IMAGE FORGERY DETECTION

A Project Report

Submitted by:

BASAV BAMRAH (1900636)

in partial fulfilment for the award of the degree

of

BACHELOR OF TECHONOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

at

BABA BANDA SINGH BAHADUR ENGINEERING COLLEGE

FATEHGARH SAHIB, PUNJAB (INDIA) - 140406

(AFFILIATED TO I.K.G. PUNJAB TECHNICAL UNIVERSITY, KAPURTHALA, PUNJAB (INDIA)

APRIL 2023

DECLARATION

I hereby certify that the project entitled ”Image Forgery Detection” submitted by Basav Bamrah (1900636) in partial fulfilment of the requirement for the award of degree of the B. Tech. (Computer Science & Engineering) submitted in I.K. Gujral Punjab Technical University, Kapurthala at Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib is an aunthentic record of my own work carried out during a period from February 2023 to May, 2023 under the guidance of Prof. Balpreet Kaur CSE department. The matter presented in this project has not formed the basis for the award of any other degree, diploma, fellowship or any other similar titles.

Signature of the Student

Place:

Date:

BABA BANDA SINGH BAHADUR ENGINEERING COLLEGE

Approved by AICTE, Govt. Of Punjab, Affiliated to IKGPTU

(Courses Accrediated by NBA (AICTE))

Dr. Lakhvir Singh

Principal

Ref. No. ..... **Date .....**

CERTIFICATE

This is to certify that the project titled "Image Forgery Detection" is the bona fide work carried out by Basav Bamrah (1900636) in partial fulfillment of the requirement for the award of degree of the B. Tech. (Computer Science & Engineering) submitted in I.K. Gujral Punjab Technical University, Kapurthala at Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib is an authentic record of my own work carried out during a period from January, 2023 to May, 2023 under the guidance of Prof. Balpreet Kaur, Deaprtment of Computer Science & Engineering. The Major Project Viva-Voce Examination has been held on _____ (DD/MM/YYYY)

Signature of the Guide

Signature of the HoD,

Department of CSE.

Signature of the Principal

BBSBEC, Fatehgarh Sahib

CHANDIGARH ROAD, FATEHGARH SAHIB – 140407 PUNJAB (INDIA)

Ph. : 01763 503056, 503143, 503141 Fax: 01763 503139

Website: www.bbsbec.edu.in **Email: principal@bbsbec.ac.in**

ABSTRACT

Throughout the last few decades, there has been a sharp rise in the use of digital images. Virtually every facet of life now makes use of digital photos. Many documents that must be filed online require images in the form of soft copies, and a lot of images are shared on social media every day. Editing or altering a digital image has become more simpler thanks to the rapid advancement of digital image processing technology and the prevalence of digital cameras, even for a novice forger. It is conceivable for any user to alter digital images in such a way that it would be difficult to tell one from the other visually. The methods are commonly referred to as Image forgery detection for the purpose of identifying these modifications in images. The detection of fake images is a difficult field of study. It is clear that in the past decade, high-quality work has been done in the area of detecting image forgeries. Yet, given the sophistication of image editing technologies, there is still a need to pay close attention in this subject. The main purpose of this paper is to conduct a survey of some of the most recent techniques for detecting image forgery concentrating on copy-move and splicing assaults that are widely used.

Marks to be filled by Guide	**Marks Obtained**
Regularity (8)	
Self Motivation and Determination (8)	
Working within Team (8)	
Total (24)	
Signature of the Guide	

ACKNOWLEDGEMENT

I express my sincere gratitude to the I.K. Gujral Punjab Technical University, Kapurthala for giving me the poortunity to work on the Major Project during my final year of B.Tech. (CSE) is an important aspect in the field of engineering.

I would like to thank Dr. Dr. Lakhvir Singh Principal and Dr. Jatinder Singh Head of Department, CSE at Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib for their kind support.

I also owe my sincerest gratitude towards Prof. Balpreet Kaur for her valuable advice and healthy criticism throughout my project which helped me immensely to complete my work successfully.

I would also like to thank everyone who has knowingly and unknowingly helped me throughout my work. Last but not least, a word of thanks for the authors of all those books and papers which I have consulted during my project work as well as for preparing the report.

LIST OF FIGURES

Table of Contents

1. INTRODUCTION

1.1 PROBLEM DEFINITION

- Forgeries are dangerous because they are frequently difficult to spot as fakes. As a result of digital forgeries, the victims of these activities may suffer **financial loss as well as a loss of reputation**
- The technology of digital resource repositories is moving at a much faster rate due to social networking sites, making it very difficult to find the original source of the forgeries

1.2 PROJECT OVERVIEW

The widespread use of desktop computers, the proliferation of smart devices with ever-improving cameras and image processing apps, and the fact that all of these devices are virtually always connected to the Internet and to distant data servers have made it possible for regular people to gather, store, and process vast amounts of digital visual data on a scale that was previously unimaginable, but because there are sophisticated tools for picture editing, anyone with even a basic understanding of computers may easily alter the image.

Digital image forgery is described as "falsely and fraudulently manipulating a digital image" in the Merriam-Webster dictionary. The idea of image falsification is not new; it first appeared around 1840.The earliest altered photograph was made by French photographer Hippolyte Bayard and was named "Self Portrait as a Drowned Man" in which Bayard claims to have committed himself. .Recently, in July 2017, a false photo of Russian President Vladimir Putin meeting with American President Donald Trump at the G20 summit was shared on social media. This bogus image earned several thousand likes and retweets[16].

Sports, legal services, medical imaging, insurance claims, and journalism are just a few of the fields where images play an impressive role. Other fields include forensic investigation, criminal investigation, surveillance systems, intelligence systems, and journalism. In the past ten years, significant study has been done in the area of image forgery detection.

There are two different types of detection methods: active forgery detection and passive forgery detection. The digital image undergoes some sort of pre-processing in an active method, such as a watermark [17] or signatures [14] produced at the moment the image was created. A significantly difficult in image processing approaches is the passive

approach , because the image is the only accessible information in this case. Passive forgery further can be categorised as dependent forgery and independent forgery. Copying and pasting (cloning) [2] can be used to alter a picture in dependent forging. Independent forgery, on the other hand, is a type of fraud in which certain aspects of the same image are changed. Resampling, retouching, picture rotation, scaling, resizing, noise addition, blurring, image compression, etc. are examples of independent forgeries.

Figure 1.1 Image Forgery Detection

1.3 OBJECTIVES

- To study recompression techniques for training the model
- To implement this technique for detection image forgery
- To create a deployable model for easy detection of image forgery

1.4 TECHNOLOGIES USED

1.4.1 Machine Learning

Machine learning is a branch of artificial intelligence (AI) and computer science which focuses on the use of data and algorithms to imitate the way that humans learn, gradually improving its accuracy.

Figure 1.2 Machine Learning

Consider writing a spam filter using traditional programming techniques:

- First you would consider what spam typically looks like. You might notice that some words or phrases (such as “4U,” “credit card,” “free,” and “amazing”) tend to come up a lot in the subject line. Perhaps you would also notice a few other patterns in the sender’s name, the email’s body, and other parts of the email.
- You would write a detection algorithm for each of the patterns that you noticed,and your program would flag emails as spam if a number of these patterns were detected.
- You would test your program and repeat steps 1 and 2 until it was good enough to launch.Since the problem is difficult, your program will likely become a long list of complex rules—pretty hard to maintain.

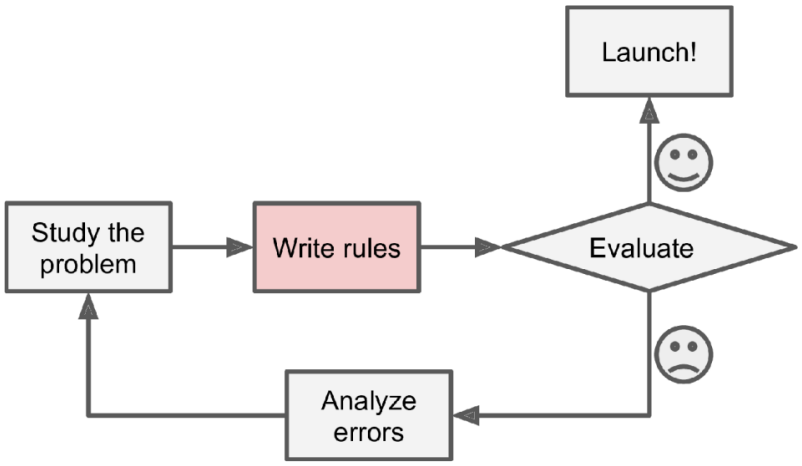

Figure 1.3 Spqam filter

Types of Machine Learning

1) Supervised Learning

In supervised learning, the training set you feed to the algorithm includes the desired solutions, called labels. The model is given input data and the corresponding correct output, and it learns to predict the output for new data based on this training. This allows the model to perform tasks such as classification and regression.

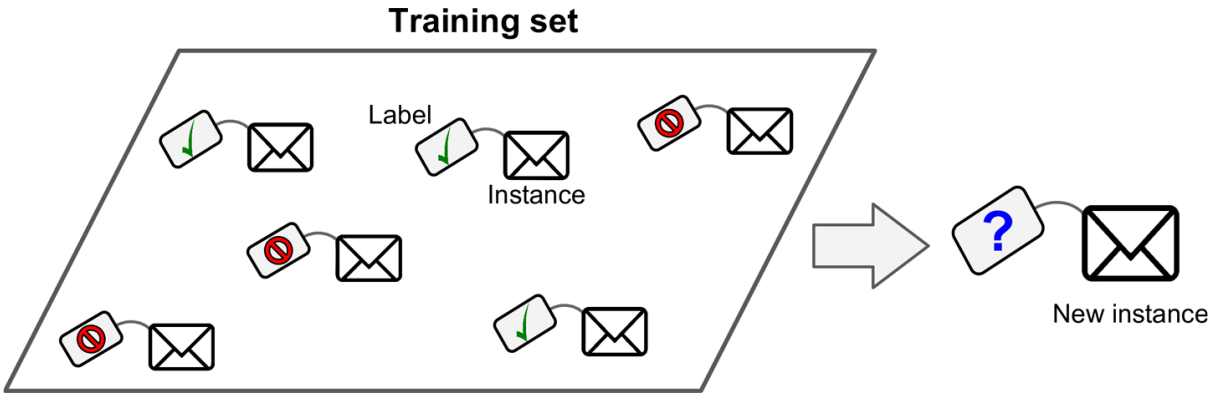

Figure 1.4 Supervised ML

Types of Supervised learning

A typical supervised learning task is ***classification***. The spam filter is a good example of this: itis trained with many example emails along with their *class* (spam or ham), and it must learn how to classify new emails.

Another typical task is to predict a *target* numeric value, such as the price of a car, given a set of *features* (mileage, age, brand, etc.) called *predictors*. This sort of task is called ***regression***.

- k-Nearest Neighbors
- Linear Regression
- Logistic Regression
- Support Vector Machines
- Decision Trees and Random Forests
- Neural networks

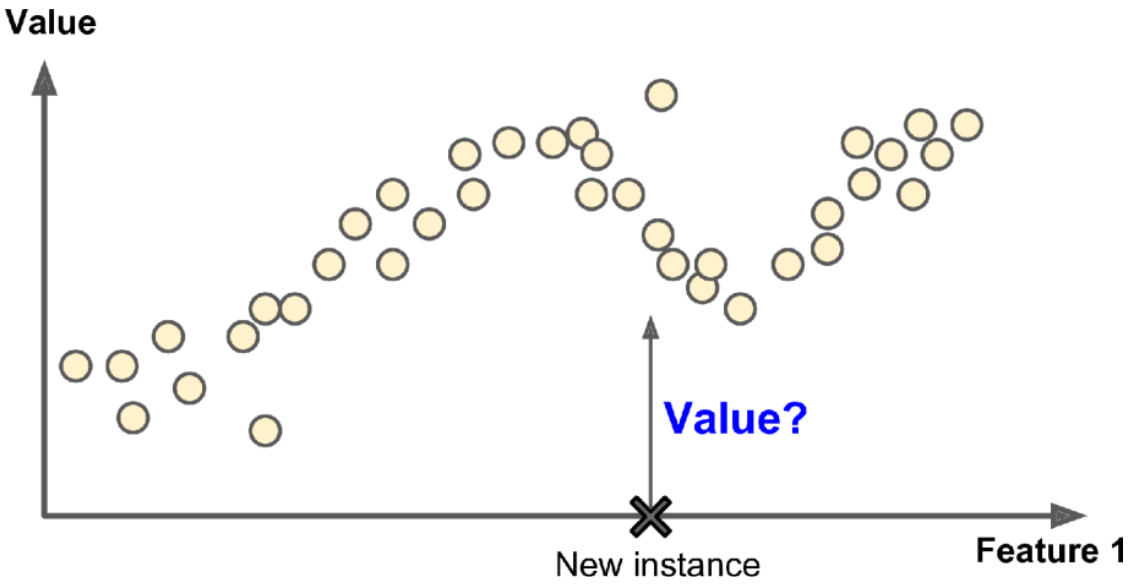

Figure 1.5 Regression

2) Unsupervised learning

In *unsupervised learning*, as you might guess, the training data is unlabelled. The system tries to learn without a teacher.

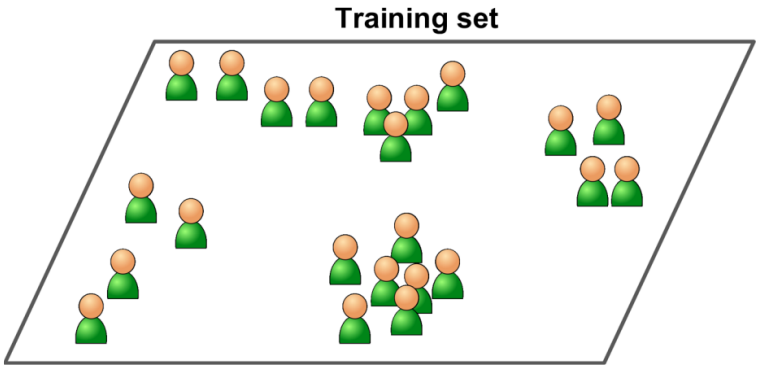

Figure 1.6 Unsupervised Learning

1.4.2 Deep learning

Deep learning is a subset of machine learning, which is essentially a neural network with three or more layers. These neural networks attempt to simulate the behavior of the human brain—albeit far from matching its ability—allowing it to "learn" from large amounts of data. While a neural network with a single layer can still make approximate predictions, additional hidden layers can help to optimize and refine for accuracy.

Deep learning drives many artificial intelligence (AI) applications and services that improve automation, performing analytical and physical tasks without human intervention. Deep learning technology lies behind everyday products and services (such as digital assistants, voice-enabled TV remotes, and credit card fraud detection) as well as emerging technologies (such as self-driving cars).

Figure 1.7 Deep Learning

Artificial Neural Networks

Deep Learning, on the other hand, is just a type of Machine Learning, inspired by the structure of a human brain. Deep learning algorithms attempt to draw similar conclusions as humans would by continually analyzing data with a given logical structure. To achieve this, deep learning uses a multi-layered structure of algorithms called neural networks.

The design of the neural network is based on the structure of the human brain. Just as we use our brains to identify patterns and classify different types of information, neural networks can be taught to perform the same tasks on data. The individual layers of neural networks can also be thought of as a sort of filter that works from gross to subtle, increasing the likelihood of detecting and outputting a correct result. The human brain works similarly. Whenever we receive new information, the brain tries to compare it with known objects. The same concept is also used by deep neural networks.

Neural networks enable us to perform many tasks, such as clustering, classification or regression. With neural networks, we can group or sort unlabeled data according to similarities among the samples in this data. Or in the case of classification, we can train the network on a labeled dataset in order to classify the samples in this dataset into different categories.

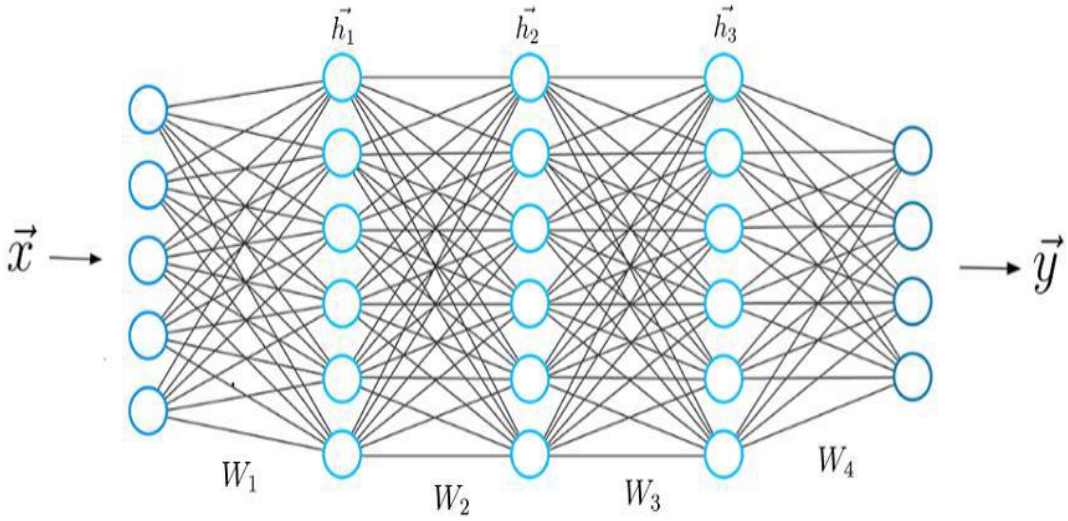

Figure 1.8 Neural Networks

Convolutional Neural Networks

The CNN architecture is complicated when compared to the MLP architecture. There are different types of additional layers and operations in the CNN architecture. CNNs take the images in the original format. We do not need to flatten the images to use with CNNs as we did in MLPs.

- Layers in a CNN: There are three main types of layers in a CNN: Convolutional layers, Pooling layers and Fully connected (dense) layers. In addition to that, activation layers are added after each convolutional layer and fully connected layer.

- Operations in a CNN: There are four main types of operations in a CNN: Convolution operation, Pooling operation, Flatten operation and Classification (or other relevant) operation.

- Convolutional layers and convolution operation: The first layer in a CNN is a convolutional layer. There can be multiple convolutional layers in a CNN. The first convolutional layer takes the images as the input and begins to process.

- Objectives: Extract a set of features from the image while maintaining relationships between the nearby pixels.There are three elements in the convolutional layer: Input image, Filters and Feature map. The *convolution operation* occurs in each convolutional layer.The convolution operation is nothing but an *elementwise multiply-sum* operation between an image section and the filter. Now, refer to the following diagram.

- Image section: The size of the image section should be equal to the size of the filter(s) we choose. We can move the filter(s) vertically and horizontally on the input image to create different image sections. The number of image sections depends on the *Stride* we use.

- Filter: This is also called *Kernel* or *Feature Detector*. This is a small matrix. There can be multiple filters in a single convolutional layer. The same-sized filters are used within a convolutional layer. Each filter has a specific function. Multiple filters are used to identify a different set of features in the image. The size of the filter and the number of filters should be specified by the user as hyperparameters. The size should be smaller than the size of the input image.

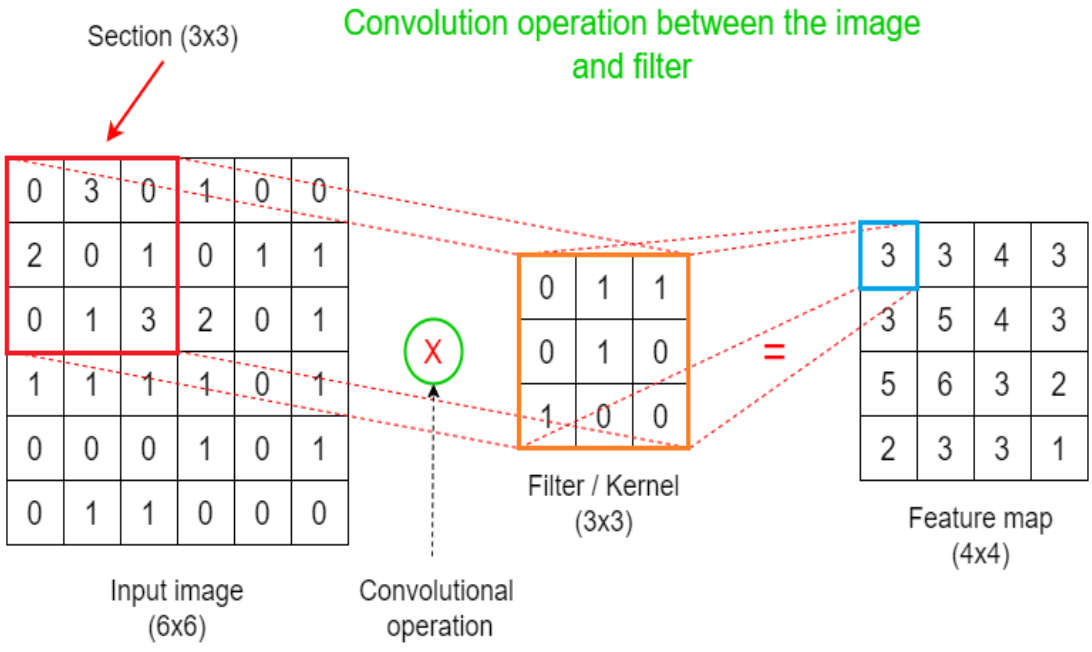

Image copyright: Rukshan Pramoditha

Figure 1.9 CNN

- Feature map: The feature map stores the outputs of different convolution operations between different image sections and the filter(s). This will be the input for the next pooling layer. The number of elements in the feature map is equal to the number of different image sections that we obtained by moving the filter(s) on the image.

- Pooling: Pooling layers are the second type of layer used in a CNN. There can be multiple pooling layers in a CNN. Each convolutional layer is followed by a pooling layer. So, convolution and pooling layers are used together as pairs.

  There are two types of pooling operations.

  Max pooling: Get the maximum value in the area where the filter is applied.
  Average pooling: Get the average of the values in the area where the filter is applied.

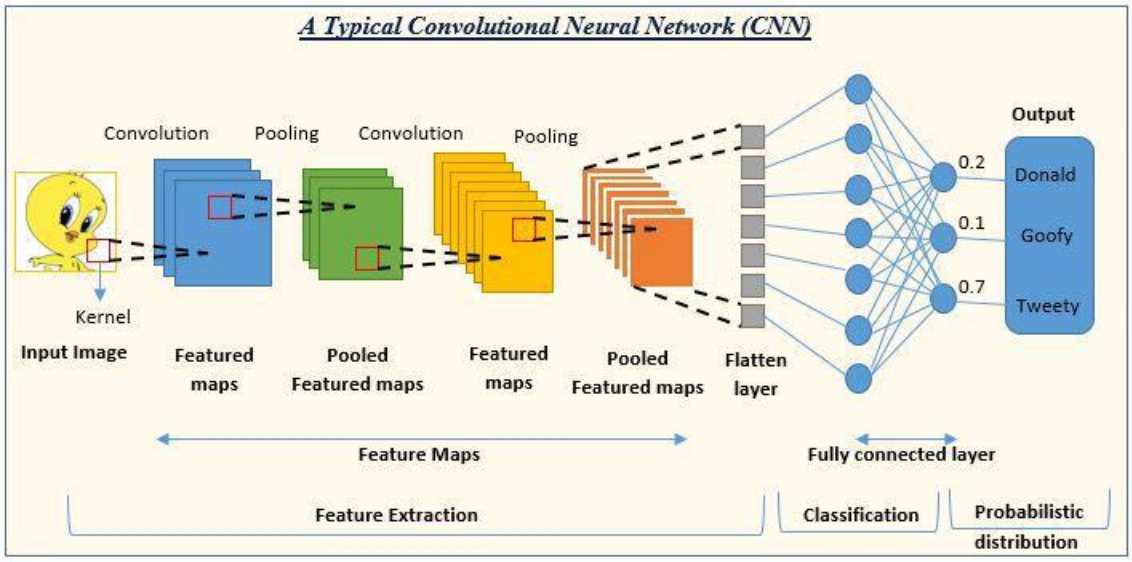

Figure 1.10 Convolution Operation

1.4.3 Streamlit

Streamlit is an open-source app framework for Machine Learning and Data Science teams. Streamlit is a free and open-source framework to rapidly build and share beautiful machine learning and data science web apps. It is a Python-based library specifically designed for machine learning engineers.

Figure 1.11 StreamLit

1.5 HARDWARE REQUIREMENTS

- Intel core i3 or greater
- Windows 10 or greater / ubuntu 20.04
- RAM 8gb or greater
- Hard disk 512gb

1.6 SOFTWARE REQUIREMENTS

- Anaconda/ Python 3.9 or greater
- Python libraries
  - Sklearn
  - TensorFlow
  - Pandas
  - NumPy
  - Pillow
  - Matplotlib
  - Joblib
- Vs Code
- Jupyter

2. LITERATURE SURVEY

2.1 EXISTING SYSTEM

The detection of image forgery has been the subject of numerous surveys over the decade. Lanh et al. [7] discussed numerous methods to detect image counterfeiting based on a camera. Author made a clear statement that, in terms of dependability, camera-based systems outperform other forgery detection methods. Pixel-based approaches, format-based techniques, camera-based techniques, physically based techniques, and geometric-based techniques are the five groups that Farid [4] divided under image counterfeiting tools. The author has thoroughly explained each technique.

Arif et al. [18], reviewed copy-move forgery detection techniques and categorised it mainly into two classes: block-based and key point-based approach. Meena K.B, Tyagi V [9] reviewed four types of tampering techniques namely image splicing, copy-move forgery, image resampling and image retouching detection.

This paper conducts survey for deep learning techniques for copy-move and splicing forgery.These methods actually date back to the pre-DL era, which is the one we are now in, and as a result, their eventual training phase requires little to no data. Traditional machine learning methods, such as clustering, support vector machines (SVM), linear/logistic regression, random forests, and so on, are often used in those that still need training data.

While they rely on models with a manageable number of parameters and don't necessitate a large amount of training data and classify here as classic approaches.

In order to speed up the training process or obtain better performance, deep learning models can also be employed in conjunction with some of the fundamental concepts and principles on which these approaches are based.

The statistical attributes derived from the image, such as JPEG recompression properties [11], lighting inconsistencies [5], chromatic aberration [6],device specific parameters [12], resampling[13] etc, were also used in previous systems to conduct image forgery detection.

2.2 PROPOSED SYSTEM

Deep learning techniques have become incredibly popular and have been used to solve a wide range of scientific issues. This is because it has been demonstrated that they excel in classification difficulties as well as regression and segmentation problems. Some techniques can even execute more accurately and precisely than humans for some tasks.

CNN has already proven to have exceptional potential in a number of computer vision applications, such as object detection and image segmentation. Due to the diverse origins of the images, a range of distortions appear when a piece of an image is transferred from one to another. CNNs can spot these distortions in falsified images even though they may be invisible to the unaided eye.

In [1], the authors have recompressed images and subtracted it from the original image. Due to the compression difference, the resulting image highlights the forged or sliced part as shown in fig 1. They trained the model by extracting the underlying features on the resulting image. By using the different compression quality, the authors have also shown that different quality leads to different accuracies of the model. In this paper two forgery techniques namely copy-move and splicing have been detected with an accuracy upto 92.3%. In [18], as a copy-move forgery detection method, deep neural network is able to detect pixel-level localization in copy-move forgery and is also able to separate the source and target region.

2.2.1 Recompression:

The image is compressed using JPEG compression and the compressed image is subtracted from the original image. Due to the compression difference, the resulting image highlights the forged or sliced part. This CNN based model detects both copy-move and splicing forgeries.

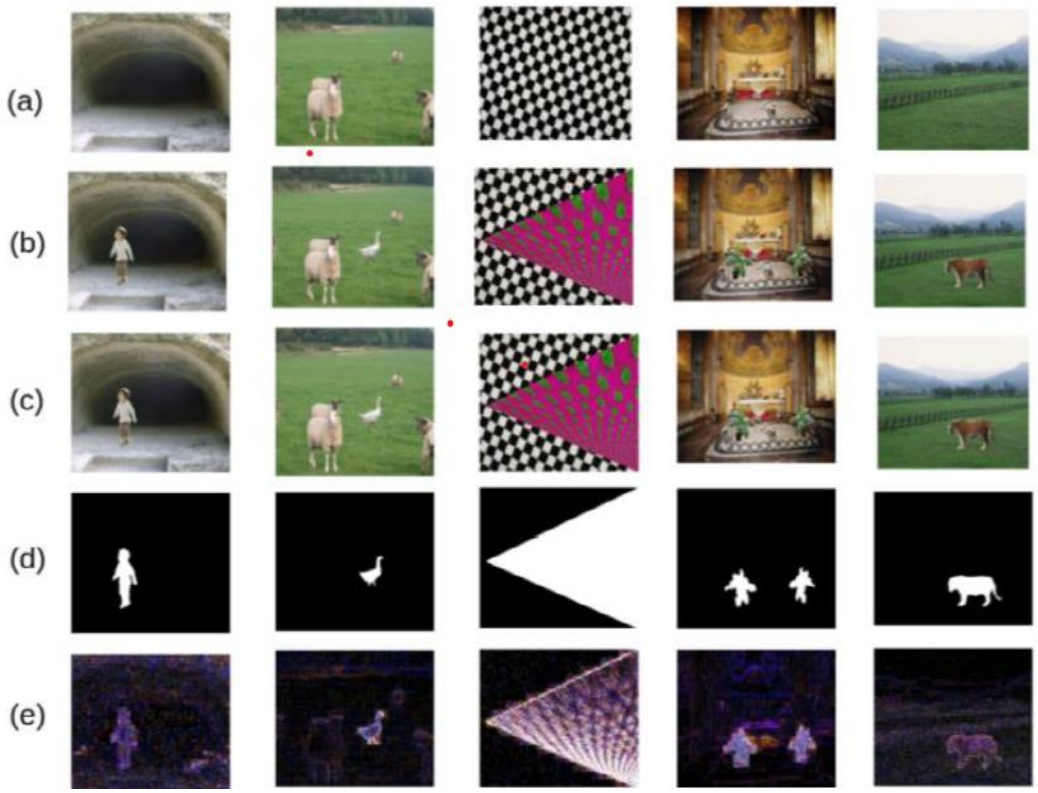

Figure 2.1 Recompression Original Image a) Forged Image b) Compressed Image c) Mask of image used to edit original image d) Subtracted Image

2.2.2 Splicing and copy-move

Copy-move Forgery

Copy-move forgery is a specific type of image tampering where a part of the image is copied and pasted somewhere else in the image with the intent to cover an important image feature. Hence, the goal in detection of copy-move forgeries is to detect image areas that are same or extremely similar. Copy-move forgery is a specific type of image tampering where a part of the image is copied and pasted somewhere else in the image with the intent to cover an important image feature.

Figure 2.2 copy move forgery

Splicing Forgery

In image splicing the contents of host images are modified by copying and pasting the contents from other images. Splicing forgery is commonly used to conceal the reality in images. Splicing introduces high contrast in the corners, smooth regions, and edges

Figure 2.3 Splicing Image forgery

These techniques fit the best in a general application context, in which the type of attack is not known a priori, so it is better to cover as many attacks as possible. In particular, we consider the methods tested on CASIA2, which is likely the most significant dataset for copy-move and splicing detection evaluation, both for its sheer size and for the various applied post-processing operations. Among the methods that we discussed, the one presented in [85] obtained the best overall accuracy. It also gives as output the localization of the forged areas, which as we mentioned is of course relevant in many application contexts. Looking at its forgery detection pipeline, it features both a pre-processing stage, in this case based on YCbCr space conversion and DCT compression, as well as a post-processing phase that through further features extraction allows to perform localization. Therefore, the good performance that it achieved indicate that an exclusively end-to-end deep learning model, without any pre-processing or post-processing, could be indeed a sub-optimal choice for the task of forgery detection. On the same note, another comment can be made about the method in [68]. Even if its performance are worse than the others in terms of accuracy, the proposed approach is quite interesting because it involves a “shallow” deep learning model. This allows reducing not only the number of network parameters (and consequently the training time), but also the risk of over-fitting. This idea is in contrast to the common trend in computer vision to use ever deeper networks to achieve high accuracy on specific datasets, that usually cannot be achieved on slightly different ones, which is a clear

indicator of over-fitting issues. A remark should be made on the approach proposed in [18]. This method has a wide applicability even outside the field of forgery detection. In fact, the possibility to extract the noise camera pattern and suppress the high-level scene content of a target image is of great utility in other forensic scenarios as well as for sophisticated camera-specific denoising applications. It is important to also note that the authors evaluated the performance of their algorithm on different datasets, which contain a wide set of forgery attacks such as copy-move, splicing, inpainting, GAN-synthesized content, face-swap, etc., thus proving its wide applicability and robustness.

2.2.3 Dataset Used

CASIA 2.0 Image Tampering Detection Dataset

Authentic images:

1. Au_ani_00001.jpg
   Au: Authentic
   ani: animal category
2. Other categories: arc (architecture), art, cha (characters), ind (indoor), nat (nature), pla (plants), txt (texture)

Tampering images

a. Spliced image

Tp_D_CRN_S_N_cha00063_art00014_11818.jpg

- Tp: Tampering
- D: Different (means the tampered region was copied from the different image)
- Next 5 letters stand for the techniques they used to create the images. Unfortunately, I don't remember exactly.
- cha00063: the source image
- art00014: the target image
- 11818: tampered image ID

b. Copy-move images

Tp_S_NRN_M_N_pla00020_pla00020_10988.jpg

- Tp: Tampering
- S: Same (means the tampered region was copied from the same image)
- And the rest is similar to case a.

3. SYSTEM ANALYSIS AND DESIGN

3.1 DFD

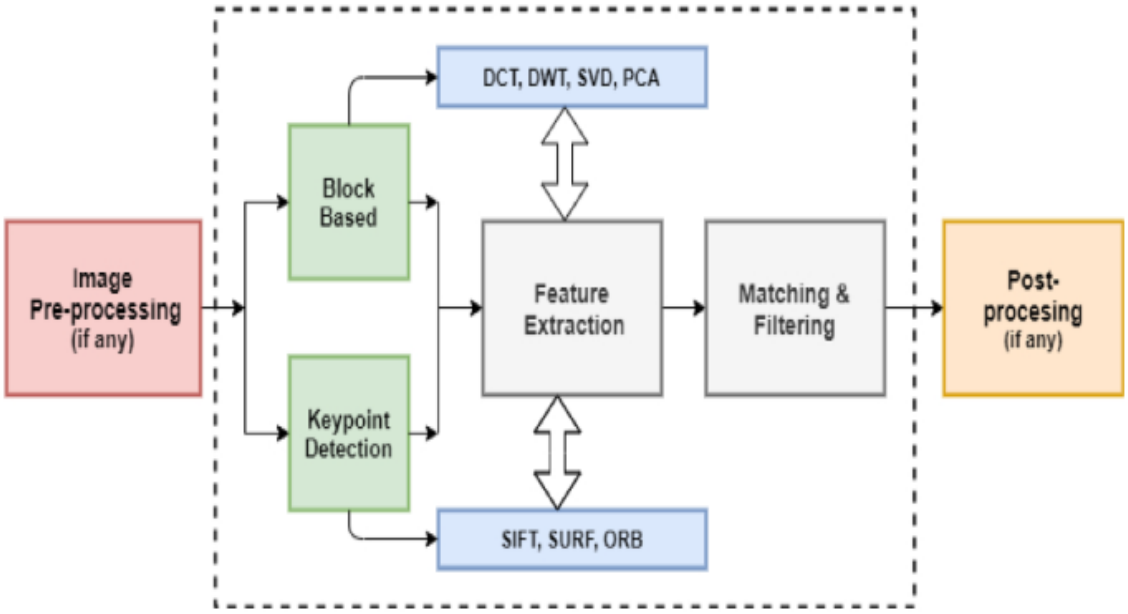

Figure 3.1 DFD

3.2 Methodology

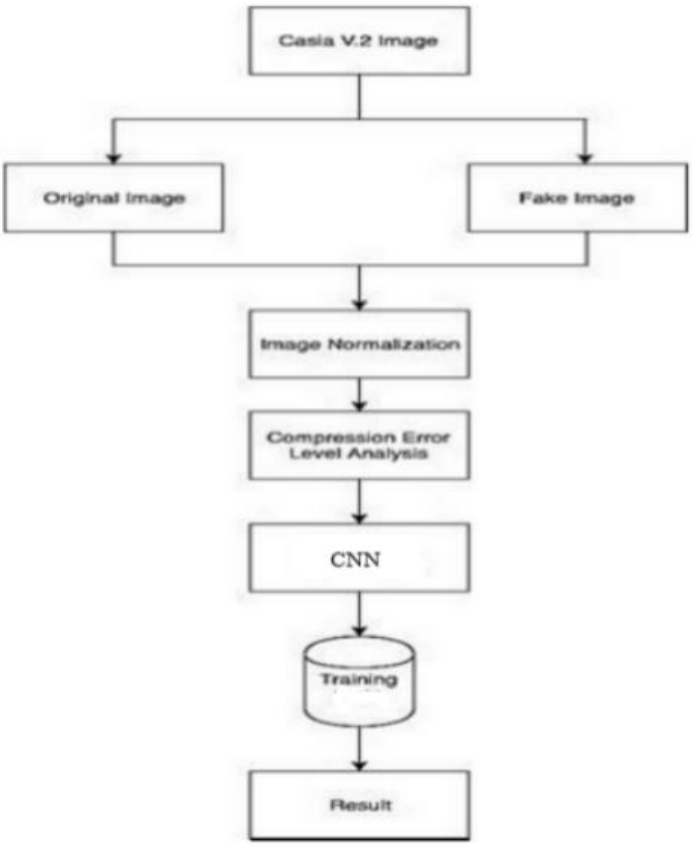

Figure 3.2 Methodology

3.3 Flow Chart

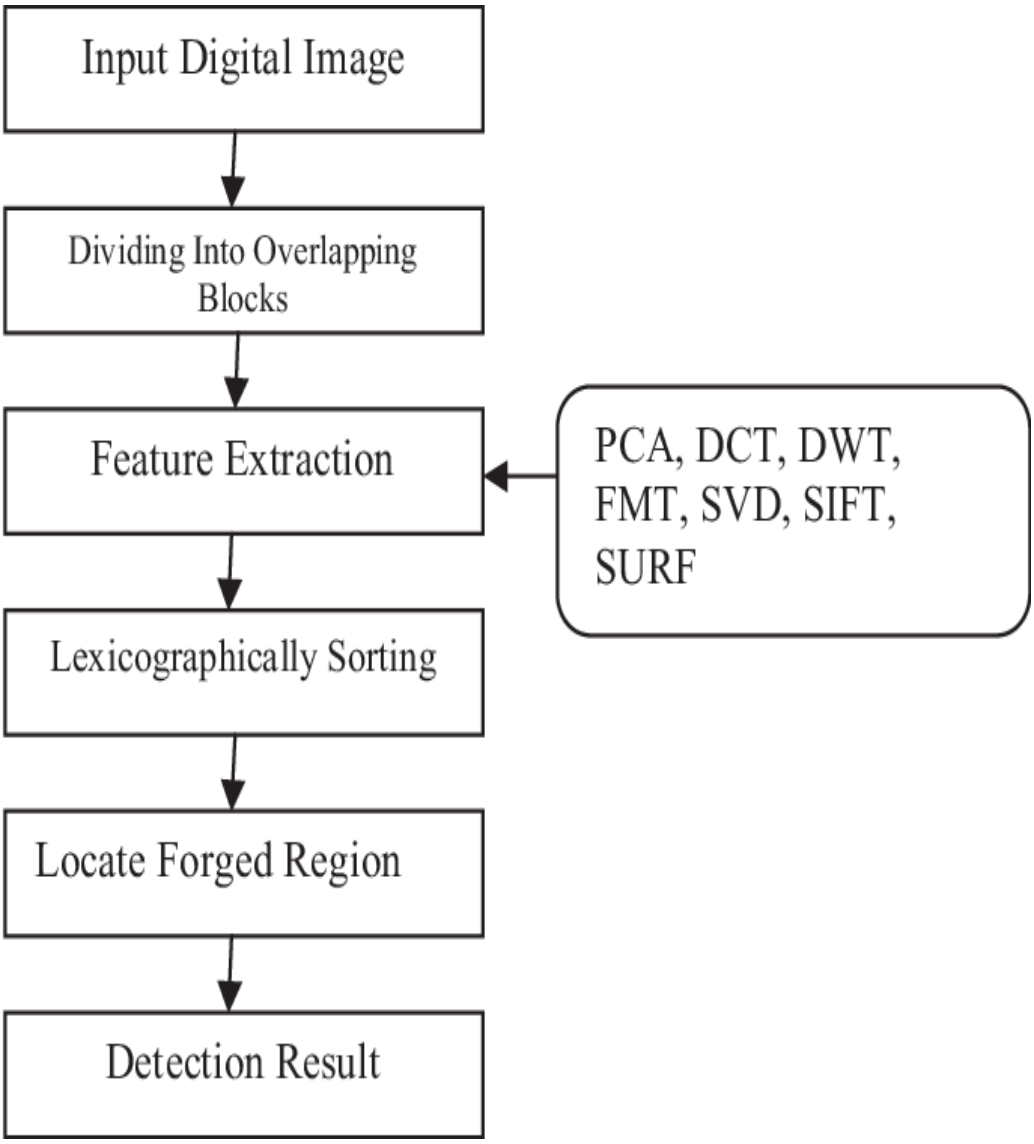

Figure 3.3 Flow Chart

4. RESULT

```
Model: "sequential"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 conv2d (Conv2D)             (None, 126, 126, 32)      896

 conv2d_1 (Conv2D)           (None, 124, 124, 32)      9248

 conv2d_2 (Conv2D)           (None, 120, 120, 32)      25632

 max_pooling2d (MaxPooling2D  (None, 60, 60, 32)       0
 )

 dropout (Dropout)           (None, 60, 60, 32)        0

 flatten (Flatten)           (None, 115200)            0

 dense (Dense)               (None, 256)               29491456

 dropout_1 (Dropout)         (None, 256)               0

 dense_1 (Dense)             (None, 2)                 514

=================================================================
Total params: 29,527,746
Trainable params: 29,527,746
Non-trainable params: 0
_________________________________________________________________
```

Figure 4 Model

```
79/79 [==============================] - 1s 16ms/step
Recall score: 0.9512195121951219
Precision score: 0.8426966292134831
Accuracy score: 0.9080459770114943
```

Figure 4.2 Accuracy

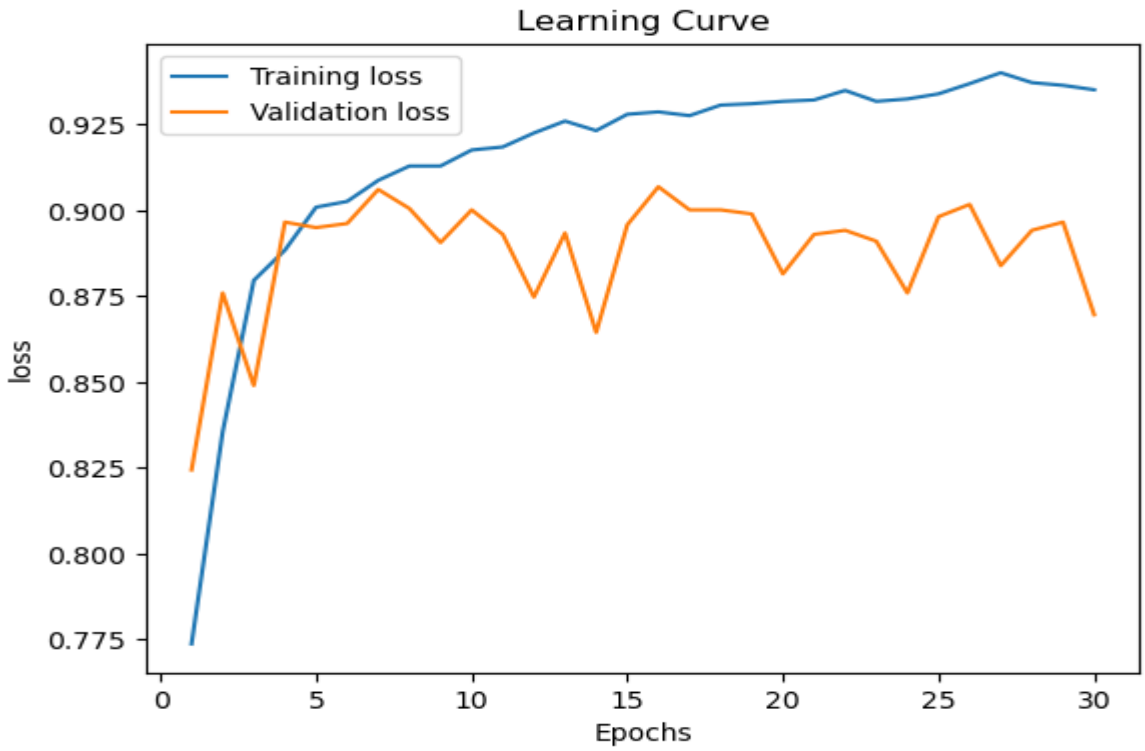

Figure 4.3 Training Loss

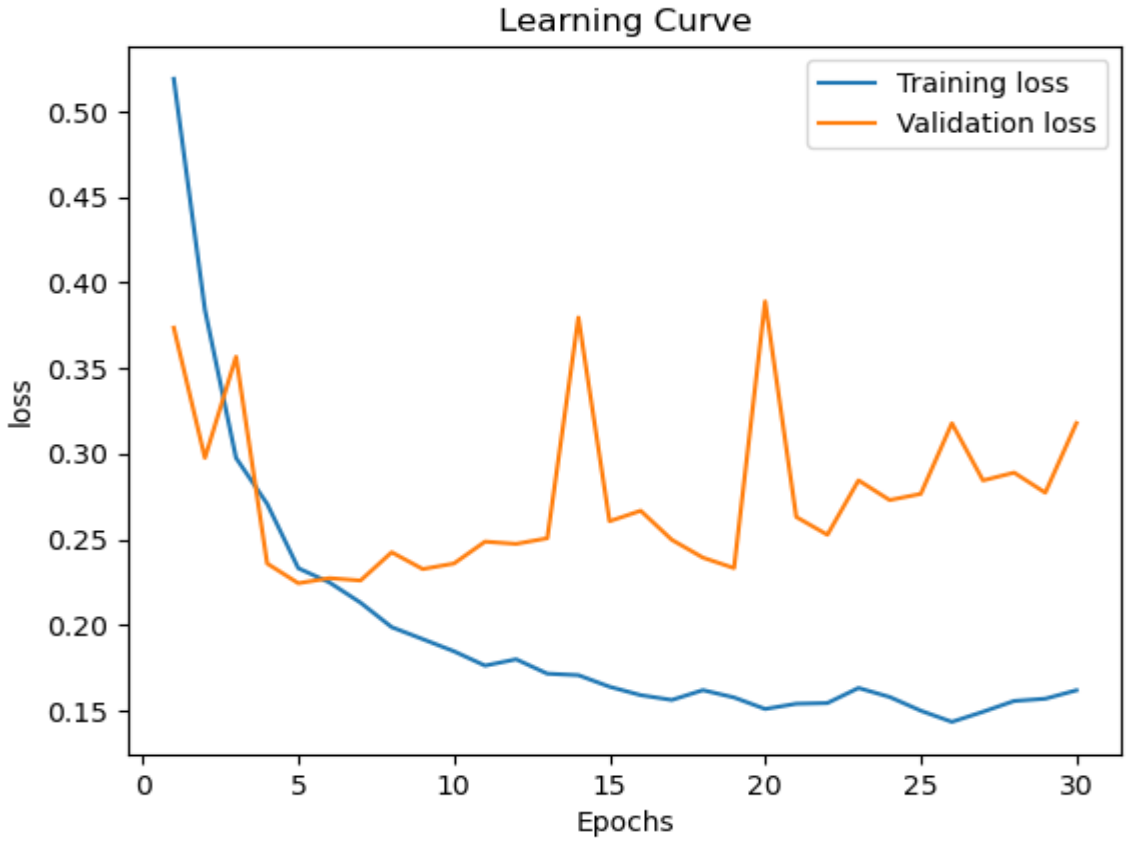

Figure 4.4 Actuary

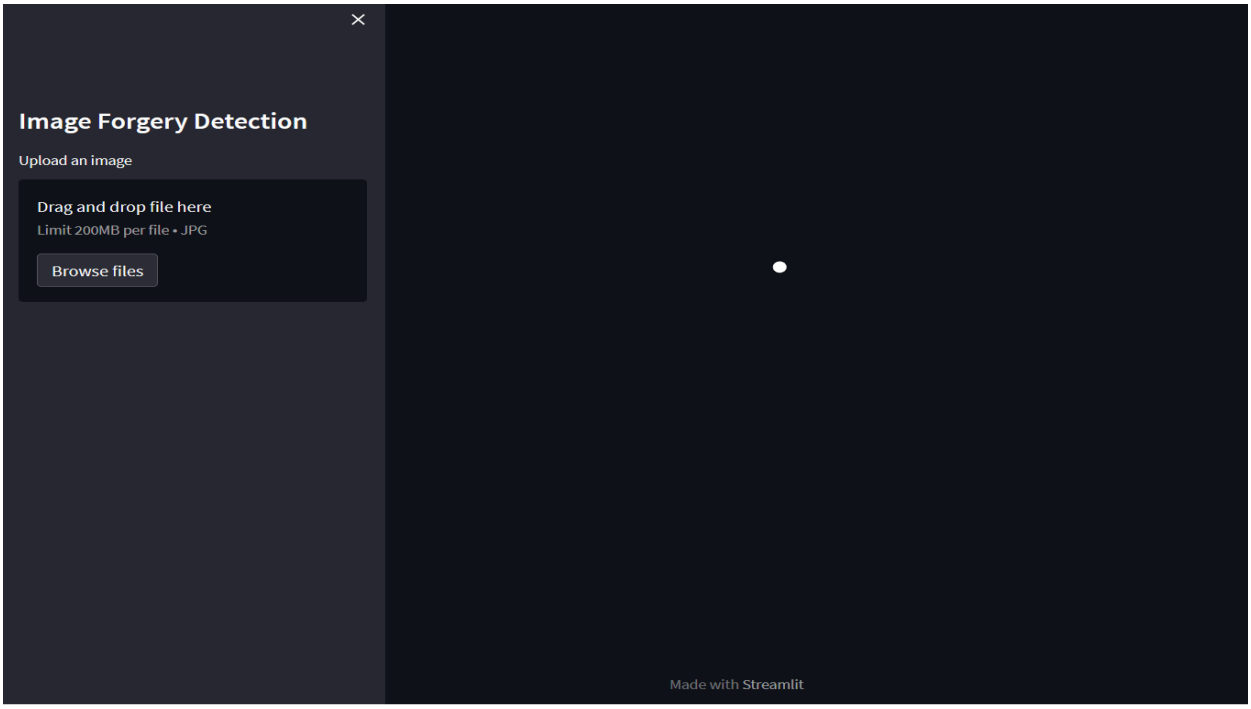

Figure 5 Output

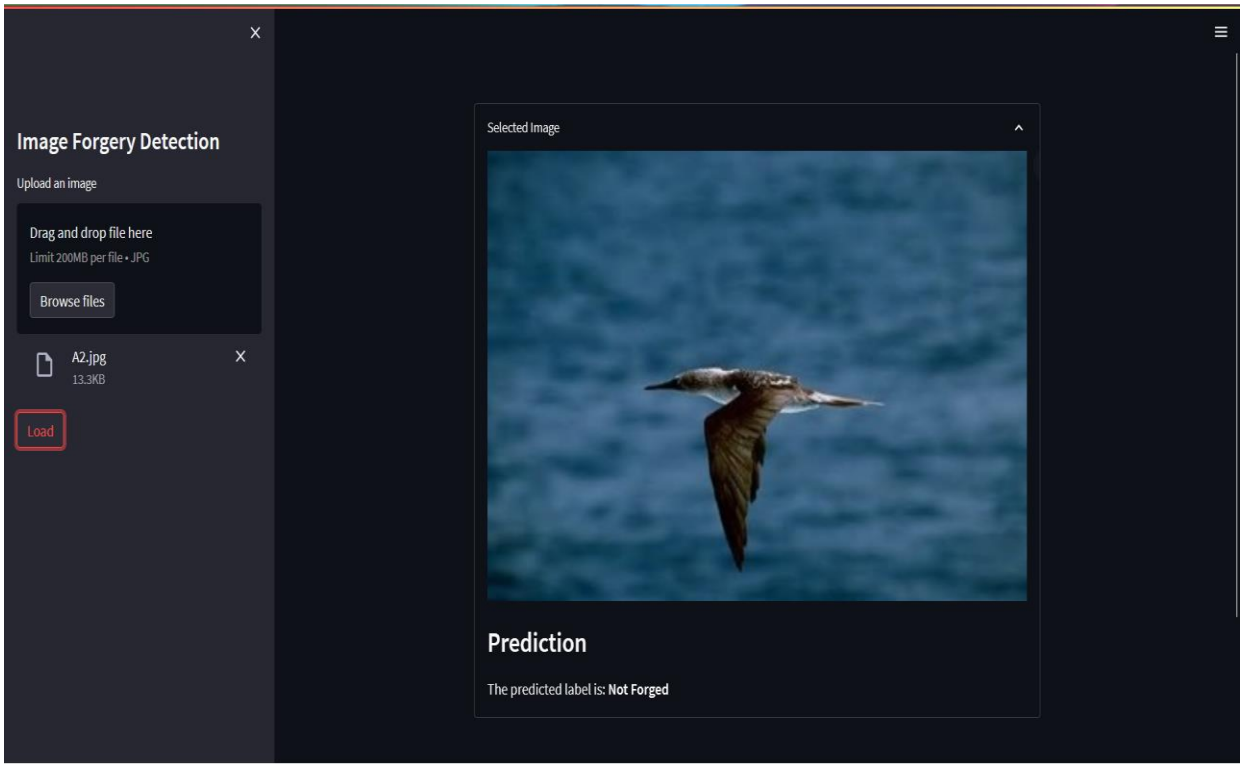

Figure 6 Output

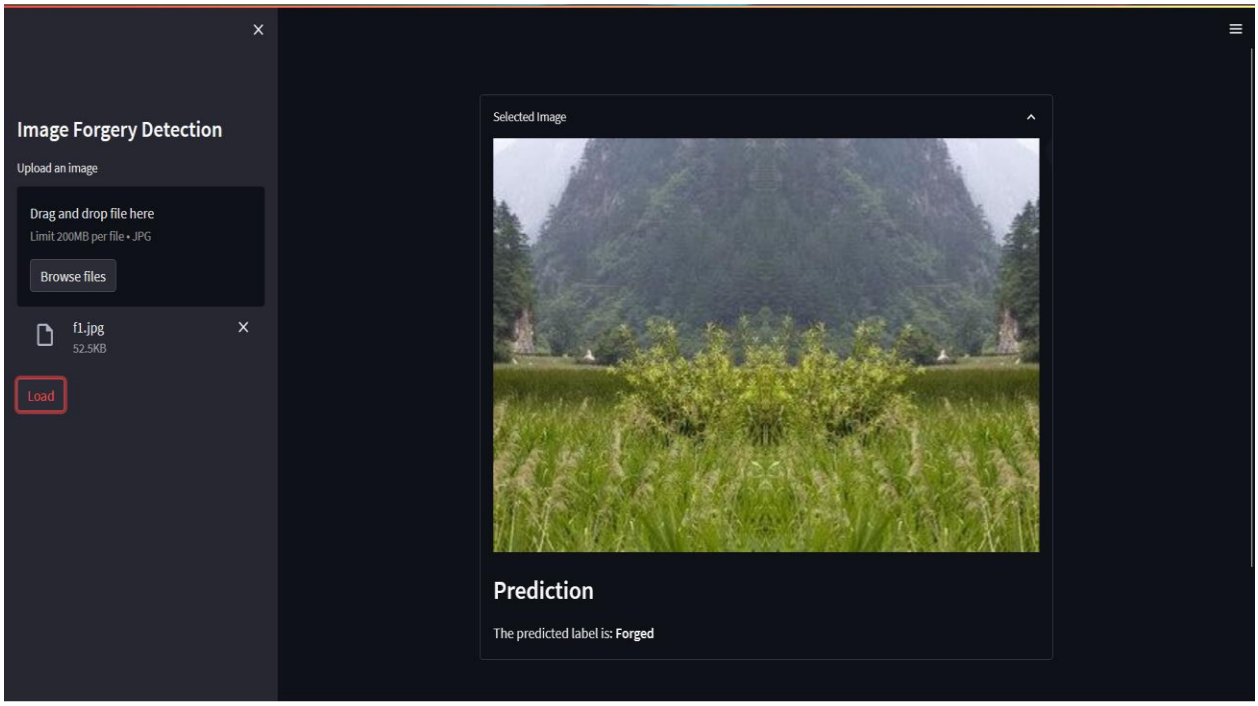

Figure 7 Output

5. CONCLUSION

The results obtained showed a high quality of image classification (97.8% accuracy for fine-tuned model and 96.4% accuracy for the zero-stage trained) and the possibility of applying the method under conditions of repeated compression of distorted images by the JPEG algorithm in a narrow range. In the future, it is planned to conduct a detailed comparison with other methods of detection of splicing and to implement detection of distorted areas.

We separated the performance analysis between copy-move only, both copy-move and splicing, From a general point of view, it can be easily inferred from the DL-based methods surveyed in this paper that a clear trend has not yet emerged. Most works have been more or less independently proposed, in the sense that the vast possibilities offered by DL architectures are still being explored, without a clear winning strategy indication

Various existing approaches such as BusterNet, Recompression, HHT and Wavelet Decomposition etc, have been examined, and it has been found that they all have one or more shortcomings such as inaccurate forgery detection, Complex computation, open to many attacks, including rotation, scaling, JPEG compression, blurring, and brightness manipulation, among others. Survey on techniques using deep learning as these are more accurate in generalizing the data and has better performance as compared to traditional techniques are focussed in this paper. Summarised overview of deep learning techniques will be useful and helpful to students and researchers in this field . From this it is inferred that Convolutional Neural Networks perform well as compared to other methods providing an accuracy of upto 92.23% while keeping various dataset in consideration.

REFERENCE

[1] Ali S.S. , Ganapathi I.I, Vu N. , Ali S. D., Saxena N and Werghi N. 2022 ‘Image Forgery Detection Using Deep Learning by Recompressing Images’ MDPI publication

[2] Christlein, V., Riess, C.C., Jordan, J., Riess, C.C., Angelopoulou, E. 2012, ‘An evaluation of popular copy-move forgery detection approaches’. IEEE Trans. Inf. Forensics Secur. 7, 1841–1854

[3] Abdalla Y, M. Iqbal.T and Shehata M 2019 ‘Convolutional Neural Network for Copy-Move Forgery Detection’ MDPI

[4] Farid, H. 2009, ‘A survey of image forgery detection techniques’. IEEE Signal Process. Mag. 26, 16–25

[5] Johnson MK, Farid H. 2005, ‘Exposing digital forgeries by detecting inconsistencies in lighting’. Proceedings of the 7th workshop on ACM Multimedia and Security Workshop, New York, pp. 1– 10

[6] Johnson MK, Farid H.2006, ‘Exposing digital forgeries through chromatic aberration’. In Proceedings of the 8th workshop on ACM Multimedia and Security Workshop, Geneva, Switzerland, pp. 48–55

[7] Lanh, T.V.L.T., Van Chong, K.-S., Chong, K.-S., Emmanuel, S., Kankanhalli, M.S. 2007, ‘A survey on digital camera image forensic methods’. In: 2007 IEEE International Conference on Multimedia and Expo, pp. 16–19

[8] Li, X., Jing, T., Li, X. 2010 ‘Image splicing detection based on moment features and Hilbert-Huang transform’ . IEEE Int. Conf. Inf. Theory Inf. Secur

[9] Meena K.B, Tyagi V : 2019, ‘Image Forgery Detection: Survey and Future Directions’ Data, Engineering and Applications pp 163–194

[10] Ng, T., Chang, S., Sun, Q. 2004 ‘Blind detection of photomontage using higher order statistics’. In: IEEE International Symposium on Circuits System, pp. 7–10

[11] Popescu AC, Farid H. 2004 ‘Statistical tools for digital forensics. 6th International Workshop on Information Hiding, Toronto’ , pp. 128–147

[12] Popescu AC, Farid H. 2005 ‘Exposing digital forgeries in colour filter array interpolated images’. IEEE Trans Signal Process 53(10):3948–3959:

[13] Popescu AC, Farid H. 2005, ‘Exposing digital forgeries by detecting traces of resampling’. IEEE Trans Signal Process 53(2):758–767:(2005)

[14] Schneider, M., Chang, S. 1996, ‘A robust content based digital signature for image authentication’. In: IEEE International Conference on Image Processing. pp. 227–230

[15] Shi, Y.Q., Chen, C., Chen, W.2007 ‘A natural image model approach to splicing detection’. In: Proceedings of 9th Workshop Multimedia Security, pp. 51–62

[16] Tait, A. 2017. ‘How a badly faked photo of Vladimir Putin took over Twitter’ . Available at: https://www.newstatesman.com/science-tech/2017/07/how-badly-faked-photo-vladimir-putin-took-over-twitter

[17] Wang, S., Zheng, D., Zhao, J., Tam, W.J., Speranza, F. 2007 ‘An image quality evaluation method based on digital watermarking’. IEEE Trans. Circuits Syst. Video Technol. 17, 98–105

[18] Warif, N.B.A., Wahab, A.W.A., Idris, M.Y.I. 2016 ‘Copy-move forgery detection: survey, challenges and future directions’ . J. Netw. Comput. Appl.

[19] Wu Y, Abd-Almageed W, Natarajan P. 2018 ‘Busternet: detecting copy-move image forgery with source/target localization’. Proceedings of the European conference on computer vision (ECCV), pp 168–184.