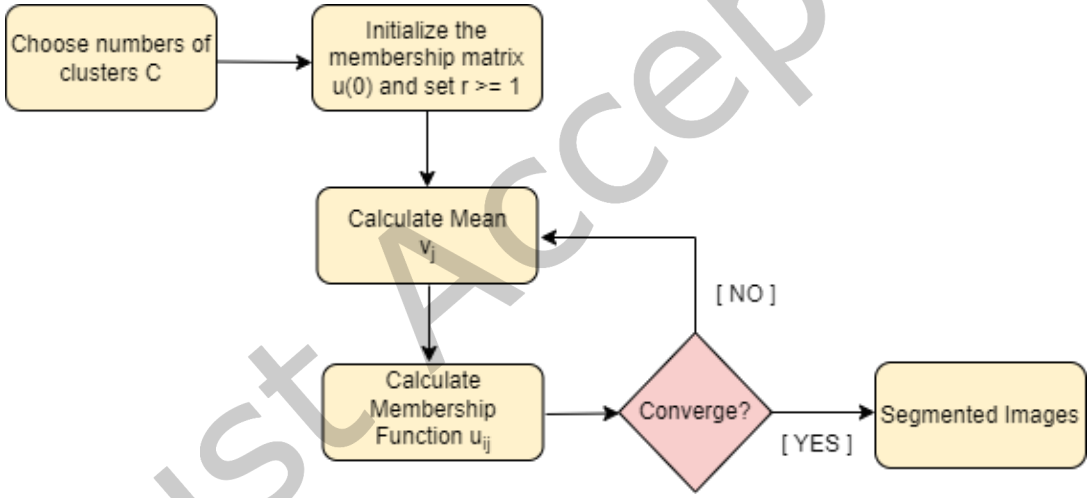


Fig. 8. Fuzzy c-means Clustering

Fuzzy c-means (FCM) clustering is a popular technique employed for fuzzy clustering, which assigns data points to clusters based on their degrees of membership. FCM algorithm aims to lessen the fuzzy objective function, often referred as FCM cost function.

The FCM cost function is defined as follows in Eq. (4):

$$J_m = \sum_{i=1}^{N} \sum_{k=1}^{C} u_{ik}^{m} \|x_i - v_k\|^2 \tag{4}$$

where:

- J_m represents the fuzzy objective function with the fuzzifier m (typically set to a value greater than 1),

Just Accepted

- N is the number of data points,
- C is the number of clusters,
- u_{ik} represents the membership degree of data point x_i in cluster k,
- v_k represents the centroid of cluster k, and
- $\|x_i - v_k\|^2$ denotes the Euclidean distance between data point x_i and centroid v_k.

To update the membership degrees u_{ik} and centroids v_k iteratively, the FCM algorithm employs the following equations:

$$u_{ik} = \left(\sum_{j=1}^{C} \left(\frac{\|x_i - v_k\|}{\|x_i - v_j\|} \right)^{\frac{2}{m-1}} \right)^{-1} \tag{5}$$

$$v_k = \frac{\sum_{i=1}^{N} u_{ik}^m \cdot x_i}{\sum_{i=1}^{N} u_{ik}^m} \tag{6}$$

where the first equation updates the membership degrees based on the distances between data points and centroids, and the second equation updates the centroids based on the revised membership degrees.

The FCM algorithm iteratively applies these equations until convergence, aiming to minimize the FCM cost function and obtain optimal fuzzy clustering results.

By using equations Eq. (4), Eq. (5), and Eq. (6), the FCM algorithm performs iterative updates of membership degrees and centroids, allowing for flexible and overlapping cluster assignments based on the degrees of membership.

5.3 Feature Extraction:

The ROI is fed into a CNN model to extract discriminative features of the signature. The CNN acquires a set of features that encompass the essential characteristics of the signature, including its shape, texture, and curvature.

The CNN model works in the following manner:

- **Convolutional Layer:** It is the basic fundamental layer of a CNN model that works by applying filters to the input image thus, allowing the features to be extracted from the input image. A convolution operation is performed by each filter, a.k.a. kernel, by sliding over the input image. A dot product is computed between the weights of the kernel and corresponding pixels of input image. A feature map is yielded as the output of this layer, is mathematically computed by following equation:

$$Y_{i,j}^k = \sigma \left(\sum_{m=1}^{M} \sum_{n=1}^{N} \sum_{c=1}^{C} X_{i+m,j+n}^c \cdot W_{m,n,c}^k + b_k \right) \tag{7}$$

In Eq. (7):
- $Y_{i,j}^k$ refers to the value at $(i, j)^{th}$ position of k^{th} feature map.
- $X_{i+m,j+n}^c$ is the value at position (i+m, j+n) of the c^{th} input channel.
- $W_{m,n,c}^k$ indicates the weights of the filter for the k^{th} feature map, such that m and n represent the filter dimensions, and c refers to the input channel.
- b_k depicts the bias term for k^{th} feature map.
- σ represents the activation function.

The activation function used in our model is **ReLU**, which is given using the formula as described in Eq. (8):

$$\sigma(a) = \max(0, a) \tag{8}$$

Just Accepted

'a' in Eq. (8) depicts the input value.
The negative values are set to zero and the non-negative values are left unaltered when this max function is applied.

- **Pooling Layer:** The output yielded by convolutional layer is next fed to the pooling layer, which performs reduction of spatial dimensions on feature maps. This helps in diminishing the computational complexity and also provides translational invariance. There are several operations that can be used in the pooling layer such as max pool, average pool etc.
  The pooling operation used to build our model is **max pool**.
  The output of this layer is computed using the following equation:

$$Y_{i,j}^{k} = \max_{m=1}^{M} \max_{n=1}^{N} X_{(i-1)\cdot M+m,(j-1)\cdot N+n}^{k} \tag{9}$$

  Here in Eq. (9),
  - $Y_{i,j}^{k}$ represents the value of k^{th} pooled feature map at position (i, j).
  - $X_{(i-1)\cdot M+m,(j-1)\cdot N+n}$ gives the value at position $((i-1)\cdot M+m, (j-1)\cdot N+n)$ of k^{th} feature map.
  M and N depict the pooling window dimensions.
- **Fully Connected Layer:** This is the final layer of the CNN model which yields the final output. It classifies the signatures into real or forged based on the computations performed in the previous layers.
  The output yielded by this layer can be depicted with the help of Eq. (10):

$$Y_k = \sigma\left(\sum_{i=1}^{N} X_i \cdot W_{i,k} + b_k\right) \tag{10}$$

  Here in Eq. (10):,
  - Y_k represents the k^{th} neuron's output in the FC layer.
  - X_i depicts the i^{th} neuron's output in previous layer.
  - $W_{i,k}$ illustrates the weight connecting the previous layer's i_{th} neuron to the k^{th} neuron of FC layer.
  - b_k depicts the bias for k^{th} neuron.
  - σ is the activation function.
  The activation function used in the FC layer in our model is **Sigmoid**, and the formula for Sigmoid function is represented in Eq. (11).

$$\sigma(a) = \frac{1}{1+e^{-a}} \tag{11}$$

  Here, in Eq. (11), a represents the input value.

5.4 Classification:

The signature images are finally classified into forged or real by the CNN model which not only represents the core objective of our research but also holds profound implications for several real-world applications especially in the healthcare sector. The ability of our system to provide this distinction is a significant step towards intensifying the security and trust in critical areas such as healthcare.

The ultimate classification of signature images into either forged or genuine forms is the culmination of our research and underscores its core mission. Beyond being a research objective, this classification process carries immense significance for a multitude of real-world applications, with a particular focus on the healthcare sector. The ability of our CNN model to make this crucial distinction marks a substantial advancement in enhancing security and instilling trust in contexts as critical as healthcare.

Just Accepted

5.5 Performance Evaluation:

The effectiveness of the proposed hybrid model is estimated using several metrics such as accuracy, precision, recall, and f1-score. The results are compared with other state-of-the-art verification systems for signatures to assess the effectiveness of the hybrid model.

In summary, the final classification of signature images achieved by our CNN model goes beyond the research realm to have far-reaching implications in multiple sectors, most notably in healthcare. This capability contributes significantly to strengthening security, instilling trust, and enhancing the efficiency of critical processes, making it a pivotal development with widespread applicability and potential benefits for various industries.

The overall detailed working of our hybrid model is depicted in Fig. 9.

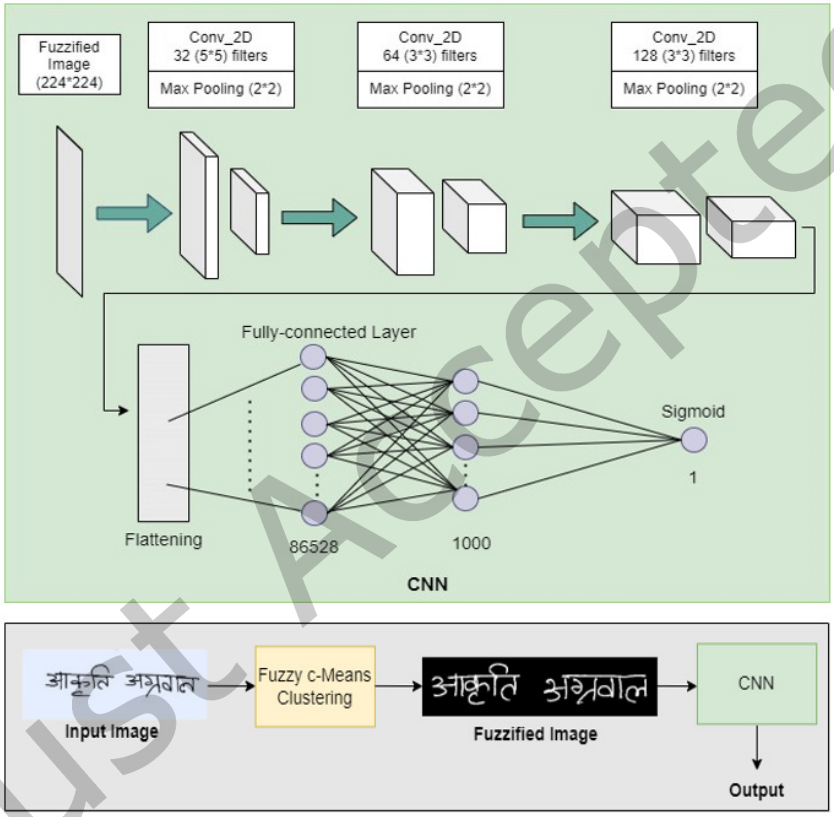


Fig. 9. Proposed Hybrid Framework for Fuzzy-CNN Model

6 EXPERIMENTAL SETUP AND DATASET USED

6.1 Dataset

In this research, we used a dataset consisting of both Hindi and English signatures to develop and evaluate our model. The Hindi signature images were sourced from the BHSig260 dataset, a widely used benchmark dataset utilized for signature verification research. The dataset contains 260 genuine & 2400 forged signatures authored by 100 individuals written in Hindi. The Hindi signature images totaled to 5640 signature images.

Just Accepted

For the English signatures, we compiled a dataset of 3420 handwritten signatures from various healthcare-related sources, including online repositories and public databases. The dataset comprises genuine and forged signatures from different individuals with varying levels of writing styles and quality.

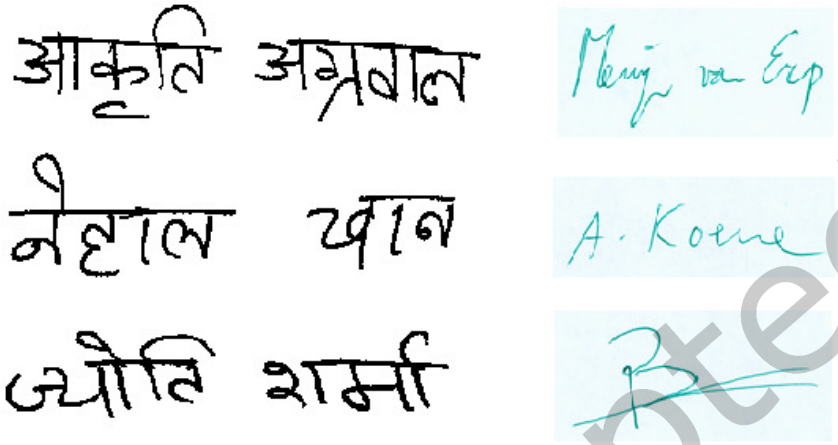


Fig. 10. Sample Healthcare Signature Images

The inclusion of the BHSig260 dataset, a renowned benchmark for Hindi signatures, and our curated collection of diverse English signatures, drawn from various healthcare-related sources, allowed us to tackle the multifaceted challenges posed by signature verification. This rich dataset diversity enabled our model to adapt to the linguistic and stylistic variations commonly encountered in healthcare documents, ultimately enhancing the reliability and effectiveness of our signature verification system. The sample images of our dataset are shown in Fig. 10.

By incorporating these comprehensive datasets, comprising signatures in both Hindi and English, we aimed to enhance the applicability and relevance of our research within the healthcare domain.

6.2 Experimental Setup

The components used to build the model have been described in table 5.

The model architecture consists of three convolutional layers, with kernel size 3x3, stride 1 and valid padding, followed by two fully connected layers with dimensions of 512 and 100, respectively. The output layer applies the Sigmoid activation function. The training dataset consisted of 9,060 samples, including 4,050 real signatures and 5,010 forged signatures. To train the model, we randomly split the data, allocating 80% (7,248 samples) for training purposes having batch size 64. Adam optimizer is used to carry out the training process with a 0.001 learning rate and BCE (Binary Cross-Entropy) loss function to evaluate any discrepancy between predicted and true labels of signatures. The model is trained for 28 epochs.

7 PERFORMANCE METRICS AND EVALUATION

Once the testing and training of the model is completed, several performance metrics are used to evaluate the effectiveness of the model. The performance parameters used in the study are described below in equations:

Just Accepted

Table 5. Experimental Setup

Component	Description
Hardware and Software	
Framework	PyTorch
GPU	Tesla T4
Operating System	Ubuntu 20.04
Model Architecture	
Architecture	Fuzzy c-Means Clustering, CNN model
Layers	3 convolutional layers
Fully Connected Layers	2 FC layers
Activation Functions	ReLU, Sigmoid
Training Procedure	
Learning Rate	0.001
Batch Size	64
Epochs	28
Loss Function	Binary Cross-Entropy (BCE)
Optimizer	Adam
Data Splitting	
Split Ratio	80:20 (Training:Testing)
Experimental Metrics	
Evaluation Metrics	Accuracy, Loss, Heat Map, Precision, Recall, f1-score, ROC AUC, Sigmoid Score

Just Accepted

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{12}$$

$$Recall = \frac{TP}{TP + FN} \tag{13}$$

$$Precision = \frac{TP}{TP + FP} \tag{14}$$

$$f1 - score = 2 * \frac{(Recall * Precision)}{(Recall + Precision)} \tag{15}$$

Apart from these parameters, to assess the performance of binary classification models, it's imperative to grasp the fundamental concepts of positive and negative instances. These instances are described below in detail:

True Positives (TP): The model correctly classified 614 instances as genuine signatures. These are instances where the model accurately identified the true positive class, indicating that the signatures were indeed genuine.

False Positives (FP): The model incorrectly classified 67 instances as genuine signatures when they were actually forged. These instances represent false alarms, where the model predicted a positive outcome (genuine signature) but it was incorrect.

False Negatives (FN): The model incorrectly classified 145 instances as forged signatures when they were actually genuine. These instances represent missed detections, where the model failed to identify a genuine signature, predicting a negative outcome (forged signature) instead.

True Negatives (TN): The model correctly classified 986 instances as forged signatures. These instances were correctly identified as negative, representing signatures that were truly forged.

Having established a robust grasp of performance metrics, this section further extends to demonstrate the valuable insights derived from the experiments conducted in our research. We provide a detailed examination of the findings obtained from the study and discuss their implications in the healthcare sector. Our findings showcase the effectiveness of the proposed system and provide insights into its potential for enhancing signature verification in the healthcare sector.

Just Accepted

- **Accuracy**

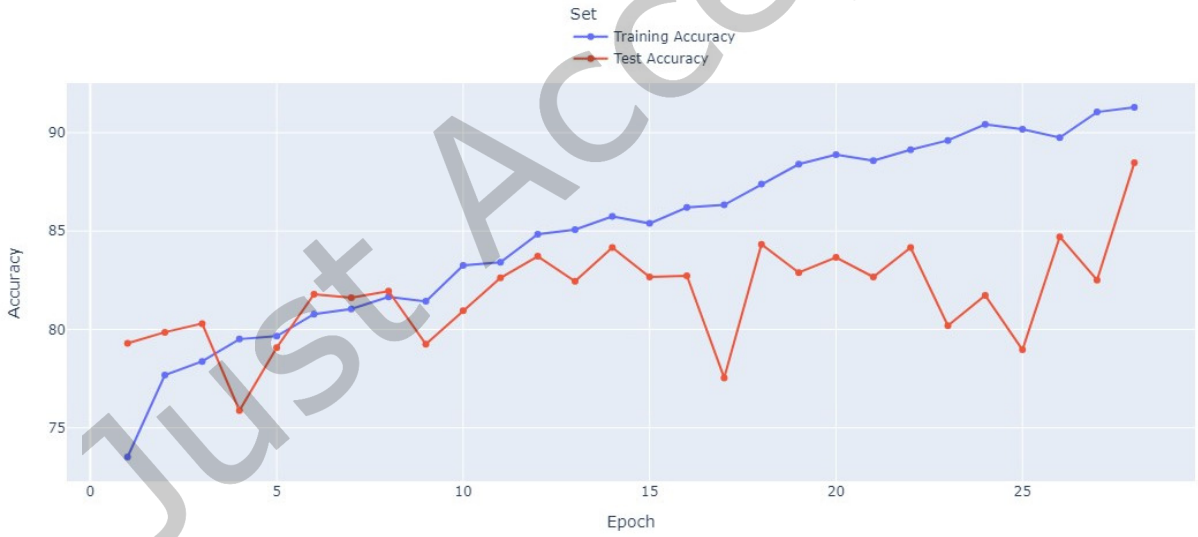


Fig. 11. Training v/s Testing Accuracy

To assess the effectiveness of our signature verification model, we plotted the model's accuracy on a line graph. The graph represents the relationship between the number of training epochs and the model's accuracy on training and test dataset, thus, allowing us to witness the model's progress in learning & adapting to intricacies of signature verification over time. Fig. 11 shows the accuracy plot.

After 28 epochs of training, our Fuzzy-CNN hybrid model achieved a training accuracy of **91.29%**. This indicates that the model can accurately classify **91.29%** of the training instances correctly. This ability to accurately classify training data indicates the model's capacity to internalize the nuances of genuine and forged signatures. Equally significant is the test accuracy, which gauges the model's performance on the unseen data. Our model demonstrated an outstanding test accuracy of **88.47%**. This graph underscores the model's robust generalization capability, implying its effectiveness to accurately predict the previously unseen signature samples. The high test accuracy is particularly critical for signature verification, signifying the model's reliability to distinguish genuine signatures from forged ones, thereby enhancing document security and trust, especially in healthcare applications.
In summary, the accuracy plot not only reaffirms the proficiency of our proposed fuzzy-CNN hybrid model but also highlights its rapid convergence and robust generalization capabilities. The model's ability to achieve exceptional accuracy on both training and test data exemplifies its readiness for real-world deployment, where accuracy and reliability are paramount.

- **Loss**

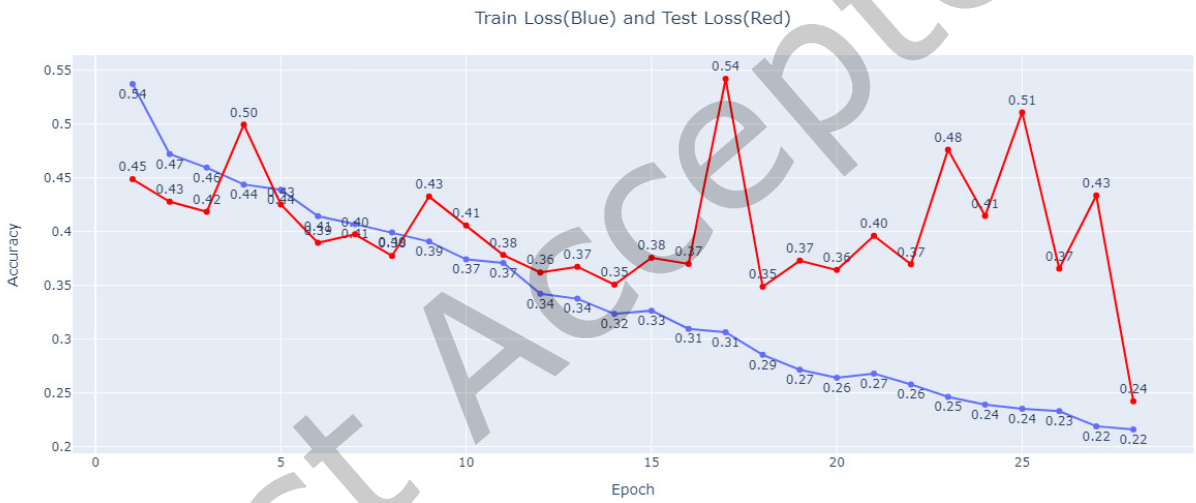


Fig. 12. Train vs Test Loss

To assess the convergence of and optimization of the model, we plotted the Train v/s Test loss graph for the same. As our model underwent training, we closely observed its behavior within this graph, and the results were indeed enlightening.
The training loss was recorded at **0.2160**, and the test loss was at **0.2422**. These low values suggest that the model effectively minimized the error during training and demonstrated reasonable performance on unseen data.
We have depicted the comparison of the train and test loss for the suggested model in Fig. 12 serves as the visual representation of this critical evaluation showcasing the comparison of training and test loss.
The train vs. test loss graph not only provides an overview of the model's learning process, giving valuable insights into the model's learning behavior but also enlightens the generalization capability of its knowledge.

Just Accepted

This analysis of the train vs. test loss confirms the effectiveness of our proposed model in capturing the underlying patterns and minimizing the prediction errors.
Most significantly, it serves as an evidence for the ability of our model to learn and generalize from the training data to achieve accurate predictions on unseen test samples. This level of model performance is vital in real-world applications, especially in the healthcare sector, where accuracy and reliability are of utmost importance, further solidifying the practical applicability of our signature verification system.

- **Heat Map**

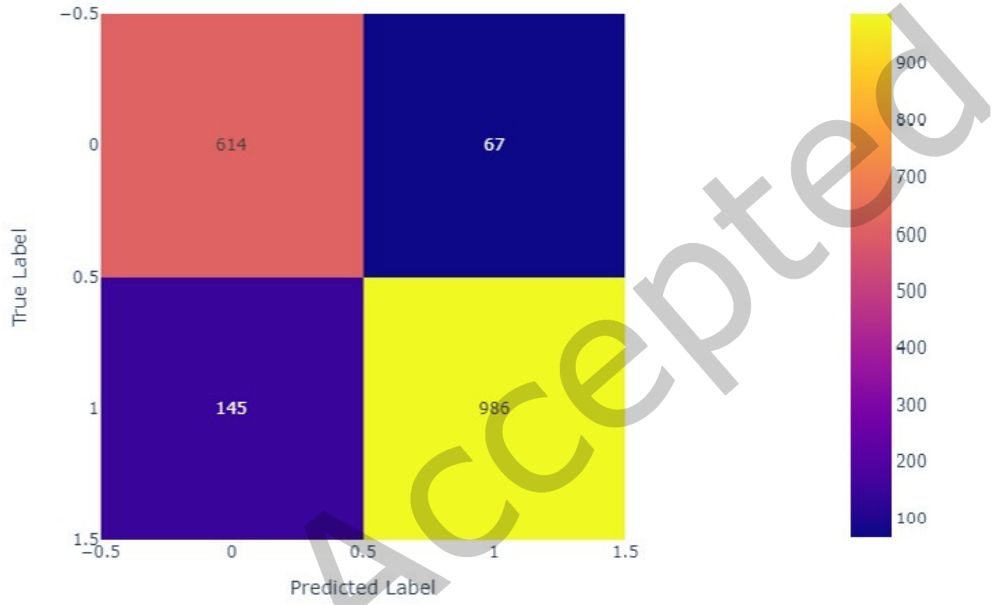


Fig. 13. Heat Map

To better understand the distribution of genuine and forged signatures in our dataset, we created a heat map to visualize the frequency of each signature type across various feature dimensions, giving a comprehensive overview of the dataset's characteristics.
The heat map for our study, as shown in Fig. 13, provides a concise and clear representation of the composition of our dataset, allowing us to identify any patterns or trends in signature characteristics, shedding light on the distinct features that set genuine and forged signatures apart. It allows us to discern at a glance how frequently each signature type occurs in the dataset, presenting an informative visual summary for the same.
To provide further clarity, the rows in the confusion matrix indicate the actual classes, while the columns are used to depict the predicted classes of the signatures.
The actual classes are the ground truth labels, signifying whether the signature is genuine or forged. On the other hand, predicted classes represent the model's classifications on the basis of the features it has extracted and learned. By aligning the actual and predicted classes in the heat map, we can estimate the performance of the model in distinguishing between genuine and forged signatures. Patterns emerging in the heat map can provide valuable insights into strengths of the model and also, the potential areas of

Just Accepted

improvement. Furthermore, it can help in identification of any biases or challenges in the dataset, thus, directing further refinements in the process of signature verification.
To summarize, heat map is a powerful tool for visualization which not only simplifies the understanding of signature distribution, but also aids in evaluating the model's performance in classifying the healthcare signatures accurately. It serves as a valuable asset in our research, allowing us to make data-driven decisions and enhance the robustness of our signature verification system in real-world healthcare applications and beyond.

- **Precision**

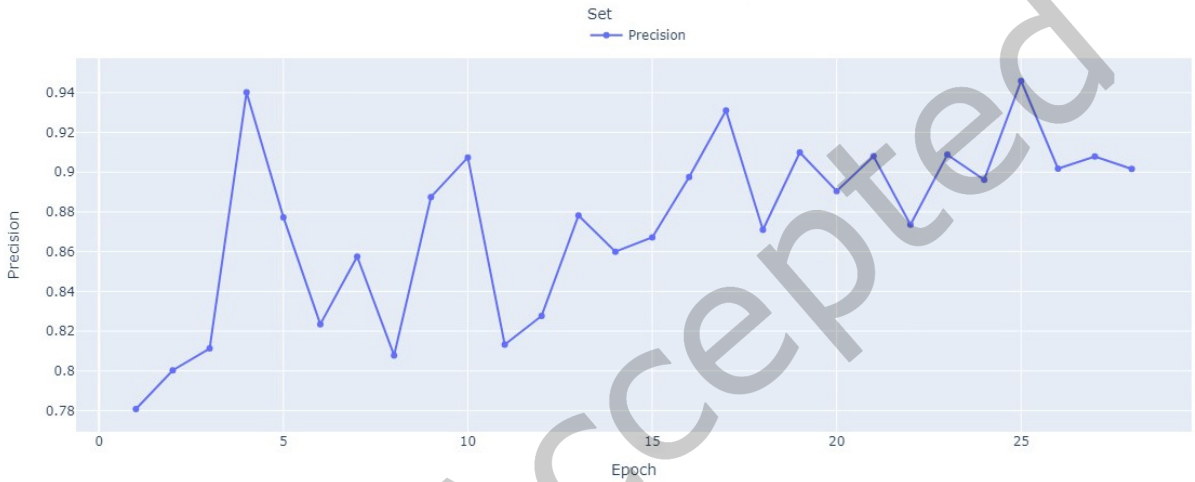


Fig. 14. Precision per Epoch

To comprehensively evaluate the performance of our model, we considered several other essential parameters, one of which is Precision. Precision, a crucial metric, is a measure to evaluate the ability of the model to correctly identify positive instances i.e genuine signature. The Precision score of our model achieved an impressive level of **0.9016**. This score signifies the model's proficiency in ensuring that the instances classified by our model as genuine, are indeed authentic.
The graph depicted in Fig. 14 for Precision per Epoch, provides vital insights into how this metric evolved throughout the training process of our model. This graph obtained allows us to track the model's precision at different stages of learning thus, providing a dynamic view of the model's ability to correctly classify the genuine signatures.
A high Precision score, such as the one achieved by our model, is particularly significant in context of signature verification, indicating that when the model asserts a signature to be genuine, it is affirming so with a high degree of accuracy. In contexts as that of healthcare, where the validity of signatures is of paramount importance, such high level of precision becomes indispensable for upholding document security as well as fostering trust, thus making our model extremely reliable for signature verification in the healthcare sector.

- **Recall**
Another critical metric considered for the evaluation of our model is Recall. Recall assesses the model's

Just Accepted

ability to find all positive instances effectively. The Recall value attained by our model was **0.809**. Fig. 15 depicts the graph obtained for Recall per Epoch.

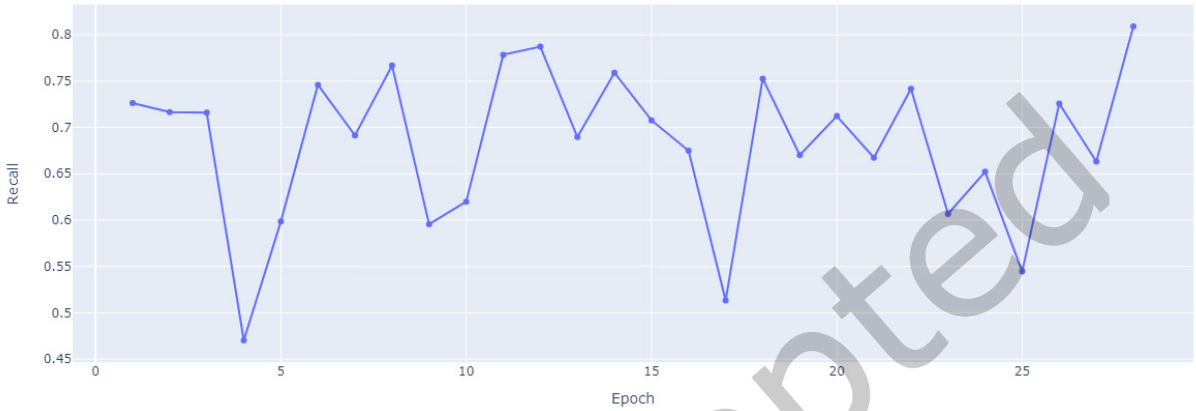


Fig. 15. Recall per Epoch

This graph allows us to observe how well the recall rate of our model fluctuates at different learning stages, showcasing a dynamic view of its ability to find genuine signatures accurately.
In signature verification's context, especially in case of healthcare sector, a Recall score of 0.809 is noteworthy. In the healthcare domain, documents usually contain sensitive patient information, treatment plans, and legal agreements etc. The authenticity of signatures on these documents is not only a matter of legal compliance but also a vital aspect of patient safety & privacy.
Henceforth, a high Recall score like 0.809 implies the model's proficiency in successfully locating a substantial portion of signatures that are genuine within the healthcare signature dataset. It indicates that the model is adept at identifying a significant proportion of genuine signatures. Furthermore, this level of Recall is instrumental in ensuring that no genuine signatures are overlooked or falsely categorized as forged ones. It helps maintain the integrity of healthcare documents, minimizing the risk of unauthorized alterations or fraudulent activities. Moreover, it enhances trust in the document management processes within the healthcare sector, where precision and accuracy play a vital role.
Overall, by showcasing the Recall per Epoch in our research, we emphasize the model's consistency in identifying genuine signatures throughout its training process. This underscores the model's readiness for real-world deployment in healthcare sector, where reliable signature verification is essential for upholding patient confidentiality, legal compliance, and overall document security.

- **f1-score**
  In the realm of healthcare sector and signature verification, the f1-score is a pivotal metric as it harmonizes two crucial aspects: precision and recall. In healthcare, the f1-score's significance lies in its capacity to capture the delicate equilibrium required for signature verification. On one hand, precision ensures that when the model asserts a signature as genuine, it is done with a high level of confidence, reducing the risk

Just Accepted

of false positives. This is imperative to prevent unauthorized access, tampering of medical records, or any fraudulent activities that could compromise patient safety and privacy.
On the other hand, recall ensures that the model doesn't overlook any genuine signatures. In healthcare, overlooking even a single genuine signature can have serious legal and operational consequences. A high recall rate ensures that all authentic signatures are appropriately accounted for in document verification processes.
The f1-score, depicted in Fig. 16, balances precision and recall, was calculated as **0.8528**. These results indicate that the model performed well in accurately identifying positive instances while maintaining a favorable balance between precision and recall.
Our obtained f1-score of 0.8528 signifies that the model has performed admirably in its ability to accurately identify positive instances, which in this case are genuine signatures. Importantly, it has achieved this while striking a commendable balance between precision and recall.

Fig. 16. f1-score per Epoch

Just Accepted

The f1-score of 0.8528 indicates that our model excels at this exquisite balancing act. It effectively identifies the genuine signatures with precision while ensuring that it doesn't miss a significant proportion of them. This level of performance is essential in healthcare, where the integrity of documents, patient confidentiality, and legal compliance are paramount concerns.
To summarize, the f1-score obtained from our research underscores the ability of model to meet stringent requirements of signature verification in healthcare sector. It witnesses the model's readiness to enhance document security, maintain trust, and safeguard the patient information in real-world healthcare applications.

- **Overall Results Obtained**
  Fig. 17 plays a pivotal role in presenting the comprehensive results derived from the evaluation of our signature verification model. By virtue of this figure, we showcase a set of performance metrics that serve

as crucial indicators of the model's effectiveness in critical task of classifying healthcare signatures into either genuine or forged.
These metrics serve as key indicators of the effectiveness of our model in classifying the given healthcare signatures into genuine or forged.
The choice of these performance metrics reflects our commitment to a thorough and rigorous evaluation process. Let's delve into the significance of these metrics:

- **Accuracy**: Accuracy is a fundamental metric that quantifies the model's overall correctness in classifying signatures. It reflects the percentage of correctly classified signatures out of the total, providing a broad overview of the model's proficiency.
- **Precision**: Precision is vital, especially in healthcare, as it gauges the model's ability to correctly identify positive instances, i.e., genuine signatures. A high precision score ensures that when the model asserts a signature as genuine, it does so with a high level of certainty, minimizing the risk of false positives that could lead to security breaches or data inaccuracies.
- **Recall**: Recall, equally crucial in healthcare, assesses the model's proficiency in finding all positive instances, in this case, genuine signatures. A high recall rate ensures that no genuine signature is overlooked or falsely classified as a forgery, safeguarding patient privacy and legal compliance.
- **f1-score**: The f1-score strikes a balance between precision and recall, providing a comprehensive measure of the model's performance. In healthcare, achieving a high f1-score indicates that the model effectively identifies genuine signatures with precision while maintaining a high recall rate, crucial for upholding document integrity.

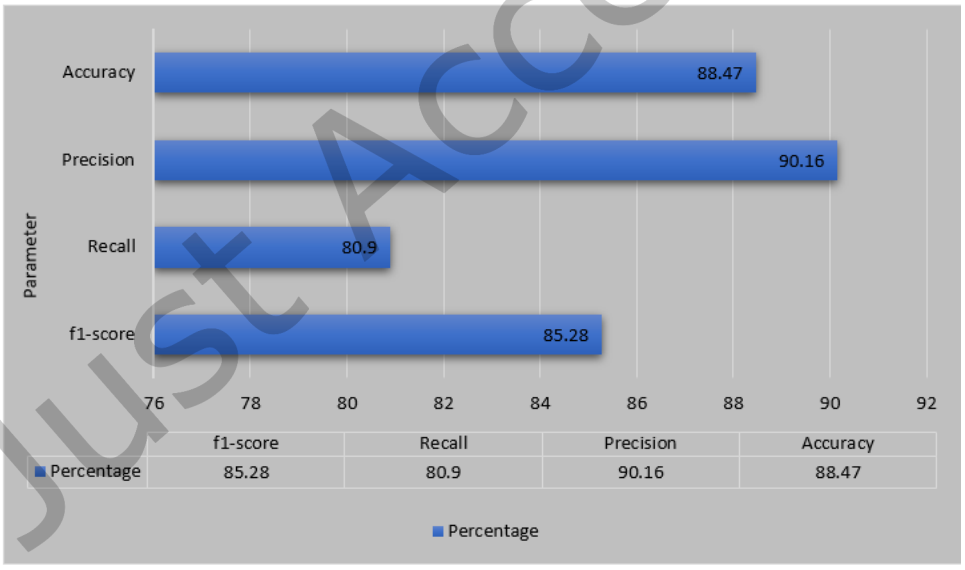


Fig. 17. Results Obtained

Fig. 17 serves as a visual summary of these metrics, offering a clear and concise representation of the model's performance in classifying healthcare signatures. It enables us to assess the model's overall efficacy and its readiness for real-world deployment in healthcare document management, where accuracy, precision, and

Just Accepted

patient data security are of paramount importance. This figure underscores our commitment to ensuring that our signature verification system meets the stringent requirements of the healthcare sector.

- **ROC Curve**
  The area under the ROC curve (AUC-ROC) for the testing data was measured at **0.937**. This indicates that the model exhibited a high ability to distinguish between positive and negative instances, demonstrating strong discriminating power. The graph for the same has been depicted in Fig. 18.
  The measurement of the area under the ROC curve (AUC-ROC) for the testing data, which stood at an impressive 0.937, represents a pivotal aspect of our model evaluation. This metric serves as a robust indicator of the model's ability to differentiate between positive and negative instances, showcasing its formidable discriminatory power.
  In the context of healthcare signature verification, a high AUC-ROC value is of paramount importance. It signifies that the model excels in distinguishing between genuine and forged signatures, which is fundamental for document security and trust. This high discriminatory power translates into a reduced risk of unauthorized access, tampering, or any fraudulent activities that could compromise patient confidentiality and data integrity.

Fig. 18. Receiver Operating Characteristic (ROC) Curve

The graph depicted in Fig. 18 provides a visual representation of the AUC-ROC measurement. This graph is instrumental in not only validating the model's strong discriminatory capabilities but also in offering a dynamic view of how well it performs across different thresholds for classifying signatures.
In summary, the AUC-ROC measurement of 0.937 underscores the model's exceptional ability to differentiate between genuine and forged signatures in healthcare documents. This high discriminatory power is a testament to the model's readiness for real-world deployment in healthcare settings, where document security and patient data integrity are non-negotiable priorities.

- **Sigmoid Score**
  Sigmoid score plays a vital role in estimating the authenticity of signatures. The Sigmoid Score represents

Just Accepted

the confidence level assigned to each signature image by the proposed signature verification model. The Sigmoid Score functions as a quantitative metric representing the probability or likelihood of a signature being attributed to the intended signer.
In context of signature verification, the Sigmoid Score, which is derived from the Logistic Function, is a key element in the CNN model's output, representing the likelihood that a given signature is real (genuine). The Sigmoid Score, also called as Logistic Score, is defined as shown in Eq. 16.

$$S(t) = \frac{1}{1 + e^{-t}} \tag{16}$$

Here, in Eq. 16,

- $S(t)$ represents the Sigmoid Score or the predicted probability that the given input image belongs to the positive class i.e., it represents the probability that the given signature input is genuine .
- t is the output of CNN model, also referred as "Logit". It is the linear combination of features and parameters of the model. Mathematically, t is represented as follows in Eq. 17.

$$t = \beta_0 + \beta_1 t_1 + \beta_2 t_2 + \ldots + \beta_n t_n \tag{17}$$

  In Eq. 17,
  * t represents the logit.
  * $\beta_0, \beta_1, \ldots, \beta_n$ represents the model coefficients or weights.
  * $t_1, t_2, \ldots, t_n$ depict the input vatiables or features.

Basically, the Sigmoid function maps the logit t to a value between 0 and 1 such that the values closer to 1 signify a higher probability of the signature being genuine, whereas the values closer to 0 indicate a lower probability.
Subsequently, the classification outcome, which is the final verdict of the healthcare signature verification system, emerges from the Sigmoid Score itself. It is obtained by applying a predefined threshold such that,

if $S(t) \geq \alpha$, the classification outcome belongs to the genuine (real signature) class.
else if $S(t) < \alpha$, the classification outcome belongs to the forged (fake signature) class.

where α represents the threshold value. The threshold value set for our model for healthcare signature verification was **0.5**.
The Sigmoid Score holds a pivotal role in the process of estimating the authenticity of signatures within our signature verification system. This score serves as a crucial component that quantifies the level of confidence assigned by our proposed signature verification model to each signature image it assesses. Essentially, the Sigmoid Score acts as a quantitative metric, providing valuable insights into the probability or likelihood that a particular signature can be attributed to the intended signer.
In the context of signature verification, the Sigmoid Score plays a central role in the CNN model's output. It represents a numerical value that signifies the model's assessment of the given signature's authenticity, with higher scores indicating a higher likelihood that the signature is genuine.
The foundation of the Sigmoid Score lies in the Logistic Function, a mathematical formula employed to transform the model's raw output into a probability-like value between 0 and 1. This transformed value essentially represents the model's degree of certainty regarding the authenticity of the signature.
By utilizing the Sigmoid Score, our signature verification system gains the capability to provide not just binary outcomes (real or forged) but also nuanced insights into the confidence level associated with each classification. This degree of granularity is invaluable, particularly in sectors like healthcare, where the assurance of signature authenticity is pivotal for patient safety, document integrity, and legal compliance.

Just Accepted

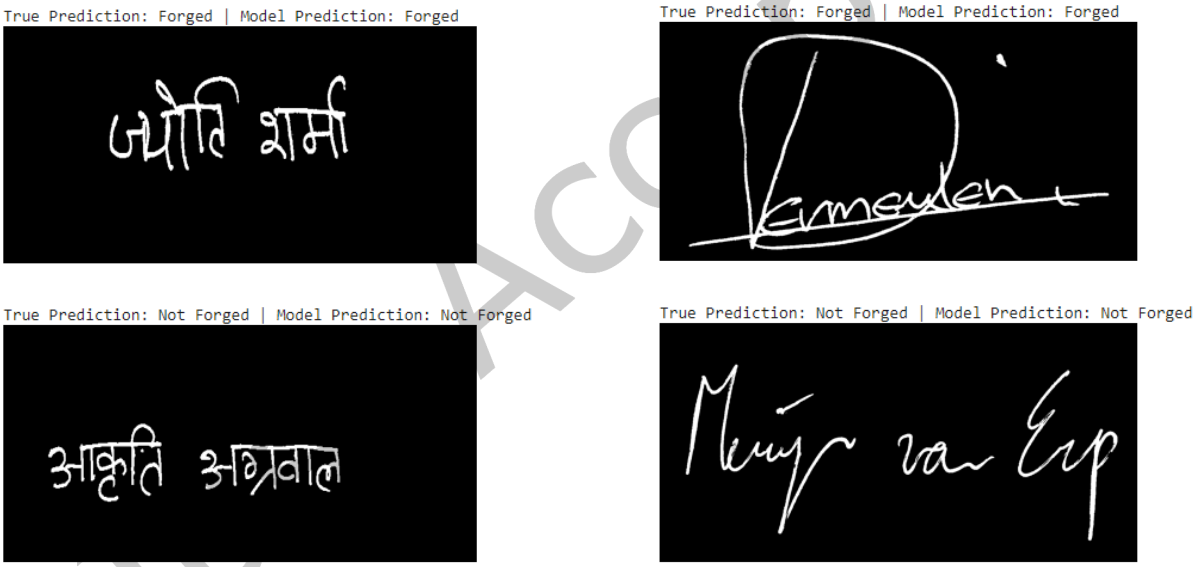
In essence, the Sigmoid Score empowers our signature verification system to make more informed and nuanced decisions, offering not just a binary verdict but also a quantitative measure of confidence. This is a significant advancement in signature verification technology, enhancing its practical utility in critical domains where precision and reliability are of utmost importance.

Table 6 focuses on the Sigmoid Scores for Hindi signatures. These scores serve as valuable reference, offering detailed information on the confidence levels assigned by our model to each signature in the respective datasets.

Similary, table 7 provides insight into the Sigmoid Scores for English signatures. By meticulously organizing and presenting the Sigmoid Scores in this manner, our research aims to provide transparency and clarity regarding the model's evaluations. This transparency is especially critical in healthcare, where precise and accountable signature verification is essential for patient safety, data integrity, and regulatory compliance.

- **Model Prediction**

  To examine the performance of our healthcare signature verification model, we generated model prediction images for a set of genuine & forged signatures. These images depict output of the model when presented with a signature image, and allow us to visually compare the model's performance on genuine and forged signatures. These predictions have been described in Fig. 19a and 19b for both Hindi and English signature images.



(a) Model Prediction for Hindi Dataset

(b) Model Prediction for English Dataset

Fig. 19. Model Prediction

The significance of these prediction images lies in their ability to offer a human-readable interpretation of the model's decisions. They allow us to see not just the model's final classifications but also the features or characteristics within signatures that influenced those decisions. This level of transparency and interpretability is invaluable, particularly in healthcare, where signature verification often has legal and privacy implications.

By presenting these prediction images, our research goes beyond quantitative metrics and embraces a qualitative assessment of the model's performance. This approach enhances our understanding of how the model operates

Table 6. Sigmoid Score for Hindi Signatures for Healthcare

in real-world scenarios and aids in refining its accuracy, precision, and overall reliability in the healthcare sector and other critical domains.

Table 7. Sigmoid Score for English Signatures for Healthcare

8 COMPARISON WITH OTHER MODELS

With the help of extensive training and model evaluation, we have proposed and developed a model that yields remarkable results on the Hindi and English dataset that has been described vividly in the previous sections. To

evince the effectiveness of our model,a comparison has been illustrated in table 8 between our model and other prominent models that have been proposed earlier in the field of signature verification.

Table 8. Comparison of proposed model with other similar models

Model	Methodology	Dataset Used	Accuracy	Precision	Recall	f1-score
[28]	Image Processing, 2-layer Feed Foward NN, EBPTA	'Grupo de Procesado Digital de Senales' (GPDS) database	82.66%	-	100%	-
[1]	kNN classifier, Discrete Radon Transform for feature extraction	MCYT-100 signature CORPUS dataset	80%	-	-	-
[14]	Deep CRNN, Image Processing, C-T Classification, BLSTM, Token Passing algorithm, beam search	Raw data from clinics and hospitals	76%	80%	89%	84%
[26]	SVM developed using Platt's SMO (Sequential Minimal Optimization) Algorithm and Kernel Perceptron, Support Vectors	Raw data from individuals for signatures	72.275%	-	-	-
[25]	VGG net, Fuzzy Layer, Classifier	'Dogs vs Cats' dataset from Kaggle	70.8%	-	-	-
[47]	CNN, RNN (LSTM), Matching algorithm, Adobe Photoshop CC 2015, CT Classification	IAM dataset	63.10%	-	-	-
[30]	GLCM (Gray Level Co-occurrence Matrix, Principal Component Analysis (PCA), Kernel PCA, Naive Bayes(NB), Random Forest(RF) and other ML algorithms	Hadwritten Signatures Dataset from Kaggle	NB: 56.66%, KNN: 82%, RF: 81.66%	-	-	-
[20]	CNN, OCR, Image Processing	Raw data from doctors	50%	-	-	-
Our Model	**Fuzzy Logic using Fuzzy c-Means Clustering, CNN classifier**	**English-Hindi Handwritten Signature Images**	**88.47%**	**90.16%**	**80.9%**	**85.28%**

The results drawn clearly illustrate that our proposed model consistently achieve tremendous accuracy, stipulating its robustness as well as effectiveness to address the problem of signature verification focusing healthcare sector. The research conducted highlights the notable progress we have made in handling this task, thus demonstrating the versatility and pertinence of our model in real-world applications.

In comparison with other models, it becomes evident that while [14] and [28] may have exhibited slightly higher recall rates than our model, it's essential to consider the holistic performance of our approach. Our proposed Fuzzy-CNN hybrid model stands out in a number of aspects listed below:

- **Balanced Performance:** While our model's recall rate of 80.9% is marginally lower than these approaches, it's important to underscore that our model strikes an exceptional balance across all the other critical metrics, including accuracy, precision, and f1-score. This balance ensures that our model is well-rounded and effective in handling a wide diversity of signature verification scenarios.
- **High Accuracy:** Accuracy, serves as a direct indicator of the model's proficiency, indeed holds paramount importance in signature verification in correctly classifying both genuine and forged signatures. We are delighted to report that our model has achieved a commendable accuracy rate of 88.47%, signifying a remarkable achievement. This elevated level of accuracy outlines the exceptional capabilities of our model in upholding document security as well as trust, a critical facet, particularly in context of healthcare sector.

Just Accepted

- **Balancing Precision and Recall:** While recall is crucial for identifying forged samples, it's equally essential to maintain a balance between precision and recall. A model with high recall might classify more samples as genuine (minimizing false negatives), but this could come at the cost of lower precision, which is evident in case of [14], potentially leading to more false positives. In healthcare, precision is critical to ensure that when a signature is classified as genuine, it is indeed genuine to avoid any unauthorized access or data integrity issues.
- **Better Precision and f1-score:** Our model achieves a precision rate of 90.16%. Precision is vital in healthcare contexts, where it's essential to minimize the false positives. Not only this, but our model also shows promising results for f1-score by achieving a remarkable value of 85.28% for f1-score. A high f1-score implies that our model effectively manages the trade-off between minimizing false positives & false negatives, thus, making it a robust and reliable solution for signature verification in healthcare.
- **Comprehensive Evaluation:** Overall, the performance of our model is assessed holistically, taking into consideration multiple performance metrics. This holistic approach corroborates that our model is well-suited for various real-world scenarios, especially in context of healthcare sector and, is not overly biased towards a single metric.

9 CONCLUSION

Overall, our proposed hybrid model for healthcare signature verification which is the amalgamation of Fuzzy c-Means Clustering and CNN has demonstrated promising results, achieving an accuracy rate of 88.47%. This level of accuracy holds significant implications, specifically within the healthcare sector, where ensuring patient safety and privacy is of utmost importance. Medical professionals and institutions relying on hand-written signatures for document verification can anticipate substantial benefits from our system's remarkable accuracy and efficiency. Furthermore, our proposed approach effectively addresses the challenges posed by inherent variations in healthcare signatures, arising because of numerous factors like age, fatigue, or illness, making the model efficient enough in detecting the forgery. Leveraging the fusion of fuzzy logic and deep learning, our system adeptly addresses these signature variations, yielding accurate and reliable signature verification outcomes in the healthcare sector. We present a solution which not only preserves the sanctity of handwritten signatures, but also enhances their utility through automation, making it a requisite contribution to ensure better and secure document management, especially in healthcare contexts.

10 FUTURE ENDEAVOURS

One potential approach to enhance the efficiency and security of signature verification systems in future is by means of federated learning. Looking ahead, we plan to encroach our research by integrating federated learning into our hybrid model. By training the model collaboratively across multiple healthcare institutions without sharing sensitive data, we can leverage the collective knowledge while maintaining data privacy and security. We intend to use the collective expertise while safeguarding the confidentiality and security of data by training the model cohesively across several institutions without disclosing sensitive data. This future direction has the potential to further enhance the robustness and generalizability of our signature verification system in the healthcare sector.

To conclude, our research contributes to the field of healthcare signature verification by introducing a novel hybrid model, showcasing effective accuracy, and also addressing the challenges posed by signature variations. It's worth noting that accuracy, as a metric, holds paramount importance in our pursuit of trustworthy signature verification system. The promising accuracy of attained by our model reflects the system's ability to achieve the fundamental objective of our research, surpassing considerations such as recall and other metrics. By embracing

Just Accepted

federated learning, we strive to further strengthen the capabilities of our model and ensure its applicability in the real-world scenarios while holding onto privacy and security standards.

REFERENCES

[1] A. A. Ahmed Abdelrahaman and M. E. Ahmed Abdallah. 2013. K-nearest neighbor classifier for signature verification system. In *2013 INTERNATIONAL CONFERENCE ON COMPUTING, ELECTRICAL AND ELECTRONIC ENGINEERING (ICCEEE)*. 58–62. https://doi.org/10.1109/ICCEEE.2013.6633907

[2] Roger Achkar, Khodor Ghayad, Rayan Haidar, Sawsan Saleh, and Rana Al Hajj. 2019. Medical Handwritten Prescription Recognition Using CRNN. In *2019 International Conference on Computer, Information and Telecommunication Systems (CITS)*. 1–5. https://doi.org/10.1109/CITS.2019.8862004

[3] Ayush Kumar Agrawal, Avinash Shrivas, and Vineet Kumar Awasthi. 2021. A Robust Model for Handwritten Digit Recognition using Machine and Deep Learning Technique. *2021 2nd International Conference for Emerging Technology (INCET)* (2021), 1–4.

[4] Y. Alginahi, I. El-Feghi, M. Ahmadi, and M.A. Sid-Ahmed. 2004. Optical character recognition system based on a novel fuzzy descriptive features. In *Proceedings 7th International Conference on Signal Processing, 2004. Proceedings. ICSP '04. 2004.*, Vol. 2. 926–929 vol.2. https://doi.org/10.1109/ICOSP.2004.1441471

[5] N Aqili, A Maazouzi, M Raji, A Jilbab, S Chaouki, and A Hammouch. 2016. On-line signature verification using point pattern matching algorithm. In *2016 International Conference on Electrical and Information Technologies (ICEIT)*. IEEE, 410–413.

[6] Neerja Arora, Anil Kumar, and Charu Jain. 2014. GMM for offline signature forgery detection. In *2014 5th International Conference - Confluence The Next Generation Information Technology Summit (Confluence)*. 576–581. https://doi.org/10.1109/CONFLUENCE.2014.6949044

[7] G.E.M.D.C. Bandara, S.D. Pathirana, and R.M. Ranawana. 2002. Use of fuzzy feature descriptions to recognize handwritten alphanumeric characters. In *2002 IEEE World Congress on Computational Intelligence. 2002 IEEE International Conference on Fuzzy Systems. FUZZ-IEEE'02. Proceedings (Cat. No.02CH37291)*, Vol. 2. 1586–1591 vol.2. https://doi.org/10.1109/FUZZ.2002.1006743

[8] K.B.M.R. Batuwita and G.E.M.D.C. Bandara. 2006. Fuzzy Recognition of Offline Handwritten Numeric Characters. In *2006 IEEE Conference on Cybernetics and Intelligent Systems*. 1–5. https://doi.org/10.1109/ICCIS.2006.252356

[9] Anastasia Beresneva, Anna Epishkina, and Darina Shingalova. 2018. Handwritten signature attributes for its verification. In *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*. IEEE, 1477–1480.

[10] Qi Chen, Tianxia Gong, Linlin Li, Chew Lim Tan, and Boon Chuan Pang. 2010. A Medical Knowledge Based Postprocessing Approach for Doctor's Handwriting Recognition. In *2010 12th International Conference on Frontiers in Handwriting Recognition*. 45–50. https://doi.org/10.1109/ICFHR.2010.121

[11] Narayana Darapaneni, Malarvizhi Subramaniyan, Aafia Mariam, Sai Venkateshwaran, Nandini Ravi, Anwesh Reddy Paduri, Sumathi Gunasekaran, et al. 2020. Handwritten form recognition using artificial neural network. In *2020 IEEE 15th International Conference on Industrial and Information Systems (ICIIS)*. IEEE, 420–424.

[12] Elaheh Dehghani and Mohsen Ebrahimi Moghaddam. 2009. On-line signature verification using ANFIS. In *2009 Proceedings of 6th International Symposium on Image and Signal Processing and Analysis*. 546–549. https://doi.org/10.1109/ISPA.2009.5297687

[13] E.Kamalanaban, M. Gopinath, and S. Premkumar. 2018. Medicine Box: Doctor's Prescription Recognition Using Deep Machine Learning. *International Journal of Engineering & Technology* (2018).

[14] Lovely Joy Fajardo, Niño Joshua Sorillo, Jaycel Garlit, Cia Dennise Tomines, Mideth B. Abisado, Joseph Marvin R. Imperial, Ramon L. Rodriguez, and Bernie S. Fabito. 2019. Doctor's Cursive Handwriting Recognition System Using Deep Learning. In *2019 IEEE 11th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM)*. 1–6. https://doi.org/10.1109/HNICEM48295.2019.9073521

[15] Paul D Gader and James M Keller. 1996. Fuzzy methods in handwriting recognition: an overview. *Proceedings of North American Fuzzy Information Processing* (1996), 137–141.

[16] Rajib Ghosh, Chinmaya Panda, and Prabhat Kumar. 2018. Handwritten Text Recognition in Bank Cheques. In *2018 Conference on Information and Communication Technology (CICT)*. IEEE, 1–6.

[17] M. Hanmandlu, K.R.M. Mohan, and S. Chakraborty. 2001. Fuzzy logic based handwritten character recognition. In *Proceedings 2001 International Conference on Image Processing (Cat. No.01CH37205)*, Vol. 3. 42–45 vol.3. https://doi.org/10.1109/ICIP.2001.958046

[18] M. Hanmandlu, K.R. Murali Mohan, S. Chakraborty, and G. Garg. 2001. Fuzzy modeling based signature verification system. In *Proceedings of Sixth International Conference on Document Analysis and Recognition*. 110–114. https://doi.org/10.1109/ICDAR.2001.953765

[19] Madasu Hanmandlu, Mohd. Hafizuddin Mohd. Yusof, and Vamsi Krishna Madasu. 2005. Off-line signature verification and forgery detection using fuzzy modeling. *Pattern Recognition* 38, 3 (2005), 341–356. https://doi.org/10.1016/j.patcog.2004.05.015

[20] Esraa Hassan, Habiba Tarek, Mai Hazem, Shaza Bahnacy, Lobna Shaheen, and Walaa H. Elashmwai. 2021. Medical Prescription Recognition using Machine Learning. In *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*. 0973–0979. https://doi.org/10.1109/CCWC51732.2021.9376141

Just Accepted

[21] Shahla Hazim Ahmad Karruffa. 2013. Using Fuzzy Logic In Image Matching. *Journal of Education and Science* 26, 4 (2013), 126–139. https://doi.org/10.33899/edusj.2013.89980

[22] Ajay Indian and Karamjit Bhatia. 2017. A survey of offline handwritten Hindi character recognition. In *2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall)*. 1–6. https://doi.org/10.1109/ICACCAF.2017.8344697

[23] Snehal K. Jadhav and M. K. Chavan. 2018. Symbolic Representation Model for Off-Line Signature Verification. In *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. 1–5. https://doi.org/10.1109/ICCCNT.2018.8494145

[24] Mohammed Zeki Khedher and Ghayda Al-Talib. 2007. A fuzzy expert system for recognition of handwritten arabic sub-words. In *2007 9th International Symposium on Signal Processing and Its Applications*. 1–4. https://doi.org/10.1109/ISSPA.2007.4555355

[25] Kseniya P. Korshunova. 2018. A Convolutional Fuzzy Neural Network for Image Classification. In *2018 3rd Russian-Pacific Conference on Computer Technology and Applications (RPC)*. 1–4. https://doi.org/10.1109/RPC.2018.8482211

[26] C. Kruthi and Deepika C. Shet. 2014. Offline Signature Verification Using Support Vector Machine. In *2014 Fifth International Conference on Signal and Image Processing*. 3–8. https://doi.org/10.1109/ICSIP.2014.5

[27] Dinuka Kulathunga, Chamika Muthukumarana, Umindu Pasan, Chamudika Hemachandra, Muditha Tissera, and Hansi De Silva. 2020. PatientCare: Patient Assistive Tool with Automatic Hand-written Prescription Reader. In *2020 2nd International Conference on Advancements in Computing (ICAC)*, Vol. 1. 275–280. https://doi.org/10.1109/ICAC51239.2020.9357136

[28] Pradeep Kumar, Shekhar Singh, Ashwani Garg, and Nishant Prabhat. 2013. Hand written signature recognition & verification using neural network. *International Journal of Advanced Research in Computer Science and Software Engineering* 3, 3 (2013).

[29] K. V. Lakshmi and Seema Nayak. 2013. Off-line signature verification using Neural Networks. In *2013 3rd IEEE International Advance Computing Conference (IACC)*. 1065–1069. https://doi.org/10.1109/IAdCC.2013.6514374

[30] Lokare, Chinmay, Patil, Rachana, Rane, Saloni, Kathirasen, Deepakkumar, and Mistry, Yogita. 2021. Offline handwritten signature verification using various Machine Learning Algorithms. *ITM Web Conf.* 40 (2021), 03010. https://doi.org/10.1051/itmconf/20214003010

[31] Ashutosh Malaviya and Liliane Peters. 1996. Handwriting Recognition with Fuzzy Linguistic Rules. (10 1996).

[32] Muhammad Imran Malik, Marcus Liwicki, Linda Alewijnse, Wataru Ohyama, Michael Blumenstein, and Bryan Found. 2013. ICDAR 2013 Competitions on Signature Verification and Writer Identification for On- and Offline Skilled Forgeries (SigWiComp 2013). In *2013 12th International Conference on Document Analysis and Recognition*. 1477–1483. https://doi.org/10.1109/ICDAR.2013.220

[33] Neha Nayak, T Prarthana, Rohit Joshi, S Vaibhavi, and K Swathi. 2023. MEDICAL PRESCRIPTION RECOGNITION USING MACHINE LEARNING: A SURVEY. *International Research Journal of Modernization in Engineering Technology and Science* 5 (2023).

[34] Riya Patil, Prasad Peshave, and Milind Kamble. 2022. Application of Fuzzy Matching Algorithms for Doctors Handwriting Recognition. In *2022 IEEE Bombay Section Signature Conference (IBSSC)*. 1–5. https://doi.org/10.1109/IBSSC56953.2022.10037486

[35] Jivesh Poddar, Vinanti Parikh, and Santosh Kumar Bharti. 2020. Offline Signature Recognition and Forgery Detection using Deep Learning. *Procedia Computer Science* 170 (2020), 610–617. https://doi.org/10.1016/j.procs.2020.03.133 The 11th International Conference on Ambient Systems, Networks and Technologies (ANT) / The 3rd International Conference on Emerging Data and Industry 4.0 (EDI40) / Affiliated Workshops.

[36] Gautam S. Prakash and Shanu Sharma. 2014. Computer vision & fuzzy logic based offline signature verification and forgery detection. In *2014 IEEE International Conference on Computational Intelligence and Computing Research*. 1–6. https://doi.org/10.1109/ICCIC.2014.7238363

[37] Md. Iqbal Quraishi, Arindam Das, and Saikat Roy. 2013. A novel signature verification and authentication system using image transformations and Artificial Neural Network. *2013 World Congress on Computer and Information Technology (WCCIT)* (2013), 1–6.

[38] ABM Ashikur Rahman, Golam Mostaeen, and Md Hasanul Kabir. 2016. A statistical approach for offline signature verification using local gradient features. In *2016 2nd International Conference on Electrical, Computer & Telecommunication Engineering (ICECTE)*. IEEE, 1–4.

[39] Seerat Rani, Abd Ur Rehman, Beenish Yousaf, Hafiz Tayyab Rauf, Emad Abouel Nasr, and Seifedine Kadry. 2022. Recognition of Handwritten Medical Prescription Using Signature Verification Techniques. *Computational and mathematical methods in medicine* 2022 (2022), 9297548. https://doi.org/10.1155/2022/9297548

[40] Ahmad Sanmorino and Setiadi Yazid. 2012. A survey for handwritten signature verification. In *2012 2nd International Conference on Uncertainty Reasoning and Knowledge Engineering*. 54–57. https://doi.org/10.1109/URKE.2012.6319582

[41] Rishil Shah. 2020. Adaptive Fuzzy Network based Transfer Learning for Image Classification. *2020 IEEE International Students' Conference on Electrical,Electronics and Computer Science (SCEECS)* (2020), 1–4.

[42] Teena Sharma, Vikas Singh, Siddharth Sudhakaran, and Nishchal K. Verma. 2019. Fuzzy based Pooling in Convolutional Neural Network for Image Classification. In *2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*. 1–6. https://doi.org/10.1109/FUZZ-IEEE.2019.8859010

[43] Jungpil Shin and Tomomi Kikuchi. 2013. On-Line Signature Evaluation Using Fuzzy Set Theory. In *2013 27th International Conference on Advanced Information Networking and Applications Workshops*. 273–277. https://doi.org/10.1109/WAINA.2013.21

[44] Mahdiyeh Soleymani-Baghshah, Saeed Bagheri Shouraki, and Shohreh Kasaei. 2005. A Novel Fuzzy Approach to Recognition of Online Persian Handwriting. In *Proceedings of the Fifth International Conference on Intelligent Systems Design and Applications (ISDA 2005), 8-10 September 2005, Wroclaw, Poland*. IEEE Computer Society, 268–273. https://doi.org/10.1109/ISDA.2005.13

Just Accepted

[45] Yan Solihin, C.G. Leedham, and Vijay K. Sagar. 1996. A fuzzy based handwriting extraction technique for handwritten document preprocessing. *Proceedings of Digital Processing Applications (TENCON '96)* 2 (1996), 927–932 vol.2.
[46] Duth P Sudharshan and RN Vismaya. 2022. Handwritten signature verification system using deep learning. In *2022 IEEE International Conference on Data Science and Information System (ICDSIS)*. IEEE, 1–5.
[47] WRAD Wijewardena. 2021. *Medical Prescription Identification Solution.* Ph. D. Dissertation.
[48] Nivedita Yadav, Santanu Chaudhury, and Prem Kalra. 2013. Off-line skilled forgery detection on handwritten Devanagri script. In *2013 Fourth National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG)*. IEEE, 1–4.
[49] Omolbanin Yazdanbakhsh and Scott Dick. 2019. A deep neuro-fuzzy network for image classification. *arXiv preprint arXiv:2001.01686* (2019).
[50] Mojtaba Yeganejou, Scott Dick, and James Miller. 2019. Interpretable deep convolutional fuzzy classifier. *IEEE transactions on fuzzy systems* 28, 7 (2019), 1407–1419.
[51] M.H.M. Yusof and V.K. Madasu. 2003. Signature verification and forgery detection system. In *Proceedings. Student Conference on Research and Development, 2003. SCORED 2003.* 9–14. https://doi.org/10.1109/SCORED.2003.1459654
[52] Chao Zhang, Zhiyao Zhou, and Lan Lin. 2020. Handwritten Digit Recognition Based on Convolutional Neural Network. In *2020 Chinese Automation Congress (CAC)*. IEEE, 7384–7388.
[53] Tai-Ping Zhang, Bin Fang, Bin Xu, Heng-Xin Chen, Miao Chen, and Yuan-Yan Tang. 2007. Signature envelope curvature descriptor for offline signature verification. In *2007 International Conference on Wavelet Analysis and Pattern Recognition*, Vol. 3. IEEE, 1262–1266. https://doi.org/10.1109/ICWAPR.2007.4421628
[54] Wei Zhou, Man Liu, and Zeshui Xu. 2022. The dual-fuzzy convolutional neural network to deal with handwritten image recognition. *IEEE Transactions on Fuzzy Systems* 30, 12 (2022), 5225–5236.

Just Accepted