

Image Forgery Detection Using Natural Scene Statistics



Engr. Ali Ahsan

01-242182-001

Supervised by: Dr Imran Fareed Nizami

Associate Professor (Electrical Engineering Dept)

A thesis submitted in the fulfillment of the Requirement for the award of the degree of
Master of Science (Computer Engineering)

Department of Computer Engineering

Bahria University Islamabad

2021

APPROVAL FOR EXAMINATION

Scholar's Name: Engr. Ali Ahsan

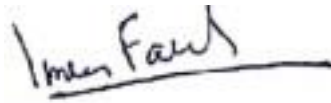
Registration No. 01-242182-001

Programmed of Study: MSCE

Thesis Title: Image Forgery Detection Using Natural Scene Statistics

It is confirmed that the thesis research indicated above was completed to my satisfaction and belief. Its standard is suitable for exam submission. I also performed a plagiarism check on this thesis using HEC-approved software system and got a similarity index of almost 17%, which is in the HEC's acceptable limit for MS thesis. I also found a thesis in a format that the BU would accept for the MS program.

Principal Supervisor's Signature: _____



Date: 09/12/2021

Name: Dr. Imran Fared Nizami

DECLARATION

I, Ali Ahsan solemnly states that my MS thesis Image Forgery Detection Using Natural Scene Statistics is my effort. It has no such material which is earlier published. All the mentions and necessary help in this study have been recognized. I affirm that the material in this research has not been used by me from Bahria University for another degree at any other institution.

Name of the scholar: Engr. Ali Ahsan

Date: 09/12/2021

PLAGIARISM UNDERTAKING

I, Ali Ahsan proclaim sincerely that the research presented in the thesis titled "Image Forgery Detection Using Natural Scene Statistics" is totally my own effort, with no significant input from anyone. Every small contribution, no matter how small, has been appropriately recognized and the entire thesis has been written by me.

I recognize the HEC and Bahria University zero-tolerance rule on plagiarism. As a result, as the writer of the aforementioned research, I certify that no section of my thesis research has been plagiarized and that any material utilized as a reference has been correctly cited.

I agree to do so if I found guilty of formal plagiarism in the aforementioned work after receiving my MS degree. The institute holds the right to withhold or cancel my MS degree, and HEC and the University reserve the right to publish my identity on the HEC/University website contains a list of researchers who have submitted plagiarized dissertations.

Author's Signature



Name of the Scholar: **Engr. Ali Ahsan**

DEDICATION

To My Father, Mother, all my Family, and Teachers.

ACKNOWLEDGMENT

First of all, I would like to thank Associate Prof. Dr. Imran Fareed Nizami for giving me the opportunity to carry out state-of-the-art research in this field. Furthermore, I would like to thank him for supervision of my thesis. Finally, I must express my heartfelt appreciation to my parents for their unwavering support and encouragement during my years of study and the effort of researching and writing this thesis. This achievement would not have been achievable without their assistance. Thank you

Abstract:

A copy-move image forgery is the most common type of image tampering. It can be done by copying a part of an image and paste on another part of the same image. Therefore, it can be one of the challenging tasks to find that forgery. This paper suggested a different approach to detect the copy move image forgery by the natural scene statistic features. These features are extracted from both original and forged images of MICC-F2000 dataset. Natural scene statistics are the statistical properties of any natural image captured by any camera, so an attempt of forging an image makes these properties un-natural. By this method, an original and forged images can be easily classified by state-of-the-art machine learning models trained on these features. The performance of this method is quantitatively assessed using the famous evaluation metrics i-e accuracy, TPR, FPR, TNR, Recall and F1-score. A comparison with other advanced techniques has shown that the presented technique has shown more better results in comparison with the other techniques.

Keywords – Copy-Move Forgery Detection, Natural Scene Statistics, Machine Learning, Ensemble Learning

Table of Contents

Contents

| | |
|---|------|
| Title Page | i |
| Approval for Examination | ii |
| Declaration | iii |
| Plagiarism Undertaking | iv |
| Dedication | v |
| Acknowledgment | vi |
| Abstract | vii |
| Table of Contents | viii |
| List of Figures | xi |
| List of Tables | xiii |
| List of Symbols and Abbreviations | xiv |
| 1 Introduction | 15 |
| 1.1 Problem Statement | 18 |
| 1.2 Objective | 18 |
| 1.3 Motivation | 18 |
| 1.4 Overview of our Proposed Methodology | 19 |
| 1.5 Organization of Thesis | 19 |
| 2 Literature Review | 20 |
| 2.1 Block-based CMFD methods | 23 |
| 2.2 Keypoint-based CMFD methods | 23 |
| 2.3 Research Gap/Limitations | 29 |
| 3 Methodology | 30 |
| 3.1 Feature Extraction | 31 |
| 3.1.1 Distortion Identification-based Image Verity and Integrity Evaluation index | 31 |
| i) Statistical Model for Wavelet Coefficient | 32 |

| | |
|---|----|
| ii) Extraction of Distortion Identification-based Image Verity and Integrity Evaluation | |
| index features | 33 |
| 3.1.2 Spatial and Spectral Entropy-Based Quality index | 34 |
| i) Spatial Entropy Features (f1 - f6) | 35 |
| ii) Spectral Entropy Features (f7 - f12) | 35 |
| iii) Spatial and Spectral Entropy-Based Quality index Features used for forgery detection | |
| | 36 |
| 3.1.3 Oriented Gradients Image Quality Assessment..... | 37 |
| 3.1.4 Oriented Gradients Image Quality Assessment Features used for forgery | |
| detection..... | 39 |
| 3.1.5 Natural Scene Statistics Combinations | 39 |
| 3.2 Machine Learning Models/Classifiers | 41 |
| 3.2.1 Support Vector Machine | 42 |
| 3.2.2 Decision Tree | 43 |
| 3.2.3 Random Forest | 43 |
| 3.2.4 K-Nearest Neighbors | 44 |
| 3.2.5 Ensemble Learning | 45 |
| i) Ada Boost Classifier | 46 |
| ii) Gradient Boosting Classifier | 46 |
| 4 Experimental Results and Discussion | 48 |
| 4.1 Dataset | 48 |
| 4.2 Experiments Procedure | 49 |
| 4.3 Performance Metrics | 49 |
| 4.3.1 Accuracy | 50 |
| 4.3.2 True Positive Rate/Precision | 50 |
| 4.3.3 False Positive Rate | 50 |
| 4.3.4 True Negative Rate | 50 |
| 4.3.5 Recall | 51 |
| 4.3.6 F1-Score | 51 |
| 4.4 Software/Tool | 51 |
| 4.5 Results | 51 |

| | |
|---|----|
| 4.6 Comparison results with other related works | 56 |
| 4.6.1 Accuracy Comparison | 57 |
| 4.6.2 True Positive Rate Comparison | 58 |
| 4.6.3 False Positive Rate Comparison | 59 |
| 4.6.4 True Negative Rate Comparison | 59 |
| 4.6.5 Recall Comparison | 60 |
| 4.6.6 F1-Score Comparison | 61 |
| 5 Conclusion and Future Work | 62 |
| 6 References | 63 |

List of Figures

| | |
|--|----|
| Figure 1.1:Forms of image Forgery..... | 16 |
| Figure 1.2:Case of forgery (shown in press The New York Times 2008) | 17 |
| Figure 3.1:Proposed Methodology | 31 |
| Figure 3.2:Support vector and Hyper-plane boundary..... | 42 |
| Figure 3.3:General decision tree structure | 43 |
| Figure 3.4:Random Forest models making predictions | 44 |
| Figure 3.5:proximity of similar data points | 45 |
| Figure 3.6:Illustration of ada-boosting for creating strong classifier based on multiple weak linear classifiers | 46 |
| Figure 4.1:Models test accuracies with all three types of NSS features | 52 |
| Figure 4.2:Models test accuracies with DIIVINE features | 53 |
| Figure 4.3:Models test accuracies with SSEQ features | 53 |
| Figure 4.4:Models test accuracies with OG-IQA features | 54 |
| Figure 4.5:Models test accuracies with SSEQ+DIVIINE features | 54 |
| Figure 4.6:Models test accuracies with SSEQ+OG-IQA features | 55 |
| Figure 4.7:Models test accuracies with OG-IQA+DIVIINE features | 55 |
| Figure 4.8:Accuracy Comparison with other methods | 57 |
| Figure 4.9:TPR Comparison with other methods | 58 |
| Figure 4.10:FPR Comparison with other methods | 59 |
| Figure 4.11:TNR Comparison with other methods | 59 |
| Figure 4.12:Recall Comparison with other methods | 60 |

Figure 4.13:F1-Score Comparison with other methods 61

List of Tables

| | |
|---|----|
| Table 2.1: Literature Review for Image Forgery Detection..... | 27 |
| Table 3.1: DIIVINE features and the way they were computed..... | 33 |
| Table 3.2:SSEQ Features..... | 36 |
| Table 3.3:Gradient and relative gradient features..... | 39 |
| Table 4.1:Natural Scene Statistics Dataset features..... | 48 |
| Table 4.2:Confusion Matrix | 49 |
| Table 4.3:Models Test metrics with best NSS Features Combination | 52 |
| Table 4.4:Comparison Results with other works on MICC-F2000 dataset | 56 |

List of Symbols and Abbreviations

| | |
|----------------|--|
| CMFD | Copy Move forgery detection |
| CMF | Copy Move Forgery |
| IFD | Image Forgery Detection |
| ML | Machine Learning |
| NSS | Natural Scene Statistics |
| DIIVINE | The Distortion Identification-based Image Verity and Integrity Evaluation |
| SSEQ | Spatial and Spectral Entropy-Based Quality |
| OG-IQA | Oriented Gradients Image Quality Assessment |

Chapter 1

Introduction:

As digital image may hold a variety of information, they are regarded as an important source of information transfer. Simultaneously, these digital photographs are widely used as evidence in publications, investigational proof, and legal problems [1]. The rapid expansion of fast web access and cell platforms has dramatically increased the demand of digital photos. Several software applications have been developed in recent years to modify digital photos, such as Photoshop and Corel Photo, however these applications are widely used for image forgeries [2, 3]. Because of technological developments, it became difficult for human being to identify forged image with their naked eye [4]. Because forged image is created in the same way as original images, numerous operations are conducted on the original image to maintain credibility in the forged image. Numerous forensic approaches, such as collage identifications and retouching, are now being established to extract tampered images from real images [5, 6]. Image forgery detection (IFD) technique is often necessary for patent protection and forgeries prevention [3]. Authentication of digital images is the most essential method in image forensics [7].

Photos in communication medium have grown extremely valuable in recent years. The image, it is believed, conveys more information than the words regarding the event or scene observed. In today's technology environment, digital photograph plays a vital role in a variety of industries [8]. With developments in digital photo technology, such as cameras, programs, and computer systems, as well as the growing usage of online media, images can now be considered a crucial knowledge point [8]. Because of the ease with which digital photos can be edited in both their origins and contents, the security of digital images has been questioned as an outcome of the increased use of digital images processing methods. Digital image analysis is the most recent branch of study aimed at ensuring image authenticity [8]. There are numerous approaches suggested in digital forensic in recent years as shown in Figure 1.1:

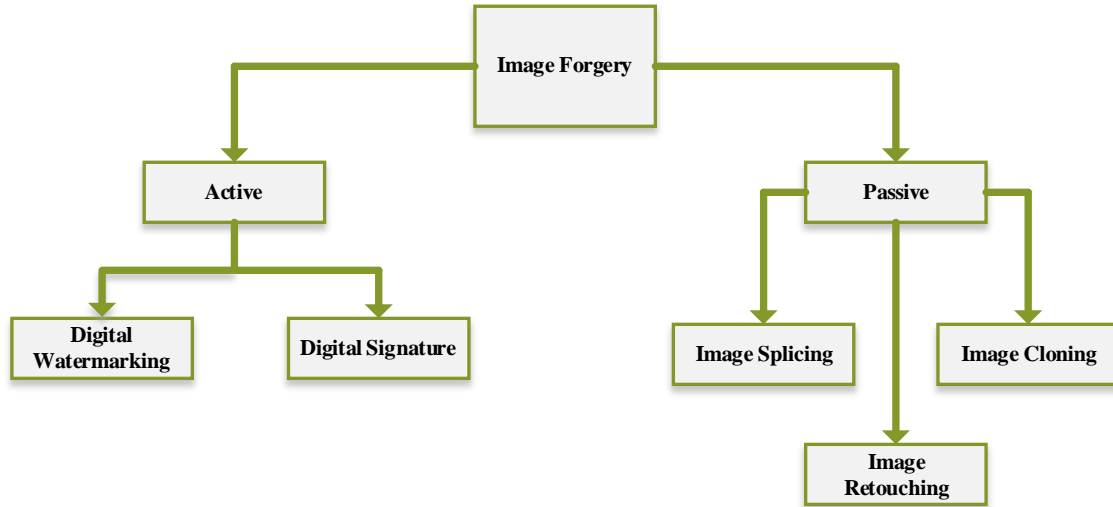


Figure 1.1: Forms of image Forgery

Digital watermarking and digital signature are two different sorts of active approaches [10]. To recognize copyright, a digital watermark is put to the image. It is the mechanism of concealing particular data (bits) in digital images [8]. The serial number of the writer, company logos, relevant text, and so forth are examples of distinctive information. Watermarks can be seen or unseen [8]. A digital signature is used to verify the authenticity of digital message, digital document, and software. Depending on the valid signatures, the receiver may think that the communication was created from authorized sender [8]. Digital signature is a mathematical approach to prevent forgery and deception in online communication [8]. While passive approaches are image retouching, image splicing, and copy-move attack [10]. Image retouching is basically an image tampering method which includes a slight harmful type of digital images [8]. Natural images do not alter significantly but few important features have been reduced. Splicing technique is a kind of forgery to produce a single photograph which includes merging of 2 or more photographs [8]. This is called as image composition which includes several procedures of image processing [8].

The most common form of forgery is a copy-move forgery (CMF) [8]. CMF in images is defined as repeating one or more areas at distinct places in the same photograph. Usually duplicate areas are large, minimized, or rotated to make photo tampering more undoubted, creating it too problematic to identify forged image [11]. CMF is famous images modification techniques that can be used to alter images [12]. In CMF, a part of the photograph is copied and pasted (with or without editing of the copied section of the photograph) into one or additional areas of the photograph [12]. The goal of this tampering is to conceal or replicate certain parts or areas

of images. A sample of copy-move forgery is presented in Figure 1.2 which is printed on the Iranian revolutionary guard website showing 4 missiles seemed to launch from a desert launch pad [12].



Figure 1.2 : Case of forgery (shown in press The New York Times 2008)

But experts reported 3 missiles that were really launched. In Figure 1.2, the prominent areas of an image are matched [12]. When alteration is attempted on images, the job of the image copy move forgery detection (CMFD) is to identify replicating regions in an image [12]. Usually, for ignorable image tampering, procedures like scaling, filtering, noise embedding, etc. are executed on the entire tampered images or copied areas of images prior to pasting on the image [12]. Recognition of forged image is necessary as in numerous places, image performed a key role in communications. Image must be authentic, and it is essential to ensure its validity in law-and-order condition. Hence, in many scenarios an IFD plays a significant role [12].

To identify image tampering, passive IFD algorithms don't need previous knowledge regarding the input image; rather, these algorithms detect tampering based on disruptions in the inherent attributes of images that may have been inserted during the image editing [13]. Because the image downloaded via web without previous data, active tampering identification method is useless for these type of tampered images [13]. As a result, it is considered that now a days passive forgery detection methods are more effective. CMF identification, image splicing forgery identification, retouching identification, and re-sampling identification approaches [13] are the 4 major kinds of passive forgery identification methods [14, 15]. Within the same picture, the copy-

move image forgeries involve replications of some regions of the picture. Generally, such type of tampering is done with the goal of suppressing meaningful information or replicating items to deceive people [13]. Recent photo edit system allows users conduct CMFs with such a refinement that determining the validity of an image simply by looking at it is very difficult [13]. As a result, a CMF detection system that can detect and locate the tampering in digital photos is required [13].

1.1 Problem Statement:

This thesis aims to solve the very common issue of digital media that is image forgery. As most of the information is traveled in the world using electronic media, so an image forensic tool must have to be available for forgery prevention. Copy-move forgery is one the most common forgeries in today's media which have to be detected by advanced tools. Natural scene statistics (NSS) have the capability to detect forgeries in an image, but these features are not applied for this purpose before. So, in the proposed method, copy move forgery detection (CMFD) is targeted using NSS features.

1.2 Objective:

The objective of this research is to utilize NSS features in image forgery detection. As in this era of modern world, media tools and communications are enhancing day by day so, it is necessary to improve image forensic methods. NSS features actually contain the natural behavior of an image, whenever someone attempts forgery in an image by any type of tool, then these NSS features get disturbed which identifies the presence of forgery in an image. So, in this research, our goal is to train our machine learning (ML) models on NSS features to detect CMF.

1.3 Motivation:

This research focused on CMFD in digital images based on machine learning algorithms. NSS features have been played a key role to detect forgery in the proposed method. NSS features have been used before in image quality assessment algorithms by several researchers, we have used these features in our research to detect forgery in digital images. So, this new technique in the world of image forensics have been created new ways for the researchers to enhance the IFD methods. After extracting NSS features from the given image, we have applied these features on

multiple ML models to achieve the best performance by any one of them. So, NSS features and the best ML model both have been utilized to achieve state-of-the-art results.

1.4 Overview of our Proposed Methodology:

In this thesis, we have targeted the most common form of image forgery which is copy-move forgery (CMF). We have proposed a unique method to solve the image forgery problem which is inspired by [16] in which it states that image and video of visual environments usually captured with any type of high-quality capture device operating in the visual spectrum are generally classified as natural scenes. This distinguishes them from texts, computer made graphic scenes, cartoon, and animation, painting and drawing, random noises, or image and video captured from nonvisual stimuli such as radars and sonars, X-ray, ultrasound, etc. [16]. Natural scene forms an extremely tiny subset of the set of all possible scenes [17], [18]. As natural scene statistics of natural images normally contains some specific pattern, so whenever forgery applied on digital images by any image processing tool like photoshop etc. then the pattern of these features gets disturbed which differentiates forged image from the natural one. MICC-F2000 dataset of copy-move forgery has been used in this research. These NSS have been used as a feature vector for the training of model to classify natural and forged images.

1.5 Organization of Thesis:

In chapter 2, we undergo the study of related works in order to accomplish the task of copy-move IFD. We have studied briefly and discussed the recent work for the development of IFD methods to sort out our problem in efficient way as compared to other recent developments. In chapter 3 we have discussed the complete methodology in detail, we have also discussed the different enhancements and all the major phases of implementing the copy move IFD using NSS. In chapter 4, we have discussed experiments and results including the feature set analysis, proposed models training and result such as accuracy in the tabular form and graphs. At final chapter 5, we have concluded our research and discussed the future scope and developments of the existing system.

Chapter 2

Literature Review

There is not a platform these days that does not employ digital photographs. They're used in practically every field, including digitized media, the defense, law, business, investigations, science, health fields, entertainment, public platforms, as well as on the internet [19]. Using many images, need of ensuring validity is must. Human beings mostly trust what they have seen than what they have heard [19]. As a result, visual content become more trustable over verbal information for us. Due to that, we put a lot of emphasis on what we see daily in magazines, newspaper, TV news, and social sites such as Instagram, Facebook, and others [19]. Digital image manipulation is the process of altering an image for the aim of achieving some criminal purpose [20][21]. Forgeries are the term used in digital forensics to describe such tampering [19]. So, image forensic tools must have to be available for forgery prevention. Many image processing tools like Photoshop etc. are available with ease for anyone to manipulate images. Previously, photographers were used to applying the photomontage method, which involved pasting, merging, overlapping, and reorganizing two or more images to produce a final picture that appeared to be a single image [19].

As a result, it becomes critical to determine whether or not the photograph in concern has been modified, as photographs are important to be utilized as proofs in courts of law, the press, research, and a variety of other professions. [19]. Therefore, effective, and accurate image manipulation detection systems that can discriminate between real and manipulated images are required [19]. Researchers are working in this area and doing their best to produce the most reliable ways due to the current needs. It has been noticed that a huge number of research articles in this domain have been published by authors from all over the world [19]. The main goal of digital image manipulation is to create illegal changes in a genuine image so that it closely resembles the authenticity of the original. As a result, distinguishing between real and forged images becomes more difficult for the human eye [19]. The goal of ongoing research is to discover solutions to the

challenge of distinguishing a manipulated image from an authentic image. As the number of forgery attempts rises, it became more necessary than ever to develop effective and real-time detection systems [22]. Following a thorough review of the papers, much less papers are related to passive approaches of IFD were discovered [19]. A comparison of numerous detection methodologies with copy-move and image splicing, as well as different image processing operation detection methods, was described in the survey work [23]. The general structure of various detection algorithms, as well as their limitations, are also examined [19]. A review paper [25] concentrated on CMF detection, while another survey work [24] presented a thorough literature on pixels-based algorithms for IFD. A survey paper [19] classified several types of image forgeries and detection strategies, with a focus on passive detection using pixel-based algorithms. There were also some extremely specific types of survey reports that concentrated on a specific type of detection approach [19]. Only 18 studies were examined in two of these surveys [26]. The block-based approaches of CMF detection were reviewed.

The work described in [19] varies from the previous surveys in that it takes a systematic method to perform a comprehensive survey and offer in-depth detail of literature concentrating on various IFD approaches. After 10 years of the first photograph was made, image forgery began to appear. During 1860s, the forgery was realistic manipulation. Prior to the advent of digital scanner and camera, traditional image manipulation was carried out using instruments such as airbrushing to alter images using any of the classical art methods [19]. Images were modified during the photographic printing process in traditional analogue photo editing. Digital photographs have become popular as a result of technological advancements, and analogue image editing has become outdated [27]. With the use of image manipulation tools like Adobe Photoshop Elements [28], Pixlr [29], GIMP [30], and others, image can also be manipulated in numerous ways. Such picture editing software is accessible for practically every platform on the internet, including Windows, cell phones, tablets, and so on [19]. Now we have discussed below the various forgery detection methods that have been done so far by different researchers. So first we talk about CMFD, Block-based CMFD approaches take a lot of time as the photograph is separated into multiple overlapping blocks [37]. Chang used a similarity vector field to eliminate the false positives to identify doubtful area and multi-region relation (MRR) used to examine the affected areas [31]. In [32], proposed a method which splits photograph into multiple non-overlapped and uneven blocks. In [33] researchers presented an Exponential Fourier's moments (EFMs) for exploring the use in space. In

[34] recommendation has been given multi-scale modification of Gaussian filter in order to obtain multi-view features map. It is the recommended anti-criminal method that identifies the stable local connection and enhanced the image classifications [35].

Key point-based approach extracts a scarce feature set, and it has been failed when image is smooth [37]. In [37] an author has been proposed a triangle-based method to identify features that correspond to an interior angles of the triangle and these attributes are shown on the vertices. SIFT and SURF approaches have been applied to locate copied area, scaling, and translations artefact and achieves excellent results [38]. In [39] researchers offered a method which identifies motion blur using images gradient, which distinguish duplicated region in the photograph. In [40] author related various approaches like SIFT and SURF, block based DCT, DWT, KPCA, PCA. After comparing these approaches, it is observed that Zernike features attain outstanding performances [40]. Also, an investigation of a machine-learning based methods has been occurred. The SVM classifying images performance is calculated [41]. In [42] researchers suggested a method to identify CMF using the detector. In [43] researchers presented an auto encoder to identify the forgery on social media platforms. Fan Yang 2017, suggested KAZE interest points detector along with SIFT, which obtains more feature points, and it achieves improved results than other techniques [44]. In [45] an author presented a method in which the quality in each SPT sub-bands using LBP histogram is described. Neenu et al. [46] suggested an approach which includes illumination and reshaping features to identify tampered image. In [47] HoG and HOGG method to identify forgery in images is presented. Tiago Carvalho 2016 proposed a technique for choosing visual features for identification of the forgery in image [48]. It is suggested in [49] that how machine learning (ML)-based method can be used for detecting image forgery using behavior knowledge space. In [51] researchers suggested an IFD system that includes the Alex Net model to extract feature set. In [52] it is presented an ensemble learning based technique that identifies numerous sorts of significant feature. In [53] an author presented a DL method to identify multiple sorts of image forgery using CNN.

In [13] researchers have been proposed a new Tetrolet transform-based copy-move IFD approach. Input images are initially divided in overlapping blocks in this technique, then 4 low-pass coefficient and 12 high-pass coefficient are obtained from blocks using the Tetrolet transform. The extracted Tetrolet features are then used to establish the feature vectors lexicographically, and identical patches are found by comparing the obtained Tetrolets feature set. In addition, some

related papers demonstrate two major types of copy-move IFD algorithms. The first is a block-based forgery detection method, while the second is a key-point-based forgery detection method. The following are some related papers on block-based forgery detection.

2.1 Block-based CMFD methods:

These techniques divide the input image into square or circle-shaped segments that overlap or not. Then, using a suitable feature transform, features from each block are extracted. Finally, the collected features are compared to see if they are similar [13]. The researcher introduced the first block-based approach in [54]. For representing feature set of each block of size 8x8 pixel, they have utilized Discrete Cosine Transform (DCT). A few more DCT-based strategies to increase accuracy, robustness and computational complexity against post-processing activities have been presented [55]. An approach of dense-field methods and Zernike moment was described by the researcher [56]. Researchers in [57] employed a super-pixel contents-based adaptive feature point detectors to detect replica tampering in digital photographs. Al-Qershi [58] proposed a strategy for detecting CMFs based on a feature matching mechanism called k-means clustering. Chen developed a technique for detecting picture forgery that uses fractional quaternion cosine transforms and a modified Patch-Match matching method [59]. A tampering detection approach based on stationary wavelet transforms and local binary patterns was suggested by Mahmood et al. [60]. Mahmood also proposed a method for detecting CMF using stationary wavelets [61], in which DCT is utilized to decrease the features dimensions. Meena and Tyagi [62] recently presented a Gaussian-Hermite moment-based IFD approach.

2.2 Keypoint-based CMFD methods:

These methods rely on key point feature (specific local feature such as corner, blob and edge) to detect forging [13]. Pan in [63] introduced a technique based on scale environment Feature Transform (SIFT) to detect CMF. Pun in [64] explained a detection method by integrating key point and block-dependent feature set. Particle swarm optimization along with SIFT keypoint was used for detecting forgery by Wenchang in [65], though this practice was incapable to identify tampering when duplicate region is small. A tampering identification method was presented by Zandi in [66] by interest point detectors. Wang in [67] presented a tampering detection method by means of Scale-Invariant Feature detector with Error Resilience (SIFER) and Fast Quaternion Radial Harmonic Fourier Moments (FQRHFM). In this approach, attributes are matched with

coherency sensitive hashing technique. Newly, Meena and Tyagi [68] have presented a hybrid approach to identify CMF based on Fourier-Mellin and scale invariant features transform.

By reviewing the above-mentioned study about block based and key-point based CMFD approaches, Meena in [13] concluded that the block-based approach is more robust and accurate than key-point based CMFD. Other limitations of key points-based approach are this method fails to identify minor duplicate regions; they also fails to distinguish between copy-move and naturally same region; and they fails to identify the exact forgeries [13]. Meena developed a novel type of block-based CMFD approach employing Tetrolet transforms (a specific scenario of Haar wavelet transforms) in [13] to solve these constraints. The suggested approach in [13] may accurately identify copy-move regions even when some basic post-processing procedures are used, such as color reduction, contrast adjustment, brightness modification, averaging filter, and JPEG compression.

IFD of both type's i-e copy-move and splicing is proposed by researchers in [69], in which discrete cosine transform (DCT) coefficients have been utilized as feature vector to classify real and forged image using SVM as a classifier. Other studies include many other works by various researchers for IFD approaches using ML for classification of forged and natural images utilizing various types of features. Shi et al. [70] presented that a natural picture mode with moment of the typical function of wavelets sub-band and Markov's transitions probabilities of variance 2-D array is used to identify image splicing. On a particular test picture, a multi-size block DCT was used to create these 2-D arrays. Another method for detecting splicing tampering was proposed by Zhongwei et al. in [71]. By increasing the original Markov feature obtained from the transition probability matrix in the DCT domain, they were capable of capturing the inter- and intra-block correlations between block DCT coefficients. In the Quaternion discrete cosine transform (QDCT) domain, Li et al. [72] suggested a technique to detect image splicing based on Markov features. The fundamental purpose of presenting the QDCT domain is to utilize all of the color data. They used intra-block and inter-block QDCT coefficient matrices to obtain enlarged Markov properties. Furthermore, classification process of an image was carried out using SVM with a significant number of characteristics acquired [69].

Another famous forgery type is copy-move forgery in which one patch/region of image is copied and pasted on another place of the same image. Reason behind this forgery attempt is either to hide any existing object of an image or to be used for duplication purpose. As a result, if

tampering is carefully implemented, the naked eye will not be able to detect it. The first method to identify CMF was presented by Fridrich et al. [73], representing DCT coefficient-based attributes are retrieved from small overlapping image blocks. Similarity check between lexicographically sorted feature vectors were used to identify the tempered region. When applied to photo with huge identical textured sections, however, the method resulted in a lot of false matches. In [74] researcher suggested a same method in which DCT coefficients were retrieved as attributes for distinct block size. However, when post-processing procedures were experienced to the forged image, these techniques resulted in excessive computational complexity and insufficient detection of tempered region. Another DCT-based method offered by Cao et al. [75] was to divide the actual photo in fixed-size blocks and execute a DCT on every block. A circular block was used to represent each DCT block, and 4 attributes were obtained to minimize the dimensions of each block. Finally, lexicographically sorted features vector was subjected to a matching method. In [76], Hayat and Qazi introduced a CMF approach built on the discrete wavelet transform (DWT) and DCT, they retrieved the DWT estimate sub band before applying DCT to the overlapping blocks of a photograph. For comparing the blocks, additional correlation coefficients were used. They did not, however, test the method with other image transformations.

All approaches described yet are effective for both CMF and image splicing, as mentioned by Shilpa in [69]. Among the above-mentioned literature, only few techniques found robust on both type of forgeries i-e copy move and splicing. There is a technique suggested in [77] that can identify CMF and splicing forgery at the same time. Local binary patterns (LBP) and discrete cosine transforms (DCT) were used in the technique. They converted every single block of the forged images LBP code to the DCT domain and calculated the standard deviation of the DCT block coefficient. This method though has not been tested for several post-processing methods. An integrated approach has been developed for detecting splicing and CMF [78]. In their work, they suggested using an advanced threshold technique on a Markov random process to get the feature from various color space. They haven't though evaluated the approach using a collection of authenticated, spliced, and copy move forgery (CMF) image for both databases.

Shilpa et al. [69] have proposed a novel integrated and exceptional IFD method. The key concept is to take use of the difference in statistical features of AC coefficient across the whole photograph by estimating the standard deviation and number of non-zero DCT coefficient for AC frequency components individually. For the test photograph and its cropped form, the proposed

features are examined. They used the retrieved feature vector in conjunction with the SVM classifier to classify original/forged image. Fridrich et al. [79] presented several block-based CMFD methods which depends on brute-force search, auto-correlations, accurate blocks matching and robust matchings. Here DCT built robust matchings technique has given excellent result than all others. In this method, CMF is identified by the quantized DCT coefficient extracted from every block of the photograph. Ryu et al. [80] presented Zernike Moment for extracting the feature set from each block. But the incorrectly identified results have not been dealt by this method. Some keypoint based forgery detection methods are proposed to overcome the limitations of block-based methods used so far. Typically, Scale Invariant Feature Transform (SIFT) [81, 82, 83, 84] and Speed-Up Robust Features (SURF) [85, 86] are largely exploited to identify the forged area due to their effectiveness against geometrical alterations.

Some other papers that have been reviewed are focused on CMFD techniques. Areej et al. [102] proposed a CMFD method using Maximally Stable External Regions (MSER) features. Loai et al. [103] proposed a CMFD method using Discrete Wavelet Transform (DWT) and Speeded Up Robust Features (SURF). Vaishnavi et al. [104] proposed a CMFD technique which have utilized KAZE feature extraction and RANSAC algorithm to prevent false positives and then declare the photograph as original or forged. Pourkashani et al. [105] proposed a cloning detection method using convolutional neural network (CNN) and K-mean clustering. Zhang et al. [106] proposed IFD method which have utilized Error Level Analysis (ELA) and Local Binary Pattern (LBP). Abdullah et al. [107] proposed a method of Inpainting tampering detection of digital images using bounded generalized Gaussian mixture model which is the form of the kernels of Support Vector Machine (SVM). Yong et al. [108] proposed a technique of CMFD by using oriented Features from Accelerated Segment Test and rotated Binary Robust Independent Elementary Features (Oriented FAST and rotated BRIEF) as feature extraction and their classifiers are 2 Nearest Neighbor (2NN) and Hierarchical Agglomerative Clustering (HAC) for forgery detection purpose. Some of the reviewed papers are shown in the following table 2.1 with their proposed methodology, datasets they have been utilized and the results they have achieved.

Table 2.1: Literature Review for Image Forgery Detection

| Paper Reference | Year of Publication | Methodology | Datasets | Results |
|------------------------|----------------------------|--|--|---|
| Abhishek et al. [37] | 2020 | CMF and Splicing detection Using Deep Convolutional Neural Network | GRIP, DVMM, CMFD and BSDS300 | 98.48% accuracy, 86.4% F1-Score |
| Shilpa et al. [69] | 2020 | IFD based on statistical features of block DCT coefficients using SVM | CASIA V1.0 and V2.0 | 98% accuracy |
| Shi et al. [70] | 2007 | Image Splicing Detection using natural image model with multi-size block discrete cosine transform (MBDCT) | Columbia Image Splicing Detection Evaluation Dataset | 85.16% accuracy, 83.91% TPR, 86.39% TNR |
| Zhongwei et al. [71] | 2012 | Image Splicing Detection using Markov Features in DCT and DWT domain and SVM | Columbia Image Splicing Detection Evaluation Dataset | 93.55% accuracy |
| Li et al. [72] | 2016 | Splicing detection using Markov Features in QDCT domain and using SVM for classification | CASIA V1.0 and V2.0 | 96.435% accuracy |
| Cao et al. [75] | 2011 | Block-based CMFD using DCT and block-matching, | Self-Prepared | More than 80% accuracy |
| Alahmadi et al. [77] | 2016 | Local Binary pattern and Discrete Cosine Transform to detect Copy-move and Splicing forgery, also SVM for classification | CASIA V1.0 , CASIA V2.0 and Columbia | 97.77% accuracy, 98.3% TPR and 97.07% TNR |
| Areej et al. [102] | 2015 | Cloning Localization using MSER, SURF and | MICC-F2000 | 97% accuracy, 97% TPR and 92% TNR |

| | | | | |
|--------------------------|------|--|------------------------------------|--|
| | | SIFT features with K-means clustering | | |
| Loai et al. [103] | 2017 | CMFD using DWT and SURF features | 50 BMP images and MICC-F2000 | 95% accuracy |
| Vaishnavi et al. [104] | 2019 | CMFD by extracting KAZE features, RANSAC algorithm for feature matching | MICC-F2000 and MICC-F220 | 92.85% TPR and 6.92% FPR |
| Pourkashani et al. [105] | 2021 | CMFD using CNN and K-mean clustering | MICC-F2000, MICC-F600 and MICC-F8 | 94.13% TPR and 96.98% F1-Score |
| Zhang et al. [106] | 2021 | Hybrid feature image Splicing Detection using Error Level Analysis (ELA) and Local Binary Pattern (LBP) | Columbia, MICC-F220 and MICC-F2000 | 100% TPR, 96.07% Recall, 97.88% F1-score and 97.30% accuracy |
| Abdullah et al. [107] | 2019 | Inpainting forgery detection using hybrid generative/discriminative approach based on bounded generalized Gaussian mixture model and SVM kernels | MICC-F220 and MICC-F2000 | 81% accuracy, 85.42% TPR and 17.85% FPR |
| Yong et al. [108] | 2018 | CMFD using Oriented FAST and rotated BRIEF as feature extraction method and 2 Nearest Neighbor (2NN) with Hierarchical Agglomerative Clustering (HAC) as feature matching method | MICC-F600 and MICC-F2000 | 84.33% accuracy and more than 91% TPR |

In this paper, we have utilized the block-based approach to detect CMF in digital image. Our target is to identify CMF in an image using natural scene statistics (NSS) feature vector. We have

compared various CMFD techniques in current section, so we have found that the key point feature-based methods are more robust, time saving and accurate than the block based forgery detection methods. The method used in this research paper is inspired by the image quality assessment technique in which NSS are utilized to evaluate the image quality score. But the pattern of these features is also become non-uniform due to the copy-move forgery attack on any image, so by using NSS feature vector this becomes easy to detect the forged image. We have compared our approach with various forgery detection approaches in this literature review section above.

2.3 Research Gap/Limitations:

We have reviewed the research work of the multiple researchers in the area of image forensics. Many of the researchers have utilized different type of intrinsic features of images and machine learning models to detect image forgeries. NSS features contain the behavior of natural images and have the capability to capture any type of distortion in an image. As forgery is also a type of distortion so, NSS can differentiate forged and original images. As we have reviewed the related works of many researchers above, NSS have been utilized only for image quality assessment approach so far, but these intrinsic features have not been utilized before for image forgery detection (IFD) purpose. This novel technique in the field of image forensics have been created new ways for the researchers to enhance the IFD methods. As forgery in images increasing day-by-day so, it is necessary to improve IFD algorithms.

Chapter 3

Methodology

Image forensic tools are now become a basic need in order to communicate an image from one place to another with authenticity. Many types of image tempering tools are now available like Photoshop etc. to easily manipulate the originality of an image for various purposes. This thesis aims to detect image forgery that may have been performed using any image manipulation tool. A famous form of image forgeries is the copy-move image forgery which means that any portion in an image is copied and pasted within that image on another place, in this way a very crucial information of an image can be hidden or wrongly delivered to viewer of that image. This paper aims to detect copy-move forgery in an image without reference image. A famous database known as MICC-F2000 of copy-move IFD has been utilized in this research for image forensic task. Many researchers have been used different types of features to detect image forgery as discussed in the literature review section above. We have inspired by these papers that have been utilized different hand crafted features to detect image forgery. So, our main goal in this research is to CMF attempt in an image by any means using our proposed hand crafted features.

Hamid et al. [16] proposed a method to predict image quality score, this method has been utilized some hand-crafted features of natural images called as natural scene statistics (NSS). For example, when anyone captures an image using his/her high quality camera, then the eye of camera captures the natural scene just like human eye does which contains specific pattern of NSS. So, when someone by any means attempt any type of forgery in an image, then these NSS pattern got disturbed which is quite helpful to detect that some manipulation has been done to original image. Any image that has been purely generated through computer graphics or any type of manipulation done in that image cannot contain correct pattern of NSS. Our proposed model has been utilized NSS features to identify whether an image given to the model is original or tempered. These NSS have been extracted using MICC-F2000 dataset's original and forged images. A block diagram given below describes the proposed image forensic scheme:

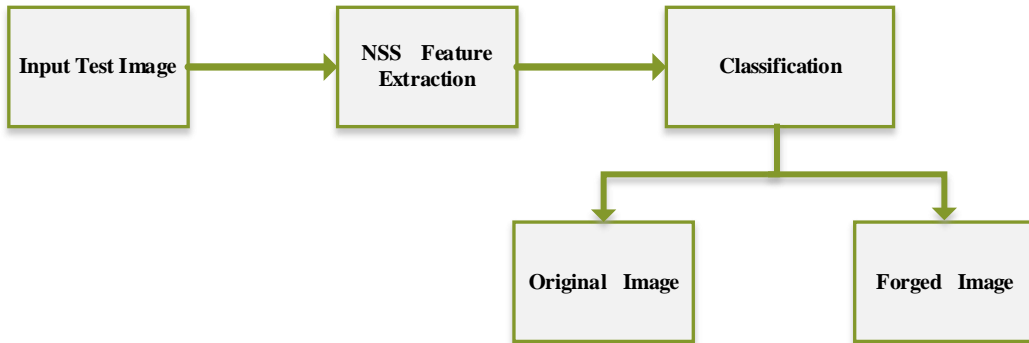


Figure 3.1: Proposed Methodology

3.1 Feature Extraction:

We have utilized natural scene statistics to classify an image being original or forged. These features are used before for the image quality assessment purpose as mentioned by Hamid et al. [16]. There are multiple types of NSS features, one property which is common among all of these is that they possess certain statistical properties which are transformed due to any distortion takes place in an image as mentioned by Anush in et al. [87]. So, forgery is also a kind of distortion in natural image which is easily catchable by these features. Following are the NSS features that we have used in our research to catch image forgery:

- i) The Distortion Identification-based Image Verity and Integrity Evaluation (DIIVINE) index.
- ii) Spatial and Spectral Entropy-Based Quality (SSEQ) index.
- iii) Oriented Gradients Image Quality Assessment (OG-IQA).

3.1.1 Distortion Identification-based Image Verity and Integrity Evaluation index:

DIIVINE is the type of NSS feature which represents that how natural image behaves normally. Anush et. al [87] proposed a method of assessing image quality/distortion based on DIIVINE features. DIIVINE can find the distortion in photograph's quality without using any reference photograph [87]. Also, DIIVINE is proved to be statistically superior as compared to famous peak-signal-to-noise ratio (PSNR) and comparable to structural similarity index (SSIM) as far as image

quality measure is concerned (87). DIIVINE plays an important role in capturing the unnaturalness of an image as these features represent strong statistical properties of the natural image, so whenever any type of distortion takes place then image become unnatural and by using DIIVINE statistics, distortion is easily catchable. In [87], authors have mentioned the DIIVINE features extraction method as follows:

- i) The scale-space-orientation decomposition method to decompose distorted photographs (somewhat, a wavelet transforms) to generate oriented band-pass response.
- ii) Attained sub-band coefficient are then used to obtain a sequence of statistical properties.
- iii) Now obtained geometric properties are then arranged together to develop a feature vector representing a statistical illustration of any type of distortion in a photograph.

They utilized these features to find the possibility that the photograph is suffered by any type of distortion. Furthermore, they have described statistical model for wavelet coefficients and then extraction of these features as follows:

i. Statistical Model for Wavelet Coefficient:

In the context of DIIVINE, adjacent wavelets coefficient are computed by means of the Gaussian Scale Mixture (GSM) model [88]. An N-dimensional random vector Y is a GSM if $Y \Rightarrow z.U$. U where \Rightarrow denoted equality in probability distributions, U is a zero-mean Gaussian random vector with covariance C_u , and z is a scalar random variable named a mixing multiplier. The density of Y is given as

$$p_Y(y) = \int \frac{1}{(2\pi)^{\frac{N}{2}} \left| z^2 C_u^{\frac{1}{2}} \right|} \exp\left(\frac{-y^T C_u^{-1} y}{z^2}\right) p_Z(z) dz \quad 3.1$$

The GSM model has been utilized to compute the marginal and joint statistic of the wavelet coefficient of original photographs [88], [89], where the vector is generated by bunching a set of adjacent wavelet coefficient in a sub-band, or around adjacent sub-bands in scales and orientations.

ii. Extraction of Distortion Identification-based Image Verity and Integrity Evaluation index features:

After that to mine features from natural and distorted photographs, they have utilized the steerable pyramid decomposition [90]. It is a wavelet transform that permits greater orientation selection. The wavelet transform was chosen because the scale-space-orientation decomposition performed by the wavelet transforms mimics the model of spatial decompositions that happens in area V1 of the primary visual cortex [91], [92]. This DIVIINE index extracts 88 features mentioned by Anush et al.[87] for a single image as shown in table 3.1 below:

Table 3.1: DIIVINE features and the way they were computed

| Feature Vector | Feature Description | Computation Procedure |
|---------------------|---|---|
| f_1 - f_{12} | Variance of subband coefficients | Fitting a generalized Gaussian to subband coefficients |
| f_{13} - f_{24} | Shape parameter of subband coefficients | Fitting a generalized Gaussian to subband coefficients |
| f_{25} - f_{31} | Shape parameter across subband coefficients | Fitting a generalized Gaussian to orientation subband coefficients |
| f_{32} - f_{43} | Correlations across scales | Computing windowed structural correlation between filter responses |
| f_{44} - f_{73} | Spatial correlation across sub bands | Fitting a polynomial to the correlation function |
| f_{74} - f_{88} | Across orientation statistics | Computing windowed structural correlation between adjacent orientations at same scale |

We have utilized 500 original and 500 forged images in our research to extract 1000 x 88 DIVIINE feature vector. As mentioned above that these features are the statistical description of the distorted and natural image, so by using this property we have used this feature vector to classify between natural and forgery afflicted images. As attempting forgery in an image is a kind of throwing a distortion in a specific region of image where forgery has been done, so DIIVINE statistical features of an image are altered/disturbed due to the presence of forgery in an image which marked an image to be unnatural or forged.

3.1.2 Spatial and Spectral Entropy-Based Quality index:

SSEQ are also one of the NSS category features. Lixiong in et al. [93] proposed a general purpose and efficient no-reference image quality assessment model that used local spatial and spectral entropy-based quality (SSEQ) features on distorted images. Images entropy specifies the quantity of information present in an image and when computed over multi-scales exposes the statistical entropy of scale space [94]. The degrees and types of image distortion predictably influence the local entropy of an image. Global entropies contained global information of images unlike local entropy, but it will not distinguish the spatial distributions of information [93], so the photograph contained same global information may be quite different. Bovik in et al. [95] mentioned that there is a close relationship between local entropy and the perceived image quality. Also, researchers in et al. [93] finds that the entropy feature is highly sensitive to distortion of images. There technique used local image's block to compute entropy, on both the blocks spatial scale responses and also on the blocks discrete cosine transform (DCT) coefficient. These entropies are all calculated locally. The spatial entropy is a function of the local pixel value's probability distribution. Spectral entropy, on the other hand, is a function of the local DCT coefficient value's probability distribution.

In comparison with other NSS based IQA approaches, which uses the statistical attributes at pixels level, this entropy-dependent technique examines the joint distributions of pixel within local patches. This method is based on the statistical features of the local region rather than pixel, which contributes to demonstrate photographs' local structural data. In [93], researchers have given a basic hypothesis that a local entropy of natural/undistorted images keeps certain statistical properties. These statistical features are due to the dependence between adjacent pixels. So, if any distortion takes place, then inherent dependence between these adjacent pixels destroys makes the change in local entropy. For example, if high frequency distortion takes place in an image, then this will cause the local entropy to obtain high values while blur distortion makes the local entropy low [93]. Following are the details of local entropy and how it affects the image quality:

i. Spatial Entropy Features (f1 - f6):

The equation of spatial entropy is

$$E_s = -\sum_x p(x) \log_2 p(x) \quad 3.2$$

Where x is pixel value in blocks, comprising empirical probability density $p(x)$, i.e., related frequency. Demonstrating the local spatial entropy behavioral value having numerous degree and categories of distortion, researchers in [93] showed a sequence of validation practical on images. Several forms of distortion (JP2K and JPEG compression, noise, blur and fast fading) apply scientifically distinct effects on the spatial entropy value. The natural images (ori) have a spatial entropy values with mean about 4 and it is left-skewed. The “left-skewed” demonstrates the less information at the left of mean value as compared to right, which leads to a lengthier left tails than right. Though, the effect of distortions vary it’s mean and skew. Such as, noise abruptly increases the mean, whereas blur and jp2k sharply decreases the mean and skewed the histogram towards right. Overall, spatial entropy reveals the form of distortions as its make clear going forward [93]. Researchers in [93], have utilized this mean and skew as a qualitative feature that demonstrates the histogram. They obtained 2 features from each scale, yielding $2 \times 3 = 6$ features.

ii) Spectral Entropy Features (f7 - f12):

Since it has been believed that there exists a strong relation between the spectral entropy feature values and the distortion degree and type [95]. The block DCT coefficients matrix C is also computed on 8×8 block. Using DCT in place of the DFT decreases blocks edge energy in the transform’s coefficient values. Then it normalizes the DCT coefficient values to generate a spectral probability map in [93]:

$$P(i, j) = \frac{c(i, j)^2}{\sum_i \sum_j c(i, j)^2} \quad 3.3$$

Where $1 \leq i \leq 8$, $1 \leq j \leq 8$, and i, j not equal to 1 (DC is omitted). Further describes the local spectral entropy

$$E_f = -\sum_i \sum_j P(i, j) \log_2 P(i, j) \quad 3.4$$

To visualize the nature of the spectral entropy feature set through various types of distortion, they performed other visual validation experiments on the same image [93]. Various types of

distortion (jp2k and jpeg compression, noise, blur and fast fading) apply analytically different effects on the spectral entropy's value. Specifically, they might recognize that natural images (ori) have a spectral entropy's values which is normally left-skewed [93]. But the attempt of alterations will alter its means and skews values. E.g., noises sharply increase the mean, whereas blur, jp2k decrease the mean and skewed the histogram to the right. The spectral entropies also strongly reveal the kind of distortion. In comparison to the spatial entropy feature histogram, the spectral entropy features histogram reveals clearer the effect of distortion in an image as compared to the undistorted image [93]. The spectral entropy well-defined here is an accurate descriptor of images' energy spectrum and highlights the main frequency and main orientations within a local patch. So, it is able to distinguish noise and blur effect more clearly. Further, spectral entropy can capture texture variations more effectively, to which human perception is very sensitive [93]. Same as spatial entropy, researchers utilized mean and skew as a feature value in spectral entropy, so by using these 2 feature values from each scale, yielding $2 \times 3 = 6$ features.

iii) Spatial and Spectral Entropy-Based Quality index Features used for forgery detection:

Total 12 features extracted by researchers in [93], to be tested with the distorted image quality as listed in table 3.2. Because of obtaining each type of feature from 3 scale (low, middle and high), each group comprises three characteristics.

Table 3.2: SSEQ Features

| Feature Vector | Feature Description |
|-------------------|--|
| $f_1 - f_3$ | Mean of spatial entropy's value for 3 scale |
| $f_4 - f_6$ | Skew of spatial entropy's value for 3 scale |
| $f_7 - f_9$ | Mean of spectral entropy's value for 3 scale |
| $f_{10} - f_{12}$ | Skew of spectral entropy's value for 3 scale |

As we have suggested in our research that, forgery is also a type of distortion. Wherever in an image forgery takes place, then the affected region gets distorted and these 12 features of SSEQ which contains a statistical properties of natural image, altered and becomes unnatural. So, by using this behavior of SSEQ features, this is easily catchable that the image is original or tempered/distorted. We have used 500 natural and 500 forged images to extract 12 SSEQ feature

vector from each image which represents the image to be original or forged. So, by using 1000 x 12 feature vector of SSEQ values, we have trained the ML classifier to classify the original and forged image.

3.1.3 Oriented Gradients Image Quality Assessment:

OG-IQA are also a type of NSS features. Natural photographs are well organized and correlated over orientation and scale [96]. Lixiong in et al. [97] mentioned that image gradient is very common and useful feature for image quality assessment (IQA). The gradient magnitude having scalar-value only carries portion of the image related to local image's brightness changes. Visual cortical neuron is extremely subtle to local orientation data in image [98, 99]. Subsequently image distortion altered local images anisotropies, it is important to find the values of the gradient's orientations to enhance NR IQA model. For illustration, both the location and distribution of the gradients orientations between natural photograph and its distorted form can be recognized clearly [97]. The gradient orientation carries data opposite to the gradient magnitude and has been utilized to get better image quality assessment [97]. The equation of estimated gradient orientation is as follows:

$$\angle \nabla I(i, j) = \arctan \left(\frac{I_y(i, j)}{I_x(i, j)} \right) \quad 3.5$$

Orientation is related, and advanced feature mining techniques that used gradient orientation information to calculate it in better way, e.g., SIFT [100] and Histogram of Oriented Gradient (HOG) [101]. Relative gradient magnitude data obtains the behavior of changes in local structure of an image, so if any distortion takes place in an image, then it changes the local structure thus changes the local orientation information of an image [97]. Orientation may well be measured categorically, in comparison to the frame of reference of the photograph coordinate system, alternatively it is also computed relative to the background of local orientation characterized as, let suppose an average value. The method of measurements described latter is better to evaluate image quality, because a related orientation feature set detects deviations based on the natural distributions of local orientation induced by photograph structure degradation locally [97].

Succeeding this proposal, researchers in [97] also describe a related gradient magnitude feature set, the same concept damages the local contrast are finest cast in contradiction of the nearby contrast. So undoubtedly, it's a method of the contrast masking principle. Therefore, 3 forms of

gradient map are calculated from I_x and I_y and used to describe the quality determined behaviors of images gradients over patch of size $M \times N$: the gradient magnitude (GM), the relative gradient orientation (RO), and the relative gradient magnitude (RM). The GM is specified by

$$|\nabla I(i,j)| = \sqrt{I_x^2(i,j) + I_y^2(i,j)} \quad 3.6$$

And the RO is given by

$$\angle \nabla I(i,j)_{RO} = \angle \nabla I(i,j) - \angle \nabla I(i,j)_{AVE} \quad 3.7$$

While the local average orientation is given by

$$\angle \nabla I(i,j)_{AVE} = \arctan\left(\frac{I_y(i,j)_{AVE}}{I_x(i,j)_{AVE}}\right) \quad 3.8$$

Using the average directional derivatives estimates as

$$I_y(i,j)_{AVE} = \frac{1}{MN} \sum_{(m,n)} \sum_{\epsilon \in W} I_y(i-m, j-n) \quad 3.9$$

And

$$I_x(i,j)_{AVE} = \frac{1}{MN} \sum_{(m,n)} \sum_{\epsilon \in W} I_x(i-m, j-n) \quad 3.10$$

Where W denotes a set of relative coordinate shift illustrating the local neighborhood over which the derivative values are taken.

The RM is given by

$$|\nabla I(i,j)|_{RM} = \sqrt{(I_x(i,j) - I_x(i,j)_{AVE})^2 + (I_y(i,j) - I_y(i,j)_{AVE})^2} \quad 3.11$$

in terms of average local derivative.

By using GM, RO and RM, researchers in [97] experimented the variations in relative gradient orientation which conveys the variations in local structure of natural image, so make it unnatural. Variance is defined as follows

$$Var[h] = \sum_x (h(x) - h')^2 \quad 3.12$$

Here h' is the sample mean of the histogram. So, we have a three-dimensional feature vector: Feature = [VGM; VRO; VRM], measured on each of the histograms of GM, RO and RM respectively.

3.1.4 Oriented Gradients Image Quality Assessment Features used for forgery detection:

There are 6 gradient oriented features are extracted by the above-mentioned approach to catch the distortion in an image on the 6-dimensional feature vector. Table 3.3 shown OG-IQA features:

Table 3.3: Gradient and relative gradient features

| Feature ID | Feature Description |
|--------------------|--|
| V_{GM1}, V_{GM2} | Variance of histogram of gradient's magnitudes over two scale |
| V_{RO1}, V_{RO2} | Variance of histogram of relative gradient's orientations over two scale |
| V_{RM1}, V_{RM2} | Variance of histogram of relative gradient's magnitudes over two scale |

As we have suggested in our research that, forgery is also a type of distortion. Wherever in an image forgery takes place, then the affected region gets distorted and these 6 features of gradient and relative gradient orientation image quality analysis (OG-IQA) which contains a local structure and orientation information of natural images, altered, and change the local structure of an image. So, by using this behavior of these features, this is easily catchable that the image is original or tempered/distorted. We have used 500 natural and 500 forged images to extract 6 OG-IQA feature vectors from each image which represents the image to be original or forged. So, by using 1000 x 6 feature vector of OG-IQA features, we have trained the ML classifier to classify the original and forged image.

3.1.5 Natural Scene Statistics Combinations:

In this research, we have already discussed about the NSS features that we have used to train the ML models so that they can classify whether an image is original or forged. Three types of NSS features we have used i-e DIIVINE, SSEQ and OG-IQA to train the ML models. We have used these features in the following combinations:

- i) DIIVINE
- ii) SSEQ

- iii) OG-IQA
- iv) DIIVINE + SSEQ
- v) DIIVINE + OG-IQA
- vi) SSEQ + OG-IQA
- vii) DIIVINE + SSEQ + OG-IQA

First of all, we have used only 88 features of DIIVINE to train the ML model for forgery detection. As we have 500 forged and 500 original images from MICC-F2000 database so we have extracted 500x88 feature vector from original and 500x88 feature vector from forged images, so finally we have extracted 1000x88 feature vector of only DIIVINE features for original and forged image classification. After that we have utilized only 12 features of SSEQ to train the ML model for forgery detection. As we have 500 forged and 500 original images from MICC-F2000 database so we have extracted 500x12 feature vector from original and 500x12 feature vector from forged images, so finally we have extracted 1000x12 feature vector of only SSEQ features for original and forged image classification. After that we have utilized only 6 features of OG-IQA to train the ML model for forgery detection. As we have 500 forged and 500 original images from MICC-F2000 database so we have extracted 500x6 feature vector from original and 500x6 feature vector from forged images, so finally we have extracted 1000x6 feature vector of only OG-IQA features for original and forged image classification.

After utilizing all three types of NSS features one by one for IFD problem. Now we have experimented multiple combinations of these feature one with the other to improve the classification ability of our ML models. We have now utilized the combination of 88 DIIVINE features with 12 SSEQ features to train the ML model for forgery detection. As we have 500 forged and 500 original images from MICC-F2000 database so we have extracted 500x100 feature vector from original and 500x100 feature vector from forged images, so finally we have used 1000x100 feature vector of combined features for original and forged image classification. We have then utilized the combination of 88 DIIVINE features with 6 OG-IQA features to train the ML model for forgery detection. As we have 500 forged and 500 original images from MICC-F2000 database so we have extracted 500x94 feature vector from original and 500x94 feature vector from forged images, so finally we have used 1000x94 feature vector of combined features for original and forged image classification. We have then utilized the combination of 12 SSEQ features with 6

OG-IQA features to train the ML model for forgery detection. As we have 500 forged and 500 original images from MICC-F2000 database so we have extracted 500x18 feature vector from original and 500x18 feature vector from forged images, so finally we have used 1000x18 feature vector of combined features for original and forged image classification.

After utilizing all three types of NSS features one by one and the combination of two for IFD problem. Now we have experimented three types of features all together as a single feature vector to improve the classification ability of our ML models. We have now utilized the 88 DIIVINE features, 12 SSEQ features and 6 OG-IQA features to train the ML model for forgery detection. As we have 500 forged and 500 original images from MICC-F2000 database so we have extracted 500x106 feature vector from original and 500x106 feature vector from forged images, so finally we have used a big feature vector of 1000x106 features for original and forged image classification.

We have utilized the above-mentioned combinations of NSS features to train the ML model for forgery detection purpose. This experiment has been conducted to visualize the efficiency of NSS features all alone and also in combinations for how well these features play an important role in training the ML model. Further we have discussed about these combination results in the next results and analysis section.

3.2 Machine Learning Models/Classifiers:

In this research, five different models/classifiers have been used to train using all NSS features and their multiple combinations for two class classification i-e either testing image is original or forged. After that we have also used ensemble learning of three various models to get state-of-the-art results. Following are the four ML classifiers:

- i) Support vector machine
- ii) Decision Tree
- iii) Random Forest
- iv) K nearest Neighbors
- v) Ensemble Learning

3.2.1 Support Vector Machine:

The objective of the support vector machine algorithm is to find a hyper-plane in an N-dimensional space (N—the number of features) that distinctly classifies the data points. Following figure 3.2 illustrates the SVM and what is actually a hyper-plane and how it can be used for binary classification using any type of features.

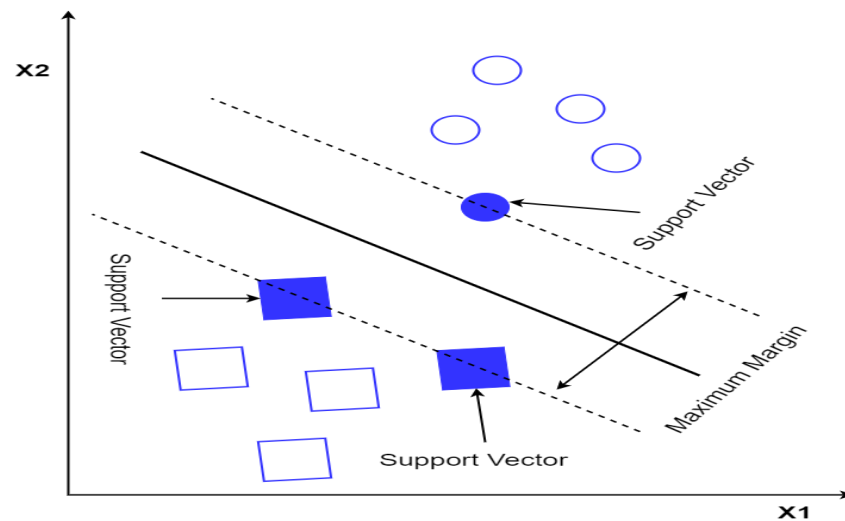


Figure 3.2 : Support vector and Hyper-plane boundary

There are many types of hyper-planes that distinguish the features and draw a boundary line between them, the best hyper-plane is that which has maximum margin between support vectors (features nearest to hyper-plane). Increasing the margin distance gives some reinforcement, allowing future data points to be classified with absolute credibility. Hyper-plane is a decision boundary that helps to classify the data points. Dissimilar classes can be assigned to data points that lie on either side of the hyperplane. Furthermore, the size of the hyper-plane is depending on the number of feature. When there are 2 input features, the hyper-plane is a simple line. When the number of input feature reaches to 3, the hyper-plane converts into a two-dimensional plane. When the number of features exceeds 3, it becomes tough to imagine. Support vectors are data points that are nearer to the hyper-plane and influence its position and orientation. These support vectors play a key role to increase the classifier's margin. The position of hyper-plane will change if the support vectors are removed. These are the points that will assist us in developing our SVM. In our research, we have

multiple features, so SVM gets in trouble to find that boundary line which distinguishes multiple features for 2 class classification.

3.2.2 Decision Tree:

The decision tree belongs to the family of supervised ML methods. It is utilized for both a classification problem as well as for regression problem. This model uses leaf nodes as a class label in classification problem and features are used as an internal node of a tree. Decision trees are decision support which have a tree like structure to take decisions and their results on basis of attributes given in figure. It behaves like an algorithm which only contains conditional control statements. There are following three types of nodes in decision tree:

- i) Decision nodes (represented by squares)
- ii) Chance nodes (represented by circles)
- iii) End nodes (represented by triangles)

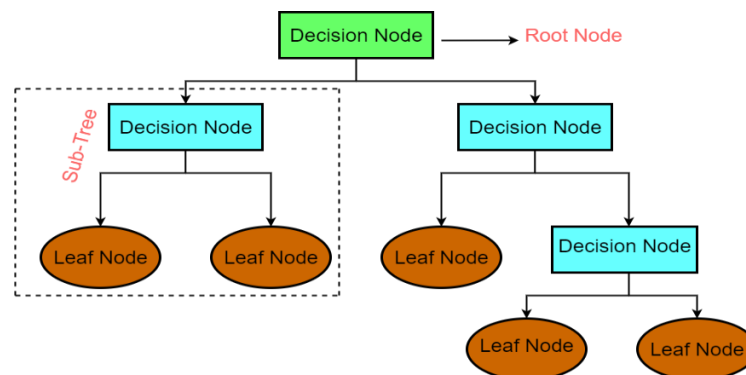


Figure 3.3: General decision tree structure

It is the general predictive model that can be applied to several fields. Decision trees are formed by using an algorithm that detects ways to allocate data depends on variation. This is among the most famous and practical approaches for supervised learning. Decision Tree is a non-parametric supervised learning technique used for both regression and classification purpose.

3.2.3 Random Forest:

As name resembles, random forest is a tremendous ML classifier which consists of large number of decision trees operating as an ensemble. Each decision tree predicts a class using data

attributes, then the class having most votes becomes prediction of the random forest. The principal concept behind random forest is very simple but powerful i-e the wisdom of crowd. In data science world speak, “the reason that the random forest model works so well is “*A large number of relatively uncorrelated models (trees) operating as a committee will outperform any of the individual constituent models*”. The main key the lowest correlation between individual decision trees. Following figure well explained the main idea.

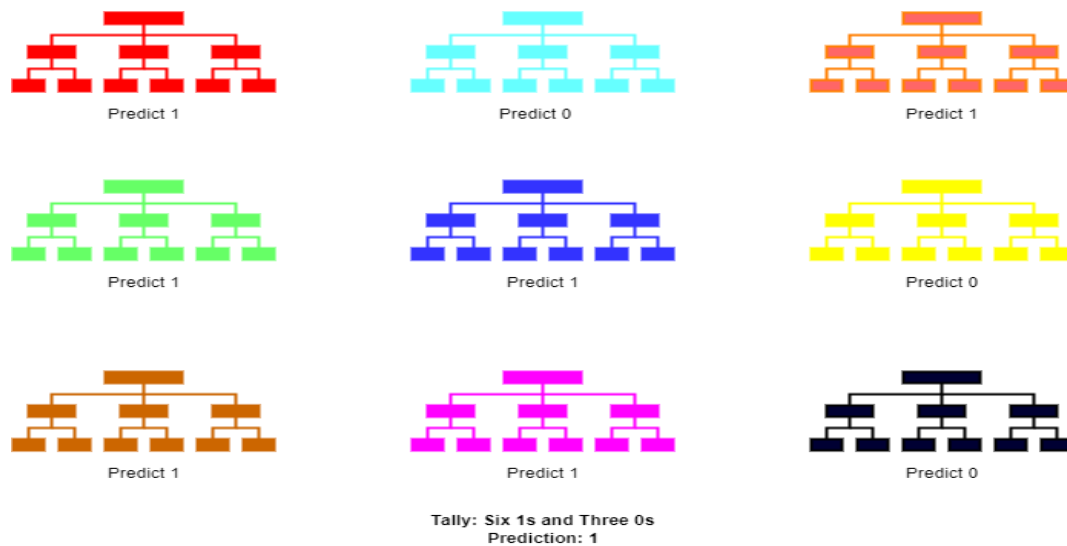


Figure 3.4: Random Forest models making predictions

This excellent result is due to the fact that trees defend one another from individual mistake (unless all are misguided in the similar way). But few trees may be incorrect, others will be correct, so as a whole trees can move towards right directions. Therefore, the best random forests conditions to work are:

- i) There must be an actual signal in our features to build the model to obtain better prediction.
- ii) Results and error made by the individual tree must have low correlation with each other.

3.2.4 K-Nearest Neighbors:

The k-nearest neighbor (KNN) method is a simple, easy-to-implement supervised ML method that can be utilized to solve both classifications and regressions problem. KNN always work on the

imagination that the matched features are in proximity or similar things are nearest to each other. Following figure illustrates that how the alike data points are near to one another.

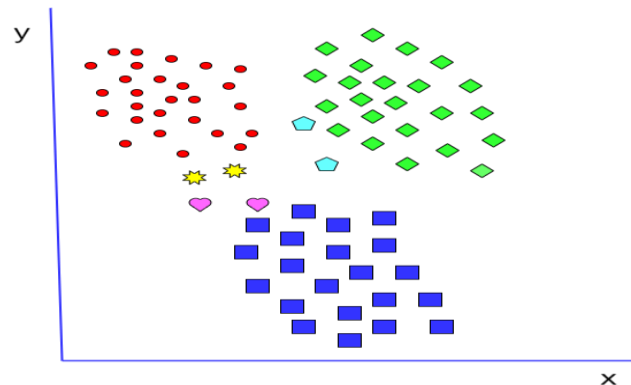


Figure 3.5:proximity of similar data points

In the above figure, it is clearly noticed that mostly alike data points are in proximity to each other. KNN often focused on this concept for being true enough to predict correctly. KNN has adopted the theory of some similarities (also called distance, proximity, or closeness) by calculating the distance between the points of a graph. KNN uses the approach that similar data points nearest to one another are categorized into a one group while others are in another group. In this way this is easy for the model to predict a class of features close to each other.

3.2.5 Ensemble Learning:

Ensemble learning is the process of combining multiple ML models to solve a classification problem, in this way all models are utilized strategically to improve the performance of models to classify, predict or function approximation tasks. It also reduces the risk of poor selection of individual model for classification, as in combination of models if one performs poor then the other one performs well. It also gives a confidence to models that ensure correct prediction, non-stationary learning, incremental learning, optimal feature selection etc. This system usually called a multiple classifier system or ensemble system. In this paper, we have utilized the following three classifiers as an ensemble way to increase the classification ability of models:

- i) Ada Boost Classifier
- ii) Gradient Boosting Classifier

i. Ada Boost Classifier:

The Ada-boost classifier is a meta-estimator, firstly it fits the classifier on the original database then fits other copies of the classifier on the same dataset. But this time it adjusts the incorrectly classified instances for making the classifier pays more attention on difficult cases. An Ada-Boost method, called as Adaptive Boosting, is a method utilized in ML as an Ensemble approach. As in this approach the weight is re-allocated to all individual instances, with higher weight to wrongly classified instance. This method minimizes both bias and variance for supervised learning. It is based-on the principles where models are grown sequentially. Excluding the first, each subsequent model is grown from previous learned models. In short, weak ML models become strong models. Following figure explained the ada-boosting shortly.

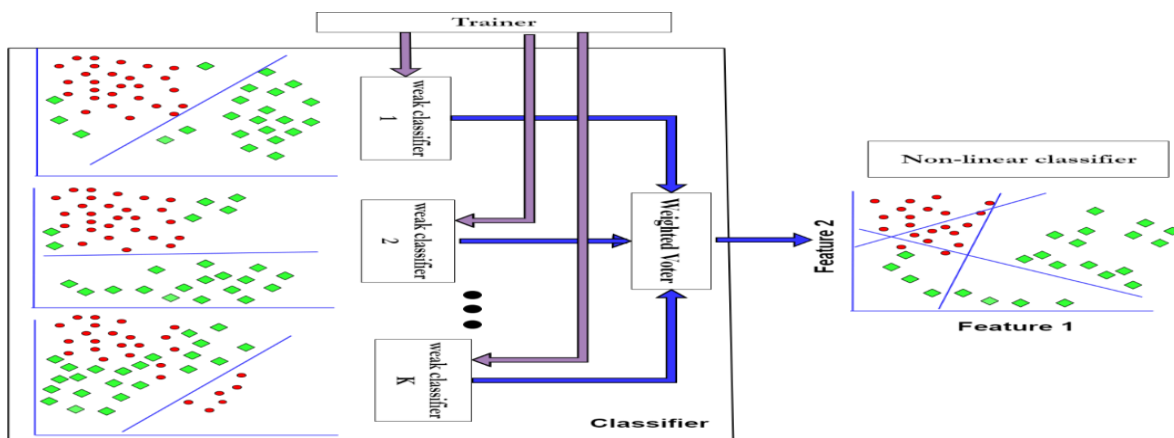


Figure 3.6: Illustration of ada-boosting for creating strong classifier based on multiple weak linear classifiers

ii. Gradient Boosting Classifier:

Gradient boosting algorithm works in a way that it creates a strong predictive ML model by combining multiple weak models. In gradient boosting, decision trees are used most of the time. Gradient boosting is now becoming popular due to its effectiveness in classifying complex datasets

and recently it has been used to win many kaggle data-science competitions because it improves speed and accuracy in classification.

We have described briefly about how we have done the IFD in this section. We have described how we are using all three types of NSS features and in combinations with each other, also we have utilized multiple ML models separately and also in ensemble learning technique. In the next section, all experiments and results analysis have been described in detail.

Chapter 4

Experimental Results and Discussion

4.1 Dataset:

In this paper, the MICC-F2000 dataset has been used which is created for copy-move forgery detection. It consists of 2000 images; among them 700 images are tampered while 1300 images are original. Images in this database are of size 2048 x 1536 pixels while a single image represents only 1.12% of tampered region in the whole image. This dataset is famous for being used as copy-move forgery detection techniques. We have taken 500 original and 500 forged images from this database and used these images to extract NSS features to train our ML models for the original and forged image classification. We have utilized MICC-F2000 dataset initially which consists of 2000 images. Among these 700 are forged while 1300 are original. Each has 2048 x 1536 pixels, and the tampered region represents only 1.12% of the whole image. We have utilized this dataset to extract NSS features, so that we have generated our new dataset including 1000 x 106 NSS features to train the classifier for IFD. Actually, our main dataset is MIC-F2000 and by using this we have created our secondary dataset to train the model. Following table 4.1 has shown the no. of NSS features per image used as a secondary feature database.

Table 4.1:Natural Scene Statistics Dataset features

| Feature Name | No. of features |
|---------------------|------------------------|
| DIIVINE | 88 |
| SSEQ | 12 |
| OG-IQA | 6 |

4.2 Experiments Procedure:

We have used multiple combinations of NSS features as described in previous chapter to experiment which one performed better and give better state-of-the-art results. We have utilized 80% of the dataset as training and 20% as testing purpose. We have used five ML models as mentioned in previous chapter for training with NSS feature dataset as mentioned. In our research, random forest has given the best state-of-the-art results among all the models we have trained.

4.3 Performance Metrics:

We have utilized multiple metrics for the evaluation of the efficiency of our algorithm. They are mostly built on the confusion matrix. Confusion matrix is a representation of a classification model's performance on test sets, which consists of 4 parameters: true positive, false positive, true negative, and false negative (see Table 4.2).

Table 4.2:Confusion Matrix

| | Predicted true | Predicted false |
|---------------------|-----------------------|------------------------|
| Actual true | True positive (TP) | False negative (FN) |
| Actual false | False positive (FP) | True negative (TN) |

We have utilized the following evaluation metrics:

- i) Accuracy
- ii) TPR/Precision
- iii) FPR
- iv) TNR
- v) Recall
- vi) F1-Score

All of these metrics are described below:

4.3.1 Accuracy:

Accuracy is a popular metric that represents the accurately predicted observation, whether correct or incorrect. The following equation can be used to find the accuracy of a model's performance:

$$Accuracy = \frac{TP+TN}{TP + TN+FP+FN} \quad 4.1$$

Mostly, a good/increased accuracy number reflects a strong model; however, given that we are training our models to predict original/forged image, in some cases original images are predicted as forged (false positive). While, in some cases forged images are predicted as original (false negative), this causes trust issue. So, we also utilized multiple other metrics that consider the wrongly classified value, i.e., precision/TPR, recall, and F1-score.

4.3.2 True Positive Rate/Precision:

TPR score is the ratio of true positive values to all images predicted as positive. In this case, precision demonstrates the amount of images that are observed as forged out of all the positively predicted (forged) images:

$$TPR/Precision = \frac{TP}{TP+FN} \quad 4.2$$

4.3.3 False Positive Rate:

This value give the ratio of actual original images to all the negatively predicted (forged) images. In this case, FPR calculates total number of images that are forged according to model from all the original images:

$$FPR = \frac{FP}{FP+TN} \quad 4.3$$

4.3.4 True Negative Rate:

This value gives the ratio of originals (true negative) to all the negatively predicted (original) images. In this paper, TNR gives the number of actual original images from all the negatively predicted (original) images:

$$TNR = \frac{TN}{TN+FP} \quad 4.4$$

4.3.5 Recall:

The number of positive predictions of our model out of the true class is referred to as recall. It is the number of images anticipated as forged out of the total number of real forged images in our example.

$$\text{Recall} = \frac{TP}{TN+FN} \quad 4.5$$

4.3.6 F1-Score:

F1-score signifies the value/trade-off between recall and precision. It determines the harmonic mean the two, it uses both the false positives and the false negatives into account. F1-score uses the following formula:

$$\text{F1 - Score} = 2 * \left(\frac{\text{Precision*Recall}}{\text{Precision+Recall}} \right) \quad 4.6$$

4.4 Software/Tool:

Training of the model takes too much time; it depends on the hardware. We have used MATLAB R2019a to extract features from 500 original and 500 forged images. We have used Intel(R) Core (TM) m3-7Y30 CPU @ 1.00GHz 1.61 GHz system and 8 GB RAM for feature extraction purpose. For implementing and training our models, we used Google Collab with CPU settings. Google Collab provides the python programming platform, fastest processor CPU, GPU or TPU and RAM, it has trained our model. The hardware specification of the lab is 2vCPU @ 2.2GHz, 13GB RAM, 100GB Free Space, Idle cut-off 90 minutes and Maximum of 12 hours. Once the model is trained and generates the output according to the requirements it has to be saved because when we need this model for another project, we load this trained model directly. We also save our time as the model takes a lot of time during the training. The mode can also be saved in the format of HDF (High-Definition File), it is always the best idea to save.

4.5 Results:

We have experimented all the combinations of NSS features and train our ML models to classify between original and forged images and to check which combination of features makes the models to perform better classification. Results of these models with best SSEQ+DIVIINE

combination are mentioned below in table 4.3 and figure 4.1 to 4.7 shows accuracies of all experimented combinations of NSS features.

Table 4.3:Models Test metrics with best NSS Features Combination

| Model | Test Accuracy | TPR | Recall | F1-Score |
|----------------------|---------------|---------------|---------------|---------------|
| Decision Tree | 92% | 91.34% | 93.13% | 92.23% |
| Random Forest | 98% | 97.11% | 99.01% | 98.05% |
| SVM | 78.38% | 71.43% | 81.63% | 76.19% |
| K Nearest Neighbor | 91% | 97.11% | 99% | 98.05% |

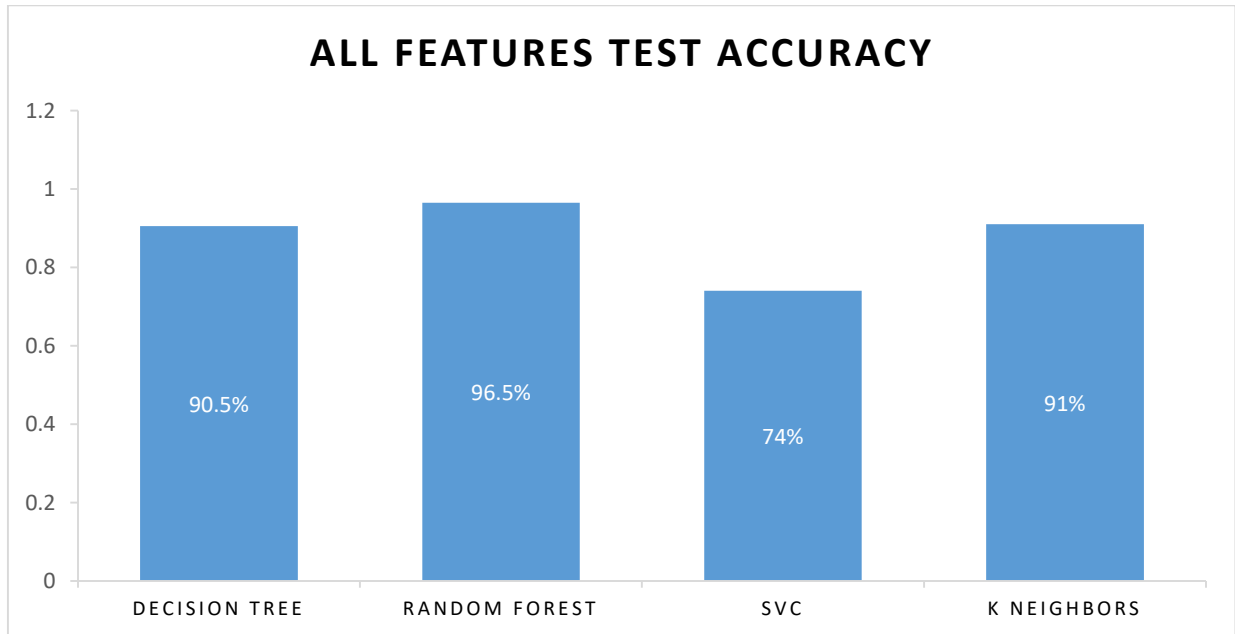


Figure 4.1:Models test accuracies with all three types of NSS features

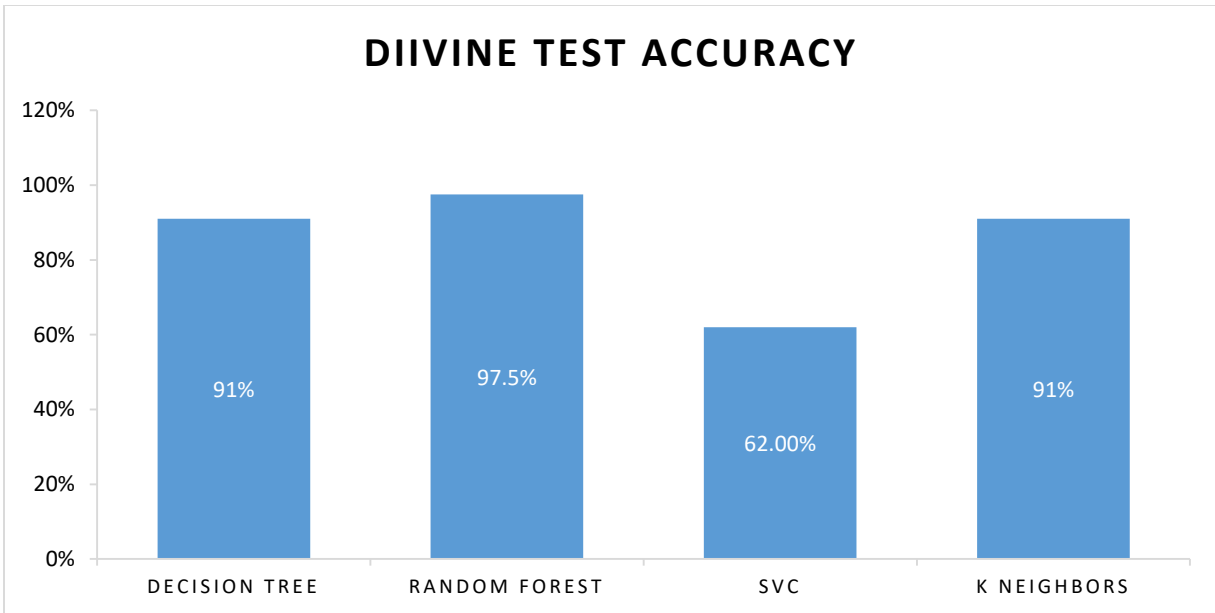


Figure 4.2: Models test accuracies with DIIVINE features

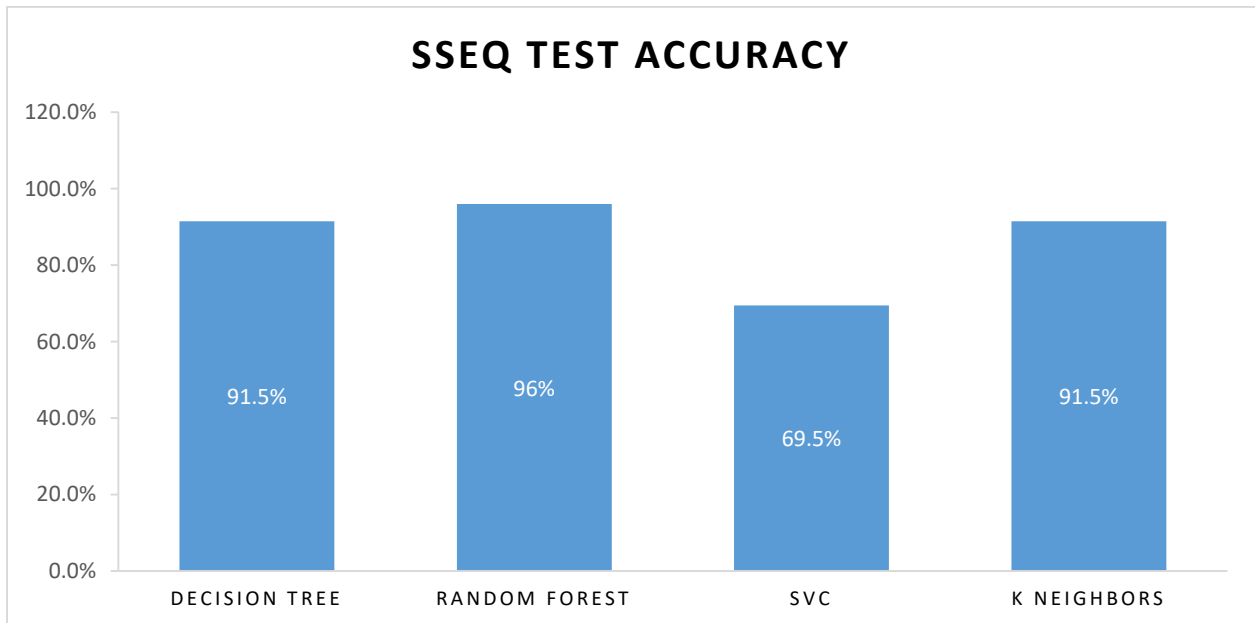


Figure 4.3: Models test accuracies with SSEQ features

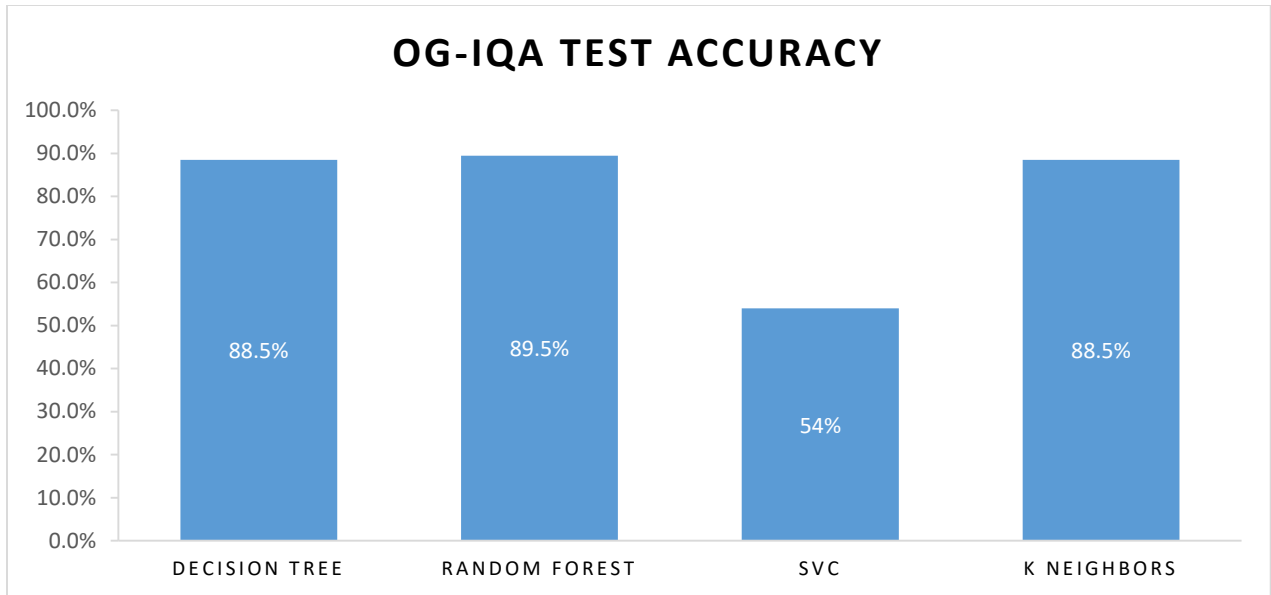


Figure 4.4: Models test accuracies with OG-IQA features

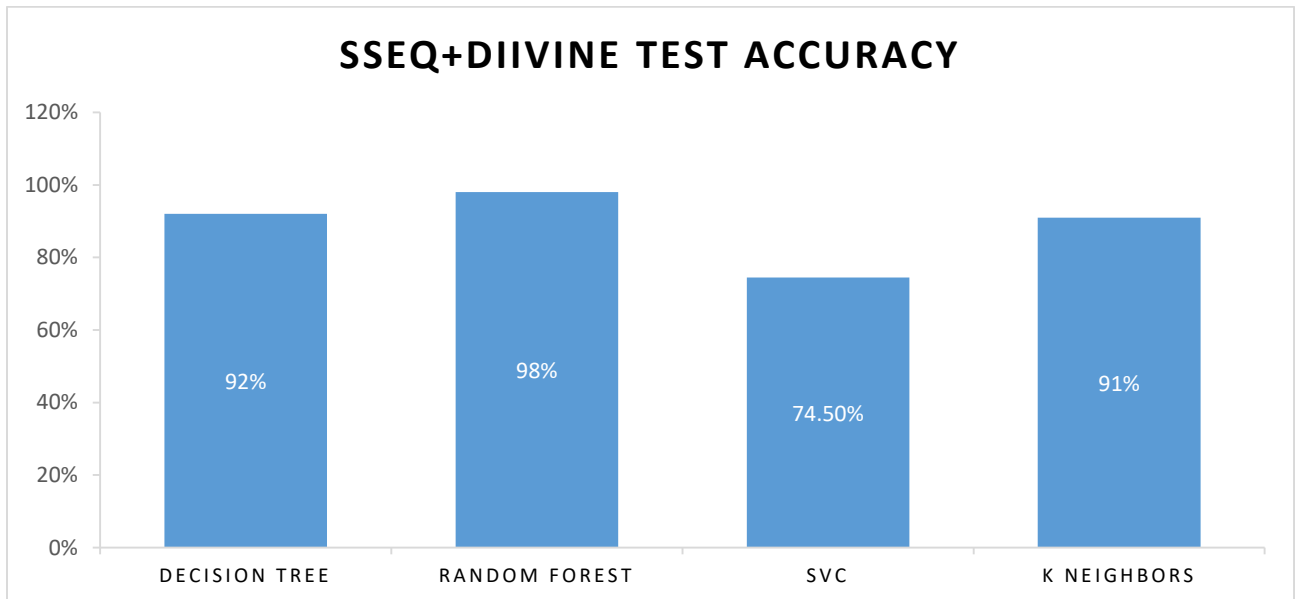


Figure 4.5: Models test accuracies with SSEQ+DIIVINE features

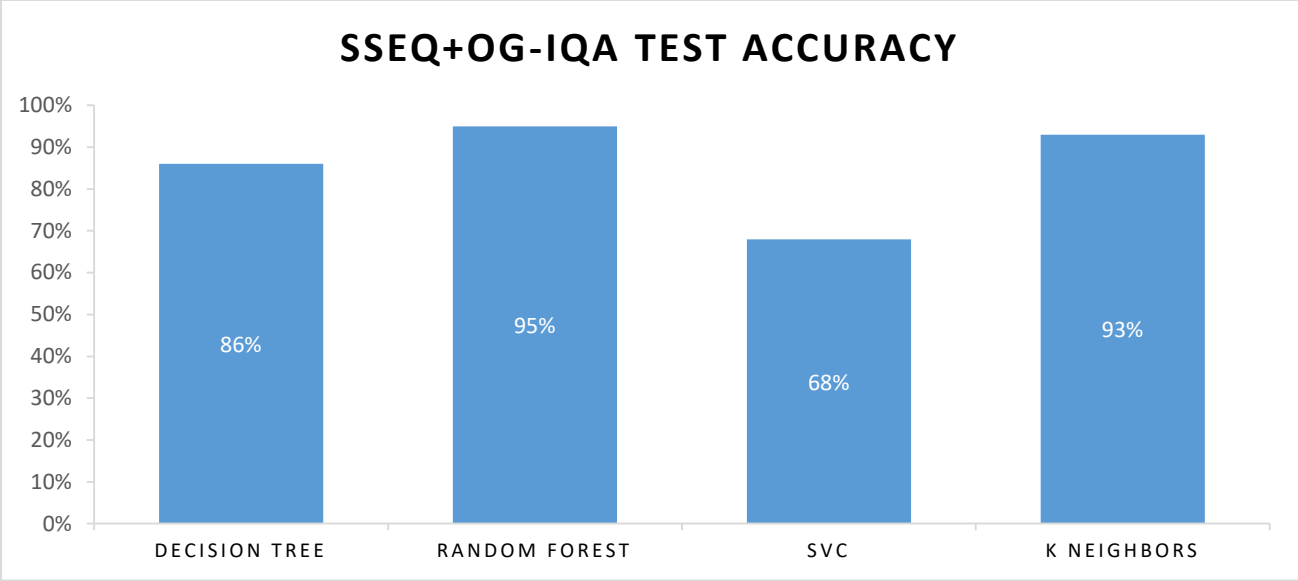


Figure 4.6: Models test accuracies with SSEQ+OG-IQA features

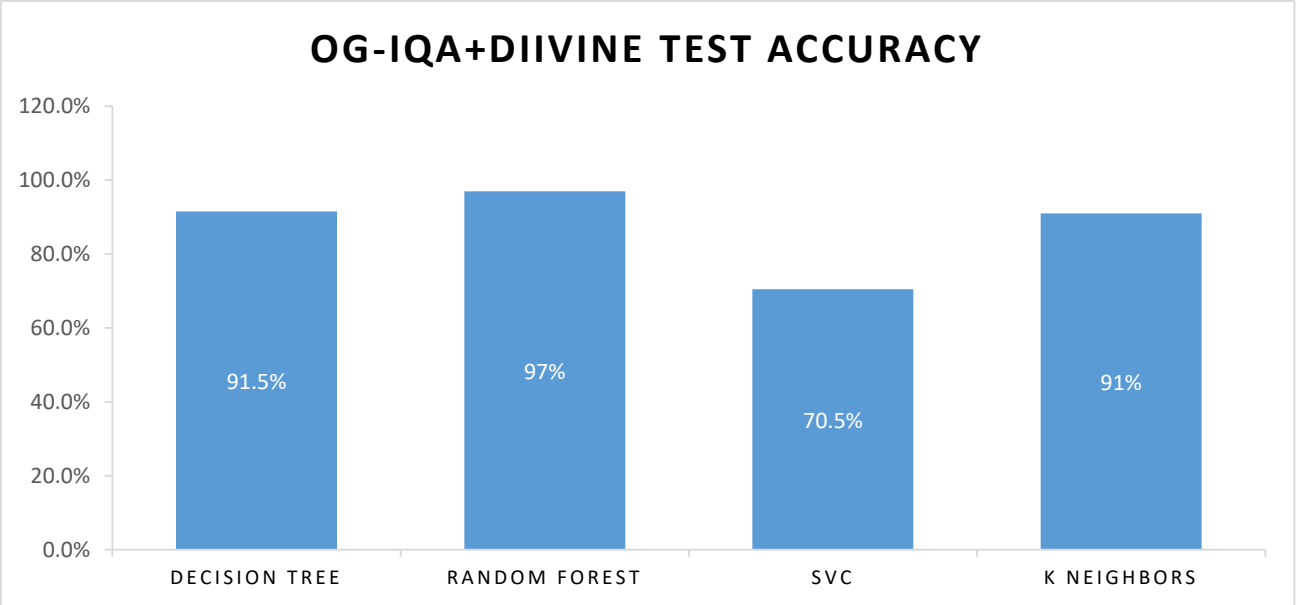


Figure 4.7: Models test accuracies with OG-IQA+DIIVINE features

By above results, it is clearly shown that our best combination of features is SSEQ+DIIVINE to achieve best state-of-the-art results with 98% accuracy, 97.11% TPR, 99.01% recall and 98.05% F1-Score. The reason behind the more efficient results of the SSEQ+DIIVINE features combination

is that both these features covers the statistical illustration of an image such that DIIVINE contains the wavelet transform based sub-band coefficients which can capture any type of distortion in an image while on the other hand SSEQ contains both the spatial and spectral entropy values of each block of an image. So, both of these features can capture any type of distortion in image better than OG-IQA features. Furthermore, Random Forest has given the best results as compared to other models as it is ensembled with multiple decision trees and have an outstanding decision making capability for the classification purpose.

4.6 Comparison results with other related works:

This is the core part of our research work; we have compared our best model metrics with some other related IFD methods on MICC-F2000 dataset in following table 4.4.

Table 4.4: Comparison Results with other works on MICC-F2000 dataset

| Methods | Test Accuracy | TPR | FPR | TNR | Recall | F1-Score |
|--------------------------|----------------------|------------|------------|------------|---------------|-----------------|
| Areej et al. [102] | -- | 97% | 8% | 92% | -- | -- |
| Vaishnavi et al. [104] | -- | 92.85% | 6.92% | -- | -- | -- |
| Loai et al. [103] | 95% | 94% | -- | 96% | -- | -- |
| Pourkashani et al. [105] | -- | 94.13% | -- | -- | 99% | 96.98% |
| Zhang et al. [106] | 97.30% | -- | -- | -- | 96.07% | 97.88% |
| Abdullah et al. [107] | 81% | 85.42% | 17.85% | -- | -- | -- |

| | | | | | | |
|-------------------|------------|---------------|--------------|---------------|---------------|---------------|
| Yong et al. [108] | 92.70% | 82.89% | 2.88% | -- | -- | -- |
| Proposed Method | 98% | 97.11% | 1.04% | 98.95% | 99.01% | 98.05% |

Now by above mentioned table it is clearly shown that how we have improved our evaluation metrics as compared to others. These seven different state-of-the-art methods are chosen for comparison as they have also used MICC-F2000 dataset and CMFD which is similar to our problem. We have increased our accuracy by 0.7%, TPR by 0.11%, TNR by 2.95%, recall by 0.01% and F1-Score by 0.17%. Also, we have decreased the FPR by 1.84%. Also following graphs have been shown individual metrics of different methods as compared to the proposed method.

4.6.1 Accuracy comparison:

Following figure 4.8 has shown the comparison of accuracy with other state-of-the-art-methods:

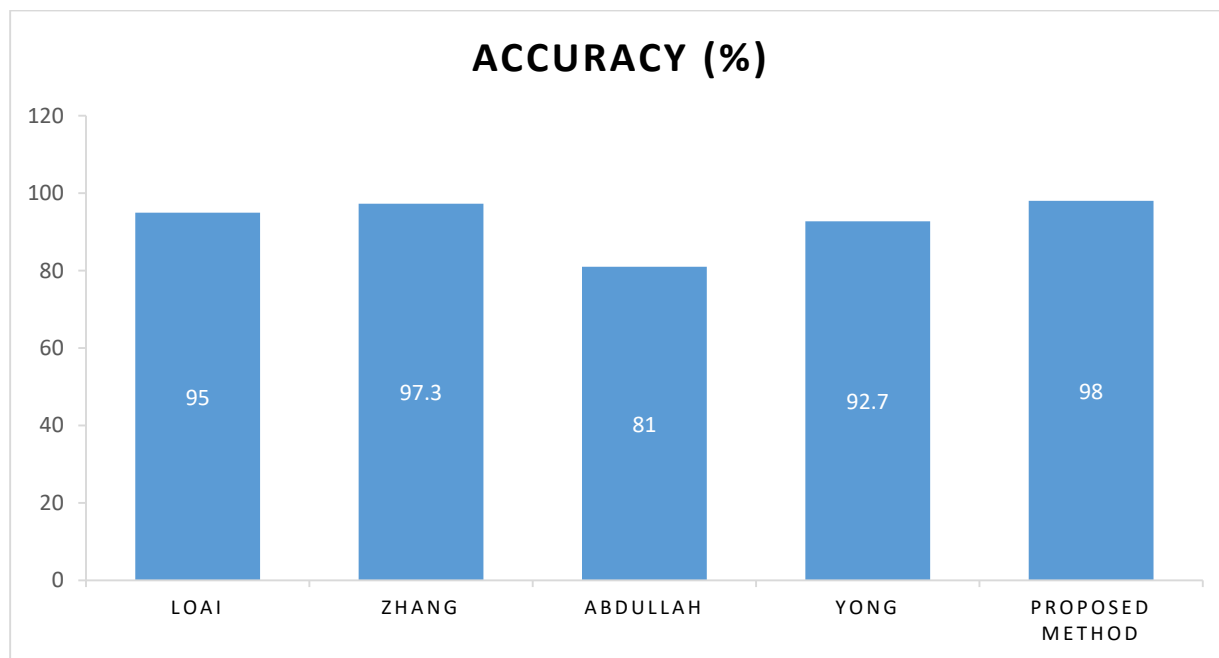


Figure 4.8: Accuracy Comparison with other methods

It is clearly shown that accuracy achieved in the proposed state-of-the-art method is 98% which is much better than other methods that have been compared in the above graph.

4.6.2 True Positive Rate comparison:

Following figure 4.9 has shown the TPR assessment with other advanced approaches:

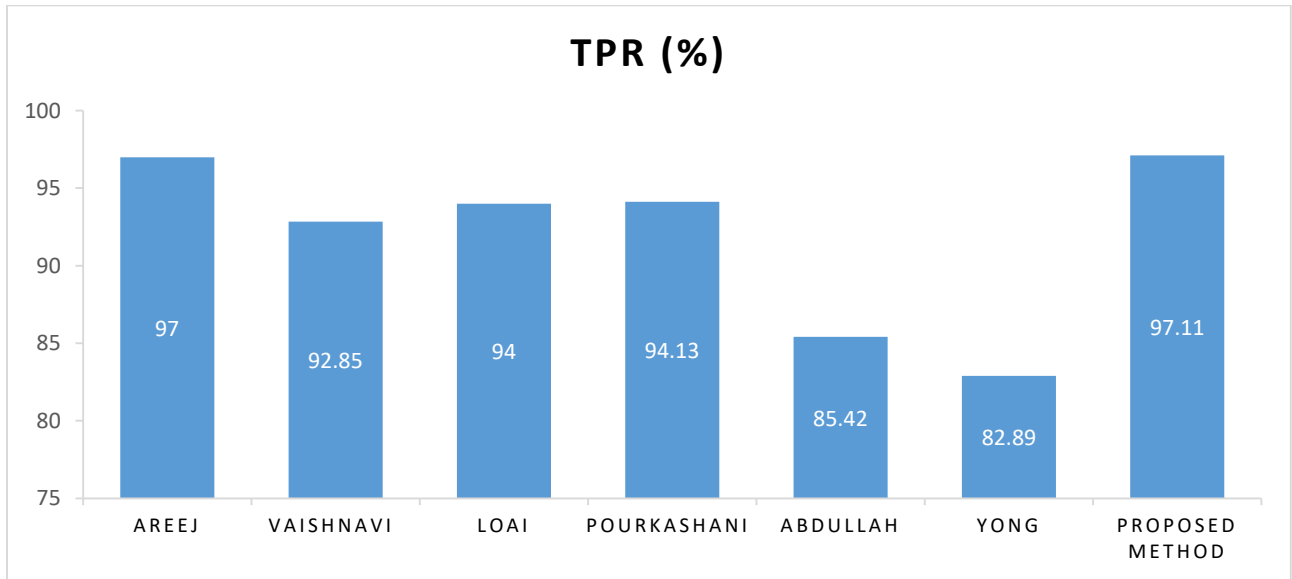


Figure 4.9:TPR Comparison with other methods

It is clearly shown that the true positive rate achieved in the proposed state-of-the-art method is 97.11% which is better than other methods that have been compared in the above graph.

4.6.3 False Positive Rate comparison:

Following figure 4.10 has shown the FPR assessment with other advanced approaches:

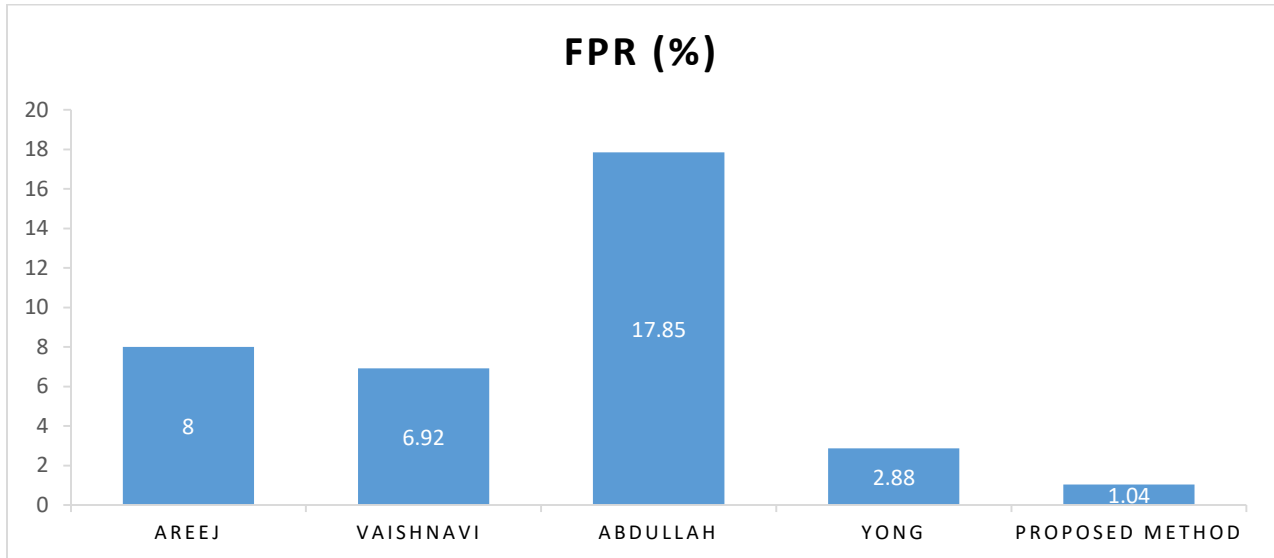


Figure 4.10:FPR Comparison with other methods

It is clearly shown that false positive rate achieved in the proposed state-of-the-art method is 1.04% which is less than other methods that have been compared in the above graph.

4.6.4 True Negative Rate comparison:

Following figure 4.11 has shown the comparison of TNR with other state-of-the-art-methods:

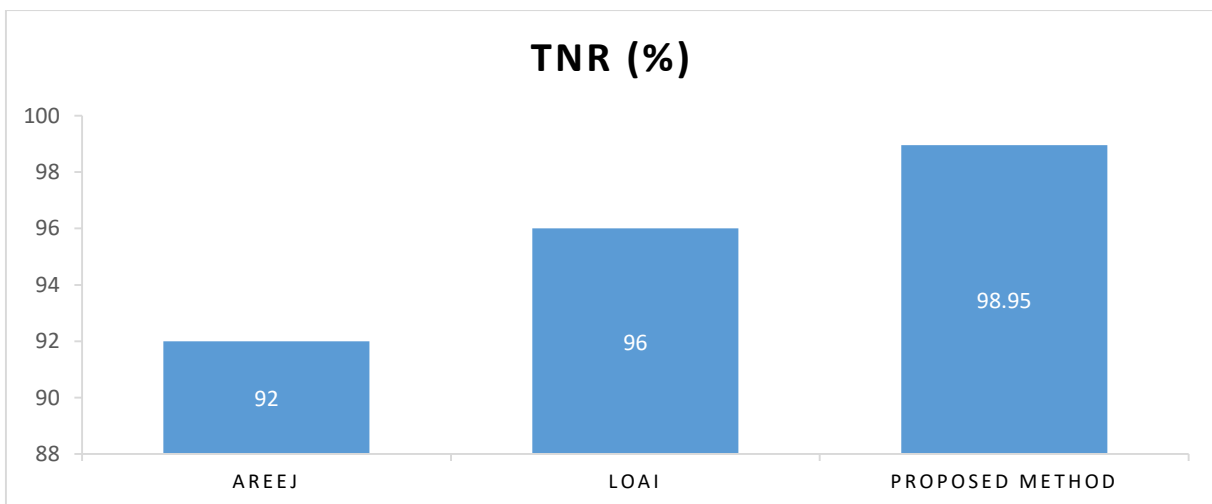


Figure 4.11:TNR Comparison with other methods

It is clearly shown that the true negative rate achieved in the proposed state-of-the-art method is 98.95% which is far better than the other methods that have been compared in the above graph.

4.6.5 Recall comparison:

Following figure 4.12 has shown the recall assessment with other advanced approaches:

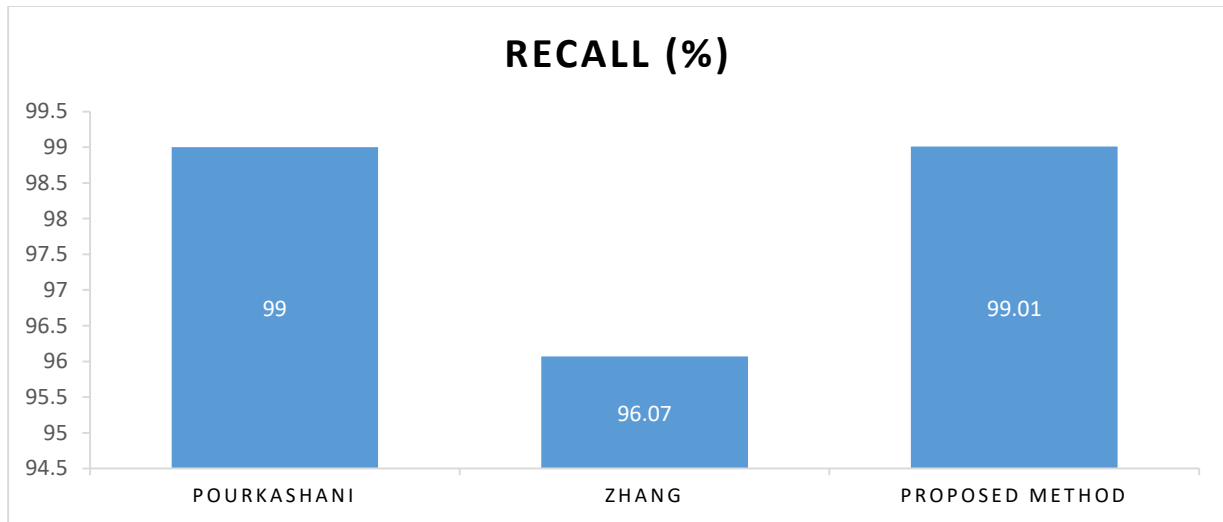


Figure 4.12: Recall Comparison with other methods

It is clearly shown that the recall achieved in the proposed state-of-the-art method is 99.01% which is better than other methods that have been compared in the above graph.

4.6.6 F1-Score comparison:

Following figure 4.13 has shown the F1-Score assessment with other advanced approaches:

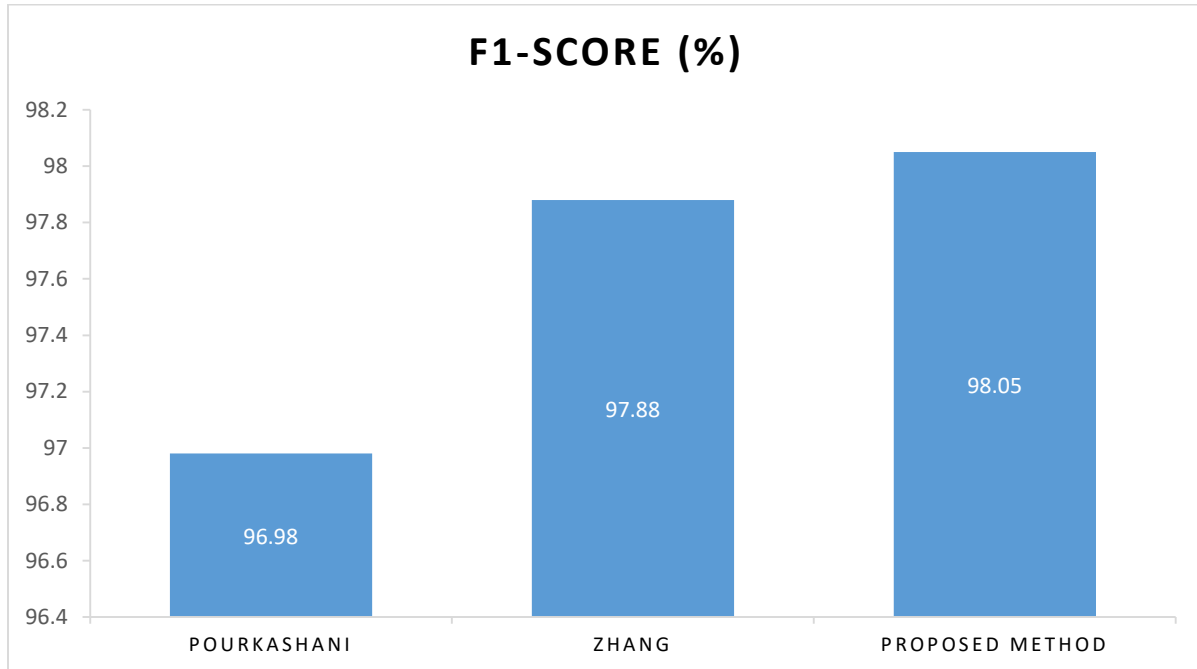


Figure 4.13:F1-Score Comparison with other methods

It is clearly shown that the F1-Score achieved in the proposed state-of-the-art method is 98.05% which is better than other methods that have been compared in the above graph.

In the above comparisons of the proposed method with other state-of-the-art methods using multiple evaluation metrics have shown that the proposed method is more efficient than other compared methods. Hence, it is proved that the NSS features clearly have a far better capability for CMFD as compared to other methods that are compared in the above graphs.

Chapter 5

Conclusion and Future Work

A technique to identify copy move image forgeries is proposed by extracting the NSS features. An algorithm is carried out using the NSS feature dataset extracted from the famous publicly available MICC-F2000 dataset. Also, the performance of the proposed method is quantitatively assessed using the accuracy, TPR, FPR, TNR, recall and the F1-score. The best model of the proposed method has produced the result of 98% accuracy and 97.11% TPR. Also, it has produced 1.04% FPR, 98.95% TNR, 99.01% recall and the F1-Score of 98.05% on MICC-F2000 database. Though the proposed technique attained a little bit lower results in terms of TPR, but it produces much superior results in terms of accuracy and TNR. Many researchers are keen to produce better and better results in this scope, as image forgery tools are evolving day by day so there is a need to improve IFD methods as much as needed to protect images from any type of forgeries.

In future a method may be built to overcome the limitations mentioned in this paper. As a unique idea is presented in this paper to detect forgeries, many researchers are working in an innovative style to extract new ideas and approaches to improve the image forensic systems. So, a need of capturing new techniques of image tampering have to be fulfilled. A novel technique has been introduced in this paper for CMFD using NSS features, these features can be utilized further in far better way to enhance the IFD techniques in future. Furthermore, the selection of ML models can be better to achieve best results such as neural network etc. Only three types of NSS features are used in this research, more types of NSS features can also be used to achieve more efficient results. So, there is a new way for the researchers to increase the efficiency of image forensic tools by using more NSS features along with the other type of ML models for IFD.

References:

- [1] A.Kumar, C.S. Prakash, S. Maheshkar and V. Maheshkar, "Markov Feature Extraction Using Enhanced Threshold Method for Image Splicing Forgery Detection". In Smart Innovations in Communication and Computational Sciences Springer, Singapore (2019)17-27.
- [2] S. Agarwal and S.Chand, "Image forgery detection using co-occurrence-based texture operator in frequency domain". In Progress in Intelligent Computing Techniques: Theory, Practice, and Applications Springer, Singapore. (2018)117-122.
- [3] M.H.Alkawaz, G.Sulong, T. Saba and A. Rehman, "Detection of copy-move image forgery based on discrete cosine transform". Neural Computing and Applications, 30(1) (2016) 183-192.
- [4] A.Parveen, Z.H. Khan and S.N.Ahmad, "Block-based copy-move image forgery detection using DCT". Iran Journal of Computer Science, (2019)1-11.
- [5] W.Shan, Y. Yi, J. Qiu and A.Yin, "Robust Median Filtering Forensics Using Image Deblocking and Filtered Residual Fusion". IEEE Access, 7 (2019) 17174-17183.
- [6] X.Y. Wang, L.X. Jiao, X.B. Wang, H.Y. Yang and P.P. Niu, "A new keypoint-based copy move forgery detection for color image". Applied Intelligence, 48(10)(2018)3630-3652.
- [7] S.Sadeghi, S. Dadkhah, H.A. Jalab, G.Mazzola and D.Uliyan, "State of the art in passive digital image forgery detection: copy-move image forgery". Pattern Analysis and Applications, 21(2) (2018) 291-306.
- [8] Zaid Nidhal Kudhair, Dr. Farhan Mohamed, Karrar A. Kadhim, "A Review on Copy-Move Image Forgery Detection Techniques", Journal of Physics: Conference Series, 1892 (2021) 012010.
- [9] Pooja Bhole, Dipak Wajgi, "An Image Forgery Detection using SIFT-PCA", International Journal of Engineering Research & Technology 2020.
- [10] Akram Hatem Saber, Mohd Ayyub Khanl, Basim Galeb Mejbel, "A Survey on Image Forgery Detection Using Different Forensic Approaches", Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 3, 361-370 (2020).
- [11] Kunj Bihari Meena and Vipin Tyagi, "A hybrid copy-move image forgery detection technique based on Fourier-Mellin and scale-invariant feature Transforms", Multimedia Tools and Applications, 2020.
- [12] Badal Soni, Pradip K.Das, Dalton Meitei Thounaojam, "CMFD: a detailed review of block based and key feature based techniques in image copy-move forgery detection", IET Image Process., 2018, Vol. 12 Iss. 2, pp. 167-178.
- [13] Kunj Bihari Meena, Vipin Tyagi, "A copy-move image forgery detection technique based on tetrolet transform", Journal of Information Security and Applications, 52 (2020) 102481.
- [14] Ansari MD, Ghrera SP, Tyagi V., "Pixel-Based image forgery detection: a review", IETE J Educ 2014;55(1):40–6.
- [15] Meena KB, Tyagi V., "Image forgery detection : survey and future directions", Data, Engineering and Applications, 2. Singapore: Springer; 2019. p. 163–95.
- [16] Hamid Rahim Sheikh, "No-Reference Quality Assessment Using Natural Scene Statistics:JPEG2000", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 14, NO. 11, NOVEMBER 2005.
- [17] D. L. Ruderman, "The statistics of natural images," Network: Comput. Neur. Syst., vol. 5, no. 4, pp. 517–548, Nov. 1994.

- [18] D. J. Field, "Relations between the statistics of natural images and the response properties of cortical cells," *J. Opt. Soc. Amer.*, vol. 4, no. 12, pp. 2379–2394, 1987.
- [19] Savita Walia & Krishan Kumar (2019) "Digital image forgery detection: a systematic scrutiny", *Australian Journal of Forensic Sciences*, 51:5, 488-526 2019.
- [20] Farid H., "Image forgery detection", *IEEE Signal Process Mag.* 2009; 26(2):16–25.
- [21] Reis G., "Digital image integrity", San Jose, CA; 1999.
- [22] Mhiripiri NA, Chari T. *Media law, ethics, and policy in the digital age*. United States of America: IGI Global; 2017.
- [23] Birajdar GK, Mankar VH. , "Digital image forgery detection using passive techniques : a survey", *Digit Investig.* 2013; 10(3):226–245.
- [24] Ali M, Deriche M, "A bibliography of pixel-based blind image forgery detection techniques", *Signal Process Image Commun.* 2015;39:46–74.
- [25] Abd Warif NB, Abdul Wahab AW, Idna Idris MY, Ramli R, Salleh R, Shamshirband S, Choo KR, "Copy-move forgery detection : survey", challenges and future directions. *J Netw Comput Appl.* 2016;75:259–278.
- [26] Mahmood T, Nawaz T, Ashraf R, Shah M, Khan Z, Irtaza A, Mehmood Z. "A survey on block based copy move image forgery detection techniques". *International Conference on Emerging Technologies (ICET)*, 2015.
- [27] Farid H. , "Digital doctoring: Can we trust photographs?" *Decept From Anc Empires to Internet Dating.* 2009:95–108.
- [28] Adobe Photoshop elements. Adobe Syst; 2016. [Online]. [cited 2017 Sep 9].
- [29] PIXLR. [Online]. [cited 2017 Sep 9].
- [30] GNU image manipulation program (GIMP); 2017. [cited 2017 Sep 9].
- [31] Chang IC, Yu JC, Chang CC , "A forgery detection algorithm for exemplar-based inpainting images using multi-region relation". *Image Vis Comput* 31(1):57–71 (2013).
- [32] Pun CM, Yuan XC, Bi XL (2015) "Image forgery detection using adaptive over-segmentation and feature point matching". *IEEE Trans Info Forensics Secur* 10(8):1705–1716.
- [33] Singh A, Singh G, Singh K , "A Markov based image forgery detection approach by analyzing CFA artifacts", *Multimed Tools Appl* 77(21):28949–28968 (2018).
- [34] Yuan Y, Yang X, Wu W, Li H, Liu Y, Liu K, "A fast single-image super-resolution method implemented with CUDA", *J Real-Time Image Proc* 16(1):81–97 2019.
- [35] Tariang DB, Chakraborty RS, Naskar R, "A robust residual dense neural network for countering Antiforensic attack on median filtered images", *IEEE Signal Process Lett* 26(8):1132–1136 2019.
- [36] Elaskily MA, Elnemr HA, Dessouky MM, Faragallah OS, "Two stages object recognition based copymove forgery detection algorithm", *Multimed Tools Appl* 78(11):15353–15373 (2019).
- [37] Abhishek, Neeru Jindal, "Copy Move and Splicing Forgery Detection using deep convolutional neural network, and semantic segmentation", Springer Science+Business Media, LLC, part of Springer Nature 2020.
- [38] Nirmala G, Thyagarajan KK, "A modern approach for image forgery detection using BRICH clustering based on normalised mean and standard deviation", *International Conference on Communication and Signal Processing (ICCSP)*: 0441-0444 2019.

- [39] Kakar P, Sudha N, Ser W, “Exposing digital image forgeries by detecting discrepancies in motion blur”, *IEEE Trans Multimed* 13(3):443–452 (2011).
- [40] Christlein V, Riess C, Jordan J, Riess C, Angelopoulou E, “An evaluation of popular copy-move forgery detection approaches”, *IEEE Trans Info Forensics Secur* 7(6):1841–1854 2012.
- [41] De Carvalho TJ, Riess C, Angelopoulou E, Pedrini H, de Rezende Rocha A, “Exposing digital image forgeries by illumination color classification”. *IEEE Trans Info Forensics Secur* 8(7):1182–1194 2013.
- [42] Costanzo A, Amerini I, Caldelli R, Barni M, “Forensic analysis of SIFT keypoint removal and injection”, *IEEE Trans Info Forensics Secur* 9(9):1450–1464 2014.
- [43] Zhang Y, Thing VL, “A multi-scale noise-resistant feature adaptation approach for image tampering localization over Facebook”, In 2017 IEEE 2nd International Conference on Signal and Image Processing (ICSIP): 272-276 2017.
- [44] Yang F, Li J, Lu W, Weng J, “Copy-move forgery detection based on hybrid features”, *Eng Appl Artif Intell* 59:73–83 2017.
- [45] Muhammad G, Al-Hammadi MH, Hussain M, Bebis G, “Image forgery detection using steerable pyramid transform and local binary pattern”, *Mach Vis Appl* 25(4):985–995 2014.
- [46] Neenu HU, Cheriyan J, “Image forgery detection based on illumination inconsistencies & intrinsic resampling properties”. In 2014 Annual International Conference on Emerging Research Areas: Magnetics, Machines and Drives (AICERA/iCMMD): 1-6 2014.
- [47] Le THN, Luu K, Savvides M, “Fast and robust self-training beard/moustache detection and segmentation”, In 2015 international conference on biometrics (ICB): 507-512 2015.
- [48] Carvalho T, Faria FA, Pedrini H, Torres RDS, Rocha A, “Illuminant-based transformed spaces for image forensics”, *IEEE Trans Info Forensics Secur* 11(4):720–733 2015.
- [49] Monson NS, Kumar KM, “Behaviour knowledge space-based fusion for image forgery detection”, In 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT) (pp. 400-403). IEEE 2017.
- [50] Cristin R, Ananth JP, Raj VC, “Illumination-based texture descriptor and fruitfly support vector neural network for image forgery detection in face images”. *IET Image Process* 12(8):1439–1449 2018.
- [51] Muzaffer G, Ulutas G, “A new deep learning-based method to detection of copy-move forgery in digital images”. In 2019 Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science (EBBT): 1-4 2019.
- [52] Liu Q, “An improved approach to exposing JPEG seam carving under recompression”, *IEEE Trans Circuits Syst Vid Technol* 29(7):1907 2018.
- [53] Long J, Shelhamer E, Darrell T, “Fully convolutional networks for semantic segmentation”, In Proceedings of the IEEE conference on computer vision and pattern recognition: 3431-3440 2015.
- [54] Fridrich J, Soukal D, Lukáš J. , “Detection of copy-move forgery in digital images”, *Digit Forensic Res Work* ;3:652–63 2003.
- [55] Meena KB, Tyagi V. , “Image forgery detection : survey and future directions”, *Data, Engineering and Applications*, 2. Singapore: Springer; 2019. p. 163–95.
- [56] Cozzolino D, Poggi G, Verdoliva L., “Efficient dense-field copy-move forgery detection”, *IEEE Trans Inf Forensics Secur* 2015;10(11):2284–97.

- [57] Wang X, Li S, Liu Y., “A new keypoint-based copy-move forgery detection for small smooth regions”, *Multimed Tools Appl* 2016;76(22):23353–82.
- [58] Al-Qershi OM, Khoo BE., “Enhanced block-based copy-move forgery detection using k-means clustering”, *Multidimens Syst Signal Process* 2018;30:1671–95.
- [59] Chen B, Yu M, Su Q, Li L. , ”Fractional quaternion cosine transform and its application in color image copy-move forgery detection”, *Multimed Tools Appl* 2018;78:8057–73.
- [60] Mahmood T, Irtaza A, Mehmood Z, Tariq Mahmood M. , ”Copy–move forgery detection through stationary wavelets and local binary pattern variance for forensic analysis in digital images”, *Forensic Sci Int Oct.* 2017; 279:8–21.
- [61] Mahmood T, Mehmood Z, Shah M, Saba T., “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* 2018; 53:202–14.
- [62] Meena KB, Tyagi V., “A copy-move image forgery detection technique based on Gaussian-Hermite moments”, *Multimed Tools Appl* 2019; 78:33505–26.
- [63] Pan X, Lyu S., “Region duplication detection using image feature matching”, *IEEE Trans Inf Forensics Secur* 2010; 5:857–67.
- [64] Pun C, Yuan X, Bi X, “Image forgery detection using adaptive oversegmentation and feature point matching”, *IEEE Trans Inf Forensics Secur* 2015;10(8):1705–16.
- [65] Wenchang S, Fei Z, Bo Q, Bin L, “Improving image copy-move forgery detection with particle swarm optimization techniques”, *China Commun* 2016; 10(1):139–49.
- [66] Zandi M, Mahmoudi-Aznavah A, Talebpour A, ”Iterative copy-move forgery detection based on a new interest point detector”. *IEEE Trans Inf Forensics Secur* 2016; 11(11):2499–512.
- [67] Wang X-Y, Jiao L-X, Wang X-B, Yang H-Y, Niu P-P, “Copy-move forgery detection based on compact color content descriptor and delaunay triangle matching”, *Multimed Tools Appl* 2018; 78(2):2311–44.
- [68] Meena KB, Tyagi V, “A hybrid copy-move image forgery detection technique based on Fourier-Mellin and scale invariant feature transforms”, *Multimed Tools Appl* 2020.
- [69] Shilpa Dua, Jyotsna Singh, Harish Parthasarathy, “Image forgery detection based on statistical features of block DCT coefficients”, *Procedia Computer Science* 171 (2020) 369–378.
- [70] Y. Q. Shi, C. Chen, W. Chen, “A natural image model approach to splicing detection”, in : *Proceedings of the 9th Workshop on Multimedia & Security, MM& ;Sec ’07*, ACM, New York, NY, USA, 2007, pp. 51–62.
- [71] Z. He, W. Lu, W. Sun, J. Huang, “Digital image splicing detection based on markov features in dct and dwt domain”, *Pattern Recogn.* 45 (12) (2012) 4292–4299.
- [72] c. li, Q. Ma, L. Xiao, M. Li, A. Zhang, “Image splicing detection based on markov features in QDCT domain”, *Neurocomputing* 228 2016.
- [73] A. J. Fridrich, B. D. Soukal, A. J. Lukáš, “Detection of copy-move forgery in digital images”: in *Proceedings of Digital Forensic Research Workshop*, 2003.
- [74] M. H. Alkawaz, G. Sulong, T. Saba, A. Rehman, “Detection of copy-move image forgery based on discrete cosine transform”, *Neural Comput. Appl.* 30 (1) (2016) 183–192.
- [75] Y. Cao, T. Gao, L. Fan, Q. Yang, “A robust detection algorithm for copy-move forgery in digital images”, *Forensic science international* 214 (2011) 33–43.

- [76] K. Hayat, T. Qazi, "Forgery detection in digital images via discrete wavelet and discrete cosine transforms", *Comput. Electr. Eng.* 62 (C) (2017) 448–458.
- [77] A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, G. Bebis, H. Mathkour, "Passive detection of image forgery using DCT and local binary pattern", *Signal, Image and Video Processing 11* Springer-Verlag London, 2016. doi:10.1007/s11760-016-0899-0.
- [78] C. S. Prakash, A. Kumar, S. Maheshkar, V. Maheshkar, "An integrated method of copy-move and splicing for image forgery detection", *Multimedia Tools Appl.* 77 (20) (2018) 26939–26963.
- [79] Fridrich, A. Jessica, B. David Soukal, and A. Jan Lukáš. "Detection of copy-move forgery in digital images." In *Proceedings of Digital Forensic Research Workshop*. 2003.
- [80] Ryu SJ, Lee MJ, Lee HK, "Detection of copy-rotate-move forgery using Zernike moments". In: *IEEE International workshop on Information Hiding (IH)*. Springer, Berlin, pp 51–65 (2010).
- [81] Amerini I, Ballan L, Caldelli R, Bimbo AD, Serra G, "A SIFT-based forensic method for copymove attack detection and transformation recovery", *IEEE Trans Inf Forensics Secur* 6(3):1099–1110 (2011).
- [82] Pan X, Lyu S, "Region duplication detection using image feature matching", *IEEE Trans Inf Forensics Secur* 5(4):857–67 (2010).
- [83] Chen, Chien-Chang, Wei-Yu Lu, and Chung-Hsuan Chou. "Rotational copy-move forgery detection using SIFT and region growing strategies." *Multimedia Tools and Applications* 78, no. 13 (2019): 18293-18308.
- [84] Jin, Guonian, and Xiaoxia Wan. "An improved method for SIFT-based copy–move forgery detection using non-maximum value suppression and optimized J-Linkage." *Signal Processing: Image Communication* 57 (2017): 113-125.
- [85] Shivakumar BL, Baboo S. "Detection of region duplication forgery in digital images using SURF", *International Journal of Computer Science Issues* 8(4) (2011):199–205.
- [86] Dhivya, S., J. Sangeetha, and B. Sudhakar. "Copy-move forgery detection using SURF feature extraction and SVM supervised learning technique." *Soft Computing* (2020): 1-12.
- [87] Anush Krishna Moorthy, Alan Conrad Bovik, "Blind Image Quality Assessment: From Natural Scene Statistics to Perceptual Quality", *IEEE transactions on image processing*, VOL. 20, NO. 12, DECEMBER 2011.
- [88] M. Wainwright and E. Simoncelli, "Scale mixtures of Gaussians and the statistics of natural images," *Adv. Neural Inf. Process. Syst.*, vol. 12, no. 1, pp. 855–861, 2000.
- [89] Q. Li and Z. Wang, "Reduced-reference image quality assessment using divisive normalization-based image representation," *IEEE J. Select. Topics Signal Process.*, vol. 3, no. 2, pp. 202–211, Apr. 2009.
- [90] E. P. Simoncelli, W. T. Freeman, E. H. Adelson, and D. J. Heeger, "Shiftable multiscale transforms," *IEEE Trans. Inf. Theory*, vol. 38, no. 2, pp. 587–607, Mar. 1992.
- [91] B. A. Olshausen and D. J. Field, "How close are we to understanding V1?," *Neural Computat.*, vol. 17, no. 8, pp. 1665–1699, 2005.
- [92] R. Sekuler and R. Blake, *Perception*. New York: McGraw-Hill, 2002.
- [93] Lixiong Liu, Bao Liu, Hua Huang, Alan Conrad Bovik, "No-reference image quality assessment based on spatial and spectral entropies", *Signal Processing: Image Communication* 29 (2014) 856–863.
- [94] J. Sponring, "The entropy of scale-space", in: *Proceedings of the 13th International Conference on Pattern Recognition*, vol. 1, August 1996, pp. 900–904.

- [95] H.R. Sheikh, A.C. Bovik, "Image information and visual quality", *IEEE Trans. Image Process.* 15 (2) (2006) 430–444.
- [96] D.L. Ruderman, "The statistics of natural images", *Netw. Comput. Neural Syst.* 5 (4) (1994) 517–548.
- [97] Lixiong Liu, Yi Hua, Qingjie Zhao, Hua Huang, Alan Conrad Bovik, "Blind image quality assessment by relative gradient statistics and adaboosting neural network", *Signal Processing: Image Communication* 40 (2016) 1–15.
- [98] D.H. Hubel, T.N. Wiesel, "Receptive fields, binocular interaction and functional architecture in the cat's visual cortex", *J. Physiol.* 160 (1) (1962) 106–154.
- [99] M. Clark, A.C. Bovik, "Experiments in segmenting texton patterns using localized spatial filters", *Pattern Recognit.* 22 (6) (1989) 707–717.
- [100] D.G. Lowe, "Distinctive image features from scale-invariant keypoints", *Int. J. Comput. Vis.* 60 (2) (2004) 91–110.
- [101] K. Velmurugan, S.S. Baboo, "Image retrieval using harris corners and histogram of oriented gradients", *Int. J. Comput. Appl.* 24 (7) (2011) 6–10.
- [102] Areej S. Alfraih, Johann A. Briffa, Stephan Wesemeyer "Cloning Localization Based on Feature Extraction and K-means Clustering", Springer International Publishing Switzerland 2015 Y.-Q. Shi et al. (Eds.): *IWDW 2014, LNCS* 9023, pp. 410–419, 2015.
- [103] Loai Alamro, Nooraini Yusoff, "Copy-Move Forgery Detection using Integrated DWT and SURF", e-ISSN: 2289-8131 Vol. 9 No. 1-2 2017.
- [104] D. Vaishnavi, G. N. Balaji, D. Mahalakshmi "KAZE Feature Based Passive Image Forgery Detection", Springer Nature Singapore Pte Ltd. 2019 R. S. Bapi et al. (eds.), *First International Conference on Artificial Intelligence and Cognitive Computing*, *Advances in Intelligent Systems and Computing* 815.
- [105] Ava Pourkashani, Asadollah Shahbahrami, Alireza Akoushideh, "Copy-move forgery detection using convolutional neural network and K-mean clustering", *International Journal of Electrical and Computer Engineering (IJECE)* Vol. 11, No. 3, June 2021, pp. 2604~2612.
- [106] Yi-Jia Zhang, Tong-Tong Shi, "Image Splicing Detection Scheme Based on Error Level Analysis and Local Binary Pattern", *Journal of Network Intelligence Taiwan Ubiquitous Information* Volume 6, Number 2, May 2021.
- [107] Abdullah Alharbi, Wajdi Alhakami, "Inpainting forgery detection using hybrid generative/discriminative approach based on bounded generalized Gaussian mixture model", *Applied Computing and Informatics* 2019.
- [108] Yong Yew Yeap, U.U. Sheikh, Ab Al-Hadi Ab Rahman, "Image Forensic for Digital Image Copy Move Forgery Detection", 2018 IEEE 14th International Colloquium on Signal Processing & its Applications (CSPA 2018), 9 -10 March 2018, Penang, Malaysia.