

A ROBUST DEEP NEURAL NETWORK FOR IMAGE FORGERY DETECTION

A thesis submitted in partial fulfillment of the requirements for the Degree of

DOCTOR OF PHILOSOPHY

By

SANJEEV KUMAR

Enrolment No: E17SOE812

Under the supervision of

Dr. Suneet Gupta and Dr. Umesh Gupta



**BENNETT
UNIVERSITY**
THE TIMES GROUP

School of Computer Science Engineering and Technology,

BENNETT UNIVERSITY

(Established under UP Act No 24, 2016)

Plot Nos 8-11, Tech Zone II,

Greater Noida-201310, Uttar Pradesh, India.

December, 2022

DECLARATION BY THE SCHOLAR

I hereby declare that the work reported in the Ph.D. thesis entitled “**A robust deep neural network for image forgery detection**” submitted at **School of Computer Science Engineering and Technology, Bennett University, Greater Noida, India**, is an authentic record of my work carried out under the supervision of **Dr. Suneet Gupta and Dr. Umesh Gupta**. I have not submitted this work elsewhere for any other degree or diploma. I am fully responsible for the contents of my Ph.D. thesis.

Signature of the Scholar

Sanjeev Kumar

(E17SOE812)

School of Computer Science Engineering and Technology

Bennett University, Greater Noida, India

Date



CERTIFICATE

This is to certify that the work reported in the Ph.D. thesis entitled “**A robust deep neural network for image forgery detection**”, submitted by **Sanjeev Kumar** at School of Computer Science Engineering and Technology, **Bennett University, Greater Noida, India**, is a bonafide record of his original work carried out under my supervision. This work has not been submitted elsewhere for any other degree or diploma.

Dr. Suneet Gupta
Bennett University, India
Date:

Dr. Umesh Gupta
Bennett University, India
Date:

PREFACE AND ACKNOWLEDGEMENT

I will always be grateful to Dr. Suneet Gupta, Associate professor and Dr. Umesh Gupta, Assistant professor, Bennett University, for their unceasing efforts to mentor and support me throughout my research career and for achieving the required research milestones. I am very thankful to them for pointing out the way forward whenever there was any difficulty. I thank my supervisors for being by my side during crucial periods of this journey.

I would like to express my deepest gratitude to Dr. Deepak Garg, Professor and Dean School of Computer Science Engineering and Technology, Bennett University, for providing such a wonderful research environment, resources, and motivational support. I am thankful to you sir for giving insightful inputs for improving the research outcomes. I am also thankful to RAC members Dr. Ayan Khan, Dr. Divya Shrivastava, for their progressive recommendations, valuable inputs and ideas. I also extend my thanks to Dr. Manjit Kaur for her support in my research work.

It's my privilege to give thank my Father (Late shri. Ashok Kumar), without the blessings of whom I can never succeed in life. I thank my beloved mother (Smt. Krishna Devi) for her emotional support and blessings that has been a great motivation to complete this journey. I also thankful to my spouse Ms. Anu Kapoor for her generous support, and encouragement that helped me in finishing my research.

I also thank to Dr. Adesh Kr. Pandey, head of IT department (KIET group of institution), for his support and encouragement for completing the research work. I am grateful to all my Faculty members, friends, colleagues, seniors and juniors, who directly or indirectly helped in completing this research journey.

Sanjeev Kumar
(E17SOE812)

LIST OF FIGURES

Figure Number	Caption of Figures	Page Number
1.1	Types of forgery	2
1.2	Example of copy move forgery	3
1.3	Example of splicing	3
1.4	Example fo morphing	3
1.5	Image retocuhing	4
1.6	Image forgery detection tehcniques	4
2.1	Different appraoches for foregery detection	12
2.2	Deep CNN model for image forgery detection	16
2.3	Two branch Deep neural network	17
3.1	Proposed CNN Architecture	26
3.2	Accuracy graph on COMOFOD dataset	28
3.3	Accuracy graph on COMOFOD+DIID dataset	29
3.4	Accuracy graph on COMOFOD+DIID+Image Manipulation dataset	29
4.1	Example (2) image forgery	32
4.2	The propsoed hybrid model	34
4.3	COMOFOD dataset sample images	37
4.4	Training and validation accruacy graphs	40
4.5	Training and validation loss graphs	41
4.6	Performance comparison hybrid with other models	43
4.7	Layer-1 Output original and forged image	44
4.8	Layer-2 Output original and forged image	44
4.9	Layer-3 Output original and forged image	45
4.10	Layer-4 Output original and forged image	45
4.11	Layer-5 Output original and forged image	45
4.12	Grad-cam Result with heatmap	46
5.1	Example of copy-move, splicing and morphing	49
5.2	Evaluation parameter result	51

6.1	Forgery detection techniques	53
6.2	Copy Move forgery example(3)	54
6.3	Sample forged images with copied blocks in red squares	60
6.4	AUC-ROC curve comparison for different datasets	64

LIST OF TABLES

Table Number	Caption of Tables	Page Number
2.1	Comparative analysis of block level approaches	13
2.2	Deep learning-based models for forgery classification	18
2.3	Transfer learning-based models for forgery detection	19
2.4	Hybrid models for forgery detection	20
2.5	Parameters on 15 studies: available data + inferred values	22
2.6	Grading scheme for the attribute evaluation.	23
3.1	Accuracy achieved on different dataset.	28
3.2	Confusion matrix results.	28
3.3	Comparison with other approaches using COMOFOD dataset	29
4.1	Diversity of images and dataset for training	36
4.2	Epochs wise Training and validation results	37
4.3	Performance evaluation results in different folds.	41
4.4	Testing results. VI-Net (Proposed) vs. Other ML/DL techniques similar dataset	42
4.5	Performance comparison of VI-Net	47
5.1	Algorithm evaluations results	50
5.2	Confusion matrix and related parameter results	51
6.1	Summary of datasets used for algorithm evaluation	59
6.2	Statistics of matching 2 sub blocks in forged and non forged images	61
6.3	Evaluation Parameters result in ascending order with different datasets	62
6.4	Statistical Result of different parameters considering all results for datasets under study	64
6.5	Benchmarking of proposed algorithm with existing literature results based on dataset.	65
6.6	Pixel level results with different number of blocks	66

LIST OF ACRONYMS/ABBREVIATIONS

S.N.	Abbreviation/ Symbol	Description
1	CNN	Convolutional Neural Network
2	CMFD	Copy-move forgery detection
3	AI	Artificial Intelligence
4	NFI	Non forged image
5	DL	Deep Learning
6	PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analysis
7	ROBINS-I	RoB In Non-Randomized Studies - of Interventions
8	PROBAST	Prediction model for RoB assessment tool
9	FNR	False Negative Ratio
10	FPR	False Positive ratio
11	COMOFOD	Copy-move forgery Database
12	TP	True Positive
13	TN	True Negative
14	FP	False Positive
15	FNR	False Negative Ratio
16	GAN	Generative adversarial network
17	FCM	Feature Correlation Matching
18	VGG	Visual Geometry Group
19	DCT	Discrete Cosine Transform
20	DWT	Discrete Wavelength Transform
21	SIFT	Scale invariant feature transform
22	SURF	Speedup robust feature transform

TABLE OF CONTENTS

	Page Number
DECLARATION BY THE SCHOLAR	i
CERTIFICATE	ii
PREFACE AND ACKNOWLEDGEMENT	iii
ABSTRACT	iv
TABLE OF CONTENTS	vi
LIST OF FIGURES	viii
LIST OF TABLES	x
ACRONYMS/ABBREVIATIONS	xi
1. INTRODUCTION	1-10
1.1 Types of image forgery	2
1.1.1 Copy move forgery	2
1.1.2 Splicing	3
1.1.3 Morphing	3
1.1.4 Image Retouching	3
1.2 Image forgery detection methods	4
1.3 Research Gaps	5
1.4 Research objectives	6
1.5 Why deep learning methodology	6
1.6 Performance evaluation parameters	7
1.7 Contributions	8
1.8 Organization of thesis	9
2. LITERATURE REVIEW	11-24
2.1 Introduction	11
2.2 Block level approaches	12
2.3 Key point based approaches	13
2.4 Deep learning based approaches	14
2.5 Assessing the Risk of Bias (ROB) of deep learning approaches	21

2.6	Strength, weakness and extensions	24
3	EFFICIENT END TO END CNN FOR FORGERY CLASSIFICATION	25-30
3.1	Customized CNN architecture	25
3.2	Result and discussion	27
3.3	Conclusion	30
4	VI-NET: A HYBRID DEEP CNN	31-47
4.1	Introduction	31
4.2	Proposed Methodology	32
4.2.1	Motivation	33
4.2.2	Proposed ensemble architecture	33
4.2.3	Underlying principle	34
4.3	VI-NET Results	35
4.3.1	Dataset	35
4.3.2	Performance analysis	37
4.4	Conclusion	47
5	BLOCK LEVEL FORGERY MASK DETECTION	48-52
5.1	Introduction	48
5.2	Proposed algorithm	49
5.3	Result	50
6	FORGERY DETECTION AND LOCALIZATION	53-67
6.1	Introduction	53
6.2	Related work	54
6.3	Proposed Algorithm (NB-Localization)	56
6.4	Results and discussion	58
6.4.1	Dataset description	59
6.4.2	Evaluation parameters	61
6.4.3	Pixel wise result for different block size	66
6.5	Conclusion	67
7	CONCLUSION AND FUTURE SCOPE	68-69
	REFERENCES	70
	LIST OF PUBLICATIONS	89

ABSTRACT

One of the crucial research areas in the field of image forensics is the detection of image forgeries. Due to the availability of cutting-edge technology, strong image editing tools, and software packages, images can be easily modified or tampered. Human being is living in the world of digitalization. We are surrounded by many images, but all images are not real, it might be fake. There are several of types image forgeries possible, copy-move forgery is one important method, which is in recent trends. In copy move forgery, one part of the image is copied and pasted at different location in the same image, which reflect different perception about the image. To handle this problem, three categories have been used such as block level, key point based and deep learning based solutions. There are various block-level approaches like local binary pattern, stationary wavelet transform, key point-based approaches such as scale invariant feature transform, speedup robust features transform and deep learning based approaches named as mobile net, Inception net and many more. Although recently, deep learning models are getting more interest towards researchers in compared to block level and key point based approaches. As the deep learning models are able to automatically learn and extract the features from the related training dataset.

We have thoroughly reviewed and investigated the available approaches in the literature for improving the image forgery classification and detection performance. We have improvised the deep neural network models for reducing the computation cost and achieve better accuracy.

In this thesis, we proposed a lightweight customized CNN model to attain better classification performance for forged images as preliminary work. Furthermore, we extend this approach and handle the limitations by proposing a new hybrid approach as VI-NET, a ensemble deep neural network. This hybrid approach utilize VGG16 and inception V3 model. The performance of VI-NET is also compared with other state of art deep learning models and will achieve better generalization performance. We also focused on the issue of localization in copy-move forgery images. Initially we implement a DCT (Discrete Cosine transform) block level features extraction approach for copy-move forgery mask detection. Here, we improved the performance of mask detection. Further, we have extended this work to detect the copy-move forged area in images using non-overlapping block level pixel comparisons, with better detection and classification accuracy. We have used structure

similarity index (SSIM) parameter to classify the image as forged or original. The algorithm is tested using a various standard and publically available datasets named MICC, CASIA, Coverage and COMOFOD. This algorithm is able to obtain a maximum accuracy of 98%. We also compared our results using additional metrics, such as precision, recall, FPR, and FNR.

CHAPTER 1

INTRODUCTION

The human being with the advancements of technology is surrounded by many images. It can be images on social media and images shared through various digital platforms with other friends and relatives. In today's life images are playing a vital role in the perception building of a person. Can we rely on the images which we are receiving or forwarding? Are we sure that we are sending the right information to the rest of the internet world? We are not confident in answering these questions. Further, If such images are used as evidence in the judiciary system, can lead to injustice for the persons being convicted. The other reason of doubting the images arises specifically in today's era when even our handheld devices have high-end capabilities to change the appearance of images. The texture of the image can be changed in such a way that it becomes difficult to identify the possibility of any tempering.

Thus, we can define image forgery (IF) as set of techniques that are applied to authentic images to hide their real meanings and interpretations [1]. The forged digital images taken from social media, newspapers, healthcare documents, and websites lose their real interpretation [2]. For example, in 2008, Iran published altered images showing four missile tests, which provided false information about the country's military capabilities [3]. Further, the transmission of forged images related to healthcare and diagnostic tests over the internet can lead to wrong diagnoses [4]. Thus, there is a clear need for effective methods for the detection of image forgery.

The images can be subject to many types of forgeries. Copy-move forgery [5][6] is most common forgery. In copy-move forgery, one image patch is copied, and the same patch is pasted at some other location in the same image. There are claims that various deep learning techniques [7][8] are more effective solutions for image forgery detection as compared to non-AI-based methods, such as block-level and key point-based methods [9]–[11]. While more modern AI-based systems like deep learning, can automatically learn the model features from training images[12], older AI approaches, such as machine learning, are primarily focused on handcrafted features [13]. For instance, a two-stage deep neural network with an encoder-decoder architecture yielded a classification accuracy of 98% [14], and a generative adversarial network (GAN) with a convolution neural network (CNN) classified and

localized the forged image area with 95% accuracy [15]. Deep learning approaches learn non-linear features and produce more generalized models in healthcare [16] and non-healthcare domains [17]-[18]. Here in this chapter a detailed introduction to image forgery, its types, and research gaps in literature, research objectives and contributions is discussed. We have also discussed the possibility of bias for effective deep learning solution for image forgery detection.

1.1 Types of image forgery

Different types of forgery can be applied on images such as copy-move forgery, image splicing, retouching, morphing etc. as shown in Figure 1.1. Our focus is on one of the passive image authentication technique, the copy - move forgery detection. The most frequently used image forgery technique that is applied on images is a copy-move forgery [5].

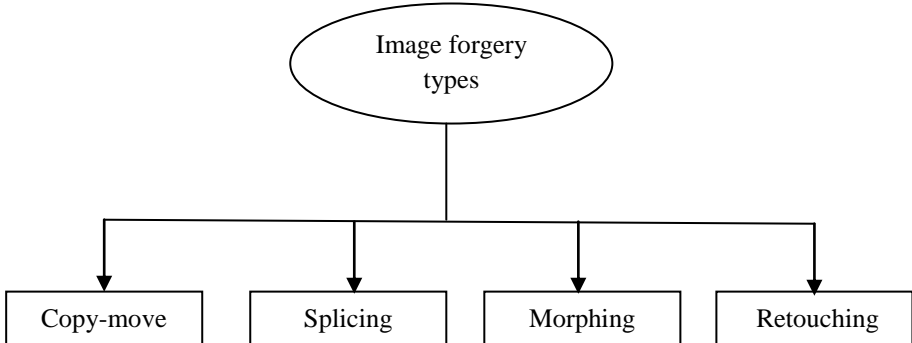


Figure 1.1: Types of forgeries

1.1.1 Copy-move forgery:

In copy-move forgery some part of image is copied and pasted on other part of image with objective of hiding some facts or to have multiplicative effect for different objects in image as shown in Figure 1.2. Various image transformation like, rotation, scaling, compression are applied on the copied patches to make the forgery detection difficult [4].

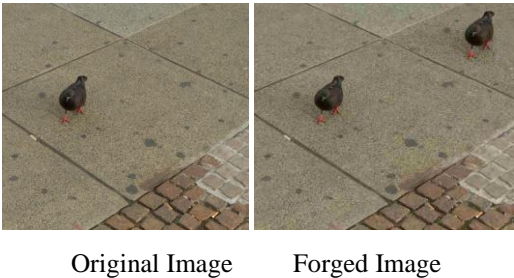


Figure 1.2: Example of copy-move forgery

1.1.2 Splicing:

Splicing is kind of forgery where two different images are combined together to indicate have different interpretation [19] which is actually not true. Image splicing used objects from different images. Tempering can be performed either using one object or we can select multiple objects as well to have splicing effect. Such type of forgery is comparatively difficult to detect. Splicing is illustrated in Figure 1.3 shown below.



Figure 1.3: Example of Splicing

1.1.3 Morphing:

An phenomenon known as morphing involves the smooth transformation of one shape image into another. It is a kind of tempering where after successive blurring or transformation or by mixing two images other image can be generated [20] similar to third person/object as shown in Figure 1.4. The change is performed gradually from one image to other. We need at least two images for this forgery to apply.



Figure 1.4: Example of Morphing

1.1.4 Image Retouching:

By using this forgery one can enhance or degrade the quality of image through some manipulations at image level [19]. The parameters that can be modified may include color of image, changing the lighting conditions of image etc. as shown in Figure 1.5.



Figure 1.5: Example of Retouching

1.2 Image forgery detection methods

Researchers have been motivated to develop a variety of different forgery detection systems as a result of the many types of image forgeries. Figure 1.6 depicts a classification tree of several strategies [23] for detecting forgeries. It was created with the help of multiple publications that can be found in the academic literature relevant to image forgery [29]–[32]. In a general sense, these kinds of solutions may be categorised into two basic groups: (i) active paradigms and (ii) passive paradigms. *Active* paradigms capture images in real-time; however, the authentic information embedded in

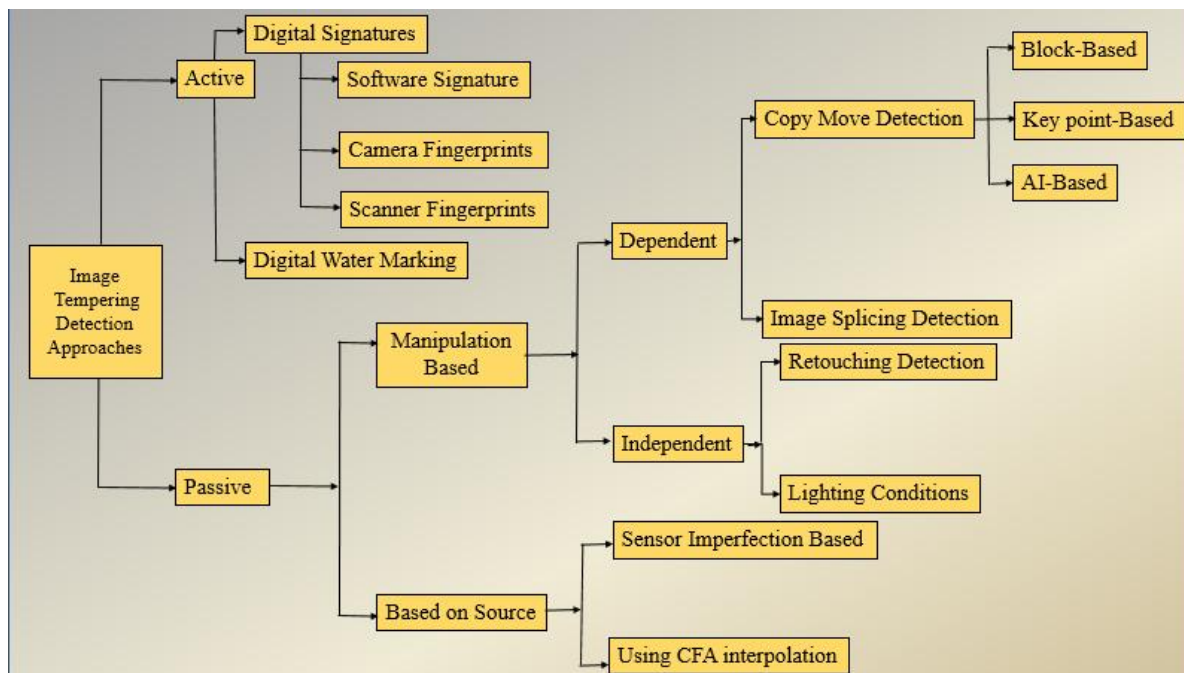


Figure 1.6: Image forgery detection techniques

the image during the generation time is always present—for example, as a digital watermarking [28] or digital signature [29]. In order to perform authentication while simultaneously getting access to the image, active paradigm detection approaches require

their own specific software procedures. The detection of forgery using passive techniques involves searching for statistical features of image attributes that include evidence of fabrication. The vast majority of the currently available algorithms for detecting image forgery rely on hand-created characteristics of features. These methods are divided into two categories: (a) block-based or (b) key point-based. Copy move passive image forgery detection methods uses block-level [30]–[36], key point based [37]–[44] and deep learning based [50]–[55] methods. Block level approaches divide the whole image into overlapping and non-overlapping blocks of fixed size. Here, feature extraction is done at the block level using block transformation techniques, such as discrete cosine transform [51] or discrete wavelet transform [52], unlike scaling and blurring, are highly efficient [53]. In key-points based approaches, several key points are extracted from an image using standard feature transformation processes. Feature extraction algorithm such as scale-invariant feature transform algorithm is used. Among the key point based techniques, the speeded-up robust feature transform algorithm is the most commonly used [54]. Using this approach, key points are extracted and matched among other key points using parametric techniques and machine learning approaches, such as clustering and Euclidian distance. Recent research [55] has proposed a modified scale invariant feature transform (SIFT) structure to remove the contrast thresholding parameter. It will be beneficial to get even better key points on homogenous surfaces while not affecting the key point distributions over textured areas of images [56].

1.3 Research Gaps

As mentioned earlier, there are several types of image forgery possible. Different types of forgeries come with different types of challenges. E.g. in case of copy-move forgery detection where sometimes the image patches are rotated or scaled. Identifying such forged patches pose a challenge. Although, if no further alteration is made to the copied region, the block level technique can quickly identify forged area in the image. However, major issues emerge when the duplicated area is rotated through some angle before being moved. This rotation complicates the detection even more since matching detection gets harder when the angle or rotation changes. Other transformations performed on the forged area include reflection or mirror image, scaling of the tempered region, and modifying the compression level of the image patch before forging. We need a strong approach that can classify the forged image even when the aforementioned modifications are performed on tempered regions.

Based on the literature study, the following gaps in existing studies identified:

- A large size dataset including different mix of social media images, images of various sizes and noise-based images can improve the robustness of model.
- Although there are various techniques, none of them are robust to all conceivable variation and lack precision.
- The key point-based techniques are not effective for images with less texture.
- For geometrically changed objects in an image, block level approaches are ineffective.
- This is a very rare use of a deep learning-based method for image forgery classification and detection. Localization has received little attention and should be pursued further. There have been few studies on hybrid deep learning models for visual forgery classification.

1.4 Research objectives (RO's)

With a comprehensive literature investigation and acknowledging the research gaps, the following are the research objectives for this research:

- RO-1: To improve performance of existing algorithms for copy-move forgery detection/classification.
- RO-2: Using CNN/Deep learning for having robust approach which will give scale invariant, rotation invariant and other manipulation invariant classification of forged images.
- RO-3: Localizing the forged area in images.

1.5 Why deep learning methodology

Recently, deep learning has become a commonly adopted method for detecting image forgery. The increased use of deep learning approaches for image forgery research problems is due to the following reasons: **(i)** they involve automatic feature extraction instead of extracting handcrafted features, **(ii)** they produce more generalized models than other approaches, **(iii)** the layers of deep learning models can be modified at any time, **(iv)** they are much easier to optimize than other models, **(v)** they allow the feature strength

computation for each layer, (vi) they allow granular probability computation, (vii), and they make it easy to generate a probability map. We have explored existing and new hybrid model based on deep convolutional neural network for better classification of original or forged images. All the listed advantages given motivation to work on hybrid model for image forgery problems. We have also worked on block level methods to locate the forged area in image.

1.6 Performance evaluation parameters

The parameters used for evaluating any deep learning model for classification of forgery are discussed below based on the literature work.

Sensitivity / TPR: The ratio of True positives (TP) results to the sum of a TP and False Negatives (FN) result. It is also equivalent to recall, which is the proportion of relevant results among all the retrieved results.

The formula for computing sensitivity is provided in equation 1.

$$\text{Sensitivity} = \frac{TP}{TP+FN} \quad (1)$$

Specificity/TNR: In terms of image forgery, it can be stated as how many times a model correctly identifies a positive class image as positive. This information can also be presented as the ratio of true negatives (TN) to the sum of true negatives and false positives (FP) (See Equation 2)

$$\text{Specificity} = \frac{TN}{TN+FP} \quad (2)$$

False positive rate (FPR): The ratio of FPs to the sum of false positives and true negatives. The sum is equivalent to total actual negative events. Equation 3 can be used to compute the FPR.

$$\text{FPR} = \frac{FP}{TN+FP} = 1 - \text{Specificity} \quad (3)$$

False Negative Rate (FNR): The ratio of false negatives (FNs) to the sum of FNs and TPs; the sum is equivalent to total actual negative events. (See equation 4)

$$\text{FNR} = \frac{FN}{FN+TP} = 1 - \text{Sensitivity} \quad (4)$$

Accuracy: A measure of how close the predicted result is to the actual result. In terms of confusion matrix parameters, accuracy can be calculated using TP, TN, FP, and FN. The formula of accuracy is presented in equation 5.

$$\text{Accuracy} = \frac{TP+TN}{(TN+FP+FN+TP)} \quad (5)$$

Precision: The ratio of the total number of sample retrieved under given class to the total number of samples classified in any class. Precision can be calculated using equation 6.

$$\text{Precision} = \frac{TP}{TP+FP} \quad (6)$$

1.7 Contributions

We have done extensive review and examination of current methods for identifying scope of improvement in forged image classification with better accuracy. The examination of the current detection techniques has been successfully completed in detail. As part of our investigation, we have looked into both machine learning and deep learning techniques for comprehending the existing processes. We have studied and analyzed the bias for using the deep learning solutions for improving the performance of the model. In this direction, We have presented some recommendation to improve the performance of deep learning models.

As an initial basic implementation we proposed a customized deep neural network that can classify images as either forged or non forged. This model aims to classify all the images having copy move forgery in presence of scaling, rotation, different compression level with accuracy of 94% on different datasets as well as their combination.

To enhance classification performance, we suggested a hybrid deep learning-based technique to classify the copy-move forged images. For classifying forged images, a deep learning (DL)-based hybrid model called VI-NET was presented, that combines two DL architectures, VGG16 and Inception V3. Furthermore, the output of two models is concatenated and linked with two more convolution layers. Also on COMOFOD dataset, cross-validation protocols K10 (90% training, 10% testing), K5 (80% training, 20% testing), and K2 (50% training, 50% testing) are used. Furthermore, VI-performance NET's is compared to transfer learning and machine learning models utilizing assessment criteria such as accuracy, precision, recall, F1 score, and so on. The proposed hybrid model performed well.

Further, to improve the performance of classification, we proposed a hybrid deep learning-based method to classify the copy-move forged images. For classifying the forged images, a deep learning (DL) based hybrid model was proposed, named as VI-NET using fusion of two DL architectures, i.e., VGG16 and Inception V3. Further, output of two models is concatenated and connected with two additional convolution layers. Cross-validation protocols, K10 (90% training, 10 % testing), K5 (80% training, 20 % testing), and K2 (50%

training, 50 % testing) are applied on the COMOFOD dataset. Moreover, the performance of VI-NET is evaluated against transfer learning and machine learning models utilizing criteria such as accuracy, precision, recall, F1 score, and so on. The proposed hybrid model functioned better than other methods, with classification accuracy of $99 \pm 0.2\%$ in comparison to accuracy of $95 \pm 4\%$ (Inception V3), $93 \pm 5\%$ (Mobile Net), $59 \pm 8\%$ (VGG16), $60 \pm 1\%$ (Decision tree), $87 \pm 1\%$ (KNN), $54 \pm 1\%$ (Naïve Bayes) and $65 \pm 1\%$ (random forest) under K10 protocol. Earlier in this study, we introduced a lightweight neural network-based method for classifying images based on whether or not they include copy-move forgeries. The suggested approach seeks to classify all images that include copy-move forgeries as well as scaling, rotation, and different compression levels. The model has been verified across many datasets to achieve an accuracy of roughly 95%.

For copy-move forgery mask detection, we used a DCT (Discrete Cosine transform) block level features extraction technique. The tampered images are used to extract block level features. Where appropriate-sized bricks are chosen experimentally. These block features are then compared using lexicographic distance between feature vectors to find related blocks. The visual results for the predicted mask and real mask comparison are shown. The average detection accuracy of counterfeit masks is 95%.

To improve localization performance even further, we suggested a unique technique to identify copy-move forgeries in images using non-overlapping block level pixel comparisons, which can yield higher detection and classification accuracy. This method splits the image into an appropriate number of blocks and compares each block by moving a sliding window over the whole image that is not overlapping with the current block. It was discovered that by varying the number of blocks, forged regions of various sizes may be easily detected. We utilized the SSIM (structural similarity index) metric to determine if the image was fabricated or genuine. The algorithm was simulated on multiple datasets such as (MICC, CASIA, Coverage, and COMOFOD, among others) and reached a maximum accuracy of 98%. We also compared our results on precision, recall, and precision.

1.8 Organization of Thesis

The thesis is organized among total of seven chapters. In the chapter 1 we have presented detailed introduction about the problem statement, gaps, research objectives and contribution

in brief. Chapter 2 comprises of detailed systematic literature survey in the field of image forgery with comparative analysis. In chapter 3 basic customized CNN model is presented to show the usage and power of deep learning model to classify the images in robust manner. A hybrid deep neural network is discussed to classify the forged images in chapter 4. A initial level basic DCT-Feature based forgery mask detection algorithm is presented in chapter 5. It describes DCT based forgery localization. The further improved solution for copy-move forgery localization is discussed in chapter 6. Finally, conclusion and future scope is discussed in Chapter 7.

CHAPTER 2

LITERATURE REVIEW

Prior to making actual contributions to an area of study, it is vital to first do research on the previous work that has been done in that subject. This chapter is dedicated to providing a comprehensive overview of the research and literature surrounding the identification and categorization of forgeries. The discussion of the work done expressly for the detection of copy-move forgeries will take up the bulk of our time in this chapter. The types of solution to image forgery may be generally divided into three different ways. The first is a block-based solution [25]-[26], the second is a key-point based solution [153][178] and the third is an AI based solution [62][63] that includes machine learning, deep learning, or transfer learning based solutions. In addition, we have demonstrated our effort to evaluate the potential for bias in image forgeries when employing deep learning techniques.

2.1 Introduction

There have been a number of articles written and published on the topic of image forgery [59]-[60]. In each and every one of the evaluations, the detection methods for copy-move forgeries have served as the major emphasis of the researchers. Within this part, the search technique that was utilised for the literature study is outlined. We investigated significant databases, such as IEEE Xplore and Science Direct, as part of our search for works in the field of image forgery that were published in the ten years prior to the present. We looked for specific search keywords such as "copy-move forgery", "image forgery detection", "image forgery using deep learning" and "image forgery using AI." We searched through the titles of published publications to categorise image forgery detection research according to transfer learning, deep learning, machine learning, block level, and key point based methodologies, as shown in Figure 2.1.

2.2 Block level approaches

The block level technique recommends dividing the input image into rectangular sections of the same size, with or without overlapping those parts. After that, a feature vector is calculated for each of these blocks when they are combined into one region. Several research publications offer suggestions regarding the methodologies or procedures that may be used to locate the feature vector from image blocks or areas. Fredric et al. provided one of the initial levels block-based technique to detect the copied region using Discrete Cosine Transformation (DCT)[68]-[69]. This strategy is based on the manual feature extraction that the authors performed. The image is cut up into pieces of varying sizes that overlap each other. After that, the discrete cosine transform (DCT) is used to get the quantized feature vectors. Either the Euclidian distance or the lexicographical distance can be used to derive a feature vector. The similarity index is used to locate patches that are similar to one another. Other block features extractors that have been employed in the literature include singular value decomposition (SVD) [66], local binary pattern (LBP) [67], Fast Fourier Transform

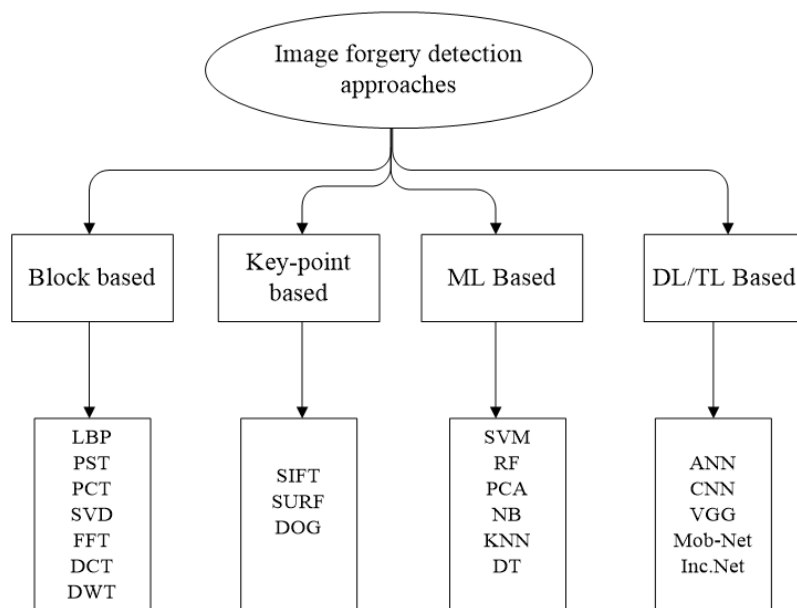


Figure 2.1. Different approaches for forgery detection

FFT [68], Zernike moments [69] and discrete wavelet transform (DWT) [70] among others. Block level technique works better in textured regions, but it requires a lot of computing power to do so. Ryu *et al.* [69] proposed a method to find the copied regions using Zernike moments. Using Tetrolet transform [71], the input image is divided into overlapping blocks.

Next, using the Tetrolet transform, four low-pass coefficients and twelve high-pass coefficients are extracted from each block. The lexicographic ordering of the feature vectors is achieved by a comparison of the recovered Tetrolet characteristics. The table that follows provides a summary comparison of a few block level techniques.

Table 2.1: Comparative analysis of block level approaches.

Sr. No	Technique	Parameters	Merits	Demerits
1.	DCT [9]	Euclidean Distance	Detects Copy Move Regions with Blur and Noise.	Small Duplicate images cannot be
2.	SVD [72]	Threshold	Detects Forged Region.	Computational cost is high
3.	LBP [73]	Neighbor Clustering	Locates duplicate images with low complexity.	Cannot detect spliced region
4.	FMT [44]	Eigen Vectors	Robust to JPEG Compression, Blurring, noise and Scaling.	Unable to detect when rotated via some angles.
6.	Zernike Moments [69]	Threshold with Euclidean distance	Medium computation complexity	Less invariant to Scaling

2.3 Key point-based methodologies

For the purpose of detecting forgeries, Sun *et al.* [74] proposed key point-based approach where different types of key points are used. The key points of an image are essentially the points of interest included within it. One of these methods is called scale invariant features transform (SIFT) [75]-[76], and it is utilised to identify and characterize clusters of points that are associated with tempered areas. Image is scaled at different levels to discover the scale space extrema points using difference of Gaussian smoothing [69], so that SIFT features may be generated from the image. After these key points are localized, directions are assigned to each key point to assist in determining whether or not rotation invariance exists. Harries corner is another method that may be utilized to identify key points. [11].

The work done in

A key point segmentation-based approach is proposed as a means of further improving accuracy in the work presented in [77]. The image is first broken up into very small patches, and then the essential features of each patch are isolated and compared with one another. The most significant disadvantage of the standard key point's technique that has been uncovered in this study is i) Insufficient key points are available for smooth or tiny regions. ii) It is tough to develop effective algorithms for grouping and segmentation of the data. iii) The present key point's methodology is not as effective as compared to state of art.

An technique that is based on hierarchical feature point matching [78] is described here in order to cover several limitations that were found in earlier studies. This strategy ended up being superior, even for relatively smooth and tiny areas. Preprocessing on the image was done, which included things such as contract thresholding and rescaling, so that a sufficient number of key points could be generated. Therefore, a hierarchical method is used in order to further minimize the complexity. At the scale level of the hierarchy of matching, the grouping of important points is carried out. Key point based approaches such as SIFT [75] and SURF [54] try to identify the interest points with a special feature extraction procedure such as scale invariant feature transform; however, the accuracy level of these approaches is not very flexible and is not very robust against changes in illumination and reflection.

2.4 Deep learning (DL) Based methodologies

The model that is described in [14] (Refer Figure 2.2) is able to determine if an image has been spliced, copy-move forged, or video forged frame. In this particular model, the initial training was carried out on a 27 layer model. Subsequently, the model's gained features were applied to a 54 layer model in order to produce more accurate classification results. During the second step, encoder decoder architectures are utilised in order to construct the forged segment for the purpose of localization. The authors of reference [79], utilised the patch-wise processing to lessen the amount of information that was lost, and as a result, they were able to provide an extremely complete analysis of any forged document. This was done to circumvent the potential issue of information loss that might occur whenever images are downsized in advance of the training process. In order to categorise the image, feature aggregation was carried out at the image level. In addition, a fresh checkpoint tactic was implemented throughout the forward run of the training process in order to preserve the activation value at checkpoint layers. The authors of the paper [80], included a limited

convolution layer before the other CNN layers. This layer was placed in front of the other CNN layers in order to suppress the unneeded image content and learn solely on the characteristics that assisted in image alteration. This layer extracted the modified fingerprints by making use of filters that were 5x5 in size and had a stride of 1. In [62], the authors proposed a segmentation-based key-point distribution approach that made use of a convolution kernel network (CKN). During the training phase, the technique was able to approximate a convolution-kernel based features map. The authors of [81], presented a deep neural network with the objective for identification of the recolored images from the natural or original images. This network was meant to differentiate between the two types of images. The image was fed to the algorithm, along with two properties of the image: the image's illumination consistency and its inter channel correlation, which is obtained statistically from the images. After that, each of the three distinct inputs is fed into three separate parallel deep CNN models in order to create features. After that, the characteristics were concatenated together using a layer called the concatenation layer to provide the final image categorization. An technique that was based on the VGG-16 deep learning architecture was proposed by the authors in the paper [82]. In this particular model, the image patches served as the inputs, and their purpose was to determine whether or not the image was authentic. When utilising the CASIA training dataset, it has a classification accuracy of 97.8% with fine-tuning and 96.4% during the first stage [83]. This article discussed three distinct forms of image distortion: copy-move, splicing, and Resampling. Every kind of distortion was created with the intention of changing the information that was already there in an image. In order to prepare the patches for the application of copy-move tampering, re-quantizing operations, affine transformations, noise addition, and brightness level adjustments were used. The model did not make use of any prior information in the process of automatically extracting the features from the training dataset. In addition, the authors have thought of using a patch size of 40 by 40 by 3, with two convolution layers and two completely dense layers. Patches are chosen from the original as well as the forged areas of the image, with a 20-pixel overlap on either side of the selection. Before training, all of the patches are brought to their original state through the process of normalisation, and the training-test ratio is set at 80:20. An architecture for deep learning was presented by the authors in paper [84], which made use of noise residual characteristics. In order to extract distinguishable features, the noise residual features were utilised as input to the ResNet-50 model. At the very end, an SVM classifier was used to the model in order to categorise the spliced forgery. A classification accuracy of 97.24% was achieved by using this

model. The authors of [63], developed a unique method employing CNN for predicting and detecting counterfeit masks. This method was presented. Using this approach, the amount of self-correlation that existed among the block level characteristics was analysed. The validation results showed that the model was accurate 97.1% of the time.

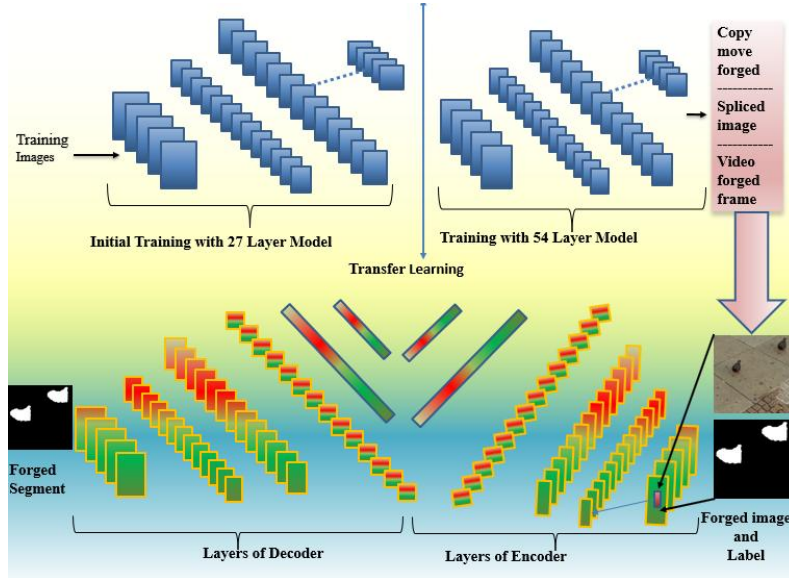


Figure 2.2. Deep CNN model for image forgery detection [12]

In addition to this, the copy-move forgery may be identified via the end-to-end network model that was developed in [85]. The structure of model included a deep convolutional neural network (CNN), a pyramid feature extractor, and a feature correlation matching module, followed by a post-processing phase. The pyramid block was responsible for extracting the dense features that were present across various dimensions and scales, while the transition block was responsible for compressing the size of the feature array. The feature correlation matching block that comes at the very end of the process is responsible for learning the correlation between the different levels of features.

The fusion-based model was utilised to identify copy-move forgeries in the architecture that was proposed in [15], and is shown in Figure 2.3. Convolution neural network (CNN) and Generative adversarial network (GAN) are two of the most prominent designs for deep learning, and the authors chose them so that they could be fused together. A GAN has the capacity to generate realistic images that have a low likelihood of being recognised as forgeries. The first thing that the generator does is construct a image out of the random noise that is fed into it. After then, the image, along with many other images that were produced from the same dataset, was shown to the discriminator. As input, the legitimate as

well as the faked images are sent to the discriminator, which subsequently calculates probabilities (as values between 0 and 1). In the end, the fused model was able to pinpoint the part of the image that had been altered and create the output mask. The results of this experiment showed that the fusion-based model could obtain an accuracy of 95%.

In reference number [54], specialised CNN architectures consisting of three convolution layers were utilised. During the training phase, the authors have utilised two distinct kinds of pooling: maximum pooling in the first layers and average pooling in the top layers. A validation accuracy of 90% was achieved as a result of the automated extraction of features made possible by the convolution network. Because there are not enough balanced data sets [86] available for use in the training of deep learning models, the results of the categorization are not as justified toward both of the classes as they should be. There is no doubt that deep learning strategies are useful in the process of automatically extracting features; however, less emphasis was placed on the analysis of computation requirements [87] despite the fact that deep learning models require a significant amount of CPU power in order to extract features. Table 2.2 provides a review of the many deep learning models available, and Tables 2.3 and 2.4 summarizes detailed parameters of transfer learning and deep learning techniques of literature respectively.

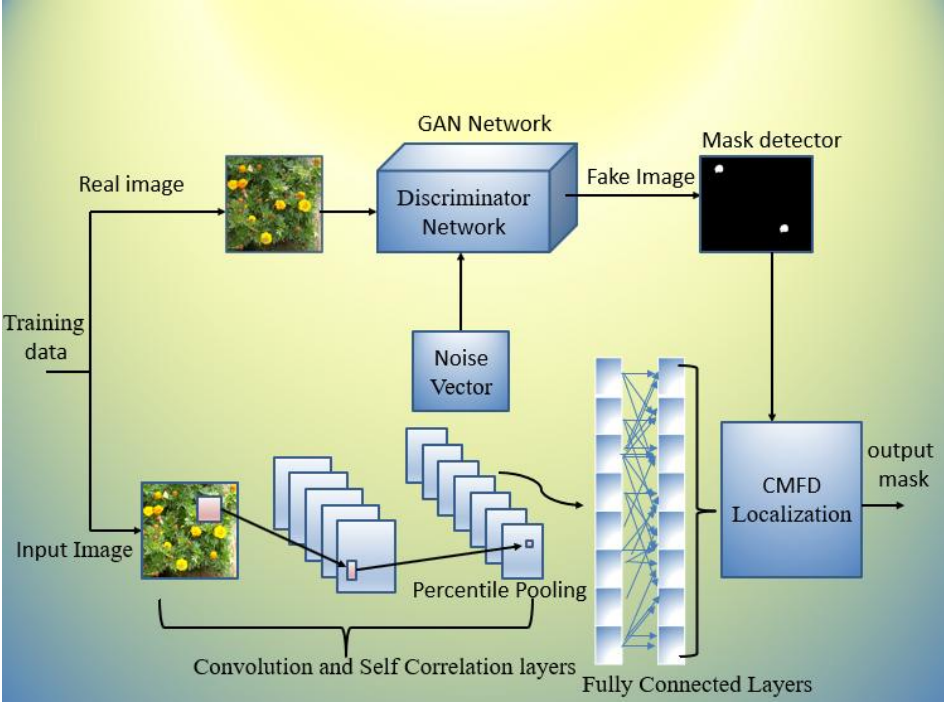


Figure 2.3: Two branches deep neural network architecture (GAN + CNN) [15]

Deep convolutional neural networks with patch-level training and no resizing operations were applied by Mara *et al.* [79]. Noise at the pixel level is used to determine whether or not there has been any manipulation. For the purpose of improving neuron memory, a checkpointing strategy has been implemented. An adaptive over-segmentation technique that utilised symmetric key point distribution was provided by Liu *et al.* [88] in order to pinpoint the portion of the image that had been altered. Conditional random field using convolutional neural networks (CNN) was proposed by Liu *et al.* [89] and it has shown to be successful for pixel-wise prediction and image augmentation. Y. Liu *et al.* [90] developed an implementation of a convolutional neural network with multiscale image processing. The tables labelled "Table 2.2" through "Table 2.4" provide a tabled summary and comparison of several AI techniques.

Table 2.2: Deep learning-based models for forgery classification

Sr.	Cit.	Architecture	Features	Hyper-Parameters	Type of Forgery
1	[91]	CNN	Automatic		Median Filtering
2	[80]	CNN	Block-level Patches used as training data, CNN Features, Filter learning errors	Momentum=0.9, Decay=0.0005, learning rate=10e-6, Batch Size=32, 9000 iterations	Manipulation detection
3	[92]	CNN, First Layer 5X5X1(4Nos) filters, Second layer filters 1X1X4(81)	Noise residuals, Histogram, Quantization,	LR=10e-6, decay 5X10e-4, Batch Size=36, Adam optimizer, 15 Epochs	Copy move forgery
4	[93]	CNN	Auto	Relu activation, Stride 2	Copy Move
5	[94]	DL	linear predictive error, First layer filter as Laplacian, Radson Transformation	64X64 Image patch Size, stride =8	Manipulations
6	[95]	9 Layer CNN	Auto, CNN Based	Adam optimizer, Epochs 200	Splicing, Retouching, Recompression

7	[90]	CNN	Segmentation-based features at different scales.	Mini Batch Gradient Descent, Momentum=0.99, wt. Decay 0.0005, LR =0.001 with 10% dec. every 8K iteration	Image forgery Localization
8	[96]	CNN	CFA features, Patch Size of 32X32	First Layer Kernels 50 of 7x7, stride=1, output learned will be 26x26x50	Copy Move forgery localization
9	[97]	CNN with Pre-processing	CNN Features based on filter learned	Input image size 64X64X3, Relu, SoftMax layer, Batch size 256, Learning Rate .0010	Copy Move Forgery
10	[98]	CNN	Block DCT, Zernike Moments, Enhanced threshold, CNN Training		Splicing Detection, Copy move forgery
11	[99]	9 Layer CNN, Image transformation and Patch Pre-processing, 2 FCN (Relu and SoftMax)		Patch Size: 64X64,	Camera Model Identification based Forgery detection

Table 2.3. Transfer learning-based models for forgery detection

Sr.	Cit.	Architecture	Features	Hyper-Parameters	Type of Forgery
1	[89]	VGG16, FCNs, CRM	353X480X(RGB) resized to 224X224, Automatic	Lr=0.0002, Mini batch Size (20), decay (.0005), momentum=0.9	Splicing
2	[100]	25-layer Pre-trained Alex net	CNN Based Deep Features	-	General Forgery /Manipulation

3	[101]	VGG-16 Pre-trained	Per-pixel Binary Mask	LR=0.0001, Momentum=0.9, Decay=0.0005	Localizing Image Splicing Forgery
4	[102]	VGG Pre-trained	An experiment was done on Various CNNs/with or without Max-pooling / with pre-training	Standard values, 300 Epochs	Manipulation
5	[85]	Dense Inception Net	Multidimensional and Multiscale Pyramid feature extractor, Feature Correlation Matching, Hierarchical Post processing	LR=0.01, SGD, Initial bias=0, Momentum =0.9, Binary Cross- entropy, Adam optimizer, 1000Epochs	Copy Move forgery
6	[103]	VGG Net 5, Conv and Max-pool layer, Adaptive Patch Matching	Segmentation, Dense Depth Reconstruction, CNN Features	momentum=0.8, LR=0.020, Epochs 40	Copy Move forgery
7	[104]	image shape 256X256*3 PATCH SIZE OF 32X32X3	CNN, Encoder based features, Patch level features	-	Image Manipulation Localization
8	[105]	VGG-16	Compression Error Analysis with CNN	-	-
9	[82]	VGG-16	CNN Training based	-	Image Splicing

Table 2.4. Hybrid models for forgery detection

Sr.	Cit.	Architecture	Features	Hyper-Parameters	Type of Forgery
1	[63]	CNN, Inception	256X256X3 input image	-	Copy Move
2	[106]	2 Branch DNN, Binary Classifier, First four blocks of VGG-16 Architecture	CNN Features, Self-correlation, Percentile Pooling	-	Copy Move, Image Manipulation
3	[15]	CNN with GAN	GAN Features, and Image comparison	32X32, 28X28 Images, 1000 Epochs	-

			through fusion		
4	[107]	2-Phased Deep CNN	Manipulation features tracing, Local Anomaly Detection	Batch Size=64, 1000 Batch/Epoch, LR=0.0001, No Decay, Cross-entropy loss	Any Forgery/ Manipulation

ML, despite the fact that it has produced higher levels of accuracy, is less appealing because of the inherent weaknesses it possesses, such as ad hoc feature extraction. When combined with other feature selection methods, such as PCA polling [115]-[116] or random forest [110], linear discriminant analysis [111], machine learning (ML) has the potential to be useful in medical imaging as well. No matter which feature selection we adopt, feature extraction still remains the bottleneck, and studies have shown that a large number of features need to be augmented for superior results, which also can make the system non-linear causing the dynamics of the system to be memorised than generalised [112].

2.5 Assessing the Risk of Bias (ROB) of DL Studies

Image forgery can lead to catastrophic decisions and financial repercussions. Conventional strategies for IF detection is ad hoc, not fully automated, and are therefore unreliable. Artificial intelligence (AI) has started to penetrate image forgery (IF) area, but due to lack of full-scale experimentation, leads to risk-of-bias (RoB). For assessing the ROB among the deep learning based solutions for image forgery detection. We filtered certain top ranking studies based the criteria discussed next. During the literature search, total of 351 articles related to image forgery were downloaded based on a manual search of query-string. Among these articles, 317 were from database searches and 34 from other sources. After removing duplicates, 188 articles were retained; out of which 60 were removed because they were not relevant to the current research approach being reviewed. Another 73 articles were excluded during the abstract review because they used non-AI techniques. Finally, 20 articles were removed for not meeting sufficient parameter criteria as these 20 articles were not addressing minimum 3 parameters (accuracy, sensitivity, dataset size) out of 8 evaluation parameters. Thus, 35 studies were ultimately considered for ROB analysis. With these 35 studies, an analysis was done through AP (ai) Bias 1.0 ranking based on ten attributes. Thereafter, from

the 35 studies, top 15 studies were selected based on ranking score cut-off of 2.4/5 (attribute mean score) (attribute mean score).

However, among these studies, 8 out of 15 did not possess the attributes required for further analysis. For this purpose, a new methodology was adopted to find the missing parameter values. This methodology was adopted for studies where only accuracy, dataset size, true-positive rate (TPR), or recall was reported. A hypothesis criterion was determined after all the studies were analysed and ranked according to the RoB assessment using ROBINS-I and the PROBAST method. The hypothesis criteria were that (a) the mean score of all attributes (e.g., accuracy, dataset size, F1-score) taken over all the AI studies should be greater than 80% and (b) all AI-based studies should be in either the low or moderate-bias zone when analysed by RoB in non-randomized studies of interventions (ROBINS-I) and that prediction model RoB assessment tool (PROBAST) method. Moreover, according to a set threshold, a minimum 50% of AI studies must satisfy either of the hypotheses stated above. The top 15 studies along with available and computed missing parameters shown table 2.5 given below.

Table 2.5. Parameters on 15 studies: available data + inferred values

StudyID		SENS	SPEC	FPR	FNR	ACC	F1-score	Precision	Recall
Liu <i>et al.</i> (2017)	[62]	0.99	0.93	0.07	0.01	0.96	0.96	0.94	0.99
Wu1 <i>et al.</i> (2018)	[63]	0.87	0.80	0.20	0.13	0.84	0.84	0.80	0.87
Liu <i>et al.</i> (2018)	[89]	0.83	0.92	0.08	0.17	0.86	0.87	0.91	0.83
Wu2 <i>et al.</i> (2018)	[106]	0.74	0.81	0.19	0.26	0.78	0.76	0.78	0.74
Doegar <i>et al.</i> (2018)	[100]	1.00	0.88	0.12	0.00	0.94	0.94	0.89	1.00
Abdalla1 <i>et al.</i> (2019)	[97]	0.80	0.95	0.05	0.20	0.91	0.88	0.70	0.80
Abdalla2 <i>et al.</i> (2019)	[15]	0.80	0.96	0.04	0.20	0.95	0.88	0.70	0.80
Rajini <i>et al.</i> (2019)	[98]	0.99	0.99	0.01	0.01	0.99	0.95	0.92	0.99
Zhong <i>et al.</i> (2019)	[85]	0.59	0.93	0.07	0.41	0.92	0.64	0.71	0.59
Agarwal <i>et al.</i> (2019)	[103]	0.90	0.97	0.03	0.10	0.95	0.94	0.98	0.90
Abhishek <i>et al.</i> (2020)	[14]	0.98	0.98	0.02	0.02	0.99	0.86	0.99	0.98
Elasakily <i>et al.</i> (2020)	[49]	0.99	1.00	0.00	0.01	1.00	1.00	1.00	0.99
Rao1 <i>et al.</i> (2020)	[113]	0.98	0.96	0.04	0.02	0.98	0.58	0.98	0.98
Rao2 <i>et al.</i> (2020)	[114]	0.98	0.95	0.05	0.02	0.97	0.97	0.95	0.98
Zhu <i>et al.</i> (2020)	[115]	0.47	0.57	0.43	0.53	0.52	0.50	0.58	0.47

The following ten attributes have been considered to evaluate the selected studies on deep learning-based image forgery detection: (i) data size, (ii) robustness, (iii) features, (iv) localization, (v) pre-processing, (vi) performance, (vii) innovation, (viii) forgery types handled, (ix) cross-validation, and (x) parameters reported. Each attribute is given a value between 0 and 5, according to specific criteria given in Table 2.6

Table 2.6. Grading scheme for the attribute evaluation.

Grading Scheme			
	High Grade	Medium Grade	Low Grade
Attributes	4-5	2-3	0-1
Data size	>20000	2000-20000	<2000
Robustness	Complete	Partial	None
Feature	Complex	Moderate	Simple
Localization	Fully focused	Partially focused	No Localization
Preprocessing	Manipulation sensitive Preprocessing	Resizing/ Normalization	Plain Image Input/ No Preprocessing
Performance	>95%	<=95, >=90	<90
Innovation	Unique	Moderate	Normal
Forgery types	2+	2	1
Cross-validation	>=10	K=5	K=1/ OR No Cross- Validation
Parameters reported	>5	3-4	1-2

In this subsection, we started our discussion to analyse the possibility of risk of bias in using AI for image forgery. A hypothesis was stated that we can summarise as follows "At least 50% of studies should more than 80% mean score over different parameters" if this hypothesis is not passed then the possibility of bias can be concluded. Now, when only 47%, 7%, and 20% of studies qualified hypothesis in three methods namely, ranking, PROBAST, and ROBINS-I, all less than 50%. So, it signals the possibility of risk of bias. As a result, following recommendations are proposed for reducing the RoB.

- (i) *Data size*: There is a need to increase the data size during training; most studies have used insufficient dataset sizes, particularly in the case of copy-move forgery, where any area of the image could be forged. Thus, a larger training size should be used to provide a more generalised model. However, using augmentation during training to increase the dataset size may harm the classification accuracy since it will make the dataset imbalanced. Thus, the forgery part can be damaged, and the results can be biased

(ii) *Pre-processing*: A model without pre-processing is likely to lead to inaccurate results.

Manipulation-oriented image pre-processing must be applied before images can be fed to the training model. Thus, it is recommended to include the pre-processing step.

(iii) *Cross-Validation*: Most studies have not considered all necessary evaluation parameters during classification, which increases the risk of bias (RoB) . Cross-validation results are either not reported or have not been applied in most studies. Thus, it is important to recommend this step.

(iv) *AI Architecture*: For transfer learning-based models, VGG-16 is one of the most preferred models, so one can take advantage of designing HDL models based on VGG-16.

2.6 Strength weakness and extensions

Deep learning models are more robust than block-based and key point-based models. The average accuracy of 90% should motivate the adoption of AI approaches for image manipulation detection. Deep learning models are easier to update and retrain with new data than other models. Using a CNN model with fewer layers means more effort is needed for feature extraction, as pre-processing can significantly reduce training time and increase accuracy. Most authors have presented their results based on a relatively small number of performance evaluation metrics (e.g., recall and accuracy) (e.g., recall and accuracy). However, a thorough analysis of results obtained in all respects is lacking, and few studies have used cross-validation, which is an essential criterion for evaluating any deep learning model. Moreover, the confusion matrix—which is a vital component of any classification task and is critical for representing results—is missing from the results sections of some studies. Data size is another limitation, as most studies have employed data sizes of less than 5000, which could cause publication bias. Moreover, more accurate results could be obtained if images are pre-processed before being transferred to neural network architecture. The leading image forgery detection applications are social media forgery detection, fake image identification, fake medical report identification, and (in the judiciary system) the identification of fake images produced as crime scene images. The most adopted models are pre-trained and fresh training done on VGG16. As data size grows, these AI methods can use big data frame works [116]. More superior methods for bias estimation such as slope methods can be tried [117]

CHAPTER 3

EFFICIENT END TO END CNN FOR FORGERY

CLASSIFICATION

The objective of the work presented in this chapter is to test the performance of customized CNN model for classifying the forged images. The types of images include copy move forgeries and also have post-processed images with scaling, rotation, and different levels of compression applied on patches. For the purpose of solving this issue, we have developed a novel customized lightweight CNN model with the that could achieving an accuracy of about 95 percent for individual datasets as well as for the integration of two or more datasets.

3.1 Customized CNN architecture

After gaining an awareness of the relevant literature, it is possible to recognise that although several methods exist, copy move forgery detection in digital images remains challenging. However, none of them are resistant to the myriad of conceivable variations and are deficient in accurate representation. In places with little to no texture, a method centred on key points could not perform very well. The block level approaches are ineffective for dealing with images that contain objects that have been geometrically altered. The methods that have been employed up to now are not mirror reflection invariant; furthermore, they are not invariant to changes in perspective. There are just a few of articles that have used deep learning to solve this issue, which has been flagged as a major need. The localization process has seen relatively little work done thus far. The purpose of this CNN architecture is to make use of deep neural networks in order to develop a robust method that is capable of providing scale invariant, rotation invariant, and other manipulation invariant classification of forged images, with a particular focus on copy move forging.

The notion of a convolutional neural network is employed in this work as a preliminary attempt to categorise the fabricated or legitimate images. A model that incorporates certain pooling and convolution layers has been suggested as a solution for this problem since it provides superior accuracy in comparison. Although there are numerous pre-trained models available, which may be utilised for random initialization, these models appear to be computationally costly and are not useful in terms of the accuracy they achieve on the

datasets. To determine the appropriate model and layer combination, a number of different layer combinations and parameter settings were experimented with and refined until an accurate prediction model could be obtained.

Reducing the overall complexity of the model while simultaneously creating a set of layers with the minimum necessary amount of computing power in mind has been a primary focus. A given input image is initially transformed to a grayscale image in order to decrease the number of parameters. This can be seen in Figure 3.1, which depicts the suggested architecture. In order to further decrease the complexity of the parameters and the amount of time spent for training, all of the input images are shrunk to a size of 32 by 32 pixels. Following the input layer is a convolution layer with 128 neurons that perform convolution operations using a 3x3 filter. After that comes another convolution layer with 64 neurons that use the relu activation function. Following that is a max pooling layer with a 3x3 filter. This is followed by another max pooling layer with a 3x3 filter. This is followed by a dense layer with 128 neurons. This is followed by a 30% dropout layer. This is followed by another max pooling layer with a 3x3 filter. This is followed by a 20% dropout layer. This is followed by another dense layer with 0.2 neurons. This is followed by a final dense layer with 2 neurons, which is used for classification into 'Forged Image' or 'Original Image'.

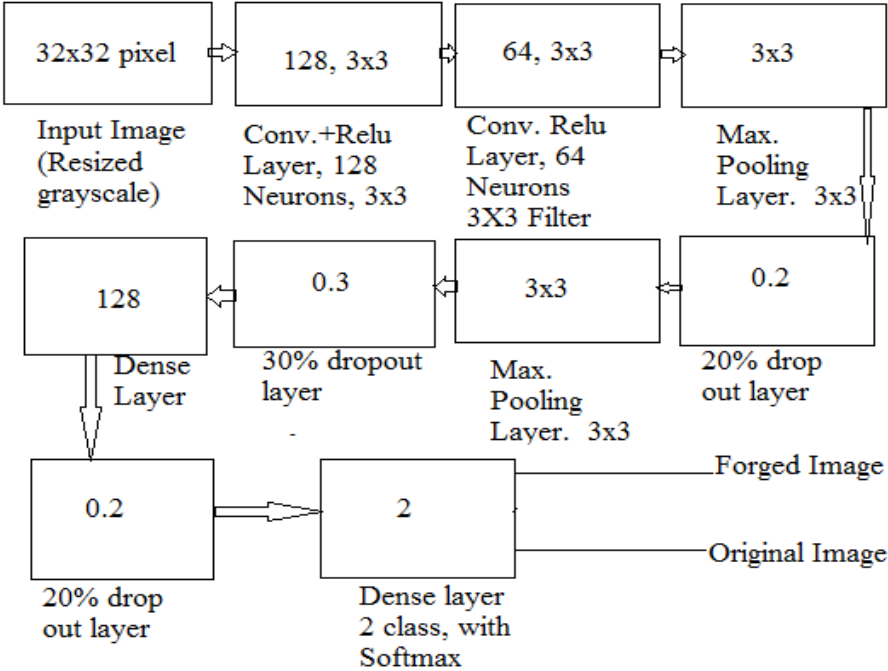


Figure 3.1: Proposed CNN architecture

Hereafter, a comparison of the accuracy of the method being discussed is presented with that of other approaches, which essentially involve the manual extraction of features. In this section, the attention will be placed on the building of a model that is based on a convolutional neural network that can automatically extract the local feature vectors. This will allow for images to be accurately identified as either forged or real.

In order to accomplish this goal, a number of different datasets, including COMOFOD, DIID, and the Image Manipulation data set, amongst others, have been subjected to experimentation. The primary experiment that contributes to the novelty is one that tests the precision of the result when it is applied to two or more of the datasets described before. Experiments are performed, and the findings are analyzed, in every one of these kinds of situations.

3.2 Results and discussion

Approximately 6050 cleaned images were taken from the COMOFOD dataset and are now being used for the purpose of training the suggested model. For the purpose of confirming the outcome, a train test with a split of 80 to 20 percent is taken. In light of this, the confusion matrix for testing 1210 images on a trained model is presented below. The model was trained on these images for around 50 iterations, and an accuracy of 93.2 percent was reached. In order to demonstrate that this model is resilient against additional kinds of invariance, various other datasets were also fed to the model while utilizing the weights that were learnt from the COMOFOD [118] dataset. The DIID [11] data set images that will be used for this further training include a collection of images with basic copy-move, images with rotation, and images with scaling. This indicates that all of the images have been adequately combined to generate a robust model. The training images also include a benchmark dataset, which was used to test the robustness of the model and ensure that it produces accurate results for the benchmark images. When these images are combined, training is performed on 8424 of them, and validation is performed on 2106 of them after training. This results in an accuracy of 94.77%, which is far better and more robust than the block level and key point based techniques.

Here, over the course of the training, every original image is assigned the number "0," while every fake image is assigned the number "1." To converge to the maximum performance, the model employs gradient descent in conjunction with the Adam optimizer. In order to avoid overfitting, the 'Adam' optimizer is being utilised here.

Further in this work, accuracy at the image level was evaluated and compared. For better validation of result, it is important to evaluate the accuracy with which the image is identified as a forgery or an original. In light of this, measures of precision and recall are taken into consideration. Precision refers to the degree to which your result matches the real outcome,

while recall refers to the degree to which your results properly reflect overall performance among all of the data.

Table 3.1: Accuracy achieved on different dataset.

Sr. No.	Dataset	Accuracy	Avg. F1 Score	Avg. Precision	Avg. Recall
1	COMOFOD [118]	93.2%	0.90	0.96	0.86
2.	COMOFOD [118]+ DIID [11]	94.4%	0.94	0.93	0.94
3.	COMOFOD+ DIID+Image Manipulation [9]	94.77%	0.95	0.95	0.94

Table 3.2: Confusion matrix results.

Original Label	COMOFOD Dataset Test Result		COMOFOD+DIID Dataset		COMOFOD+DIID+ Image Manipulation Dataset	
0	228	87	438	59	1229	38
1	0	895	24	971	72	767
Predicted label→	0	1	0	1	0	1

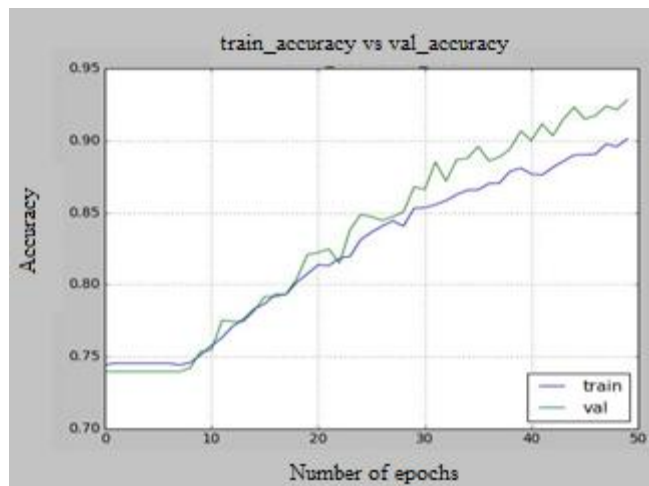


Figure 3.2: Accuracy graph on COMOFOD dataset

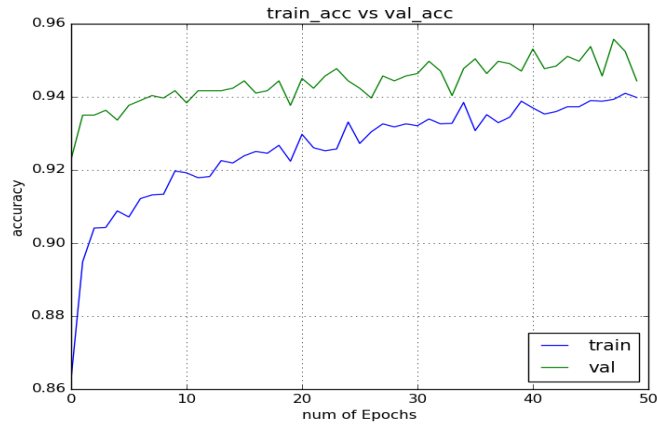


Figure.3.3: Accuracy graph on COMOFOD+DIID dataset

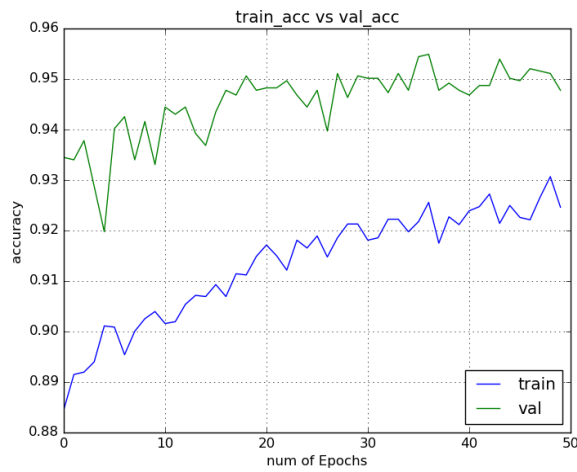


Figure.3.4: Accuracy graph on COMOFOD+DIID+Image Manipulation dataset

Table 3.3. Comparison with other approaches using COMOFOD dataset

Methods	Precisio n	Recall	F1 Score
SIFT [119]	77.83	82.5	80.10
Segmentation [120]	77.19	66.00	71.16
Non-overlapping Block level Copy Move[74]	89.30	83.5	87.55
Proposed CNN Model	96.0	86.0	90.1

3.3 Conclusion

As it is observed from the findings and the literature that accuracy is high in methods in which the result is not invariant to multiple transformations, we need to investigate whether or not there is a method that can withstand all of these different kinds of modifications.

Although we have shown via the literature a good accuracy, the penalty of that precision is that it is not resilient to certain manipulations. Despite this, we have observed a decent accuracy. With The proposed method of tempering is capable of being classified without any deficiency in terms of challenges posed in the form of sensitivity towards reflection, image compression, rotation, and scaling altogether. This is the major outcome of the CNN approach that was applied in this paper to reach an accuracy of approximately 95% with a model that was constructed from scratch. This model is able to identify images even when such images have been treated and post-processed in many ways, such as by blurring, changing the lighting, reducing the color, etc. There is room for more accuracy improvement as a future project with a CNN model that covers the entire process from beginning to end. We have worked to improve the accuracy of classification by proposing a new hybrid CNN model the detail of the same is discussed in next chapter of the thesis.

CHAPTER 4

VI-NET: A HYBRID DEEP CNN

Deep learning has been the topic of discussion in this chapter since it is a relatively new approach to machine learning [121]. The use of neural network-based solutions to a variety of classification problems has been shown to have a considerable impact [122]–[128]. A fusion model [106] that takes output features from conventional architectures like VGG and Inception V3 and combines them is something that has been suggested using deep learning. These are concatenated and used as input to layers that are densely connected. As we progress from the beginning layer to the output layers, features are automatically extracted from high-level down to low-level features in order to determine if the images have been altered or are authentic. The manual approaches of feature extraction are used to extract features of a certain dataset. On the other hand, by utilizing deep learning, it is possible to create a specialised model that could then be applied in the future to train a fresh collection of images or data.

The following are some of the most important points covered in this chapter:

- There is a discussion of a unique hybrid architecture, which is a mix of VGG16 and deep inception V3. This combination delivers superior accuracy when compared to the performance of separate models.
- The performance of the hybrid model was superior to that of individual models as well as other machine learning approaches, and a benchmarking of several methods is shown in the result section

4.1 Introduction

An example of copy-move forgery is depicted in Figure 4.1. The image shown as 4(a) is an original image and 4.1(b) is a forged image where forged area is indicated by an arrow [6]. It is easy to see, using figure 1(b), that the person who is supposed to be standing in the middle of the picture has been cut out, duplicated, and then put somewhere else [1]. There exist certain types of pre-processing before applying the copy-move operation that makes the detection more difficult. These procedures include rotating the patch before pasting it, scaling the patches, modifying the pixel attributes or colour value, and inserting blur into the picture patch. Over the course of the past several years, a variety of strategies employing manual

feature extraction have been developed in order to circumvent the copy-move forgery [72]. The majority of these may be placed into one of two groups, which are called key point-based and block-based techniques [129]. Approaches that are based on key points are superior in terms of their ability to detect the duplicated portion in a picture. Scale Invariant Feature Transform, also known as SIFT, and Speeded-up Robust Feature Transform, also known as SURF, are the two primary methods that are utilised within the key-point category [54]. Moreover, the primary emphasis in key point-based methods is placed on the extraction of the textured regions [74]. The researchers also came up with a different method that they call the brute force-based technique.



Figure 4.1: (a) Original image (b) forged image with the forged area indicated through arrow[118]

in which autocorrelation exhaustive search is applied [130]. All of the strategies that have been mentioned up to this point, however, have significant downsides, such as the fact that none of them are reliable enough to provide good outcomes. In a scenario like this one, where there is a presence of geometric alteration in the forged image, block level approaches are effective. However, the block-based methods need a significant amount of computing power.

4.2 Proposed Methodology

There are several different deep learning architectures, such as VGG, Mobile Net, and InceptionV3, among others, that have been shown to be useful at solving image classification task. For the purpose of identifying forgeries, we suggested using ensemble architecture. As you'll see in the next part, the discussion of the suggested approach is broken up into three subsections: rationale, proposed architecture, and underlying concept

4.2.1 Motivation

Major research efforts have concentrated on the manual extraction of features, which are then employed for the classification of image forgeries. In recent times, there has been a rise in interest about the use of deep learning to solve classification problems. Even in the presence of many attacks, such as rotation, scaling, and blurring, the results of forgery classification performed using deep learning architectures have been demonstrated to be substantial. However, the results are acquired by either employing transfer learning architectures or utilising small-sized neural networks that have been specifically designed. Therefore, the innovative concept is to leverage the feature extraction capabilities of both a customised neural network and a standard architecture in order to investigate the influence on the classification accuracy.

4.2.2 Proposed ensemble architecture

The idea of a convolutional neural network is used in conjunction with a variety of deep learning architectures, both for the purpose of learning filter weights and for the reduction of features. The VGG16 and Inception neural networks have been combined in the designing the hybrid model that has been presented. In order to achieve fusion, the pre-processed image tensors are introduced into two models that are already in existence. Models VGG16 and Inception V3 are being used. After that, these models are altered so that a distinct output is produced for the classification probability. In this step, the output of the very last layer of both VGG16 and InceptionV3 are split into two separate outputs. After that, the outputs are merged together to create the output fusion layer, which is located on the second layer (See Figure 4.2). The concatenated outputs from the fusion layer are then applied to a fully connected layer-3 (FCN) of 1024 neurons equipped with a Relu activation function, which is then followed by another fully connected layer of a size comparable to the first (Layer-4). Feature map of the input image produced at layer-2 and layer-5 (FCN-2; the layer with 2 neurons) is depicted in figure 4.2. At last, an output layers containing the binary result is affixed with SoftMax activation in order to determine if the image in question is authentic or a forged. The learning rate when the algorithm is being trained is 0.001, and the momentum is set at 0.9. The stochastic gradient derivative is used for the weight update procedure. Training for the fusion architecture takes place over the course of 30 epochs, and the batch size is 64.

4.2.3 Underlying principle

Forward and backward propagation is the fundamental technique that underpins the training of neural network designs such as VGG and Inception V3, as well as other neural network architectures. Any deep neural network is, at its core, a feed forward network. This type of network requires an image tensor to be fed into the model, and the tensor must have particular dimensions and channels. With the assistance of forward and backward propagations, the required characteristics from the image may be automatically extracted.

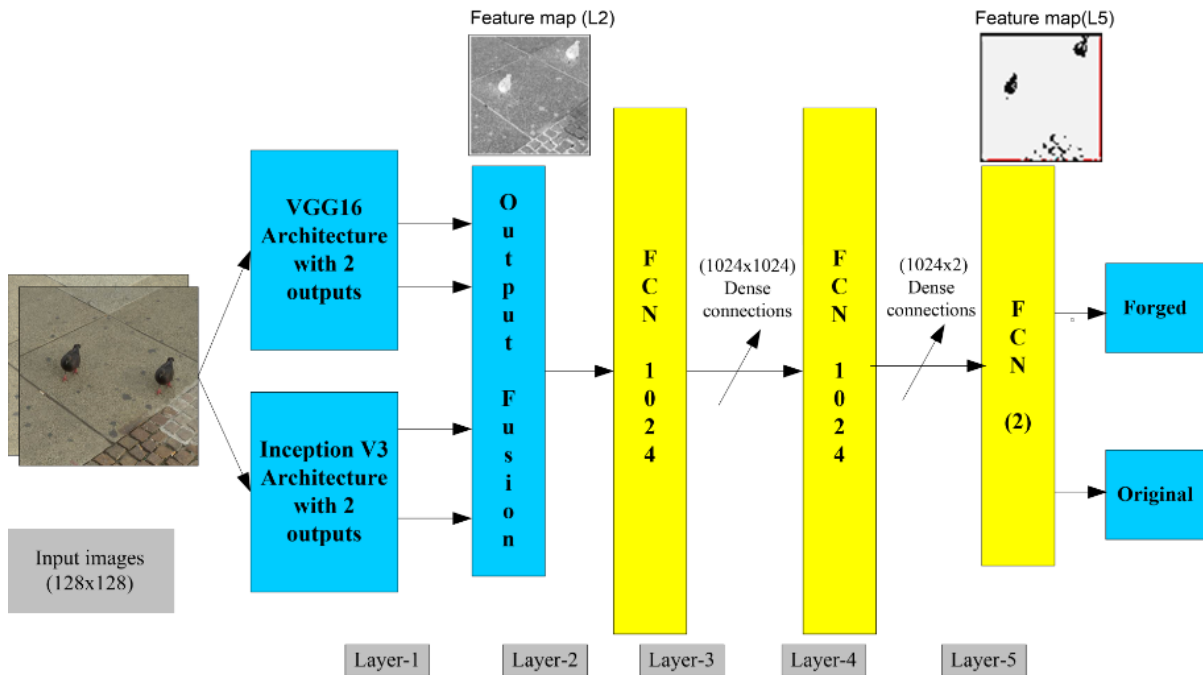


Figure 4.2: The proposed hybrid network using VGG16 and Inception V3

During the forward propagation step, the normalized image with dimensions 128 by 128 is individually fed into the VGG16 and Inception V3 models with their respective pre-trained weights. The non-trainable flag is set on all of the VGG and inception levels throughout the training process for the fusion model, with the exception of the very final layers. The output features that are created by these models are concatenated and then transferred to the fusion layer, where they are combined with other features and then passed on to the gradient learning process of the fully connected layers to extract the appropriate features. During the back-propagation stage, the errors that are computed during each iteration are used to change the learned weights in order to lower the error rate. The errors are estimated based on the

projected likelihood once the process has been completed. Adjustments are made to the biases and weights in accordance with the gradient descent technique, which is expressed as:

$$\text{loss}(P, E) = -(E \log(P) + (1 - E) \log(1 - P)) \quad (1)$$

In this case, error is denoted by "loss," the predicted output of the model is denoted by "P," and the expected output of the model for a given image is denoted by "E". To ensure that the model quickly converges on the correct solution while it is learning through the forward and back propagation process, we need to modify key hyper parameters. The number of layers, the learning rate, the number of neurons in each layer, the technique for computing gradients, the batch size, and other parameters fall under the category of hyper parameters.

4.3 VI-NET classification Results

The NVIDIA DGX v100 machine serves as the platform for the implementation and training of the proposed fusion architecture. This computer has a total of 128 gigabytes of RAM and is fitted with 40600 CUDA cores in addition to 5120 tensor cores. The COMOFOD (copy move forgery dataset [123] dataset, together with images from the DIID [11] dataset, are combined and used in the training process. The results of benchmarking are computed on the same system using a variety of machine learning and deep learning methods.

4.3.1 Dataset

After going through some processing on dataset images, the individual datasets are then used for training purposes. Instead of concentrating on improving the model's ability to localise objects, the primary focus of this model is on increasing the accuracy of classification. As a result, the images from the various datasets are filtered so that the altered and original versions of the images may be distinguished within the context of the forged and original category. In the first step of training, the COMOFOD dataset is utilised for the purpose of learning the intermediate model weights. After that, a mixture of the datasets COMOFOD

COMOFOD[131] and other similar domain datasets DIID[11][132], some random images from image manipulation dataset(IMD) [9][133], and MICC F220 [134][135] dataset were used for training. The combined dataset [136] is produced by first creating two folders, one

each for forged and non-forged images, and then inserting images from the COMOFOD, DIID, IMD, and MICC-F220 that correspond to those categories in those folders.

The preliminary training phase of the COMOFOD dataset has been utilised for further phases of testing and validation [21][58]. This dataset contains two different types of images: those with a small file size and those with a high file size. Each category has further subcategories of images, some of which contain modified and fabricated versions of the originals. Images may be seen in pairs, each consisting of a forged version and its original counterpart, together with colored and binary masks for the forged areas. The collection contains a variety of forgery images that were made by the application of various post-processing techniques in their creation. Compressing the image using JPEG, adding noise to it, blurring it, adjusting the contrast, changing the brightness, and reducing the colors are some of the approaches. These post-processing techniques improve the overall quality of the dataset, which in turn helps to more effectively train the model. Table 4.1 displays the number of images that fall into each of the categories that it covers. Figure 4 provides a presentation of the few examples of images that were provided.

Table 4.1. Diversity of images and dataset for training

Sr. No.	Dataset	Category	Subcategory	Forged Images	Original Images
1	COMOFOD	Translated (40)	Each image with 24 types of Post processing	960	960
		Rotated (40)		960	960
		Scaled (40)		960	960
		Distorted (40)		960	960
		Combined (40)		960	960
2	DIID	Combined	-	50	50
3	IMD	Rotated and scaled	-	48	48
4	MICC-F220	-	-	110	110

Each of the images in the collection is resized to have a consistent resolution of 128 by 128 pixels. After that, the images are changed to grayscale before being fed into the model.



(a)



(b)

Figure 4.3: (a) Sample original images and (b) Corresponding forged images from COMOFOD dataset.

Images are separated between training and testing sets with the following ratios for different fold validation: 90:10, 50:50, and 80:20, respectively. Images from many smaller datasets, such as DIID [11], IMD and MICC-F220 are combined in the corresponding category of COMOFOD dataset images in order to expand the size of the collection and increase its variety. Following the separation of all of the images in the dataset into their respective original and forged categories, a total of 9746 images were utilised for the training procedure.

4.3.2 Performance analysis

According to Table 4.2, after only ten cycles of training, there is already a significant increase in the accuracy. The weight matrix is improved via the back propagation technique, which helps to reduce the amount of loss. Figure 4.4 is a visualization that shows the total accuracy growths of both the training results and the validation results for each unique epoch.

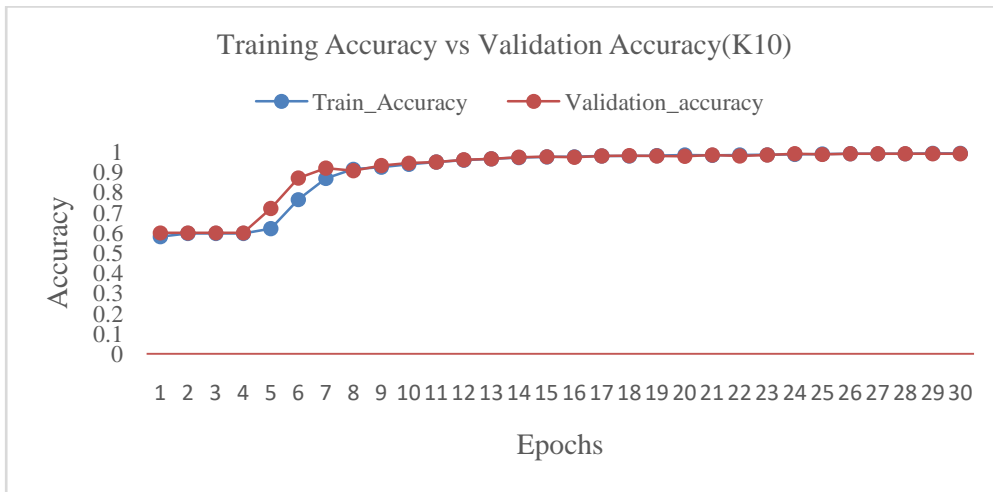
Table 4.2: Epochs wise Training and validation results

*En	K2 CV Protocol				K5 CV Protocol				K10 CV Protocol			
	At	Lt	Av	Lv	At	Lt	Av	Lv	At	Lt	Av	Lv
1	0.58	0.69	0.59	0.68	0.57	0.69	0.60	0.68	0.58	0.68	0.60	0.68
2	0.61	0.68	0.59	0.68	0.60	0.68	0.60	0.67	0.60	0.68	0.60	0.67
3	0.61	0.67	0.59	0.68	0.60	0.67	0.60	0.66	0.60	0.67	0.60	0.66
4	0.61	0.67	0.59	0.67	0.60	0.66	0.60	0.64	0.60	0.65	0.60	0.62

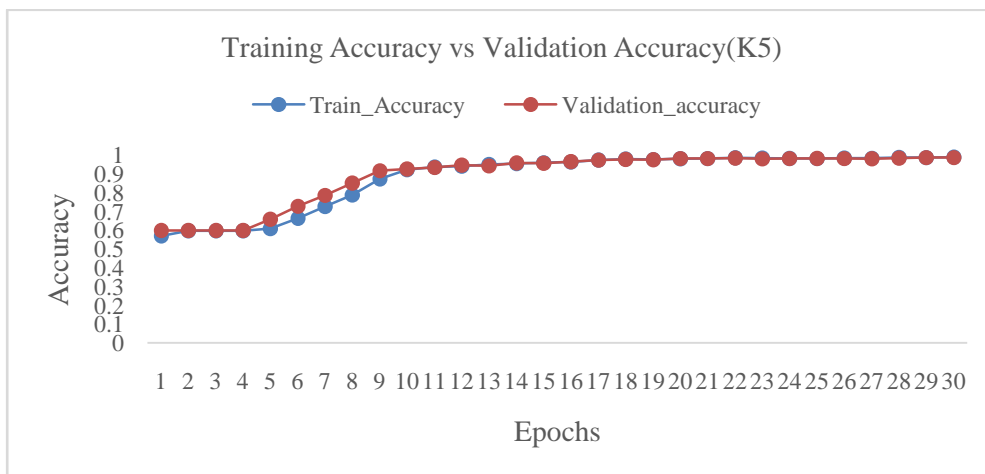
5	0.61	0.67	0.59	0.67	0.61	0.64	0.66	0.61	0.62	0.60	0.72	0.53
6	0.61	0.66	0.59	0.66	0.66	0.59	0.73	0.54	0.77	0.51	0.87	0.43
7	0.61	0.64	0.59	0.63	0.73	0.53	0.79	0.47	0.87	0.40	0.92	0.32
8	0.61	0.62	0.59	0.59	0.79	0.45	0.85	0.39	0.92	0.31	0.91	0.28
9	0.63	0.58	0.73	0.54	0.87	0.37	0.92	0.32	0.92	0.25	0.93	0.21
10	0.71	0.53	0.86	0.49	0.92	0.30	0.93	0.25	0.94	0.20	0.95	0.17
11	0.82	0.46	0.89	0.42	0.94	0.23	0.93	0.21	0.95	0.16	0.95	0.16
12	0.89	0.40	0.88	0.39	0.94	0.19	0.95	0.17	0.96	0.14	0.96	0.13
13	0.91	0.35	0.90	0.32	0.95	0.16	0.94	0.17	0.97	0.11	0.96	0.11
14	0.92	0.29	0.90	0.29	0.95	0.15	0.96	0.13	0.97	0.09	0.97	0.09
15	0.92	0.27	0.89	0.30	0.96	0.13	0.96	0.14	0.97	0.08	0.98	0.08
16	0.90	0.31	0.91	0.27	0.96	0.12	0.96	0.11	0.98	0.08	0.97	0.08
17	0.93	0.24	0.92	0.22	0.97	0.09	0.97	0.08	0.98	0.07	0.98	0.07
18	0.93	0.23	0.90	0.28	0.98	0.07	0.98	0.08	0.98	0.07	0.98	0.07
19	0.92	0.24	0.89	0.31	0.98	0.08	0.97	0.09	0.98	0.07	0.98	0.07
20	0.93	0.22	0.93	0.20	0.98	0.07	0.98	0.06	0.98	0.06	0.98	0.08
21	0.94	0.19	0.94	0.19	0.98	0.06	0.98	0.06	0.98	0.06	0.98	0.05
22	0.94	0.20	0.93	0.22	0.98	0.05	0.98	0.05	0.98	0.06	0.98	0.08
23	0.94	0.21	0.93	0.22	0.98	0.06	0.98	0.07	0.99	0.05	0.98	0.06
24	0.94	0.19	0.94	0.18	0.98	0.07	0.98	0.07	0.99	0.04	0.99	0.04
25	0.95	0.17	0.93	0.21	0.98	0.07	0.98	0.07	0.99	0.04	0.99	0.04
26	0.93	0.21	0.92	0.25	0.98	0.07	0.98	0.06	0.99	0.04	0.99	0.04
27	0.94	0.21	0.95	0.18	0.98	0.06	0.98	0.07	0.99	0.03	0.99	0.03
28	0.94	0.20	0.93	0.25	0.99	0.05	0.98	0.06	0.99	0.03	0.99	0.03
29	0.94	0.21	0.95	0.16	0.99	0.05	0.99	0.05	0.99	0.03	0.99	0.03
30	0.97	0.12	0.96	0.13	0.99	0.04	0.99	0.04	0.99	0.03	0.99	0.04

*(En: Epoch number, At: Training accuracy, Lt: Training loss, Av: Validation accuracy, Lv: Validation loss)

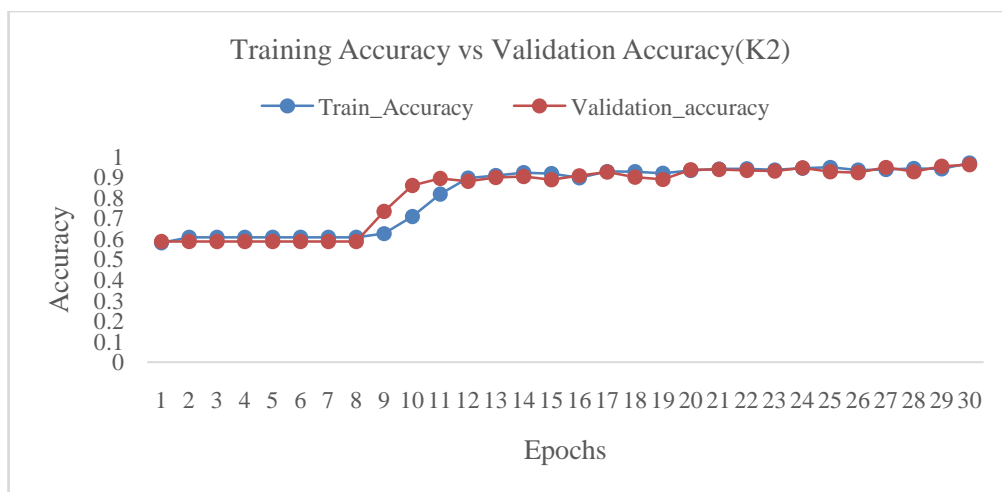
The K2, K5, and K10 procedures are used in the calculations to determine the training and validation accuracy (see Figure 4.4). The iterations that we progress through bring about an increase in the accuracy of the validation. Following the completion of 12 epochs, the performance begins to oscillate about 97%, with a mean difference of 0.012%. The highest levels of validation accuracy that is attained are 97%, 99%, and 99%, respectively, when using K2, K5, and K10 validation.



(a)

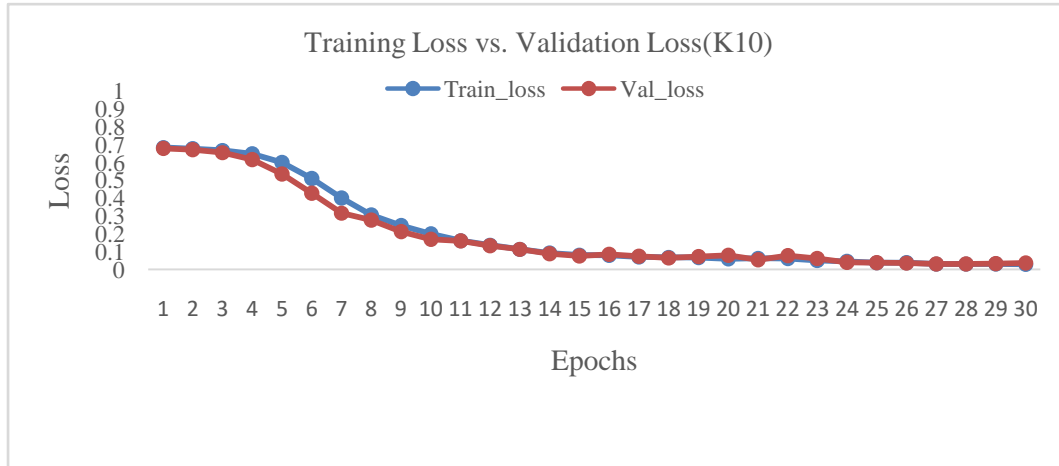


(b)

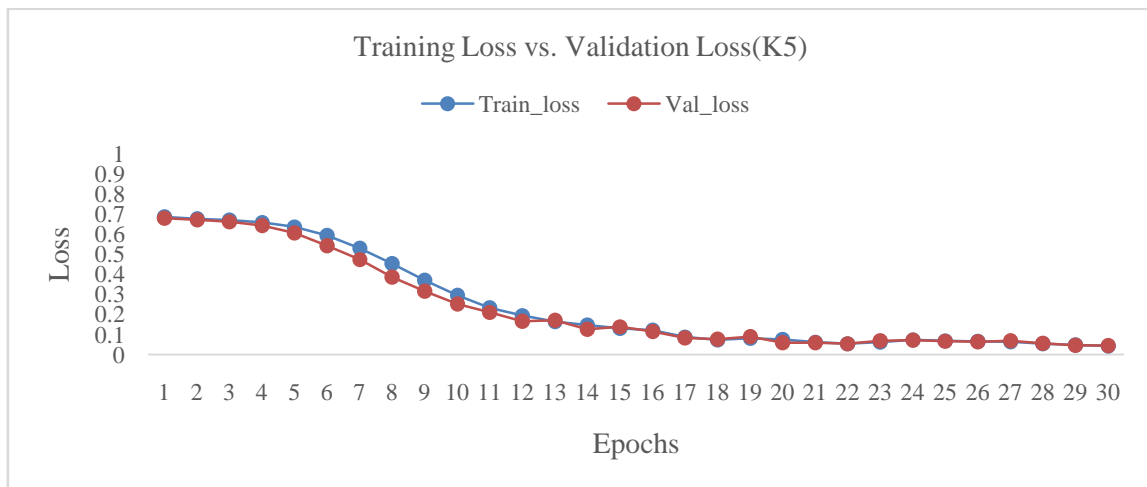


(c)

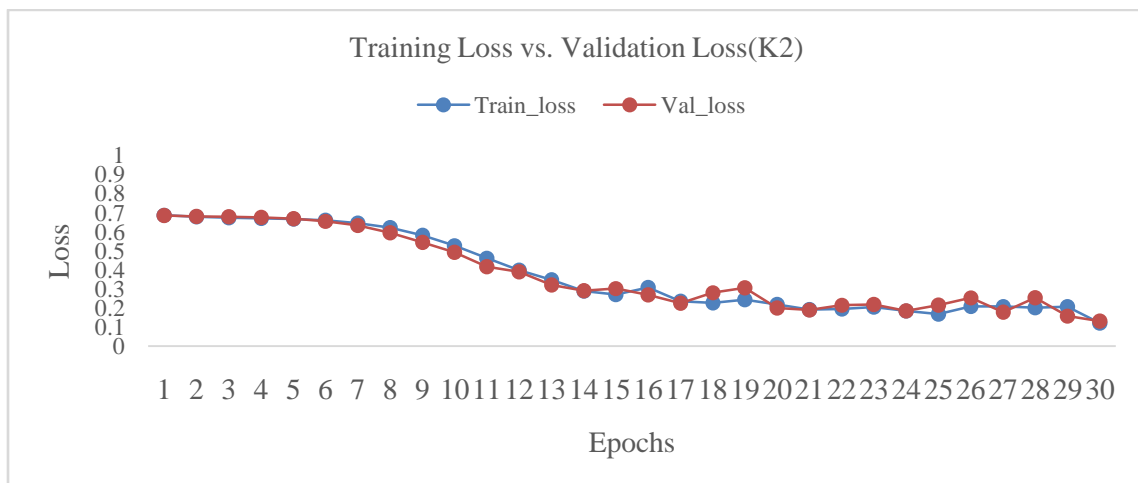
Figure 4.4: Training accuracy and validation accuracy graph (a) K10 protocol, (b) K5 protocol and (c) K2 protocol



(a)



(b)



(c)

Figure 4.5: Training loss and validation loss graph (a) K10 protocol, (b) K5 protocol, and (c) K2 protocol

The validation and training losses are depicted for comparison in Figure 4.5. It gets better the more times you go through the training iteration. During the forward propagation, the step loss is determined, and then the gradient is changed in accordance with that calculation in order to reduce the loss even more.

The results of training loss and validation loss are compared for 30 epochs. Here, K10, K5, and K2 fold results are visualized. Validation loss decreases as we move forward through different iterations. A consistent loss is observed during the last few iterations. The minimum validation loss obtained is 0.12%, 0.04% and 0.03% in K10, K5, and K2 validation protocols, respectively. In the confusion matrix (Refer Table 4.3), true positive and false positive results of the trained model are shown.

Table 4.3: Performance evaluation results in different folds.

Confusion Matrix Results		K10		K5		K2	
		Predicted Label		Predicted Label		Predicted Label	
		Original	Forged	Original	Forged	Original	Forged
True Label	Original	382	3	773	6	1981	36
	Forged	2	587	5	1164	146	2707
Validation Images / Total Images		974/9746		1948/9746		4870/9746	

ROC-AUC value	0.99	1	0.94
P-value	<0.001	<0.0001	<0.0001

In each fold, the suggested VI-Net model is used to verify a total of 974, 1948, and 4870 images, respectively. This number of images is used in the K10, K5, and K2 folds. The overall accuracy of classification attained is almost 99% on average. We evaluated our model using a dataset called "COVERAGE," which is open to the public, to assess how well it performed with unseen images [143]. Our suggested model achieved a true positive rate of about 97% when used this dataset for the classification of tampered images. However, while integrating two datasets (COMOFOD and MICC), some of the images were retained separate so that they could be evaluated on trained models. These images were not included in the training set. Testing these images on trained models revealed a true positive rate of almost 99%.

Table 4.4: Testing results. VI-Net (Proposed) vs. Other ML/DL techniques similar dataset

	ROC-AUC	Precision		Recall		F1-Score		Accuracy	
		Mean	SD	Mean	SD	Mean	SD	Mean	SD
VI-Net (Proposed)	0.99	0.99	0.00	0.99	0.00	0.99	0.00	0.99	0.00
Inception V3	0.95	0.96	0.02	0.94	0.02	0.95	0.01	0.95	0.04
Mobile net	0.95	0.92	0.01	0.94	0.01	0.93	0.02	0.93	0.05
VGG16	0.53	0.65	0.09	0.58	0.06	0.61	0.09	0.59	0.08
Ensemble Learning	0.85	0.73	0.02	0.73	0.02	0.73	0.02	0.73	0.02
Decision Tree	0.63	0.70	0.02	0.55	0.01	0.48	0.02	0.60	0.01
KNN	0.99	0.88	0.01	0.88	0.01	0.87	0.01	0.87	0.01
Logistic Regression	0.96	0.91	0.02	0.91	0.02	0.91	0.02	0.91	0.02
MLP	0.67	0.59	0.04	0.55	0.05	0.49	0.10	0.59	0.03
NB	0.57	0.55	0.02	0.55	0.01	0.54	0.01	0.54	0.01
RF	0.87	0.77	0.01	0.61	0.01	0.57	0.02	0.65	0.01
SVC	0.92	0.81	0.01	0.81	0.01	0.81	0.01	0.81	0.01

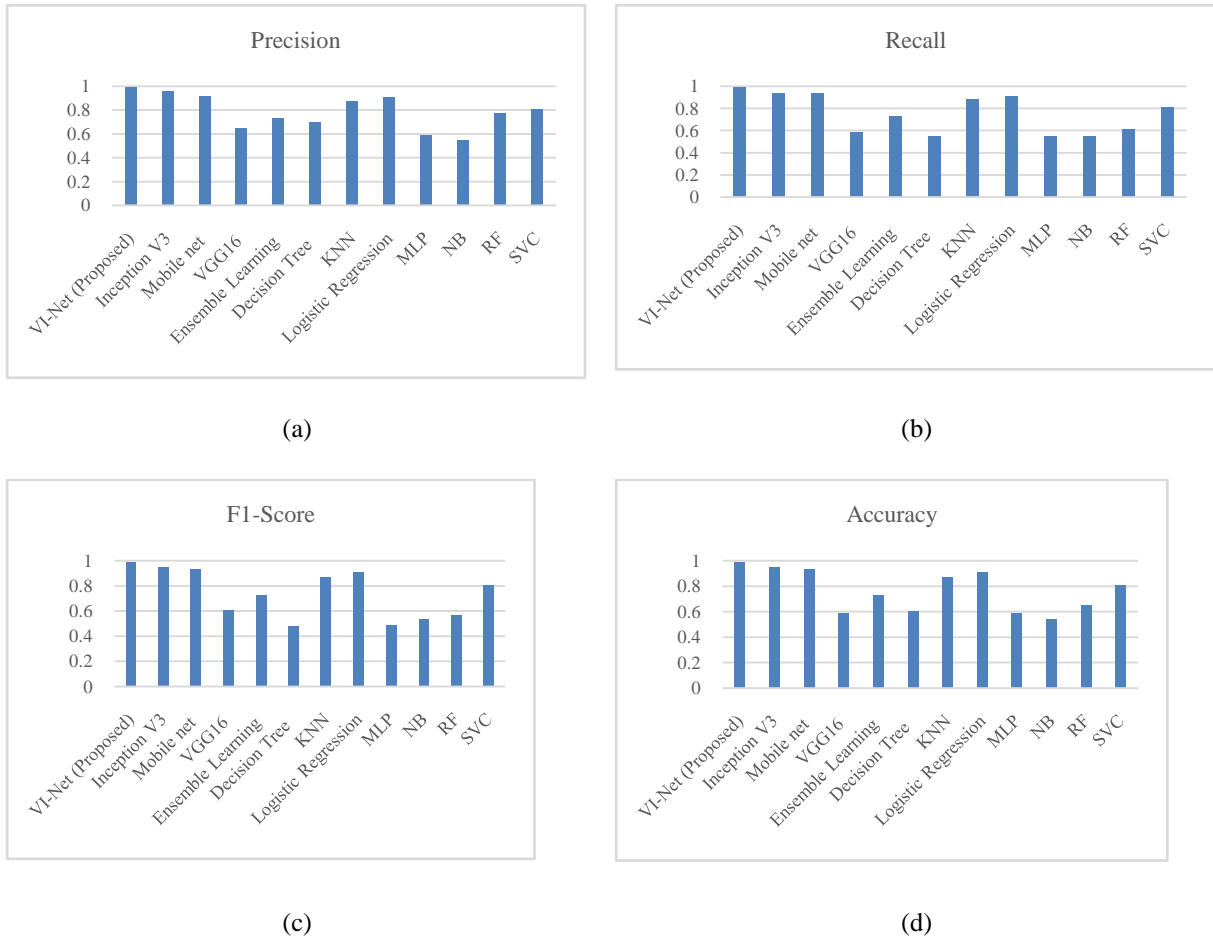


Figure 4.6. Graphical Comparison of Proposed Model Performance vs. other ML/DL methods (a) Precision (b) Recall (c) F1-Score (d) Accuracy.

Table 4.4 presents a comparison of the performance of the proposed VI-Net model with that of current techniques, which make use of the same training dataset (i.e., COMOFOD and DIID). In terms of accuracy, recall, and F1 score, the suggested model performs better than alternative techniques. The visual study of the suggested model's performance in comparison to other current techniques is depicted in Figure 4.6.

The aesthetic effects of applying intermediate layer filters on single original and forged images are illustrated in Figure 4.7 through Figure 4.11, respectively. It has been seen that higher layers filter out the most frequent aspects and extract the traits that distinguish the forged region from other areas. When the image is first given to the model, several

characteristics, such as the edges of the various objects, are extracted. In addition, the model retrieves the characteristics that are comparable to the forged image. In the end, the output of the fifth and final filter in the layer identifies the forged patches of interest in the image quite clearly. When such automated characteristics are transformed to a flattened array, the computation carried out via the SoftMax layer at the very end provides a probability value indicating whether or not an image has been tampered with. Figure 4.8 shows an example of the original image from the training dataset, and it also shows an example of the forged image from the training dataset. Both of these images are of layer-1 in the network result feature map of VGG16 or Inception-V3. It is easy to see that the strength of the features in the image created by Layer-1 (the final layer of VGG16/Inception-V3) is relatively greater, and that these features are subsequently lowered to by the non-linearity introduced by successive dense layers. Concatenations are utilised to combine the key features that were created by VGG16 and Inception-V3. Additional training is then done using these features, which results in improved classification outputs.

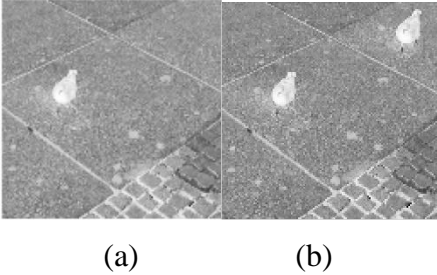


Figure 4.7: Layer 1 output of (a) original image and (b) forged image

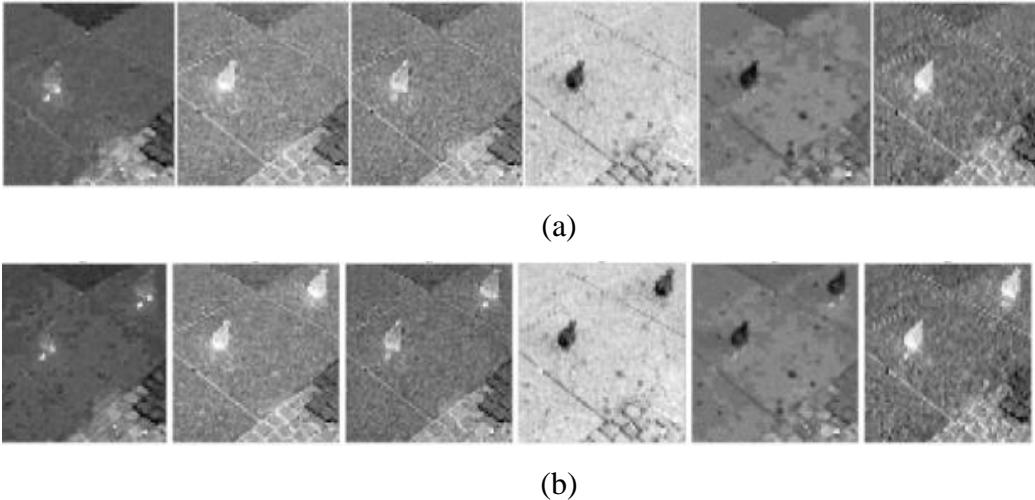
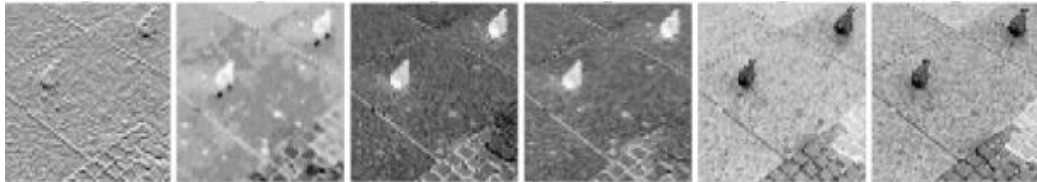


Figure 4.8: Layer 2 output of top 6 filters for (a) original image and (b) forged image



(a)



(b)

Figure 4.9: Layer 3 output of top 6 filters for (a) original image (b) forged image

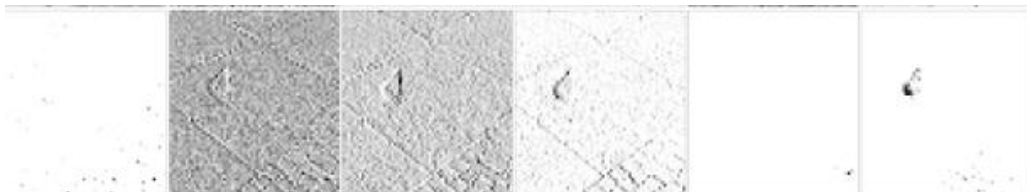


(a)

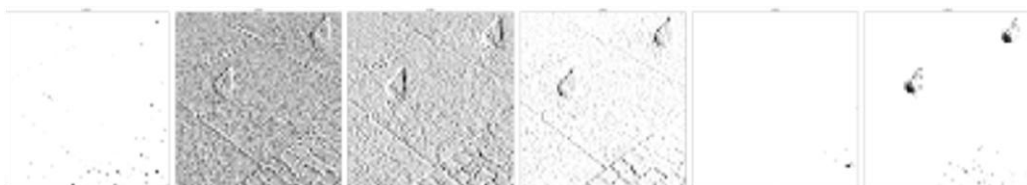


(b)

Figure 4.10: Layer 4 output of top 6 filters for (a) original image and (b) forged image



(a)



(b)

Figure 4.11: Layer 5 output of top 6 filters for (a) original image and (b) forged image

The visual results of the sample input image have also been calculated and are provided in figure 4.12 in order to facilitate viewing of the class activations using gradient heat maps. As

a demonstration, we have used the grad-cam method to derive the heat map from the four intermediate layers that are located between the input and the output. The activations of VGG16 and InceptionV3 are represented as output maps at the intermediate layer-1 level. Following that, the activation heat maps of the densely connected layers are presented.





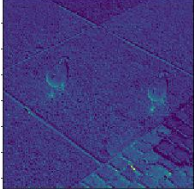
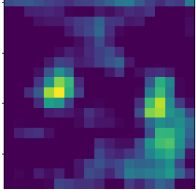
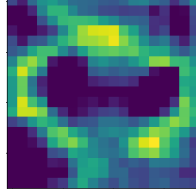
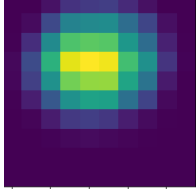

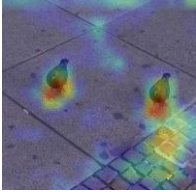
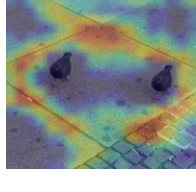

Description	Intermediate Layers-1	Intermediate Layer-2	Intermediate Layer-3	Intermediate Layer-4
Input image				
Class activation Heat map.				
Image superimposed with heat map image.				
	(a)	(b)	(c)	(d)

Figure 4.12: Grad-Cam (Gradient class activation map) result with heat map and superimposed input image with heat map for a) Intermediate layer-1 b) Intermediate layer-2 c) Intermediate layer 3 d) Intermediate layer-4.

The activation gradients are limited down to areas of interest where the risk of forging is higher, as can be seen in the heat maps of intermediate layer-2 through layer-4. This can be observed to be the case when looking at the intermediate layers. As a result, the model determines the likelihood of the image being fabricated through the use of these gradients. Table 4.5 compares the proposed architecture VI-Net’s performance to that of the existing techniques. When contrasted with alternative deep learning architectures, the suggested model demonstrates superior levels of performance. The convergence of the model was accomplished in only thirty iterations, which resulted in an accuracy of ninety-nine percent on the testing data.

Table 4.5: Performance comparison of VI-Net

Model	Major Dataset Used	Performance
Custom Deep CNN[86]	COMOFOD	95.97%
Convolutional Kernel Network[88]		59%
AR-NET with [115]		54.21%
Deep CNN [14]		98.58%
Dense Inception-Net [85]		46.1%
Buster-Net (Two branch DNN) [106]		92.74%
VI-Net (Proposed)		99%

4.4 Conclusion

There are several methods that involve manually feature extraction, but they only function properly in certain contexts. They do not function very well when another situation is present, such as when the image patch is rotated, resized, or when any lighting changes are made to the image. Other scenarios include: The categorization of forged images is carried out using a model that is based on a hybrid convolutional neural network. As part of the training process, the COMOFOD dataset has been combined with a number of other, smaller datasets, such as DIID. Scaling, compression, blurring, and rotation are some of the several properties of images that are taken into consideration in the dataset. The many different methods of machine learning, including Naive Bayes, decision trees, KNN, and random forest, are taken into consideration for the purpose of making a performance comparison. The findings of the experiments indicate that the suggested hybrid neural network has a higher level of efficiency in comparison to the current methods in terms of accuracy, precision, recall, and F1-score. The proposed hybrid model performed better, with a classification accuracy of $99 \pm 0.2\%$, in comparison to accuracy levels of $95 \pm 4\%$ (Inception V3), $93 \pm 5\%$ (MobileNet), $59 \pm 8\%$ (VGG16), $60 \pm 1\%$ (Decision tree), $87 \pm 1\%$ (KNN), $54 \pm 1\%$ (Naive Bayes), and $65 \pm 1\%$ (random forest) using the K10 protocol. The outcomes of this research might further stimulate the researchers to employ various combinations of a wide range of new and current models with the purpose of achieving better categorization results.

CHAPTER 5

BLOCK LEVEL FORGERY MASK DETECTION

In chapter 3 and chapter 4 our major focus was on image forgery classification. Here in chapter 5 our major focus shifted to work on algorithm for localizing the image forgery. As primary work for this purpose we explored one of the block level techniques for forgery mask detection. In this chapter, we demonstrated a methodology for detecting copy-move forging masks that uses a modified version of the discrete cosine transform (DCT) block level features extraction method. For this, a procedure in which blocks of the proper size are chosen for experimentation. In addition, these blocks are compared by calculating the lexicographic distance between the feature vectors in order to find blocks that are similar to one another. The visual findings are demonstrated for comparison between the real mask and the one that was anticipated. The detection accuracy of forgery masks is around 95% on average.

5.1 Introduction

Finding the copy-move forgery mask in the images that have been altered is the primary objective of this work. Generally speaking, detection approaches for copy-move forgeries may be broken down into two types. Approaches that are centred on and on blocks-based [239] key points based [241]. The key points approach is based on the concept of discovering the interest points in images by looking for places where there are sharp changes in color or lighting. SIFT and SURF feature descriptors can be used to express key point descriptors.

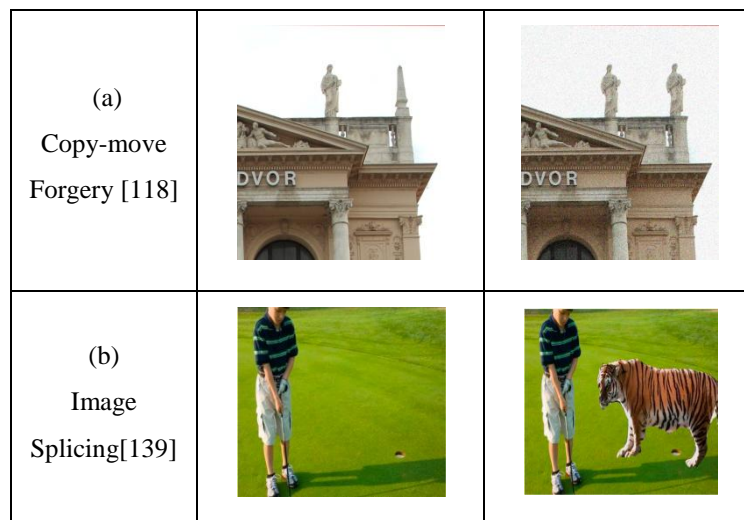




Figure 5.1: Example of copy-move, splicing and morphing.

Similarly, block level techniques segment the whole image into smaller blocks or patches of varying sizes. After that, the characteristics of the image blocks are retrieved depending on the various transformations of the features. Our block level method is based on the DCT features. To implement this technique, we split the images into 8x8 patches, and then for each patch, we ranked the DCT features depending on how similar they were to one another. A comparison of patches or blocks that are identical, depending on a threshold, can assist in the identification of forged patches. Deep learning-based methods are doing very well for image forgery detection. These solutions are in addition to key-point techniques [140] and block level approaches [141]. Deep learning-based solutions [124] are superior for classification purposes; nevertheless, the accuracy is often confined to a certain dataset. The solutions for deep learning require a significant amount of resources. On the other hand, key-point based techniques and block-based ones are superior at localizing instances of forgeries in images. It is possible to detect the forged region in a image by employing the block or key point technique for localisation, which can operate even on a single image. Although a large number of training images are necessary for solutions based on deep learning.

5.2 Proposed Algorithm

In the technique that we have presented, we have chosen to extract the block level characteristics utilising a block-based approach. The discrete cosine transformation based feature vectors are computed at block-level. After the block features have been retrieved in this manner, a comparison is made along each axis, and they are then organized lexicographically. In accordance with a predetermined minimum Euclidean distance, blocks that do not match are removed, while the feature vectors of blocks that do match are kept. The forged area mask is developed using these preserved feature vectors as its foundation. The specific steps that make up algorithms are discussed below.

Algorithm: Forgery Localization and mask detection







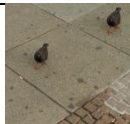





Input: image, input mask

1. Initialize quantization $\leftarrow 10$, block $\leftarrow 10$, threshold $\leftarrow 5$
2. Resize image as (512x512) \diamond Set rows $\leftarrow 512$, cols $\leftarrow 512$, Normalize all images
3. Resize the mask as (512x512)
4. Convert the mask and image array to grayscale
5. Initialize the dct array with quantization=10
6. for i in range(0, rows)
7. for j in range(0, cols)
8. slice = block[i to i+block, j to j+block]
9. scale slice array
10. find dct (scale)
11. add matching pixel of blocks at 0 in solution vector
12. Sort matching block features through Euclidian distance
13. Eliminate the non matching vectors.
14. Draw the mask based on matching vectors.

5.3 Result

The algorithm is simulated on an Intel Core i5 processor that has 8 gigabytes of RAM and NVIDIA GPU capability. Images taken from the CMOFOD dataset, which is well-known in the field of image forgery, are utilised in the assessment of the method. The table that follows displays some of the results obtained by analyzing the images included in the dataset. One can see the formula for several performance criteria from [25-26].

Table 5.1: Algorithm evaluations results (Sample COMOFOD dataset Images)

Sr.	Input Image	Input Mask	Predicted Mask	Accruacy
1				0.95
2				0.97
3.				0.97
4				0.93

Through the use of the method, the accuracy of 200 different forged and non-forged images from the COMOFOD dataset is determined. After that, the images are evaluated against a standard threshold of 80% accuracy value, images are categorised as either authentic or forged. If the accuracy of the anticipated mask is more than 80 percent, the image is regarded to be fabricated; otherwise, it is considered to be original. In light of this, the confusion matrix for the outcome of the categorization is presented. Table 5.2 presents the confusion matrix along with a number of other relevant parameters.

Table 5.2: Confusion matrix and related parameter results

Confusion Matrix		Predicted Label	
		Original	Forged
True Label	Original	97	6
	Forged	4	93
Average accuracy		0.95	
True Positive Rate (TPR)		0.96	
True Negative Rate (TNR)		0.90	
False Postive Rate (FPR)		0.10	
Precision		0.94	
F1-Score		0.95	

Figure 5.2 is a graphical representation of the findings that were calculated based on the output of the confusion matrix for the COMOFOD dataset. When we compare the true negative rate to the accuracy and the true positive rate, we see that the true negative rate is somewhat lower. This indicates that the algorithm has some bias towards positive image classification.

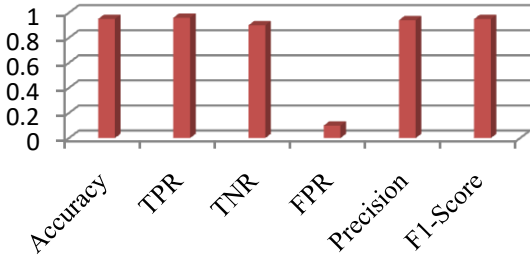


Figure 5.2: Evaluation parameters result

All of the images from the COMOFOD dataset were run through the algorithm for forgery mask detection, and the results showed that it had an average accuracy of 95%, as seen in the table of results just above this one. The precision was accomplished with a need for very little computation at all. It only took the aforementioned computer five seconds to detect the mask in a single image of the dataset using the given method.

The block level image forgery approach has been investigated by us. It has been suggested to use a forgery detection algorithm that is based on DCT features in order to find the forgery mask. Block-based techniques are more simpler to put into action as it takes far smaller amount of resources to for computing the outcome in comparison to deep learning-based solutions. The input image was scaled up to 512 by 512 pixels and then split into 10 by 10 square patches. After that, the block level characteristics were converted into a grayscale format, extracted, and compared lexicographically to find blocks that have a match. When the predicted mask and the actual mask for each image in the COMODOD dataset were compared, the results indicated that the accuracy was 95%. In next work discussed in upcoming chapter i.e. chapter 6, we can boost performance by utilising a hybrid method, which will ultimately lead to better outcomes.

CHAPTER 6

FORGERY DETECTION AND LOCALIZATION

It is important to localize the forged area in image. We can determine, via the use of localization, the precise location of the forged area in the image. We offer a unique method for the purpose of localization that can identify copy-move forgeries in images using non-overlapping block level pixel comparisons, and it is capable of achieving improved detection and classification accuracy. This method uses non-overlapping block level pixel comparisons. With this method, the picture is divided into 5x5 such image blocks, and then each block is compared by moving a sliding window across the full image so that it does not overlap with the currently active block. It was discovered that the forged zone may be readily located with a variable number of blocks, and that this region can be of varying sizes. We determined whether the image was a forged or an original by using a measure called SSIM, which stands for structural similarity index. We simulated the algorithm on several datasets, such as MICC, CASIA, Coverage, and COMOFOD, among others, and reached a maximum accuracy of 98%. Additionally, we compared our result on precision, recall, FPR, and FNR, as well as other metrics.

Introduction

6.1 Introduction

Figure 6.1 [145] illustrates several distinct sorts of mechanisms that may be used to identify forgeries. Active approaches need the possession of some previous knowledge concerning the source image in order to provide evidence of its genuineness [146]. As is the case with watermarking [147], the additional information is embedded in the picture itself at the moment of image production, and it is visible in the image. This is similar to how watermarking works.

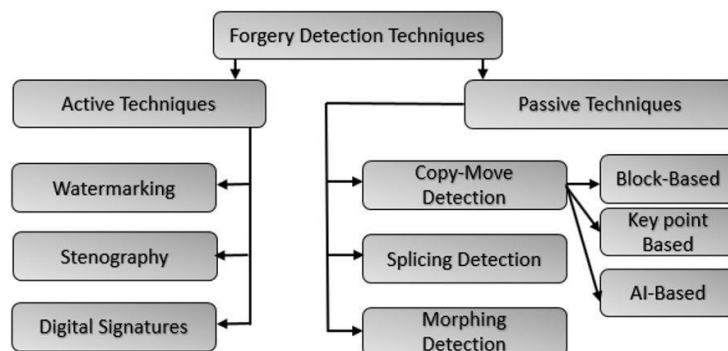


Figure 6.1: Forgery Detection Techniques

However, this time it is accomplished by manipulating the original images. Passive approaches [143] do not employ or rely on any prior knowledge that is encoded in the image. Instead, it considers the full image as input in order to discover the traces of any possible alteration in the image. In the process known as copy move forgery, a specific portion of the original image is cut out and copied into a new location within the same image in order to provide a different representation and interpretation, as seen in Figure 6.2. Retouching, splicing, morphing, and scaling are some of the different forms of image forgeries that may be committed. There are various types of solutions to choose from.

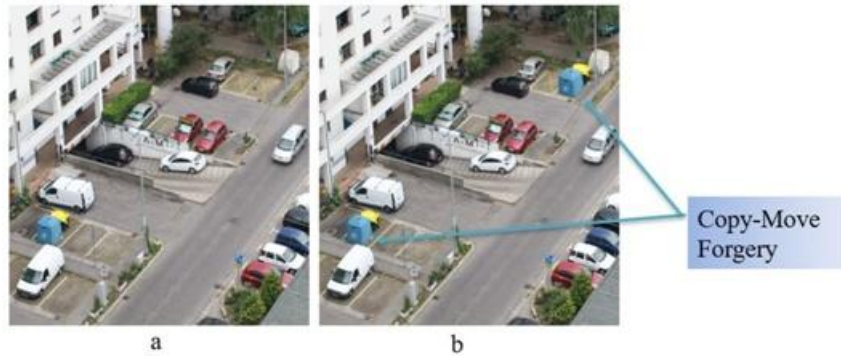


Figure 6.2 Copy-move forgery examples

The DCT [9], DWT [144], LBP [73], SVD [72], and PCA [112] are the most used mathematical foundations for block-level features. The SURF [145] or SIFT [55] features based descriptor is typically used in key-point-based techniques. Both of these descriptors are robust in terms of scaling and rotation. In this chapter, we provide an unique block-based approach for detecting and localizing copy-move forged areas in images.

6.2 Related work

The identification and categorization of image forgery, more especially copy-move forgery, has been the subject of the literature using a variety of different methodologies. In significant investigations, the use of manual procedures for the extraction of characteristics based on blocks or key-points is preferred. The block level was utilised by Rohini et al. [13], along with feature reduction at the block level with the assistance of

discrete cosine transformation. After the features have been retrieved, a comparison is made to determine whether or not there are any duplicates based on a predetermined threshold. In order to improve the quality of the Localization output, Haodong et al. [146] combined two different methods that were already in use to obtain the fused tampering potential map findings. Extraction of SURF keypoints at the first level was proposed by Wu et al [41], who said that this should be followed by reduction of features using a local binary pattern operator with rotation, which would provide rotation invariant features. Calculation of local binary patterns is accomplished by comparing two or more pixels. Patch-match and the closest neighbour field were utilised for the purpose of identifying forged areas by Cozzolino et al. [147]. The image is then separated into patches, each of which is analysed independently using the closest neighbour method. Iteratively applying the algorithm with varying values of displacement allows for the best value of displacement to be identified, which results in an approximate and rapid match. Zernike moments are used to extract rotation-invariant features for use in matching step input. Through the use of overlapping blocks of circulars in shape for [66], a robust solution that is resistant to scaling and rotation may be derived. The goal here is to extract features from the data that are unaffected by the geometry being transformed. The polar exponential transform is applied to each circular block in order to accomplish this goal. Through the use of singular value decomposition, dimensionality reductions may be accomplished, and the technique can be put into practice with a minimal cost of computing. Meena et al. [148] offer a hybrid strategy that is based on a mixture of FMT and SIFT. This strategy is more effective for working with textured as well as smooth areas. SIFT is supportive for the textured-based features, whereas FMT performed exceptionally well for the smooth slice features. The Gaussian-Hermite moments were utilised by Meena et al. in order to extract the block level characteristics. Lexicographically, the extracted features at the block level were compared in order to locate the blocks in the input image that were comparable. This method offers a reliable answer to the problem of locating the forged region [149]. Twofold technique has been implemented by Qiyue Lyu et al. [150] , whereby the first level matching is done using key-point based on (Delaunay triangles) to estimate the region of forgery in image. During the second stage, the key-points that were obtained during the first level are enlarged with the assistance of surrounding key-points, which are then classified using an algorithm known as DBSCAN (Density-based spatial clustering of applications with

noise). In their study, Ritu *et al.* [151] developed a method for the extraction of block-level features that was based on FCM (Fuzzy C-Means) Clustering and utilised emperor penguin optimization. After that, the segmented block characteristics are run through a gabour filter, which uses an algorithm called RANSAC (Random sample consensus) to eliminate any false matches. Chen *et al.* [152] developed a novel strategy to extract the features, in which the input image was sent to a two-layer deep neural network. The neural network will get rid of any unnecessary or irrelevant characteristics, but the weakened feature signals that are based on tempering will be kept. In comparison to RCNN, this approach has demonstrated superior performance. Hossein *et al.* [153] came up with a novel approach that is based on the deletion of SIFT key points. Their goal was to get rid of or minimize the number of key points that were extracted through the use of the SIFT algorithm using a Gaussian function

6.3 Proposed Algorithm (NB-Localization)

In Algorithm part of this section, the NB-localization procedure is discussed. This is the algorithm that is used to match the duplicated blocks in a forged image. In this, the value of the variable 'block' is set to 5, which will result in the image being divided into 5X5 chunks. On the other hand, the blocks were also tried with 4, 5, 6, and even more of such numbers, and the results obtained with 5 were the best. The method consists of four nested for loops, the first of which scans the image in a block-by-block fashion from the top to the bottom along the height of the image. The second for loop scans the image in a block-by-block fashion, moving from left to right across the breadth of the image. The third for loop searches the image for matching pixels block-wise, moving along the height of the image from top to bottom. It does this by going to each and every conceivable pixel. The last iteration of the for loop searches the image for matching pixels block by block, moving down the breadth of the image from left to right and visiting each and every available pixel. Therefore, the first and second iterations of the for loop scan the image by splitting it into blocks. The third and fourth iterations of the for loop scan the image by selecting blocks of the same size. The top left corner of the block can be located on any pixel. Therefore, lastly, we are able to determine whether or not a block has the greatest number of pixels that match at any of the blocks in the first two loops or any of the

blocks in the last two loops. The difference between the image blocks that were acquired from the first two loops and the image blocks that were obtained from the last two loops is used to calculate the greatest matching block. After that, we count how many pixels in this difference image block have a value of 0. We maintain the maximum zero count from the previous crop and retain the location of two blocks cropped. This process will work on images that have not been forged, and it will show the maximum matching block in those images as well. Finally, after completing all four for loops, we get the position of blocks and pixels that have the maximum number of zeros, and we plot two rectangles with red boundaries to show forgery, as shown in Figure 6.3. Therefore, we utilize the SSIM index of two clipped blocks, and if the result is larger than 0.5, then we can confidently say that the image was fabricated; otherwise, we can classify it as non-forged. Because we are concentrating on two separate image segments that were cloned and made to seem the same, we have not taken into account the overlapping resemblance. If we take into consideration overlapping blocks, then it will attempt to match an area that is replicated over itself by slightly shifting it in the x and y directions. If it is successful, then there will not be two such regions present.

The structural similarity index measure, often known as SSIM, is determined by looking at three different aspects of an image: its luminance (l), contrast (c), and structure (s). The following three equations are required for this equation to be valid:

$$I(x, y) = \frac{2\mu_x \mu_y + c_1}{\mu_x^2 + \mu_y^2 + c_1} \quad (1)$$

$$c(x, y) = \frac{2\sigma_x \sigma_y + c_2}{\sigma_x^2 + \sigma_y^2 + c_2} \quad (2)$$

$$s(x, y) = \frac{\sigma_{xy} + c_3}{\sigma_{xy} + c_3} \quad (3)$$

With additional condition:
$$c_3 = \frac{c_2}{c_1} \quad (4)$$

The equation for SSIM can now be written as:

$$SSIM(x, y) = [I(x, y)^\alpha \cdot c(x, y)^\beta \cdot s(x, y)^\gamma] \quad (6)$$

Setting weights α , β and γ to 1 the equation reduces to:

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_x\sigma_y + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (7)$$

Here μ_x is the average of x , μ_y is the average of y , σ_x^2 is the variance of x , σ_y^2 is the variance of y , and σ_{xy} is the covariance of x and y .

Algorithm 1 : Detect copied blocks in forged images

Input : img ▷ Image matrix of test image

1: **procedure** DeTECTForgery(img) ▷ Detect the copied blocks

2: $h \leftarrow img.height$

3: $w \leftarrow img.width$

4: $maxzero \leftarrow 0$

5: $max_i \leftarrow 0$

6: $max_j \leftarrow 0$

7: $max_h \leftarrow 0$

8: $max_w \leftarrow 0$

9: $blocks \leftarrow 5$

10: $blockh \leftarrow h/blocks$

11: $blockw \leftarrow w/blocks$

12: **for** i in range(0, blocks) **do**

13: **for** j in range(0, blocks) **do**

14: **for** k in range(0, height - block h) **do**

15: **for** l in range(0, width - block w) **do**

16: $blk1 = img.crop(i * blockh, j * blockw, (i + 1) * blockh, (j + 1) * blockw)$

17: $blk2 = img.crop(k, l, k + blockh, l + blockw)$

18: $diff_blk = blk1 - blk2$

19: ▷ Count number of zeros in $diff_blk$ and assign to z

20: **if** $z > max\ zero$ **then**

21: $maxzero = z$

22: $max_i = i$

23: $max_j = j$

24: $max_h = k$

25: $max_w = l$

26: $blk1 = img.crop(max_i * blockh, max_j * block w, (max_i + 1) * blockh, (max_j + 1) * blockw)$

27: $blk2 = img.crop (max_k, max_l, max_k + block h, max_l + blockw)$

28: Calculate the SSIM on $blk1$ and $blk2$

29: ▷ Change border color of $blk1$ and $blk2$ to red to show copied regions

6.4 Results and discussion

Experiments were carried out on an NVIDIA DGX v100 supercomputer, which is equipped with a sum of 40,600 CUDA cores and a speed of 1000 Tera FLOPS. We were able to quickly accomplish results with a fairly large collection of images help of the machine, and we computed a variety of different performance measures.

6.4.1 Dataset Description

For the purpose of evaluating our algorithm, we used eight different datasets. Each dataset contains images of varying quality, which assures to arrive at a result that is both reliable and accurate regarding forgery classification and localization. Table 6.1 contains a summary of the data sets that were utilised in the study. The detection of copy-move forgery is complicated by a number of factors, including the rescaling of copied patches, rotation of copied patches, translation of patches, and so on. Therefore, we have taken into consideration various datasets that contain images that belong to a variety of categories (such as scaled, rotated, and translated). The inclusion of patched images that have been rescaled, rotated, and translated is being done with the intention of verifying the robustness of the proposed algorithm. In Table 6.1, you'll find a description of the various datasets that were utilised in this proposed work, as well as the categories of images that were accessible.

Table 6.1. Summary of datasets used for algorithm evaluation

Parameters	COMOFOD	CASIA-1	CASIA-2	IMD	MICC-F2000	COVERAGE
Total Images	10400	1721	12323	96	2000	200
Forged	5200	921	5123	48	700	100
Original	5200	800	7200	48	1300	100
Image Size/s	512X512, 3000X2000	384x256	320X240 to 800*600	1024X683 to 3264X2448	2048X1536	410X421 to 534X438
Scaled Images	Yes	Yes	Yes	Yes	Yes	Yes
Rotated Images	Yes	Yes	Yes	Yes	Yes	Yes
Translation	Yes	Yes	Yes	Yes	Yes	Yes
Combination	Yes	Yes	Yes	Yes	Yes	Yes







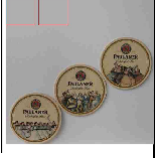

Figure 6.3 displays the localization result that was achieved by applying the suggested algorithm to two different sample images. The maximum number of matching results are displayed here with red squares surrounding the region that was copied.



Figure 6.3: Sample forged images with copied blocks in red squares.

Table 6.2 illustrates the difference in the value of the SSIM between forged and non-forged images in two maximum matching sub-blocks. As can be evidently seen, both the zero count and the SSIM are quite high for images that have been forged. If we set the threshold for SSIM at 0.5, then it will be simple for us to determine whether or not the image has been tampered with. We have substituted the well-known descriptors with the SSIM parameter in this case because, in a non-forged image, the algorithm will return the maximum number of blocks that are similar to one another. Descriptors such as DCT (Discrete cosine transform) and DWT (Discrete wavelength transform) are utilised in the process of image compression; as a result, they will not function properly in this context. Because we need to yet again determine either the Euclidean distance, the cosine similarity, or the difference between these feature vectors. The SSIM is a measure of the similarity of images and can differentiate between image crops that are exactly the same and those that are nearly the same. Several different datasets were taken into consideration during the NB-localization algorithm evaluation process. COMOFOD [118], CASIA V1 [83], CASIA V2 [101], Image manipulation dataset (IMD) [9], MICC-F220 [134], MICC-F2000, MICC-F600 and coverage [154] are the primary datasets that are utilised in the field of image forgery detection. For the sake of simplicity and randomness, we have taken approximately one hundred sample images from the datasets to test on our algorithm. Some of the results are presented in Table 6.2 which can be found further down on this page. Precision, recall, F1-score, and accuracy are the primary evaluation parameters that have been taken into consideration.

Table 6.2: Statistics of matching 2 sub blocks in forged and non forged images

Image	Zero Count	SSIM	Type of Image
	7563	0.622	Forged
	6544	0.578	Forged
	6943	0.598	Forged
	6214	0.552	Forged
	5843	0.532	Forged
	944	0.251	Non Forged
	711	0.232	Non Forged
	1243	0.372	Non Forged

6.4.2 Evaluation parameters

After applying the algorithm to the evaluation datasets that were mentioned, the results are computed in a variety of dimensions so that their performance can be compared. The parameters, as well as their importance, are discussed further.

Accuracy: is an evaluation regarding the performance of the model in terms of prediction [128][49]. This parameter gives an indication of the percentage of total predictions made by the algorithm that actually turn out to be accurate with regard to forged images [155]. Accuracy is calculated for each of the datasets that have been described, and the COMOFOD and converge datasets have the highest accuracy, coming in at 97%, as can be seen in Table 6.3. (a).

Precision: It refers to the number of images that can be accurately identified as forged images by using the algorithm [151][156]. The best value of precision is 0.98 with four datasets as shown in Table 6.3(b). Consistent value of more than 90% for each dataset reflects the robustness of proposed algorithm.

Recall: In terms of problems under consideration, recall or sensitivity is assessment of images that are predicted to be forged out of total forged images [151]. Result of recall on different dataset of forgery domain are shown in Table 6.3(c) and best recall value of 0.98 is achieved on IMD (Image manipulation dataset).

Specificity: It is also called TNR (True negative rate). Specificity is about calculation of ratio of original images predicted with respect to total original images [157]. It signifies the extent of deviation towards particular class. Both recall and specificity should approach 1 or 100% equally to demonstrate the unbiased classification. In our case the best value of specificity is 0.98 for image manipulation dataset that is very close to 1 as shown in Table 6.3(d).

Similar to above parameters there are other evaluation parameter chosen such as False negative rate (FNR) [157], False Postive rate (FPR) [87], False discovery rate (FD) [158] [131], Prevalence threshold (PT) [159] to explore the robustness of algorithm, Mathews correlation co-efficient (MCC) [160], F1-Score [161], False omission rate (FOR) [162] and Fowlkes mallows index(FMI) [163] etc. Result of all the parameters are shown in Table 6.3(a) to 6.3(l). Result of all the parameters is consistent with different dataset.

Table 6.3 shows the result of proposed algorithm for various parameters discussed above with different public datasets like CASIA, MICC-F2000, COMOFOD that are majorly used by authors in the area of image forgery.

Table 6.3. Various Evaluation Parameters result in ascending order with different datasets. a) Accuracy b) Precision c) Sensitivity d) Specificity e) FNR f) FPR g) FDR h) PT i) MCC j) F1-Score k) FOR l) FMI

(a) Accuracy		(b) Precision	
Dataset	Value	Dataset	Value
CASIA-2	0.92	CASIA-2	0.92

MICC-F2000	0.93	IMD	0.94
CASIA-1	0.94	MICC-F600	0.94
MICC-F600	0.94	MICC-F2000	0.96
IMD	0.96	CASIA-1	0.98
MICC-F220	0.96	MICC-F220	0.98
COMOFOD	0.97	COMOFOD	0.98
Coverage	0.97	Coverage	0.98

(c) Recall		(d) Specificity	
Dataset	Value	Dataset	Value
CASIA-1	0.90	CASIA-1	0.90
MICC-	0.90	MICC-F2000	0.90
CASIA-2	0.92	CASIA-2	0.92
MICC-F220	0.94	MICC-F220	0.94
MICC-F600	0.94	MICC-F600	0.94
COMOFOD	0.96	COMOFOD	0.96
Coverage	0.96	Coverage	0.96
IMD	0.98	IMD	0.98

(e) FNR		(f) FPR	
Dataset	Value	Dataset	Value
IMD	0.02	IMD	0.02
COMOFOD	0.04	COMOFOD	0.04
Coverage	0.04	Coverage	0.04
MICC-F220	0.06	MICC-F220	0.06
MICC-F600	0.06	MICC-F600	0.06
CASIA-2	0.08	CASIA-2	0.08
CASIA-1	0.10	CASIA-1	0.10
MICC-F2000	0.10	MICC-F2000	0.10

(g) FDR		(h) PT	
Dataset	Value	Dataset	Value
COMOFOD	0.02	IMD	0.13
Coverage	0.02	COMOFOD	0.17
MICC-F220	0.02	Coverage	0.17
CASIA-1	0.02	MICC-F220	0.20
MICC-F2000	0.04	MICC-F600	0.20
IMD	0.06	CASIA-2	0.23
MICC-F600	0.06	CASIA-1	0.25
CASIA-2	0.08	MICC-F2000	0.25

(i) MCC		(j) F1 Score	
Dataset	Value	Dataset	Value
MICC-F2000	0.83	CASIA-2	0.92
CASIA-2	0.84	MICC-F2000	0.93
CASIA-1	0.84	CASIA-1	0.94

MICC-F600	0.88	MICC-F600	0.94
MICC-F220	0.90	IMD	0.96
COMOFOD	0.93	MICC-F220	0.96
Coverage	0.93	COMOFOD	0.97
IMD	0.94	Coverage	0.97

(k) FOR		(l) FMI	
Dataset	Value	Dataset	Value
IMD	0.02	CASIA-2	0.92
COMOFOD	0.04	MICC-F2000	0.93
Coverage	0.04	CASIA-1	0.94
MICC-F220	0.06	MICC-F600	0.94
MICC-F600	0.06	IMD	0.96
CASIA-2	0.08	MICC-F220	0.96
CASIA-1	0.09	COMOFOD	0.97
MICC-F2000	0.09	Coverage	0.97

In Figure 6.4 the AUC-ROC graph is shown for AUC values computed through CASIA-1, CASIA-2, Coverage, MICC-F2000, COMOFOD and MICC-F6000. Best values are obtained on COMOFOD dataset and remarkably equivalent results are shown for others datasets as well.

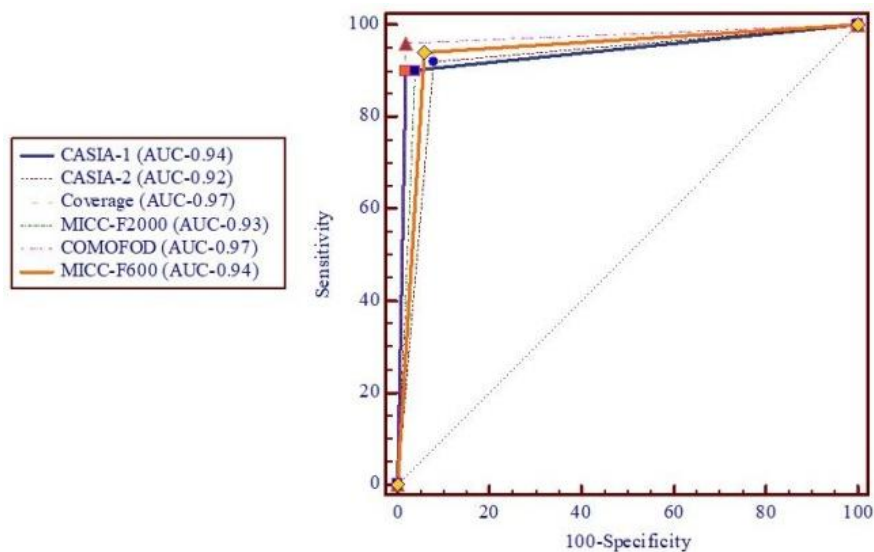


Figure 6.4: AUC-ROC curve comparison for different datasets

Table 6.4. Statistical Result of different parameters considering all results for datasets under study

Sr.	Parameter	Avg.	Std. Dev.	Min.	Max.
1	Accuracy	0.95	0.02	0.92	0.97
2	Precision	0.96	0.02	0.92	0.98
3	Sensitivity	0.94	0.03	0.90	0.98
4	F1-Score	0.95	0.02	0.92	0.97

5	Specificity	0.94	0.03	0.90	0.98
6	FPR	0.06	0.03	0.02	0.10
7	FNR	0.06	0.03	0.02	0.10
8	FDR	0.04	0.02	0.02	0.08
9	PT	0.20	0.04	0.13	0.25
10	MCC	0.89	0.04	0.83	0.94
11	FOR	0.06	0.03	0.02	0.09
12	FMI	0.95	0.02	0.92	0.97

For each dataset under consideration, comparisons of the average accuracy, precision, recall, and F1-score are provided in Table 6.4. Through datasets, the average sensitivity or TPR is 93%, and the average accuracy is 95%. Results are contrasted in Table 6.5 with previous progressive studies on copy move forgery. With the exception of the IMD dataset, where all 96 images were used to generate the result, we randomly selected 100 images from each dataset to produce the results presented in Table 6.5. The coverage dataset showed 97 percent accuracy and an F1-Score. In terms of precision outcomes, the COMOFOFOD dataset outperformed all others. The benchmarking table in shows that the suggested algorithm had 97% accuracy while using COMOFOFOD.

Table 6.5. Benchmarking of proposed algorithm with existing literature results based on dataset.

Dataset	Approach/Features	#Acc	Pre.	Sen.	F1-S.	Sp.	FPR	FNR
COMOFOD	NB-Localization [Proposed]	0.97	0.98	0.96	0.97	0.96	0.04	0.04
	Tetrolet Transform [156]	-	0.99	0.96	0.96	-	-	-
	SIFT [119]	-	0.77	0.82	0.8	-	-	-
	Segmentation [120]	-	0.77	0.66	0.71	-	-	-
	Dense field Matching[164]	-	0.71	0.88	0.78	-	-	-
	Adaptive over segmentation [165]	-	0.81	0.84	0.82	-	-	-
CASIA-1	Block Level Features [74]	-	0.89	0.83	0.87	-	-	-
	NB-Localization [Proposed]	0.94	0.98	0.90	0.94	0.90	0.10	0.10
	Inception-Net [85]	-	0.71	0.55	0.64	-	-	-
	Surface Probability [166]	-	-	-	0.54	-	-	-
	U-Net [167]	0.76	-	-	0.84	-	-	-
CASIA-2	RCNN [138]	-	-	-	0.4	-	-	-
	NB-Localization [Proposed]	0.92	0.92	0.92	0.92	0.92	0.08	0.08
	2-D Markov Model [138]	0.89	-	-	-	-	-	-
	Stacked Auto encoder [168]	0.91	57.67	-	-	-	-	-
CASIA-2	CNN, Camera based Features [169][124]	0.73	-	0.96	-	0.6	-	-

MICC-F220	NB-Localization [Proposed]	0.96	0.98	0.94	0.96	0.94	0.06	0.06
	SVM, SURF [170]	0.8	-	-	-	-	-	-
	Key-point Matching [171]	0.92	-	-	-	-	-	-
	DCT, SURF	0.95	-	-	-	-	-	-
	KNN, YCbCr(Color) [172]	0.94	-	-	-	-	-	-
MICC-F2000	NB-Localization [Proposed]	0.93	0.96	0.90	0.93	0.90	0.10	0.10
	BRIEF, SURF [173]	0.82	-	-	-	-	-	-
	SVM, SURF [170]	0.81	-	-	-	-	-	-
	Key-point Matching [171]	0.85	-	-	-	-	-	-
MICC-F600	NB-Localization[Proposed]	0.94	0.94	0.94	0.94	0.94	0.06	0.06
	FAST, BRIEF [174]	0.84	-	-	-	-	-	-
	LIOP, DBSCAN [150]	-	0.74	0.81	0.77			
	SIFT, ORB,SVM [173]	0.9	-	-	-	-	-	-
Coverage	NB-Localization [Proposed]	0.97	0.98	0.96	0.97	0.96	0.04	0.04
	RCNN [175]	-	-	-	0.47	-	-	-
	LSTM, Radon Transform [176]	0.98	-	-	0.91	-	-	-
	CFA features with CNN [177]	-	-	-	0.19	-	-	-

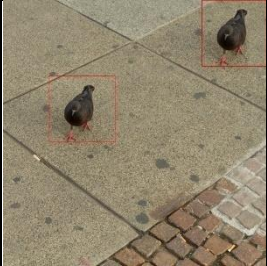
Acc=Accuracy, Pre. =Precision, Sen=Sensitivity, F1-S=F1-Score, Sp=Specificity


6.4.3 Pixel results for different block numbers

The results were examined in relation to the various block numbers (4, 5, 6) into which the image was divided. In order for any image processing system to take these values and act in accordance with them, the pixels of the top left corner of matched blocks were also recorded. Table 6.6 displays the results using various block sizes on a sample image.

As a result, it was discovered that the technique is reliable for varied block sizes and that a user can modify it to locate forged blocks of various sizes. The user can run the procedure with the number of blocks as an input parameter and compare the results graphically to identify the best matching forged region.

Table 6.6: Pixel level results with different number of blocks

Image	Blocks	1 st block top left	2 nd block top left
	4	(0, 384)	(146, 89)

	5	(58,397)	(204, 102)
	6	(24, 380)	(170, 85)

6.5 Conclusion

In general, block level techniques or key-point based approaches are used to implement forgery detection. In order to locate the forged region in such images, we used a block level method. On the basis of the differences in block level features, a block wise method is used to locate matched blocks. The blocks taken in this manner have been contrasted in terms of SSIM parameters and the maximum number of zeros. Blocks localized by a rectangle boundary have the most matching zeros. To determine if an image is forged or real, classification is based on the SSIM value. For scaled and translated blocks, the method is effective.

CHAPTER-7

CONCLUSION AND FUTURE SCOPE

We have worked on extensive review of deep learning methods where we elaborated the role of deep learning in image forgery while keeping (i) the bias in Artificial Intelligence and (ii) benchmarking against non-randomized paradigms in the framework. A set of recommendations were presented for improving the RoB and the most premium were sample size, ability to generalization, superior feature extraction paradigm, scientific validation, and evaluation.

We first proposed a customized CNN model to classify the forged images in a robust way with an accuracy of 94% on diverse datasets as well as their combination in order to get superior classification results. This model was intended to classify the forged images. Further In this thesis, we proposed an approach for tempering Classification without any deficiency in terms of challenges posed in the form of sensitivity towards reflection, image compression, rotation, and scaling altogether. This is the major outcome of the CNN approach, and it is what we believe to be the most important contribution it makes. There are a lot of manual features extraction-based approaches out there, but they only work in certain circumstances. They do not function very well when another situation is present, such as when the image patch is rotated, resized, or when any lighting changes are made to the image. In order to achieve this goal, we suggested a hybrid Convolution Neural Network that would consist of a mix of the VGG16 and Inception V3 models, with some additional dense layers that would increase the performance of forgery classification. The findings of the experiments indicate that the hybrid neural network that was developed has a higher level of efficiency. The outcomes of this research might further stimulate the researchers to employ various combinations of a wide range of new and current models with the purpose of achieving better categorization results.

For the purpose of copy-move forgery mask detection, we have developed and implemented a DCT (discrete cosine transform) block level features extraction method. The altered images have their feature information retrieved at the block level. The visual findings are offered for comparison between the real mask and the one that was anticipated. The detection accuracy of fake masks is around 95% on average. A pristine method that is block-

based has been suggested as a way to further improve the outcomes of the localization of the forged area. A method that is applied block by block in order to locate matching blocks on the basis of differences in block-level attributes is used. The blocks that were taken have been evaluated based on their maximum number of zeros as well as their SSIM characteristics. The rectangular Boundary is used to locate blocks that have the largest number of matched zeros. The strategy is effective for both translated and scaled blocks in the application.

In deep learning models, there is a scope of parameter setting that may be further explored as part of future study. This is something that can be done. Because of the substantial research that has been done on hybrid deep learning models, it has the potential to be one of the options that can be used to copy move forgery localization. Further investigation may benefit from the application of ensemble techniques in conjunction with medical or thermal images. Within the realm of picture forgery detection and localization, the future focus of these proposed approaches will be on the application of compression techniques. In most cases, much computational work is required for ensemble models. These types of models are able to be improved using strategies that include model compression.

REFERENCES

- [1] M. Sridevi, C. Mala, and S. Sanyam, “Comparative study of image forgery and copy-move techniques,” in *Advances in Intelligent and Soft Computing*, 2012. doi: 10.1007/978-3-642-30157-5_71.
- [2] R. Dixit and R. Naskar, “Review , analysis and parameterisation of techniques for copy – move forgery detection in digital images,” 2017, doi: 10.1049/iet-ipr.2016.0322.
- [3] D. analyst M. Fitzpatrick, “Iran ‘faked missile test image,’” 2008. http://news.bbc.co.uk/2/hi/middle_east/7500917.stm
- [4] A. Ghoneim, G. Muhammad, S. U. Amin, and B. Gupta, “Medical Image Forgery Detection for Smart Healthcare,” *IEEE Commun. Mag.*, 2018, doi: 10.1109/MCOM.2018.1700817.
- [5] M. E. C. Science, “Detection Techniques,” *J. Chromatogr. Libr.*, vol. 52, no. C, pp. 55–154, 1992, doi: 10.1016/S0301-4770(08)60330-9.
- [6] L. Zheng, Y. Zhang, and V. L. L. Thing, “A survey on image tampering and its detection in real-world photos,” *J. Vis. Commun. Image Represent.*, vol. 58, no. December, pp. 380–399, 2019, doi: 10.1016/j.jvcir.2018.12.022.
- [7] A. Doegar, S. Hiriyannaiah, S. G. Matt, S. K. Gopaliyengar, and M. Dutta, “Image forgery detection based on fusion of lightweight deep learning models,” *Turkish J. Electr. Eng. Comput. Sci.*, vol. 29, no. 4, 2021, doi: 10.3906/ELK-2005-37.
- [8] R. Agarwal, D. Khudaniya, A. Gupta, and K. Grover, “Image Forgery Detection and Deep Learning Techniques: A Review,” *Proc. Int. Conf. Intell. Comput. Control Syst. ICICCS 2020*, no. Icices, pp. 1096–1100, 2020, doi: 10.1109/ICICCS48265.2020.9121083.
- [9] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, “An evaluation of popular copy-move forgery detection approaches,” *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 6, pp. 1841–1854, 2012, doi: 10.1109/TIFS.2012.2218597.
- [10] B. Yang, X. Sun, H. Guo, Z. Xia, and X. Chen, “A copy-move forgery detection method based on CMFD-SIFT,” *Multimed. Tools Appl.*, vol. 77, no. 1, pp. 837–855,

- 2018, doi: 10.1007/s11042-016-4289-y.
- [11] E. Ardizzone, A. Bruno, and G. Mazzola, "Copy-Move Forgery Detection by Matching Triangles of Keypoints," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 10, pp. 2084–2094, 2015, doi: 10.1109/TIFS.2015.2445742.
- [12] G. R. Sinha and Jasjit S. Suri, "Cognitive Informatics, Computer Modelling, and Cognitive Science," *Comput. Model. Cogn. Sci.*, vol. 1, 2019.
- [13] R. A. Maind, A. Khade, and D. K. Chitre, "Image Copy Move Forgery Detection using Block Representing Method," no. 2, pp. 49–53, 2014.
- [14] Abhishek and N. Jindal, "Copy move and splicing forgery detection using deep convolution neural network, and semantic segmentation," *Multimed. Tools Appl.*, 2020, doi: 10.1007/s11042-020-09816-3.
- [15] Y. Abdalla, M. Tariq Iqbal, and M. Shehata, "Copy-move forgery detection and localization using a generative adversarial network and convolutional neural-network," *Inf.*, vol. 10, no. 9, 2019, doi: 10.3390/info10090286.
- [16] P. K. Jain, N. Sharma, A. A. Giannopoulos, L. Saba, A. Nicolaides, and J. S. Suri, "Hybrid deep learning segmentation models for atherosclerotic plaque in internal carotid artery B-mode ultrasound," *Comput. Biol. Med.*, vol. 136, no. 1, p. 104721, 2021, doi: 10.1016/j.compbio.2021.104721.
- [17] S. J. Saba L, Biswas M, Kuppili V, Cuadrado Godia E, Suri HS, Edla DR, Omerzu T, Laird JR, Khanna NN, Mavrogeni S, Protogerou A, Sfikakis PP, Viswanathan V, Kitis GD, Nicolaides A, Gupta A, "The present and future of deep learning in radiology," *Eur J Radiol*, vol. 114, no. 5, pp. 14–24, 2019, doi: 10.1016/j.ejrad.2019.02.038.
- [18] M. Biswas *et al.*, "State-of-the-art review on deep learning in medical imaging," *Frontiers in Bioscience - Landmark*. 2019. doi: 10.2741/4725.
- [19] D. Chauhan, D. Kasat, S. Jain, and V. Thakare, "Survey on Keypoint Based Copy-move Forgery Detection Methods on Image," *Procedia Comput. Sci.*, vol. 85, no. Cms, pp. 206–212, 2016, doi: 10.1016/j.procs.2016.05.213.
- [20] E. et. al. Vasilis, "Face Morphing, a Modern Threat to Border Security: Recent

Advances and Open Challenges,” *Appl. Sci.*, vol. 11, no. 7, 2021.

- [21] J. Suri *et al.*, “Systematic Review of Artificial Intelligence in Acute Respiratory Distress Syndrome for COVID-19 Lung Patients: A Biomedical Imaging Perspective,” *IEEE J. Biomed. Heal. Informatics*, vol. 25, no. 11, pp. 4128–4139, 2021, doi: 10.1109/JBHI.2021.3103839.
- [22] C.-G. E. *et al.*, “Ranking of stroke and cardiovascular risk factors for an optimal risk calculator design: Logistic regression approach,” *Comput. Biol. Med.*, vol. 108, no. 1, pp. 182–195, 2019.
- [23] M. D. Ansari, S. P. Ghrera, and V. Tyagi, “Pixel-Based Image Forgery Detection: A Review,” *IETE J. Educ.*, vol. 55, no. 1, pp. 40–46, 2014, doi: 10.1080/09747338.2014.921415.
- [24] S. Teerakanok and T. Uehara, “Copy-Move Forgery Detection: A State-of-the-Art Technical Review and Analysis,” *IEEE Access*, vol. 7, pp. 40550–40568, 2019, doi: 10.1109/ACCESS.2019.2907316.
- [25] W. D. Ferreira, C. B. R. Ferreira, G. da Cruz Júnior, and F. Soares, “A review of digital image forensics,” *Comput. Electr. Eng.*, vol. 85, 2020, doi: 10.1016/j.compeleceng.2020.106685.
- [26] W. Nanda, N. Diane, S. Xingming, and F. K. Moise, “A Survey of Partition-Based Techniques for Copy-Move Forgery Detection,” vol. 2014, no. 2014, 2014.
- [27] I. Castillo Camacho and K. Wang, “A comprehensive review of deep-learning-based methods for image forensics,” *J. Imaging*, vol. 7, no. 4, 2021, doi: 10.3390/jimaging7040069.
- [28] A. H. Saber, M. A. Khan, and B. G. Mejbil, “A survey on image forgery detection using different forensic approaches,” *Adv. Sci. Technol. Eng. Syst.*, vol. 5, no. 3, pp. 361–370, 2020, doi: 10.25046/aj050347.
- [29] P. Raja, M. A. Professor, and D. Lalitha Bhaskari, “Image Tamper Detection and Localization based on self-generated Verification Code during Image Acquisition,” *Int. J. Appl. Eng. Res.*, vol. 13, no. 5, 2018.

- [30] C. Engineering *et al.*, “Medical Image Duplication Copy Move Forgery Detection Using DCT Method,” vol. 7, no. 2, pp. 510–513, 2020.
- [31] S. Sharma and U. Ghanekar, “A rotationally invariant texture descriptor to detect copy move forgery in medical images,” *Proc. - 2015 IEEE Int. Conf. Comput. Intell. Commun. Technol. CICT 2015*, pp. 795–798, 2015, doi: 10.1109/CICT.2015.88.
- [32] B. Gurunlu and S. Ozturk, “Efficient Approach for Block-Based Copy-Move Forgery Detection,” in *Lecture Notes in Networks and Systems*, 2022, vol. 286. doi: 10.1007/978-981-16-4016-2_16.
- [33] S. Roy and K. Roy, “Block Based Copy–Move Forgery Detection for Digital Image Forensic,” 2022. doi: 10.1007/978-981-16-5207-3_42.
- [34] V. Kour, P. Aggarwal, and R. Kaur, “A Fast Block-Based Technique to Detect Copy-Move Forgery in Digital Images,” 2022. doi: 10.1007/978-981-16-3342-3_25.
- [35] H. Li, W. Luo, X. Qiu, and J. Huang, “Image Forgery Localization via Integrating,” *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 5, pp. 1240–1252, 2017, doi: 10.1109/TIFS.2017.2656823.
- [36] K. N. Venu and B. K. Sujatha, “Enhanced block based copy paste image forgery detection,” *Mater. Today Proc.*, 2021, doi: 10.1016/j.matpr.2021.01.189.
- [37] A. Diwan, R. Sharma, A. K. Roy, and S. K. Mitra, “Keypoint based comprehensive copy-move forgery detection,” *IET Image Process.*, vol. 15, no. 6, 2021, doi: 10.1049/ipr2.12105.
- [38] “Keypoint Descriptors-Based Image Forensic Approach for Copy-Move Forgery Detection,” *J. Xidian Univ.*, vol. 15, no. 6, 2021, doi: 10.37896/jxu15.6/044.
- [39] P. Niu, C. Wang, W. Chen, H. Yang, and X. Wang, “Fast and effective Keypoint-based image copy-move forgery detection using complex-valued moment invariants,” *J. Vis. Commun. Image Represent.*, vol. 77, 2021, doi: 10.1016/j.jvcir.2021.103068.
- [40] H. Chen, X. Yang, and Y. Lyu, “Copy-move forgery detection based on keypoint clustering and similar neighborhood search algorithm,” *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.2974804.

- [41] Y. Wu *et al.*, “Copy-Move Forgery Detection Exploiting,” *Multimed. Tools Appl.*, vol. 2, no. 2, pp. 57–64, 2020, doi: 10.1007/978-981-10-7644-2.
- [42] X. Y. Wang, S. Li, Y. N. Liu, Y. Niu, H. Y. Yang, and Z. li Zhou, “A new keypoint-based copy-move forgery detection for small smooth regions,” *Multimed. Tools Appl.*, vol. 76, no. 22, 2017, doi: 10.1007/s11042-016-4140-5.
- [43] K. Rathi and P. Singh, “Copy Move Forgery Detection by Using Integration of SLIC and SIFT,” in *Lecture Notes in Networks and Systems*, 2022, vol. 209. doi: 10.1007/978-981-16-2126-0_43.
- [44] N. B. Nor, M. Y. I. Idris, A. W. Abdul Wahab, R. Salleh, and A. Ismail, “CMF-iteMS: An automatic threshold selection for detection of copy-move forgery,” *Forensic Sci. Int.*, vol. 295, pp. 83–99, 2019, doi: 10.1016/j.forsciint.2018.12.004.
- [45] A. Thakur and N. Jindal, “Hybrid deep learning and machine learning approach for passive image forensic,” *IET Image Process.*, vol. 14, no. 10, 2020, doi: 10.1049/iet-ipr.2019.1291.
- [46] Monika and A. Passi, “Digital Image Forensic based on Machine Learning approach for Forgery Detection and Localization,” in *Journal of Physics: Conference Series*, 2021, vol. 1950, no. 1. doi: 10.1088/1742-6596/1950/1/012035.
- [47] L. M. Dang, K. Min, S. Lee, D. Han, and H. Moon, “Tampered and computer-generated face images identification based on deep learning,” *Appl. Sci.*, vol. 10, no. 2, 2020, doi: 10.3390/app10020505.
- [48] N. Nanthini, S. Sasipriya, S. K. Sahoo, B. Pattanaik, S. A. Sivakumar, and B. M. Shankar, “A Novel Deep learning and Machine Learning powered approach for Image Forgery Detection,” in *Proceedings of the 6th International Conference on Inventive Computation Technologies, ICICT 2021*, 2021. doi: 10.1109/ICICT50816.2021.9358484.
- [49] M. A. Elaskily *et al.*, “A novel deep learning framework for copy-moveforgery detection in images,” *Multimed. Tools Appl.*, vol. 79, no. 27–28, pp. 19167–19192, 2020, doi: 10.1007/s11042-020-08751-7.
- [50] P. Karthikeyan, R. Bhavani, D. Rajiniginath, and R. Priya, “A Novel Deep Learning

- Framework for Image Forgery Detection,” vol. XII, no. 1, pp. 1–12, 1945.
- [51] Y. Huang, W. Lu, W. Sun, and D. Long, “Improved DCT-based detection of copy-move forgery in images,” *Forensic Sci. Int.*, vol. 206, no. 1–3, pp. 178–184, 2011, doi: 10.1016/j.forsciint.2010.08.001.
- [52] A. Kannammal and S. S. Rani, “Authentication of Medical Images using Integer Wavelet Transforms,” *Int. J. Emerg. Technol. Adv. Eng.*, vol. 2, no. 9, pp. 104–108, 2012, [Online]. Available: <https://www.researchgate.net/publication/281448444>
- [53] B. Soni and D. Biswas, “Image Forensic using Block-based Copy-move Forgery Detection,” *2018 5th Int. Conf. Signal Process. Integr. Networks*, pp. 888–893, 2018, doi: 10.1109/SPIN.2018.8474287.
- [54] H. Bay, A. Ess, T. Tuytelaars, and L. Van Gool, “Speeded-Up Robust Features (SURF),” *Comput. Vis. Image Underst.*, vol. 110, no. 3, pp. 346–359, 2008, doi: 10.1016/j.cviu.2007.09.014.
- [55] Y. Gan, J. Zhong, and C. Vong, “A Novel Copy-Move Forgery Detection Algorithm via Feature Label Matching and Hierarchical Segmentation Filtering,” *Inf. Process. Manag.*, vol. 59, no. 1, p. 102783, 2022, doi: 10.1016/j.ipm.2021.102783.
- [56] M. Mirmehdi, X. Xie, and J. Suri, *Handbook of texture analysis*. 2008. doi: 10.1142/P547.
- [57] T. Mahmood, Z. Mehmood, M. Shah, and T. Saba, “A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform,” *J. Vis. Commun. Image Represent.*, vol. 53, pp. 202–214, 2018, doi: 10.1016/j.jvcir.2018.03.015.
- [58] P. Niyishaka and C. Bhagvati, “Copy-move forgery detection using image blobs and BRISK feature,” *Multimed. Tools Appl.*, 2020, doi: 10.1007/s11042-020-09225-6.
- [59] A. Badr, A. Youssif, and M. Wafi, “A Robust Copy-Move Forgery Detection in Digital Image Forensics Using SURF,” *8th Int. Symp. Digit. Forensics Secur. ISDFS 2020*, 2020, doi: 10.1109/ISDFS49300.2020.9116433.
- [60] S. S. Narayanan and G. Gopakumar, “Recursive Block Based Keypoint Matching for

- Copy Move Image Forgery Detection,” in *2020 11th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2020*, 2020. doi: 10.1109/ICCCNT49239.2020.9225658.
- [61] E. Silva, T. Carvalho, A. Ferreira, and A. Rocha, “An End-to-End Dense-InceptionNet for Image Copy-Move Forgery Detection,” *J. Vis. Commun. Image Represent.*, vol. 29, pp. 16–32, 2015, doi: 10.1016/j.jvcir.2015.01.016.
- [62] Y. Liu, Q. Guan, and X. Zhao, “Copy-move forgery detection based on convolutional kernel network,” *Multimed. Tools Appl.*, vol. 77, no. 14, pp. 18269–18293, 2018, doi: 10.1007/s11042-017-5374-6.
- [63] Y. Wu, W. Abd-Almageed, and P. Natarajan, “Image copy-move forgery detection via an end-to-end deep neural network,” *Proc. - 2018 IEEE Winter Conf. Appl. Comput. Vision, WACV 2018*, vol. 2018-Janua, no. d, pp. 1907–1915, 2018, doi: 10.1109/WACV.2018.00211.
- [64] N. B. A. Warif *et al.*, “Copy-move forgery detection: Survey, challenges and future directions,” *J. Netw. Comput. Appl.*, vol. 75, pp. 259–278, 2016, doi: 10.1016/j.jnca.2016.09.008.
- [65] S. Walia and K. Kumar, “Digital image forgery detection: a systematic scrutiny,” *Aust. J. Forensic Sci.*, vol. 51, no. 5, pp. 488–526, 2019, doi: 10.1080/00450618.2018.1424241.
- [66] Y. Wang, X. Kang, and Y. Chen, “Robust and accurate detection of image copy-move forgery using PCET-SVD and histogram of block similarity measures,” *J. Inf. Secur. Appl.*, vol. 54, p. 102536, 2020, doi: 10.1016/j.jisa.2020.102536.
- [67] M. M. Islam, G. Karmakar, J. Kamruzzaman, and M. Murshed, “A robust forgery detection method for copy–move and splicing attacks in images,” *Electron.*, vol. 9, no. 9, pp. 1–22, 2020, doi: 10.3390/electronics9091500.
- [68] C. M. Pun and J. L. Chung, “A two-stage localization for copy-move forgery detection,” *Inf. Sci. (Ny)*, vol. 463–464, pp. 33–55, 2018, doi: 10.1016/j.ins.2018.06.040.
- [69] S. J. Ryu, M. Kirchner, M. J. Lee, and H. K. Lee, “Rotation invariant localization of

- duplicated image regions based on zernike moments,” *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 8, pp. 1355–1370, 2013, doi: 10.1109/TIFS.2013.2272377.
- [70] M. Bashar, K. Noda, N. Ohnishi, and K. Mori, “Exploring duplicated regions in natural images,” *IEEE Trans. Image Process.*, no. 99, pp. 1–40, 2010, doi: 10.1109/TIP.2010.2046599.
- [71] K. B. Meena and V. Tyagi, “A copy-move image forgery detection technique based on tetrolet transform,” *J. Inf. Secur. Appl.*, vol. 52, 2020, doi: 10.1016/j.jisa.2020.102481.
- [72] R. Dixit, R. Naskar, and S. Mishra, “Blur-invariant copy-move forgery detection technique with improved detection accuracy utilising SWT-SVD,” *IET Image Process.*, vol. 11, no. 5, pp. 301–309, 2017, doi: 10.1049/iet-ipr.2016.0537.
- [73] M. M. Isaac and M. Wilscy, “Image forgery detection using region - Based Rotation invariant Co-occurrences among adjacent LBPs,” *J. Intell. Fuzzy Syst.*, vol. 34, no. 3, pp. 1679–1690, 2018, doi: 10.3233/JIFS-169461.
- [74] Y. Sun, R. Ni, and Y. Zhao, “Nonoverlapping Blocks Based Copy-Move Forgery Detection,” in *Security and Communication Networks*, vol. 2018, 2018. doi: 10.1155/2018/1301290.
- [75] N. B. A. Warif, A. W. A. Wahab, M. Y. I. Idris, R. Salleh, and F. Othman, “SIFT-Symmetry: A robust detection method for copy-move forgery with reflection attack,” *J. Vis. Commun. Image Represent.*, vol. 46, pp. 219–232, 2017, doi: 10.1016/j.jvcir.2017.04.004.
- [76] A. Dosovitskiy, P. Fischer, J. T. Springenberg, M. Riedmiller, and T. Brox, “Discriminative unsupervised feature learning with exemplar convolutional neural networks,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 38, no. 9, pp. 1734–1747, 2016, doi: 10.1109/TPAMI.2015.2496141.
- [77] M. Ikhlayel, M. Hariadi, and K. E. Pumama, “A Study of Copy-Move Forgery Detection Scheme Based on Segmentation,” vol. 18, no. 7, pp. 27–32, 2018.
- [78] Y. Li and J. Zhou, “Fast and Effective Image Copy-Move Forgery Detection via Hierarchical Feature Point Matching,” *IEEE Trans. Inf. Forensics Secur.*, vol. PP, no. c, p. 1, 2018, doi: 10.1109/TIFS.2018.2876837.

- [79] F. Marra, Di. Gragnaniello, L. Verdoliva, and G. Poggi, “A Full-Image Full-Resolution End-to-End-Trainable CNN Framework for Image Forgery Detection,” *IEEE Access*, vol. 8, pp. 133488–133502, 2020, doi: 10.1109/ACCESS.2020.3009877.
- [80] B. Bayar and M. C. Stamm, “A Deep Learning Approach to Universal Image Manipulation Detection Using a New Convolutional Layer,” pp. 5–10, 2016, doi: 10.1145/2909827.2930786.
- [81] Y. Yan, W. Ren, and X. Cao, “Recolored Image Detection via a Deep Discriminative Model,” *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 1, pp. 5–17, 2019, doi: 10.1109/TIFS.2018.2834155.
- [82] A. Kuznetsov, “Digital image forgery detection using deep learning approach,” *J. Phys. Conf. Ser.*, vol. 1368, no. 3, 2019, doi: 10.1088/1742-6596/1368/3/032028.
- [83] J. Dong, W. Wang, and T. Tan, “CASIA image tampering detection evaluation database,” *2013 IEEE China Summit Int. Conf. Signal Inf. Process. ChinaSIP 2013 - Proc.*, pp. 422–426, 2013, doi: 10.1109/ChinaSIP.2013.6625374.
- [84] K. B. Meena and V. Tyagi, “A deep learning based method for image splicing detection,” *J. Phys. Conf. Ser.*, vol. 1714, no. 1, 2021, doi: 10.1088/1742-6596/1714/1/012038.
- [85] J. L. Zhong and C. M. Pun, “An End-to-End Dense-InceptionNet for Image Copy-Move Forgery Detection,” *IEEE Trans. Inf. Forensics Secur.*, vol. 15, no. c, pp. 2134–2146, 2020, doi: 10.1109/TIFS.2019.2957693.
- [86] Y. Rodriguez-Ortega, D. M. Ballesteros, and D. Renza, “Copy-Move Forgery Detection (CMFD) Using Deep Learning for Image and Video Forensics,” *J. Imaging*, vol. 7, no. 3, 2021, doi: 10.3390/jimaging7030059.
- [87] M. N. Abbas, M. S. Ansari, M. N. Asghar, N. Kanwal, T. O’Neill, and B. Lee, “Lightweight Deep Learning Model for Detection of Copy-Move Image Forgery with Post-Processed Attacks,” in *SAMI 2021 - IEEE 19th World Symposium on Applied Machine Intelligence and Informatics, Proceedings*, 2021. doi: 10.1109/SAMI50585.2021.9378690.
- [88] Y. Liu, Q. Guan, and X. Zhao, “Copy-move forgery detection based on convolutional

- kernel network,” *Multimed. Tools Appl.*, vol. 77, no. 14, pp. 18269–18293, 2018, doi: 10.1007/s11042-017-5374-6.
- [89] B. Liu and C. M. Pun, “Locating splicing forgery by fully convolutional networks and conditional random field,” *Signal Process. Image Commun.*, vol. 66, pp. 103–112, 2018, doi: 10.1016/j.image.2018.04.011.
- [90] Y. Liu, Q. Guan, X. Zhao, and Y. Cao, “Image Forgery Localization Based on Multi-Scale Convolutional Neural Networks,” *Proc. 6th ACM Work. Inf. Hiding Multimed. Secur.*, vol. June, no. June, pp. 85–90, 2018, doi: 10.1109/TGRS.2018.2848473.
- [91] Jiansheng Chen, Xiangui Kang, Ye Liu, and Z. Jane Wang, “Median Filtering Forensics Based on Convolutional Neural Networks,” *IEEE Signal Process. Lett.*, vol. 22, no. 11, pp. 1849–1853, 2015, doi: 10.1109/LSP.2015.2438008.
- [92] D. Cozzolino, G. Poggi, and L. Verdoliva, “Recasting Residual-based Local Descriptors as Convolutional Neural Networks,” no. Section 2, pp. 159–164, 2017, doi: 10.1145/3082031.3083247.
- [93] J. Ouyang, Y. Liu, and M. Liao, “Copy-move forgery detection based on deep learning,” *Proc. - 2017 10th Int. Congr. Image Signal Process. Biomed. Eng. Informatics, CISP-BMEI 2017*, vol. 2018-Janua, pp. 1–5, 2018, doi: 10.1109/CISP-BMEI.2017.8301940.
- [94] J. Bunk *et al.*, “Detection and Localization of Image Forgeries Using Resampling Features and Deep Learning,” *IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Work.*, vol. 2017-July, pp. 1881–1889, 2017, doi: 10.1109/CVPRW.2017.235.
- [95] N. Huang, J. He, and N. Zhu, “A Novel Method for Detecting Image Forgery Based on Convolutional Neural Network,” *Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018*, pp. 1702–1705, 2018, doi: 10.1109/TrustCom/BigDataSE.2018.00255.
- [96] L. Liu, Y. Zhao, R. Ni, Q. Tian, and S. Antonio, “Copy-Move Forgery Localization Using Convolutional Neural Networks and CFA Features,” vol. 10, no. 4, pp. 140–155, 2018, doi: 10.4018/IJDCF.2018100110.

- [97] Y. Abdalla, M. T. Iqbal, and M. Shehata, “Convolutional neural network for copy-move forgery detection,” *Symmetry (Basel)*, vol. 11, no. 10, pp. 1–17, 2019, doi: 10.3390/sym11101280.
- [98] N. Hema Rajini, “Image forgery identification using convolution neural network,” *Int. J. Recent Technol. Eng.*, vol. 8, no. 1 Special Issue 4, pp. 311–320, 2019.
- [99] B. Diallo, T. Urruty, P. Bourdon, and C. Fernandez-Maloigne, “Robust Forgery Detection for Compressed Images using CNN Supervision,” *Forensic Sci. Int. Reports*, vol. 2, no. September 2019, p. 100112, 2020, doi: 10.1016/j.fsir.2020.100112.
- [100] A. Doegar, M. Dutta, and G. Kumar, “CNN based Image Forgery Detection using pre-trained AlexNet Model,” *Proc. Int. Conf. Comput. Intell. IoT 2018*, pp. 402–407, 2018.
- [101] R. Salloum, Y. Ren, and C. C. Jay Kuo, “Image Splicing Localization using a Multi-task Fully Convolutional Network (MFCN),” *J. Vis. Commun. Image Represent.*, vol. 51, no. December 2017, pp. 201–209, 2018, doi: 10.1016/j.jvcir.2018.01.010.
- [102] M. T. H. Majumder and A. B. M. Alim Al Islam, “A tale of a deep learning approach to image forgery detection,” *Proc. 2018 5th Int. Conf. Networking, Syst. Secur. NSysS 2018*, pp. 1–9, 2019, doi: 10.1109/NSysS.2018.8631389.
- [103] R. Agarwal, “An Efficient Method of Copy Move Forgery Detection Using a deep learning based Feature Extraction and Matching Algorithm by Ritu Agarwal,” *Multimed. Tools Appl.*, vol. 79, no. 11, pp. 7355–7376, 2019.
- [104] J. H. Bappy, C. Simons, L. Nataraj, B. S. Manjunath, and A. K. Roy-Chowdhury, “Hybrid LSTM and Encoder-Decoder Architecture for Detection of Image Forgeries,” *IEEE Trans. Image Process.*, vol. 28, no. 7, pp. 3286–3300, 2019, doi: 10.1109/TIP.2019.2895466.
- [105] I. B. K. Sudiatmika, F. Rahman, Trisno, and Suyoto, “Image forgery detection using error level analysis and deep learning,” *Telkomnika (Telecommunication Comput. Electron. Control)*, 2019, doi: 10.12928/TELKOMNIKA.V17I2.8976.
- [106] Y. Wu, W. Abd-Almageed, and P. Natarajan, “BusterNet: Detecting copy-move image forgery with source/target localization,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11210 LNCS, pp. 170–186,

2018, doi: 10.1007/978-3-030-01231-1_11.

- [107] Y. Wu, W. Abdalmageed, and P. Natarajan, “Mantra-net: Manipulation tracing network for detection and localization of image forgeries with anomalous features,” in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2019. doi: 10.1109/CVPR.2019.00977.
- [108] S. J. Araki T, Ikeda N, Shukla D, Jain PK, Londhe ND, Shrivastava VK, Banchhor SK, Saba L, Nicolaidis A, Shafique S, Laird JR, “PCA-based polling strategy in machine learning framework for coronary artery disease risk assessment in intravascular ultrasound: A link between carotid and coronary grayscale plaque morphology.,” *Comput Methods Programs Biomed*, vol. 58, no. May, p. 128:137, 2016, doi: 10.1016/j.cmpb.2016.02.004.
- [109] S. J. Saba L, Jain PK, Suri HS, Ikeda N, Araki T, Singh BK, Nicolaidis A, Shafique S, Gupta A, Laird JR, “Plaque Tissue Morphology-Based Stroke Risk Stratification Using Carotid Ultrasound: A Polling-Based PCA Learning Paradigm,” *J Med Syst.*, vol. 41, no. 6, p. 98, 2017, doi: 10.1007/s10916-017-0745-0.
- [110] S. J. Maniruzzaman M, Jahanur Rahman M, Ahammed B, Abedin MM, Suri HS, Biswas M, El-Baz A, Bangeas P, Tsoufias G, “Statistical characterization and classification of colon microarray gene expression data using multiple machine learning paradigms,” *Comput Methods Programs Biomed*, vol. 176, no. 7, pp. 173–193, 2019, doi: 10.1016/j.cmpb.2019.04.008.
- [111] S. J. Maniruzzaman M, Kumar N, Menhazul Abedin M, Shaykhul Islam M, Suri HS, El-Baz AS, “Comparative approaches for classification of diabetes mellitus data: Machine learning paradigm,” *Comput Methods Programs Biomed*, vol. 152, no. 12, pp. 23–34, 2017, doi: 10.1016/j.cmpb.2017.09.004.
- [112] V. K. Shrivastava, N. D. Londhe, R. S. Sonawane, and J. S. Suri, “A novel and robust Bayesian approach for segmentation of psoriasis lesions and its risk stratification,” *Comput. Methods Programs Biomed.*, vol. 150, 2017, doi: 10.1016/j.cmpb.2017.07.011.
- [113] Y. Rao, J. Ni, and H. Zhao, “Deep Learning Local Descriptor for Image Splicing Detection and Localization,” *IEEE Access*, vol. 8, pp. 25611–25625, 2020, doi:

10.1109/ACCESS.2020.2970735.

- [114] A. V. Rao and A. Pradesh, “AN INNOVATIVE AND EFFICIENT DEEP LEARNING ALGORITHM FOR COPY MOVE FORGERY DETECTION IN DIGITAL IMAGES,” vol. 29, no. 05, pp. 10531–10542, 2020.
- [115] Y. Zhu, C. Chen, G. Yan, Y. Guo, and Y. Dong, “AR-Net: Adaptive Attention and Residual Refinement Network for Copy-Move Forgery Detection,” *IEEE Trans. Ind. Informatics*, vol. 3203, no. c, pp. 1–1, 2020, doi: 10.1109/tii.2020.2982705.
- [116] J. S. S. El-Baz, Ayman, *Big Data in Multimodal Medical Imaging*. CRC Press, 2019.
- [117] N. N. K. et al. Suri, Jasjit S., Mrinalini Bhagawati, Sudip Paul, Athanasios Proteron, Petros P. Sfikakis, George D. Kitas, “Understanding the bias in machine learning systems for cardiovascular disease risk assessment: The first of its kind review.,” *Comput. Biol. Med.*, no. 1, p. 105204, 2022.
- [118] D. Tralic, I. Zupancic, S. Grgic, and M. Grgic, “CoMoFoD - New Database for Copy-Move Forgery Detection,” *55th Int. Symp. ELMAR*, no. September 2013, pp. 25–27, 2013.
- [119] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, “A SIFT-based forensic method for copy-move attack detection and transformation recovery,” *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3 PART 2, pp. 1099–1110, 2011, doi: 10.1109/TIFS.2011.2129512.
- [120] J. Li, X. Li, B. Yang, and X. Sun, “Segmentation-based image copy-move forgery detection scheme,” *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 3, pp. 507–518, 2015, doi: 10.1109/TIFS.2014.2381872.
- [121] O. Mayer and M. C. Stamm, “Forensic Similarity for Digital Images,” *IEEE Trans. Inf. Forensics Secur.*, vol. 15, no. 1, pp. 1331–1346, 2020, doi: 10.1109/TIFS.2019.2924552.
- [122] M. Agarwal, R. K. Kaliyar, G. Singal, and S. K. Gupta, “FCNN-LDA: A faster convolution neural network model for leaf disease identification on apple’s leaf dataset,” in *Proceedings of 2019 International Conference on Information and Communication Technology and Systems, ICTS 2019*, 2019. doi:

10.1109/ICTS.2019.8850964.

- [123] M. Agarwal, A. Sinha, S. K. Gupta, D. Mishra, and R. Mishra, "Potato Crop Disease Classification Using Convolutional Neural Network," in *Smart Innovation, Systems and Technologies*, 2020, vol. 141. doi: 10.1007/978-981-13-8406-6_37.
- [124] S. Kumar and S. K. Gupta, "A Robust Copy Move Forgery Classification Using End to End Convolution Neural Network," in *ICRITO 2020 - IEEE 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)*, 2020. doi: 10.1109/ICRITO48877.2020.9197955.
- [125] M. Agarwal, S. Gupta, and K. K. Biswas, "A new Conv2D model with modified ReLU activation function for identification of disease type and severity in cucumber plant," *Sustain. Comput. Informatics Syst.*, 2020, doi: 10.1016/j.suscom.2020.100473.
- [126] M. Agarwal, S. K. Gupta, and K. K. Biswas, "Development of Efficient CNN model for Tomato crop disease identification," *Sustain. Comput. Informatics Syst.*, vol. 28, p. 100407, 2020, doi: 10.1016/j.suscom.2020.100407.
- [127] U. Gupta and D. Gupta, "Regularized based implicit Lagrangian twin extreme learning machine in primal for pattern classification," *Int. J. Mach. Learn. Cybern.*, vol. 12, no. 5, 2021, doi: 10.1007/s13042-020-01235-y.
- [128] D. Gupta, A. Choudhury, U. Gupta, P. Singh, and M. Prasad, "Computational approach to clinical diagnosis of diabetes disease: a comparative study," *Multimed. Tools Appl.*, vol. 80, no. 20, 2021, doi: 10.1007/s11042-020-10242-8.
- [129] S. Mushtaq and A. H. Mir, "Image Copy Move Forgery Detection: A Review," *Int. J. Futur. Gener. Commun. Netw.*, vol. 11, no. 2, pp. 11–22, 2018, doi: 10.14257/ijfgcn.2018.11.2.02.
- [130] M. Du, S. Pentylala, Y. Li, and X. Hu, "Towards Generalizable Deepfake Detection with Locality-aware AutoEncoder," 2019, [Online]. Available: <http://arxiv.org/abs/1909.05999>
- [131] "COMOFOD dataset repository," 2021, [Online]. Available: <https://www.vcl.fer.hr/comofod/>

- [132] “DIID Dataset Repository,” 2021, [Online]. Available: http://www.diid.unipa.it/cvip/?page_id=48#CMFD
- [133] “IMD dataset repository link,” 2021, [Online]. Available: <https://www5.cs.fau.de/research/data/image-manipulation/>
- [134] H. A. Alberry, A. A. Hegazy, and G. I. Salama, “A fast SIFT based method for copy move forgery detection,” *Futur. Comput. Informatics J.*, pp. 1–7, 2018, doi: 10.1016/j.fcij.2018.03.001.
- [135] “MICC-F220 Public repository,” 2021, [Online]. Available: <http://www.micc.unifi.it/downloads/MICC-F220.zip>
- [136] “Kaggle dataset repository,” 2021, [Online]. Available: <https://www.kaggle.com/c/tensorflow-speech-recognition-challenge>
- [137] P. M. Raju and M. S. Nair, “Copy-move forgery detection using binary discriminant features,” *J. King Saud Univ. - Comput. Inf. Sci.*, no. xxxx, 2018, doi: 10.1016/j.jksuci.2018.11.004.
- [138] X. Zhao, S. Wang, S. Li, and J. Li, “Passive image-splicing detection by a 2-D noncausal markov model,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 25, no. 2, 2015, doi: 10.1109/TCSVT.2014.2347513.
- [139] Hammid et.al., “New Texture Descriptor Based on Modified Fractional Entropy for Digital Image Splicing Forgery Detection,” *MDPI*, vol. 21, no. 4, 2019.
- [140] H. Y. Huang and A. J. Ciou, “Copy-move forgery detection for image forensics using the superpixel segmentation and the Helmert transformation,” *Eurasip J. Image Video Process.*, vol. 2019, no. 1, 2019, doi: 10.1186/s13640-019-0469-9.
- [141] U. Gupta and D. Gupta, “Bipolar fuzzy based least squares twin bounded support vector machine,” *Fuzzy Sets Syst.*, vol. 449, pp. 120–161, 2022.
- [142] U. Gupta, D. Gupta, and U. Agarwal, “Analysis of Randomization-Based Approaches for Autism Spectrum Disorder,” in *Pattern Recognition and Data Analysis with Applications*, Springer, 2022, pp. 701–713.
- [143] S. Manjunatha and Dr. Malini. M. Patil, “A Study on Image Forgery Detection

- Techniques,” *CiiT Int. J. Digit. Image Process.*, vol. 9, no. 5, 2017.
- [144] G. Li, Q. Wu, D. Tu, and S. Sun, “A Sorted Neighborhood Approach for Detecting Duplicated Regions in Image Forgeries Based on DWT and SVD,” *Multimed. Expo, 2007 IEEE Int. Conf.*, pp. 1750–1753, 2007, doi: 10.1109/ICME.2007.4285009.
- [145] M. A. Elaskily, H. A. Elnemr, M. M. Dessouky, and O. S. Faragallah, “Two stages object recognition based copy-move forgery detection algorithm,” *Multimed. Tools Appl.*, vol. 78, no. 11, pp. 15353–15373, 2019, doi: 10.1007/s11042-018-6891-7.
- [146] H. Li, W. Luo, X. Qiu, and J. Huang, “Image Forgery Localization via Integrating Tampering Possibility Maps,” *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 5, 2017, doi: 10.1109/TIFS.2017.2656823.
- [147] L. V. Davide Cozzolino, Giovanni Poggi, “COPY-MOVE FORGERY DETECTION BASED ON PATCHMATCH Davide Cozzolino , Giovanni Poggi , Luisa Verdoliva Universit ´ a Federico II di Napoli , DIETI , 80125 Naples Italy,” pp. 5312–5316, 2014.
- [148] K. B. Meena and V. Tyagi, “A hybrid copy-move image forgery detection technique based on Fourier-Mellin and scale invariant feature transforms,” *Multimed. Tools Appl.*, vol. 79, no. 11–12, pp. 8197–8212, 2020, doi: 10.1007/s11042-019-08343-0.
- [149] K. B. Meena and V. Tyagi, “A copy-move image forgery detection technique based on Gaussian-Hermite moments,” *Multimed. Tools Appl.*, vol. 78, no. 23, 2019, doi: 10.1007/s11042-019-08082-2.
- [150] Q. Lyu, J. Luo, K. Liu, X. Yin, J. Liu, and W. Lu, “Copy Move Forgery Detection based on double matching,” *J. Vis. Commun. Image Represent.*, vol. 76, no. September 2019, p. 103057, 2021, doi: 10.1016/j.jvcir.2021.103057.
- [151] R. Agarwal and O. P. Verma, “Robust copy-move forgery detection using modified superpixel based FCM clustering with emperor penguin optimization and block feature matching,” *Evol. Syst.*, vol. 13, no. 1, 2022, doi: 10.1007/s12530-021-09367-4.
- [152] H. Chen, Q. Han, Q. Li, and X. Tong, “Digital image manipulation detection with weak feature stream,” *Vis. Comput.*, vol. 38, no. 8, 2022, doi: 10.1007/s00371-021-02146-x.
- [153] Z. Hossein-Nejad and M. Nasri, “Clustered redundant keypoint elimination method for

- image mosaicing using a new Gaussian-weighted blending algorithm,” *Vis. Comput.*, vol. 38, no. 6, 2022, doi: 10.1007/s00371-021-02261-9.
- [154] B. Wen, Y. Zhu, R. Subramanian, T. T. Ng, X. Shen, and S. Winkler, “COVERAGE - A novel database for copy-move forgery detection,” in *Proceedings - International Conference on Image Processing, ICIP*, 2016, vol. 2016-August. doi: 10.1109/ICIP.2016.7532339.
- [155] S. Kumar, S. K. Gupta, U. Gupta, and M. Kaur, “VI-NET: A Hybrid deep convolutional neural network using VGG and inception V3 model for copy-move forgery classification,” *J. Vis. Commun. Image Represent.*, p. 103644, 2022, doi: <https://doi.org/10.1016/j.jvcir.2022.103644>.
- [156] K. B. Meena and V. Tyagi, “A copy-move image forgery detection technique based on tetrolet transform,” *J. Inf. Secur. Appl.*, vol. 52, p. 102481, 2020, doi: 10.1016/j.jisa.2020.102481.
- [157] R. K. Kaliyar, A. Goswami, P. Narang, and S. Sinha, “FNDNet – A deep convolutional neural network for fake news detection,” *Cogn. Syst. Res.*, vol. 61, pp. 32–44, 2020, doi: 10.1016/j.cogsys.2019.12.005.
- [158] V. A. Krylov, G. Moser, S. B. Serpico, and J. Zerubia, “False Discovery Rate Approach to Unsupervised Image Change Detection,” *IEEE Trans. Image Process.*, vol. 25, no. 10, 2016, doi: 10.1109/TIP.2016.2593340.
- [159] P. Lagouvardos, N. Spyropoulou, and G. Polyzois, “Perceptibility and acceptability thresholds of simulated facial skin color differences,” *J. Prosthodont. Res.*, vol. 62, no. 4, 2018, doi: 10.1016/j.jpor.2018.07.005.
- [160] M. Dilshad Ansari and S. Prakash Ghreera, “Copy-move image forgery detection using direct fuzzy transform and ring projection,” *Int. J. Signal Imaging Syst. Eng.*, vol. 11, no. 1, pp. 44–51, 2018, doi: 10.1504/IJSISE.2018.090606.
- [161] R. Agarwal and O. P. Verma, “Robust copy-move forgery detection using modified superpixel based FCM clustering with emperor penguin optimization and block feature matching,” *Evol. Syst.*, vol. 13, no. 1, pp. 27–41, 2022, doi: 10.1007/s12530-021-09367-4.

- [162] S. Alamuru and S. Jain, "Video event classification using KNN classifier with hybrid features," *Mater. Today Proc.*, 2021, doi: 10.1016/j.matpr.2021.03.154.
- [163] L. Barghout and J. Sheynin, "Real-world scene perception and perceptual organization: Lessons from Computer Vision," *J. Vis.*, vol. 13, no. 9, 2013, doi: 10.1167/13.9.709.
- [164] D. Cozzolino, G. Poggi, and L. Verdoliva, "Efficient Dense-Field Copy-Move Forgery Detection," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 11, pp. 2284–2297, 2015, doi: 10.1109/TIFS.2015.2455334.
- [165] C. M. Pun, X. C. Yuan, and X. L. Bi, "Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 8, 2015, doi: 10.1109/TIFS.2015.2423261.
- [166] I. Amerini, T. Uricchio, L. Ballan, and R. Caldelli, "Localization of JPEG Double Compression Through Multi-domain Convolutional Neural Networks," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, 2017, vol. 2017-July. doi: 10.1109/CVPRW.2017.233.
- [167] X. Bi, Y. Wei, B. Xiao, and W. Li, "RRU-net: The ringed residual U-net for image splicing forgery detection," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, 2019, vol. 2019-June. doi: 10.1109/CVPRW.2019.00010.
- [168] Y. Zhang, J. Goh, L. L. Win, and V. Thing, "Image region forgery detection: A deep learning approach," *Cryptol. Inf. Secur. Ser.*, vol. 14, pp. 1–11, 2016, doi: 10.3233/978-1-61499-617-0-1.
- [169] L. Bondi, S. Lameri, D. Guera, P. Bestagini, E. J. Delp, and S. Tubaro, "Tampering Detection and Localization Through Clustering of Camera-Based CNN Features," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, 2017, vol. 2017-July. doi: 10.1109/CVPRW.2017.232.
- [170] A. Alharbi, W. Alhakami, S. Bourouis, F. Najjar, and N. Bouguila, "Inpainting forgery detection using hybrid generative/discriminative approach based on bounded generalized Gaussian mixture model," *Appl. Comput. Informatics*, 2020, doi: 10.1016/j.aci.2019.12.001.

- [171] V. T. Manu and B. M. Mehtre, “Copy-move tampering detection using affine transformation property preservation on clustered keypoints,” *Signal, Image Video Process.*, vol. 12, no. 3, 2018, doi: 10.1007/s11760-017-1191-7.
- [172] H. Kasban and S. Nassar, “An efficient approach for forgery detection in digital images using Hilbert – Huang transform,” *Appl. Soft Comput. J.*, vol. 97, p. 106728, 2020, doi: 10.1016/j.asoc.2020.106728.
- [173] R. Kaur and A. Kaur, “Copy-Move Forgery Detection Using ORB and SIFT Detector,” *Int. J. Eng. Dev. Res.*, vol. 4, no. 4, 2016.
- [174] Y. Y. Yeap, U. Sheikh, and A. A. H. A. Rahman, “Image forensic for digital image copy move forgery detection,” *Proc. - 2018 IEEE 14th Int. Colloq. Signal Process. its Appl. CSPA 2018*, no. March, pp. 239–244, 2018, doi: 10.1109/CSPA.2018.8368719.
- [175] P. Zhou, X. Han, V. I. Morariu, and L. S. Davis, “Learning Rich Features for Image Manipulation Detection,” *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, pp. 1053–1061, 2018, doi: 10.1109/CVPR.2018.00116.
- [176] H. Chen, C. Chang, Z. Shi, and Y. Lyu, “Hybrid features and semantic reinforcement network for image forgery detection,” in *Multimedia Systems*, 2022, vol. 28, no. 2. doi: 10.1007/s00530-021-00801-w.
- [177] P. Ferrara, T. Bianchi, A. De Rosa, and A. Piva, “Image forgery localization via fine-grained analysis of CFA artifacts,” *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 5, 2012, doi: 10.1109/TIFS.2012.2202227.

LIST OF PUBLICATIONS

(A) Journal publications

(i) Published

- Sanjeev Kumar, Suneet Gupta, and Umesh Gupta “VI-NET: A Hybrid deep convolutional neural network using VGG and inception V3 model for copy-move forgery classification”. *Journal of Visual Communication and Image Representation*, 89, 11(2022). <https://doi.org/10.1016/j.jvcir.2022.103644>. [SCIE, IF= 2.887]
- Sanjeev Kumar, Suneet Gupta, Umesh Gupta *et al.* “Non-overlapping block-level difference-based image forgery detection and localization (NB-localization)”. *Vis Comput* (2022). <https://doi.org/10.1007/s00371-022-02710-z> [SCIE, IF: 2.835]

(ii) Communicated (Under Review)

- Sanjeev Kumar, Suneet Gupta, Umesh Gupta *et al.* “Deep learning in Image forgery: A systematic review”. *Forensic Science International- Digital Investigations* (SCIE, IF= 1.805).

(B) International Conferences

- Sanjeev Kumar and Suneet K. Gupta. “A Robust Copy-move Forgery Classification Using End to End Convolution Neural Network.” *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*. IEEE, 2020. [published]
- Sanjeev Kumar, Suneet K. Gupta, Umesh Gutpa. “Discrete cosine transforms features matching-based forgery masks detection for copy-move forged images”. *2nd International Conference on Innovative Sustainable Computational Technologies (CISCT)*. IEEE, 2022. [Communicated]

A ROBUST DEEP NEURAL NETWORK FOR IMAGE FORGERY DETECTION

A thesis submitted in partial fulfillment of the requirements for the Degree of

DOCTOR OF PHILOSOPHY

By

SANJEEV KUMAR

Enrolment No: E17SOE812

Under the supervision of

Dr. Suneet Gupta and Dr. Umesh Gupta



**BENNETT
UNIVERSITY**
THE TIMES GROUP

School of Computer Science Engineering and Technology,

BENNETT UNIVERSITY

(Established under UP Act No 24, 2016)

Plot Nos 8-11, Tech Zone II,

Greater Noida-201310, Uttar Pradesh, India.

December, 2022

CHAPTER-7

CONCLUSION AND FUTURE SCOPE

We have worked on extensive review of deep learning methods where we elaborated the role of deep learning in image forgery while keeping (i) the bias in Artificial Intelligence and (ii) benchmarking against non-randomized paradigms in the framework. A set of recommendations were presented for improving the RoB and the most premium were sample size, ability to generalization, superior feature extraction paradigm, scientific validation, and evaluation.

We first proposed a customized CNN model to classify the forged images in a robust way with an accuracy of 94% on diverse datasets as well as their combination in order to get superior classification results. This model was intended to classify the forged images. Further In this thesis, we proposed an approach for tempering Classification without any deficiency in terms of challenges posed in the form of sensitivity towards reflection, image compression, rotation, and scaling altogether. This is the major outcome of the CNN approach, and it is what we believe to be the most important contribution it makes. There are a lot of manual features extraction-based approaches out there, but they only work in certain circumstances. They do not function very well when another situation is present, such as when the image patch is rotated, resized, or when any lighting changes are made to the image. In order to achieve this goal, we suggested a hybrid Convolution Neural Network that would consist of a mix of the VGG16 and Inception V3 models, with some additional dense layers that would increase the performance of forgery classification. The findings of the experiments indicate that the hybrid neural network that was developed has a higher level of efficiency. The outcomes of this research might further stimulate the researchers to employ various combinations of a wide range of new and current models with the purpose of achieving better categorization results.

For the purpose of copy-move forgery mask detection, we have developed and implemented a DCT (discrete cosine transform) block level features extraction method. The altered images have their feature information retrieved at the block level. The visual findings are offered for comparison between the real mask and the one that was anticipated. The detection accuracy of fake masks is around 95% on average. A pristine method that is block-

based has been suggested as a way to further improve the outcomes of the localization of the forged area. A method that is applied block by block in order to locate matching blocks on the basis of differences in block-level attributes is used. The blocks that were taken have been evaluated based on their maximum number of zeros as well as their SSIM characteristics. The rectangular Boundary is used to locate blocks that have the largest number of matched zeros. The strategy is effective for both translated and scaled blocks in the application.

In deep learning models, there is a scope of parameter setting that may be further explored as part of future study. This is something that can be done. Because of the substantial research that has been done on hybrid deep learning models, it has the potential to be one of the options that can be used to copy move forgery localization. Further investigation may benefit from the application of ensemble techniques in conjunction with medical or thermal images. Within the realm of picture forgery detection and localization, the future focus of these proposed approaches will be on the application of compression techniques. In most cases, much computational work is required for ensemble models. These types of models are able to be improved using strategies that include model compression.