FEATURE DEVELOPMENT BASED ON CFA ARTIFACTS FOR IMAGE FORGERY DETECTION

Dissertation submitted towards the partial fulfilment of the requirement for the award of degree of

Master of Engineering

in

Wireless Communication

Submitted by:

Amneet Singh

Roll No: 801463002

Under the guidance of:

Dr. Kulbir Singh

Professor, ECED

ELECTRONICS AND COMMUNICATION ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004 (PUNJAB)

JULY 2016

DECLARATION

I, **Amneet Singh**, hereby declare that the dissertation entitled, **"Feature Development based on CFA artifacts for Image Forgery Detection"**, is an authentic work carried out by me towards the partial fulfilment for the award of degree of Masters of Engineering (ME) in Wireless Communication (WC), accomplished under the esteemed guidance of **Dr. Kulbir Singh**, Professor, Electronics and Communication Department, Thapar University, Patiala, and refer other's research work which are listed in the reference section.

The content presented in this dissertation has not been submitted in any form in other University/Institute for the award of any other degree.

Date: 13/07/2016

Amneet Singh

Roll No: 801463002

This is certified that the above statement made by the student is correct to best of my knowledge and belief.

Date: 13/07/2016.

Kulbir Singh

Professor, ECED

Thapar University, Patiala

Countersigned by:

Sanjay Sharma

Professor and Head, ECED

Thapar University, Patiala

S. S. Bhatia

Dean of Academic Affairs

Thapar University, Patiala

ACKNOWLEDGEMENT

Firstly, I want to thank the Almighty God for providing me good health, well-being, and ample patience that was necessary for carrying out my thesis work.

I would like to express my gratitude to **Dr. Kulbir Singh**, Professor, Electronics and Communications Department, Thapar University, Patiala, for his patient guidance and substantial support throughout my work. I am truly very fortunate to have the opportunity to work under his esteemed counsel.

I am also thankful to **Dr. Sanjay Sharma**, Professor and the Head of the Department, **Dr. Amit Kumar Kohli**, Associate Professor and PG Coordinator, and **Dr. Hemdutt Joshi**, Assistant Professor and Program Coordinator, for providing me with adequate environment to carry out my work. I would like to extend my thanks to **Dr. Neeru Jindal**, Assistant Professor for her valuable inputs and concern.

I am profoundly grateful to my parents and my loving sister for their constant encouragement, attention and support. I would like to acknowledge my friends for their devoted help and time any way possible to make my work successful. I am highly indebted to **Mr. Gurinder Singh** and **Ms. Nidhi Jamwal** for their constant support and utmost cooperation in carrying out my work.

Finally, I would like to express thanks to all those persons who directly or indirectly helped me and contributed towards this work.

Amneet Singh

801463002

ABSTRACT

Nowadays, a lot of information is being shared in the form of digital images. Along with the actual images, there are some cases when misleading information is being shared in the form of tampered images. Thus, there is a need to curb these incidents so that the reliable information can reach the masses. These issues can be handled through 'Digital Image Forensics'.

The basic ideology behind Digital Image Forensics is to reconstruct the image history, also known as 'Digital Image Life Cycle'. It includes all the steps that are involved to make the real scene a digital image. It starts from the real scene acquisition and all the in-camera and post-camera processing techniques which leads an image to its final fruition. This has been observed that each process in the digital image life cycle, leaves a distinct trace or fingerprint that can be analyzed while reconstructing the image history. The inconsistencies in the fingerprint can be sufficient to expose the forgery that has been introduced in the image.

The motivation of this report is to analyze the fingerprints left during the interpolation process. The image interpolation process is to assign the values to the pixels that were not gathered when the light was filtered by the Color Filter Array (CFA). The interpolation technique employs a demosaicing algorithm that assign the values to the missing pixels. In doing so, the algorithm leaves a certain trace, known as CFA artifacts, whose presence can lead to the identification of the demosaicing algorithm. The inclusion of forgery in the image would conclusively remove or alter the structure of the present CFA artifacts.

A scheme is proposed which finds out the probability of the presence or absence of the CFA artifacts in a 2x2 blocks of image. The probability is based on the standard deviation as well as skewness of the prediction error that is calculated between the acquired and interpolated pixels. This probability is then used to create a forgery map that depicts the region(s) that has been tampered with.

The approach is compared with previous approaches and the results have been discussed. The proposed scheme is also applied on a few doctored images that have been taken from social networking websites. The performance analysis of the scheme is performed on UCID image dataset that provided 80% accuracy.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS

ASD	Sum of Absolute Difference
CCD	Charge Coupled Device
CFA	Color Filter Array
CMOS	Complementary Metal Oxide Semiconductor
CRF	Camera Response Function
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
EM	Expectation Maximization
GMM	Gaussian Mixture Model
IDCT	Inverse Discrete Cosine Transform
JPEG	Joint Photographic Experts Group
LPIP	Locally Planar Irradiance Points
MAP	Maximum a-posteriori Estimation
MSE	Mean Square Error
PCA	Principal Component Analysis
PIB	Press Information Bureau
PRNU	Photo Response Non Uniformity
PSNR	Peak Signal-to-Noise Ratio
RGB	Red Green Blue
ROC	Receiver Operating Characteristic curve
SD	Standard Deviation
SIFT	Scale Invariant Feature Transform
SSIM	Structural Similarity Index
SVM	Support Vector Machine
WWW	World Wide Web

Chapter 1

Introduction

1.1 Preamble

The world is a beautiful place where a lot is happening each moment. It is observing new discoveries and inventions, and technological advancements every second. Thus, there is a requirement to spread the word about these developments across the world. This constraint leads to the foundation of a proper and secure communication system. Through this communication system, information, thoughts, and ideas can be shared in the form of text documents, images, and videos etc. The growth of World Wide Web (WWW) and easy availability of the technology through smartphones, a bulk of information is now being shared on the internet. Images, unlike text, are a competent and innate mode of communication for humans, due to their immoderacy and the ease in understanding the content it contains. There has always been confidence in the solidity of the visual data in form of image. The picture printed in a newspaper is generally received to be actual and true. This applies same to the video surveillance recordings and can be used as probationary material in legal issues as evidence [1].

The rapid dispersal of cheap and easy to use devices, the visual content of an image being altered. This leads to the sharing of misleading information through images. Thus, there is a need to curb these forgery attacks so as to make sure right or actual information is being shared. Digital Image Forensics is the branch of digital image research field dealing with the validation and authentication of the image, through recovering information of the image and testing its source. This situation focuses the requirement for techniques which allow the restoration of the history of a digital image in order to validate its trustworthiness and evaluate its integrity. Two important objectives about the account and integrity of an image can be stated as: i) The device with which the image has been captured, and ii) if the image is originally captured or is computer generated. The first objective is of prime concern

when the information of the tangible acquisition device of the image portrays as the proof itself since it specifies that the device or user that developed the picture; the second objective has more practical importance. These cases are the one where almost no evidence can be gathered to be known *a priori* about the original image. Thus, the detection approach has to be carried out in a blind way [1].

1.2 History of Image Tampering

Though photo tampering has become more familiar in the age of digital cameras and image editing software, it actually dates back almost as far as the invention of photography. Photography lost its purity many years ago. Only a few decades after Niepce created the first photograph in 1814, photographs were already being manipulated. With the advent of high-resolution digital cameras, powerful personal computers and sophisticated photo-editing software, the manipulation of photos are becoming more common [2].

Figure 1.1: A doctored image of Russian team of cosmonauts [2].

On April 12, 1961, a Russian team of cosmonauts led by Yuri Gagarin, was the first humans to complete an orbit of the earth. One of the cosmonauts, Grigoriy Nelyubov, was removed from a photo of the team taken after their journey. Nelyubov had been expelled from the program for misbehavior.

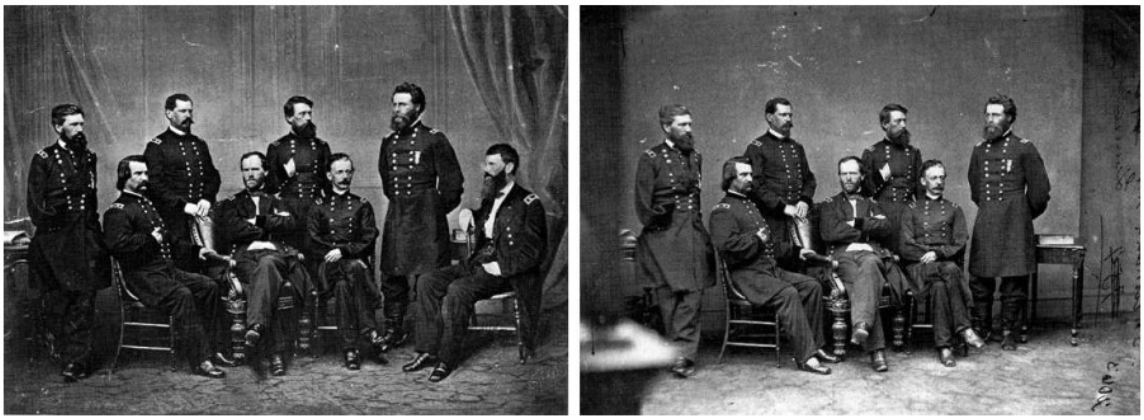


Figure 1.2: A doctored image of U. S. Generals [2].

In this photo by famed photographer Mathew Brady back in 1865, General Sherman is seen posing with his Generals. General Francis P. Blair, shown on the far right, was inserted into this photograph.

Figure 1.3: A doctored image of Queen Elizabeth with Canadian Prime Minister [2].

In this doctored photo from 1939 of Queen Elizabeth and Canadian Prime Minister William Lyon Mackenzie King in Banff, Alberta, King George VI was removed from the original photograph. This photo was used on an election poster for the Prime Minister. It is hypothesized that the Prime Minister had the photo altered because a photo of just him and the Queen painted him in a more powerful light.

1.3 Digital Image Life Cycle

The digital image life cycle can be portrayed as a combination of various steps, namely, acquisition phase, coding phase, and editing phase. In the acquisition phase, the light coming from the real scene is gathered by the digital camera and is then focused on the camera sensor (CCD or CMOS) by the camera lens. The digital image signal is produced in this step only. The light is generally filtered by the CFA (Color Filter Array) before it reaches the sensor. CFA is basically a thin film on the sensor that allows only a certain amount of light to go through it. To each pixel, only one color of Red, Green, or Blue is allotted. The sensor output is then interpolated to acquire all the colors for each pixel to develop a full color image. This process is known as demosaicing process. This signal goes through additional in-camera processing steps that is generally employed to enhance the perception of the image. These processes include the processes like color processing, white balancing, contrast enhancement, image sharpening, gamma correction etc. [1].

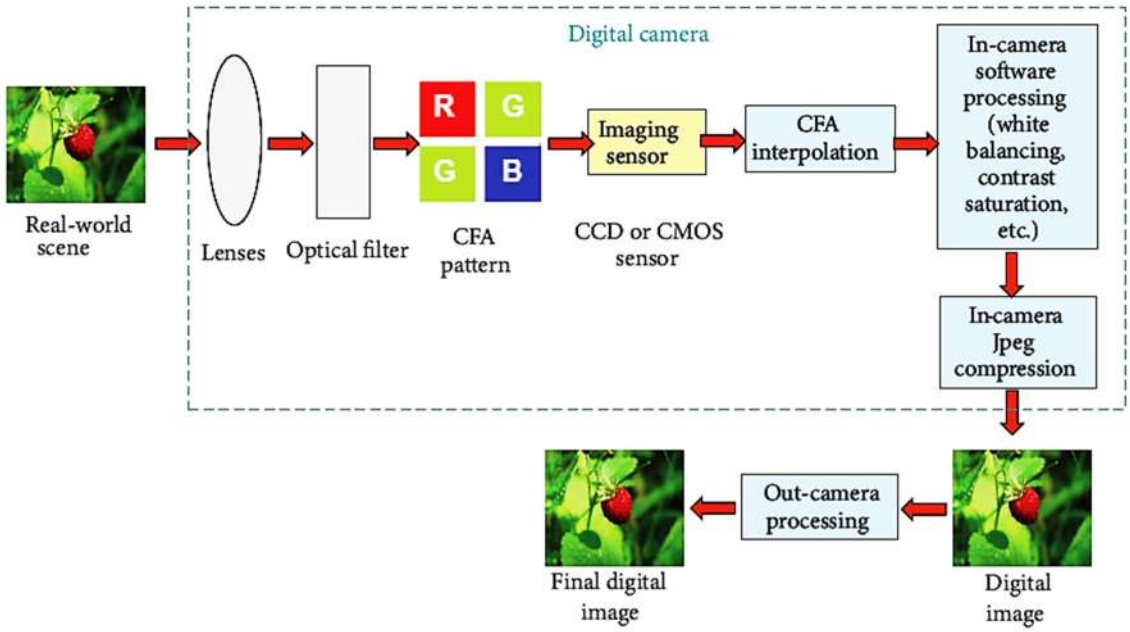


Figure 1.4: A scheme portraying the steps involved in a digital image life cycle [1].

The processed signal is then stored in the camera memory with the application of coding technique. In most commercially used cameras, the lossy compression, JPEG being

specific, is used because a load of memory is saved while storage. Ultimately, the produced image can be post-processed to improve or to alter its information. Various image editing processes can be experienced by an image during its life cycle: the most common being the blurring, contrast adjustment, sharpening, image splicing, geometric transformation (scaling, rotation, etc.), and image splicing (developing an image with one or more parts of the image), and cloning (or copy-move, the creation of the similar image). Finally, after editing, the image is compressed in JPEG format, so that it can be recompressed afterwards [1].

The fundamental thought of digital image forensics is the analysis of the characteristic traces (like digital fingerprints) that are left behind in a digital image during both the acquisition step and other consecutive processes happening during its life cycle. Thus, these digital traces can be isolated for evaluation of the image and apprehending the history of digital information. According to the demonstration of the digital image life cycle, these traces can be categorized in three classes of fingerprints, namely, acquisition fingerprints, coding fingerprints, and editing fingerprints [1].

1.3.1 Image Acquisition

Image Acquisition is the primary step in the digital image life cycle. In image acquisition, the real image scene is clicked by a camera and a few in-camera processing is performed on the image. The light coming from the object is projected on the camera lens which is then passed to the optical filter. Optical filters are devices that selectively transmit light of different wavelengths, usually implemented as plain glass or plastic devices in the optical path which is either dyed in the bulk or has interference coatings. Optical filters selectively transmit light in a particular range of wavelengths, that is, colors, while blocking the remainder. They are basically used to restrict the light from the object to a limited spectral band of interest.

The light after filtered by optical filters is projected on a CFA pattern. The most commonly used CFA pattern is the Bayer's pattern. The Bayer's pattern is a mosaic of three colors Red (R), Green (G), and Blue (B). The basic ideology behind the Bayer filter pattern is that any color can be represented as a combination of these three colors, i.e. red, green and blue.

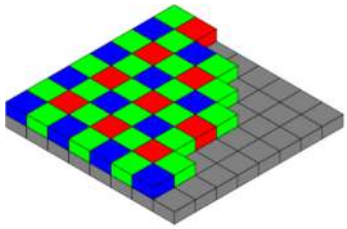


Figure 1.5: The Bayer arrangement of color filters on the pixel array of an image sensor [3].

The mosaic contains RGB color filters arranged in a manner with Red and Blue color filters on adjacent rows with Green color filters placed between the same color filters. The number of green filters in the mosaic is twice the number of red and blue color filters because the human visual system is highly sensitive to the green color than any of the colors due to luminance perception of the human eye [3]. For each pixel, only one color is assigned from the RGB color channels. The output of the Bayer's filter is known as Bayer's pattern image. It is an incomplete image as the true color is not allotted to the pixels.

This can be done through image interpolation. Image interpolation processes to fill the missing pixel values based on an algorithm which uses the neighboring pixel values to assign the values to the new pixels. The algorithm used for the interpolation process is known as a demosaicing algorithm. A demosaicing (also de-mosaicing, demosaicking or debayering) algorithm is a digital image process used to develop a full-color image from the incomplete color samples output from an image sensor surfaced with a CFA. It is also known as CFA interpolation or color reconstruction. As the interpolation is done by following a certain algorithm, some kind of artifacts are left in the image due to it [3].

After a full-color image has been obtained, to improve the quality of the image, some in-camera processing operations, like white balancing, contrast adjustment can be applied. The color map image received after the CFA interpolation can be assumed to be a RAW image as it is minimally processed. The processing techniques applied to the RAW image is done to enhance or improve the reception of image by a user. The content of the image is not altered, just adjusted in a way so that it can be perceived properly [3].

(a) (b)

Figure 1.6: An example demonstrating difference between (a) a RAW image and (b) an in-camera processed image [2].

1.3.2 Image Coding

The next main step in the digital image life cycle is the image coding. Image coding is basically done to save the image in a manner so that it can be used or reconstructed afterward. If the image is stored pixel by pixel it would consume a lot of space. The image contains some high-frequency components that are undetectable to the human eye. Thus, the presence or absence of these components would not create any difference to the perception of the image. But, if these components are omitted, a lot of memory would be saved. This process is generally known as image compression.

The objective of image compression is to reduce irrelevance and redundancy of the image data in order to be able to store or transmit data in an efficient form. An image is full of these redundancies, thus can be compressed to a large extent. There are basically two types of image compression, namely, lossless and lossy. Lossless is the one in which the each pixel value is considered, whether high frequency or not, and lossy being the one in which high-frequency components are discarded [4]. The lossless compression is preferred for medical imaging as the resolution preservation of the image is an important aspect. The lossy compression is used for most practical purposes with JPEG compression a widely used one. The basic steps involved in JPEG compression are discussed as follows.

The first step in the JPEG compression is Discrete Cosine Transform (DCT). The DCT of the image is performed by dividing the whole image into 8×8 blocks. The DCT provide us with DCT coefficients $D_{i,j}$ (ij-th coefficient from each 8×8 block in the image) [4].

$$D_{i,j} = \sum_{k,l=0}^{7} a_{k,l}(i,j) B_{k,l} \tag{1.1}$$

where B is the 8×8 block,

$$a_{k,l} = \frac{1}{4} w(k) w(l) \cos\frac{\pi}{16} k(2i+1) \cos\frac{\pi}{16} k(2j+1) \tag{1.2}$$

and

$$w(k) = \begin{cases} 1/\sqrt{2}, & k = 0 \\ 1, & otherwise \end{cases} \tag{1.3}$$

The DCT is performed to segregate the high-frequency components from the low-frequency components of the image [4]. In doing so, it becomes easy to compress the high-frequency components with a high factor than the low-frequency frequency components. This can be done through the process known as quantization by employing a quantization matrix, $Q^1_{i,j}$ (performed similarly on 8×8 blocks of image), by dividing the $D_{i,j}$ with $Q^1_{i,j}$, where rounding off is performed to provide the quantized coefficients $D^q_{i,j}$ [4].

$$D^q_{i,j} = round\left(\frac{D_{i,j}}{Q^1_{i,j}}\right) \tag{1.4}$$

To reconstruct the image, the quantized coefficients $D^q_{i,j}$ are then decompressed by multiplying with $Q^1_{i,j}$, and then inverse Discrete Cosine Transform (IDCT) is performed. The pixel values are integers that are rounded and truncated to the values in the interval [0,255]. Due to this truncation and rounding off, $D_{i,j}$ doesn't remain multiples of $Q^1_{i,j}$, but spread around these multiples. The high-frequency components are altered to a great extent due to rounding and truncation processes. This leads to high change in the content of actual pixel values. The double compressed image is formed by performing the similar compression technique on this reconstructed image earlier discussed but now with different

quantization table, $Q_{i,j}^{1}$. After the second compression, the image quality is reduced to a great extent. The next step after the image is compressed is its encoding. The image encoding is also a way to reduce the redundancies. Some of the basic encoding schemes are run-length encoding, entropy encoding etc., and are widely used in various image compression schemes. The ideology is to assign a single value to the most frequent data rather than a particular value to each data, though, the method of doing this varies with different entropyschemes. In this way, the code length for an image is reduced to a great amount [4].

The technique of reading this code is also a very important concept for image compression. This method is known as scanning. The main purpose of scanning is to collect maximum information of the image map with minimum computation. This leads to allocation of minimum code length to an image, thus reducing the overall size of the image that helps in storage and transfer. Some of the widely used scanning patterns are provided in figure 1.7. The various image compression formats generally differ in the transformations, coding techniques, and scanning patterns, but, the ideology behind them is basically the same [5].

1.3.3 Image Editing

In most general scenarios, the image is edited to enhance the perception of the image. It can be done to improve the quality of the image or to change the semantic content. The main purpose of image editing is to make the information of image more useful. But, this step is sometimes misused to hide or change the original content of the image. This type of editing is known to be malicious [1].

The most concerning malicious attacks on the image are the cut-paste scenarios and copy-move scenarios. In copy-move attacks, a small portion of an image of arbitrary shape is pasted on alternative location on the same image. This method is helpful when the counterfeiter is trying to conceal some content of the image, by pasting a portion of the same image onto it. In cut-paste attacks, a portion of an image of random shape or size is pasted onto another image. This attack is also known as splicing. Splicing is more reliable as it has the flexibility to create a wide range of photorealistic images. The discussion about

the detection of the forgery is similar to previous approaches, i.e. the analysis of the traces left by the editing operators [1].

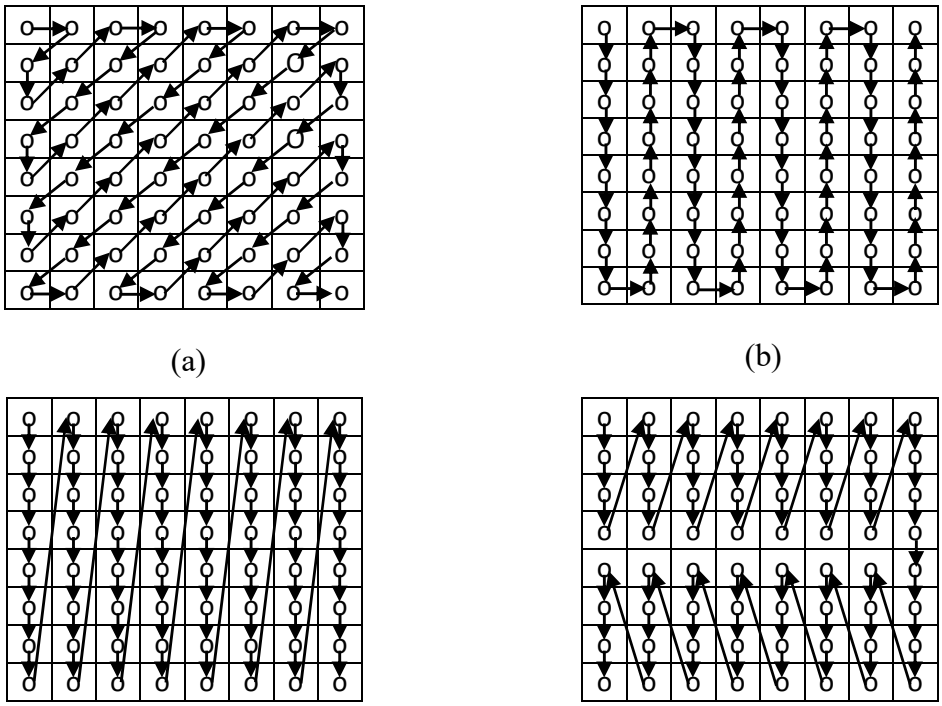


Figure 1.7: The scanning methods usually use, (a) Zig-zag scanning, (b) Raster type-1 scanning, (c) Sawtooth type-1 scanning, and (d) Sawtooth type-2 scanning [5].

1.4 Digital Fingerprints

The digital image, through its digital image life cycle, from its acquisition to its fruition, experiences various image processing operations. Each process operates in a unique way that is different for different camera make and model. This uniqueness can be described as a digital traces or digital fingerprint. The changes in the actual structures of the fingerprint left by the different processes can be acknowledged during detection of any forgery introduced in the image. Various fingerprints are classified according to their inclusion in the image during the digital image life cycle as discussed in later sections.

1.4.1 Acquisition Fingerprints

The acquisition fingerprints are left during the digital image acquisition step. The lens of

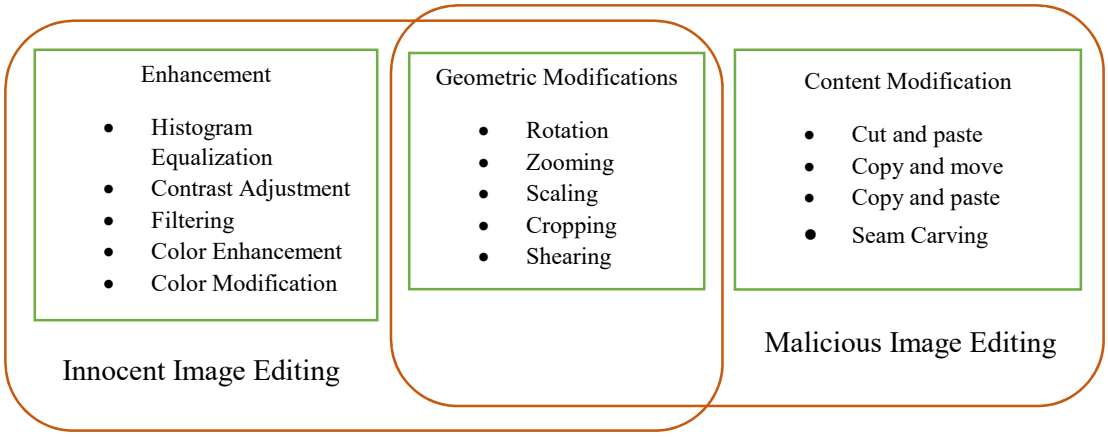


Figure 1.8: Basic Image editing operations [1].

each acquisition device, i.e. digital camera, possesses particular lens characteristics. This is basically due to the design and manufacturing process, a distinct fingerprint can be observed in the form of some aberration. This aberration would be uniform in all the images acquired from the same device. Thus, its presence in an image can easily connect the image to the camera make and model from which it has been taken. These aberrations can be named lens characteristics of the image that can be studied to detect any forgery. Each camera sensor possesses a specific radiometric response, which is typically dispensed among digital cameras of the same model, can be regarded as distinct camera fingerprints. The radiometric response, which is unique for each camera sensor is also seen as a digital fingerprint [1].

The term purple fringing is a common term used in photography, although all purple fringing cannot be credited to chromatic aberration. Similar colored fringing patterns near highlighted regions may be caused by lens flare. Colored fringing around highlights or dark regions is due to the fact that receptors for different colors have the differing dynamic range or sensitivity. Therefore, detail in one or two color channels is preserved, while blow out in the other channel or channels. On the digital cameras, the particular demosaicing algorithm tends to affect the on the depth of this issue. Another reason of this fringing effect is a chromatic aberration in the very small microlenses that are used to

collect more light that can be projected on each CCD pixel. Since these lenses are mainly tuned to focus green light correctly, the incorrect focusing of red and blue results in purple fringing around highlight regions [1].

The CFA interpolation technique involves a demosaicing algorithm. The demosaicing algorithm follows a pattern like, bilinear, bicubic, nearest neighboring algorithm etc. The interpolated pixels of the image follow a pattern that is spread out on the full image. This can be treated as a digital fingerprint. Any changes in this fingerprint can be useful to evaluate the authenticity of the image.

1.4.2 Coding Fingerprints

As it is already discussed, the coding of the image is also based on an algorithm. The fingerprint can be thought of as a pattern that is followed for overall image while coding. The most prominent approach for this would be analysis of the quantization table. It has been observed that image is compressed using a quantization table applied on 8×8 block of image. Thus, the DCT coefficients would have experienced compression by same factor, when image is categorized into 8×8 blocks. This would have formed a pattern in the whole image [6].

While testing the image the quantization table can be detected. The compression of the image would be in accordance to this quantization table. Suppose, a forgery is introduced into the image. The forged region of the image would not be following the quantization scheme of the image. So, in other words the fingerprint left during the compression is altered when the forgery is performed on the image.

Also, the fingerprint is also left during the image coding. A coding technique, like run-length coding, Huffman Coding, Lempel Ziv coding is used, is also important aspect of the image compression. It can be credited that each coding scheme is different from other and when performed on an image, the code would be unique. Any change in the code would provide unwanted results, thus revealing forgery on the image. The coefficients obtained after transformations, i.e. discrete cosine transform (DCT), discrete wavelength transform

(DWT), Haar transform etc. create coefficients in a different way and can be analyzed to validate the content of the image [6].

1.4.3 Editing Fingerprints

Editing of an image is to improve the visual perception. It includes processing like color enhancement, saturation adjustment, color modification, hue controlling etc. along with processing like zooming, shrinking, rotating etc. Similarly, a pattern or method is followed by these processes too. In other words, while adjusting the saturation of the image, the saturation is applied to the whole image with same percentage. If it is applied to a region, then saturation is also uniform in that region. If any inconsistency is observed, it would lead to the fact that the image is doctored. Also, while analyzing the color enhancement of the image, the intensity of the color is changed with equal factor on all the pixels of image [7].

While zooming, shrinking or rotating, the interpolation is used through application of a demosaicing algorithm. The algorithm shrinks or zooms or rotate the image by altering the pixel values accordingly. This change is uniform throughout the image corresponding to the algorithm used. This algorithm pattern can be regarded as a digital fingerprint left during the editing process [7].

1.5 Digital Image Forensics

In previous sections, it can be easily observed that the image can be forged at any level in the digital image life cycle. With an increase in accessibility of social media in a general form has made information security a prime concern. It has become important to identify the originality of the content that is being shared as it affects a lot of people. In case of images, it is important to make sure that the content of the image is intact and easily identify that the image is altered with. This field of image processing is known as digital image forensics.

1.5.1 What is Digital Image Forensics?

Digital image forensics is a field of research which verifies and validates the authenticity of an image through analyzing the digital fingerprints left in the image during digital image life cycle. The image under test is analyzed by reconstructing its digital image life cycle. The various traces left during the processes are then checked for any anomalies. The inconsistencies in the image would ultimately reveal the forgery.

1.5.2 Image Forensics Techniques

The techniques to compute the authenticity of an image, can be classified into two broad classes. The first being when the information of reference image is known. If the doctored image and the information of the reference image is known, it becomes very simple to locate the tampered regions of the image, even manually. The second being when only the doctored image is available. In this case, statistical properties of the image are evaluated to find any inconsistencies, which would conclusively reveal the forgery. This approach has a broader application scenario because generally, there is very less information available of the reference image. This approach is widely used and is known as blind approach, as the image history is reconstructed with no information of the source.

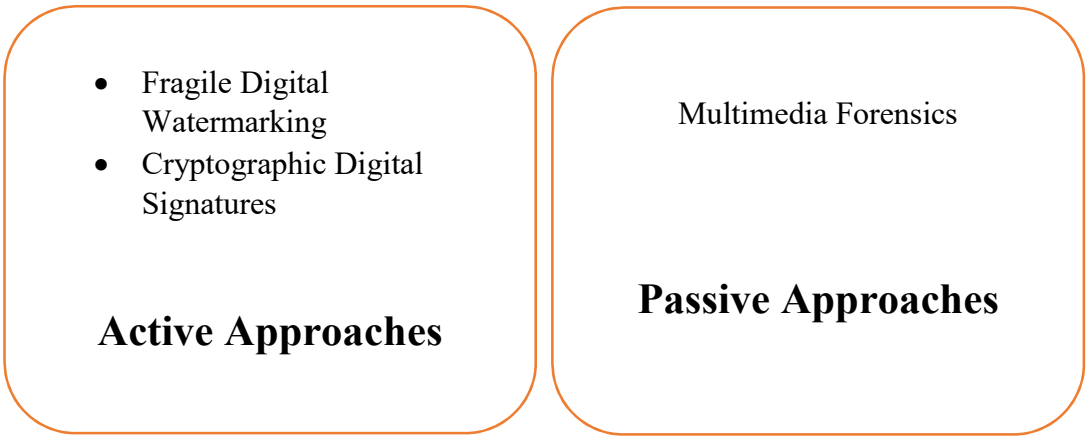


Figure 1.9: A scheme representing the possible approaches for the valuation of the history and reliability of a digital image [1].

1.5.2.1 Active Approaches

The active approaches refers to the techniques when the information of the image is assessed at the source side. In these approaches a digital watermark or a digital signature is introduced in the image upon acquisition. In this way, the image has an additional information embedded to it that can easily be accessed when verifying the authenticity of the image. The problem with this technique is that every acquisition device, i.e. digital camera needs to have this mechanism within itself so that this signature or watermark is inserted just after acquisition. This requires a system to instruct all the camera manufacturers about the norms to be followed, a standard protocol, while inserting additional information to the image, which is quite laborious.

1.5.2.2 Passive Approaches

The passive approaches are the one in which only the image at the final fruition end is accessed for its validation. The major advantage of these approaches is that they require almost no information of the source of image. The history of the image is constructed in a blind way, and the processes which image has experienced, are evaluated. The statistical modelling of image is done and any inconsistencies in the model is enough to expose the forgery.

1.6 Image Anti-forensics

Virtually all modern lossy image compression techniques are sub band coders, which are themselves a subset of transform coders. Transform coders operate by applying a mathematical transform to a signal, then compressing the transform coefficients. Sub band coders are transform coders that decompose the signal into different frequency bands or sub-bands of transform coefficients. Typical lossy image compression techniques operate by applying a two-dimensional invertible transform, such as the DCT or discrete wavelet transform (DWT), to an image as a whole, or to each set of pixels within an image that has been segmented into a series of disjoint sets. As a result, the image or set of pixels is mapped into multiple sub-bands of transform coefficients, where each transform coefficient is denoted. Once obtained, each transform coefficients must be mapped to a binary value both for storage and to achieve lossy compression [8].

Because some sub-bands of transform coefficients are less perceptually important than others, and thus can accommodate greater loss during the quantization process, the set of quantization interval boundaries is chosen differently for each sub band. After each transform co-efficient is given a binary representation, the binary values are reordered into a single bit stream which is often subjected to lossless compression. When the image is decompressed, the binary bit stream is first rearranged into its original two-dimensional form. Each decompressed transform coefficient is assigned a value through dequantization. During this process, each binary value is mapped to a quantized transform coefficient value be-longing to the discrete set [8].

1.7 Organization of Thesis

The thesis work has been organized in the following chapters:

Chapter 2 Literature Review: An overview of the existing methods of Image forgery detection is provided with main emphasis on CFA interpolation and demosaicing process. The review is extended to image compression and methods to detect forgeries in these scenarios are discussed in this chapter

Chapter 3 Feature development based on CFA artifacts for Image Forgery Detection: A method based on the CFA interpolation artifacts is developed, that calculates the prediction error between the acquired and interpolated pixels. The standard deviation and skewness is then evaluated to create a feature that generates a forgery map.

Chapter 4 Results and Discussions: The proposed scheme is then compared with previous established algorithms. Then the scheme is also employed to various social networking images and results are provided. At last, the performance of the scheme is discussed.

Chapter 5 Conclusion and Future Scope: The processing and observed results of the thesis are concluded here in this chapter and also the future work in this field is also suggested.

Chapter 2

Literature Review

2.1 Introduction

The basic ideology of the digital image forensics is to reconstruct the history of the digital image from its final stage to initial stage. In doing so, various processes that an image has encountered are observed. As discussed earlier, the various processes leave a distinct trace in the image that can be extracted and can be used to analyze the authenticity of the image. The thesis report is dedicated to the Color Filter Array (CFA) artifacts that are left in the image during CFA interpolation using a demosaicing algorithm. In this chapter, various techniques that are dedicated to interpolation are discussed. A brief overview for other techniques that are used to detect the forgery is also provided. Forensics, however, are never perfect. The inconsistencies may depend upon wrong tool settings, deviation from the assumed settings etc. Barny *et al.* [9] found out that generally each forensic technique deals with detection of a particular footprint left by a single processing tool under specific settings. Also, the tampering is not result of single processing tool, but the combination of various tools.

2.2 Image Acquisition

The acquisition process, as categorized in the previous chapter, comprises the fingerprints left by the lens, the sensor, and the CFA. Also, the image acquisition can also be executed with digital scanners, and many of the techniques evolved for camera fingerprint examination have been mapped to their scanner equivalents. Also, the images could be recaptured and printed, thus, a digital to analog (D/A) conversion also comes into play. The ground idea of image acquisition is image interpolation that creates a full-color image. Dehnie *et al.* [10] developed an approach that is based on the concept that the image acquisition in a digital camera is fundamentally different from the generative algorithms

deployed by computer generated imagery. The difference is captured in terms of digital camera image's noise properties extracted by a wavelet based denoising filter.

Most of the images contain a miscellany of anomalies that result from irregularities and artifacts of the optical imaging system through which light passes through the lens and is focused to a single point on the sensor [1]. Lateral aberration exhibits itself as a spatial shift in the locations, where light of different wavelengths reach the sensor. This shift is in proportion to the distance from optical center. Chromatic aberration leads to various form of color irregularities.

2.2.1 CFA Interpolation and Demosaicing process

The incoming light is filtered by CFA before it reaches the sensor, so that for a particular pixel, only one color is acquired. Only one-third of the image is sensed directly. The missing pixel values are then computed by process called image interpolation, which employs a demosaicing algorithm. The algorithm uses a single layer mosaic of red (R), green (G) and blue (B) colors. Upon interpolation, a specific correlation can be observed in the pixels that can be analyzed. The works crediting CFA demosaicing as digital fingerprint can easily be categorized in two broad classes: algorithms that aim at estimating the parameters of the interpolation algorithm for color and the structure of the pattern filter and algorithms that aim at assessing the presence or absence of demosaicing traces [1].

The first class proves fruitful when the information and classification of camera make and model is intended. The second class is when the detection of forgery in an image is intended. The both classes focus on search for the presence or absence of CFA artifacts in an image for their respective justifications.

The technique to detect and classify the demosaicing artifacts was delivered by Bayram *et al.* [10] so as to identify camera make and model. The technique requires to compute probability of pixels being correlated to their neighboring pixels. The above approach along with CFA coefficients and photo response non-uniformity (PRNU) noise features are used in [7] to evaluate the image source. Swaminathan *et al.* in [11] proposed a process for source camera identification by estimating the CFA pattern and kernel used for image

interpolation, while in [12] the same authors exploited the irregularities among the evaluated demosaicing factors to reveal the forgery introduced. Therefore, the existence of demosaicing artifacts is recognized by associating the changes in variance of sensor noise in interpolated pixels and in the pixels acquired straightly. Conclusively, in [13], authors employed an SVM trainer to identify the camera model that was used to capture the image.

Similarly, various techniques have been proposed for the detection of forgery in the image considering the CFA pattern. Popescu and Farid in [14] proposed a scheme to detect the CFA interpolation by assuming linear interpolation kernel and by employing simple Expectation Maximization (EM) algorithm to approximate the factors that develop a probability map indicating probability of each pixels being correlated to neighboring pixels. Any inconsistencies in the probability map would reveal forgery. Considering the actual CFA pattern, some pixels would be interpolated and some would be acquired. The correlation map would exhibit a periodic behavior, which can be applied to the image to localize the tampered portion, i.e. regions where the periodicity is not uniform. This concept periodicity was observed by Gallaghar in [15] and postulated that the variance of second derivative of interpolated signal is periodic in nature. Gallaghar and Chen [16] extended the previous approach by applying Fourier transformation to the image for detection of periodicity in the variance of interpolated and acquired pixels. This detection of periodicity further helps in the localization of tampered regions in the image.

Dirik and Memon [17] proposed two methods to check the presence of demosaicing artifacts. In first method, the image is reinterpolated assuming different CFA patterns, and one providing the minimum mean square error is selected. This process is generally employed to estimate the CFA configuration of the source camera. The second scheme uses the low pass property of demosaicing kernel to detect the presence of demosaicing kernel. The detection is done by collating the changes in variances of sensor noise in interpolated pixels to the directly acquired pixels.

Ferrara *et al.* in [18] assumed that the image is acquired using CFA and the introduction of any forgery removes the demosaicing artifacts from the tampered region. The approach

combines the techniques of [19] to develop a feature which tests the presence of the CFA artifacts at a 2×2 block level, and reveal the forged regions based on its absence.

2.2.2 In-camera Processing techniques

The imperfections of the image sensor is the main reason behind the sensor pattern noise because it results in slender variations between the captured scene and the image developed by the camera [20]. PNRU is a high frequency multiplicative noise which remains unchanged and is unique in cameras of same make and model. This makes this noise an important parameter for device identification, and inconsistencies in it would ultimately help in forgery detection. The most approaches concentrates on producing the PRNU evaluation more resilient. In doing so various denoising filters are developed, which are provided in [21]. The authors in [21] obtained a PRNU predictor based on maximum likelihood criterion, using a specific training dataset. The anomalies recorded in the extracted PRNU reveal that the particular region of the image is not taken from the expected device. Thus, the two hypothesis tests can be applied block-wise to the image, to conclusively test the integrity of the image.

The camera sensor (CCD or CMOS) has a particular radiometric response. This fingerprint of a sort, is common across the cameras of same make. This radiometric response is categorized in [22] using a single grayscale image. The geometric invariants and the planar region identification [23] are employed together to obtain the source camera classification. The categorization of the source device is presented in [24] on the basis of structural and color features. These features can also be used to distinguish between the real and the computer generated images. Hsu and Chang [25] explored a new class of camera artifact, known as camera response function (CRF). The CRF is tested for inconsistencies, while the image is segmented. The CRF is assessed on locally planar irradiance points (LPIPs) close to the boundaries. The CRF obtained is then tested for any inconsistencies. The approach is fed to a SVM classifier which provided a 90% accuracy with 70% precision, however the results were not satisfactory for real world images.

Similarly, scanner fingerprints can also be used for acquisition device classification. Also, forgery detection in a scanned image is of precise importance as it involves legal

documentations like scanned copies of bank proof, address proof etc. [26]. The noise patterns from various scanned images are extracted to form an equivalent scanner PNRU [27]. The authors in [28] discuss the cases where scanner PRNU extraction is difficult due to deficiency in uniform tones and dominance of saturated pixels.

2.3 Image Coding

The most common operation that is executed on an image is the image compression, and lossy in that case. The compression is basically performed to reduce the storage size of the image because the image has a large number of redundancies which are not recognized by human eye, and storing these redundancies would increase the storage size of the image. Owing to the lossy nature, the coding process leaves typical fingerprints in the image which can be identified.

2.3.1 Image Compression and Decompression

The basic steps involved in a standard JPEG compression can be easily demonstrated in a block diagram shown in figure 2.1.

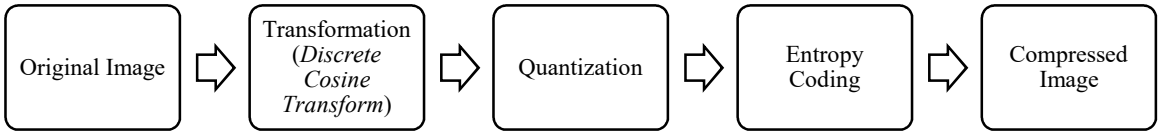


Figure 2.1: A block diagram demonstrating steps involved in a standard JPEG compression [4].

- *Discrete Cosine Transform*: The image is distributed into 8×8 non-overlapping blocks. The block of 64 pixels then goes through two dimensional transformation. The basic ideology behind this is that the low frequency components and high frequency components separate themselves from each other. The DCT coefficients corresponding to low frequencies club themselves to the top left corner of the block with topmost left value providing the lowest frequency DCT component. Similarly,

high frequency DCT coefficients tends towards the bottom right corner of the block, with lowest right DCT coefficient providing the highest frequency DCT coefficient. The 8x8 blocks are generally used because the larger block size would create more frequency components and thus, it would become difficult to compress these much frequency components. A lower block size would increase the computational complexity and it would take more time to compress an image.

- *Quantization*: The DCT coefficients obtained are then quantized using a specific quantization table. Generally, a quantization table is standardized in accordance to the compression ratio. As it has been established in previous chapter, that the human visual system is less profound to high frequencies. Thus, the DCT coefficients corresponding to higher frequencies are quantized with high factor so that a similar value can be allotted to them. The low frequencies contain the most of the image information and thus are quantized with lower factors.

  The quantization uses rounding and truncation as it has certain fixed values, the information at high frequencies is lost. Thus, when image is reconstructed, it is not same as the original acquired image. This amount of information lost can be useful in identification of the quantization table.
- *Entropy Coding*: The quantized DCT coefficients are then losslessly coded into a bitstream following a coding scheme like Huffman coding, Lempel Ziv coding etc.

A method to detect the tampering of digital image was proposed by Saha *et al.* in [29]. Initially discrete wavelet transmission is applied after that image has been taken to detect the tampering. Digital watermarking is one of the techniques used for tampering detection. In this DCT is applied and after that the difference of the both the image is observed. Then the Discrete Wavelet Transformation (DWT) applied and Single Value Decomposition (SVD) watermark is applied. The use of DCT, DWT and SVD make this method comparatively robust and accurate. But this technique is not compatible to detect tampering for low scale images.

The inconsistencies and modifications that do not match the object can be detected using different quantization tables as proposed by Kumar in [30]. The investigation of the dynamic forged copy detection problem is based upon image source Artificial Neural

Network (ANN) identification. The different image features are used to train an ANN. This approach is useful in detecting copy/paste forgery and can still be useful even the image is enhanced after tampering. The authors in [31, 32] described a method capable of detecting the JPEG compression artifacts when compression is very light, i.e. as high as 95% of the content is preserved.

A blocky image is formed as there is an interference of nonblocky images with a pure blocky signal. To overcome the problem of evaluating the blocky signal power without being access to an original image, absolute value of gradient is calculated individually between the row and column of an image [33]. This approach has been extended in [34] when locations of block and size of block is recognized. In similar way, horizontal and vertical grades are calculated. Using DFT, periodicity is also computed in the frequency domain. After this step, a metric is calculated for blockiness distortion evaluation.

Tjoa *et al.* [35] introduced a method that used the periodicity of directional gradient for estimation of block size. To further increase the peaks, authors subtracted a median filtered version to gradient and then threshold is applied depending on the sum of gradients, so as to avoid the specious peaks originated by edges from object in the image. By applying a maximum likelihood estimation algorithm, period of resulting function is calculated that is generally used for pitch detection. In [36], the researchers introduced a method for calculating the quantization steps of whole quantization table. To proceed with this, for every DCT coefficient subband, different histograms are calculated individually. After the analysis of periodicity of power spectrum of histogram, quantization step $\Delta(i, j)$ for each subband can be extracted. A method applied to the histograms that is based on second-order derivative can be used to detect the periodicity. Also, the presence of tempering may be known by possible blocking artifact inconsistencies.

There is also a compression in which specific quantization tables can be employed for specific color components. The estimation of these quantization tables is provided in [34]. The authors introduced maximum *a posteriori* (MAP) estimation to extract quantization step size of the greyscale images. The approach exploited in this is the periodicity in histograms of DCT coefficients [37]. This periodicity is then used to create histograms

when the image is mapped to the colorspace, and the artifacts left during image interpolation are removed.

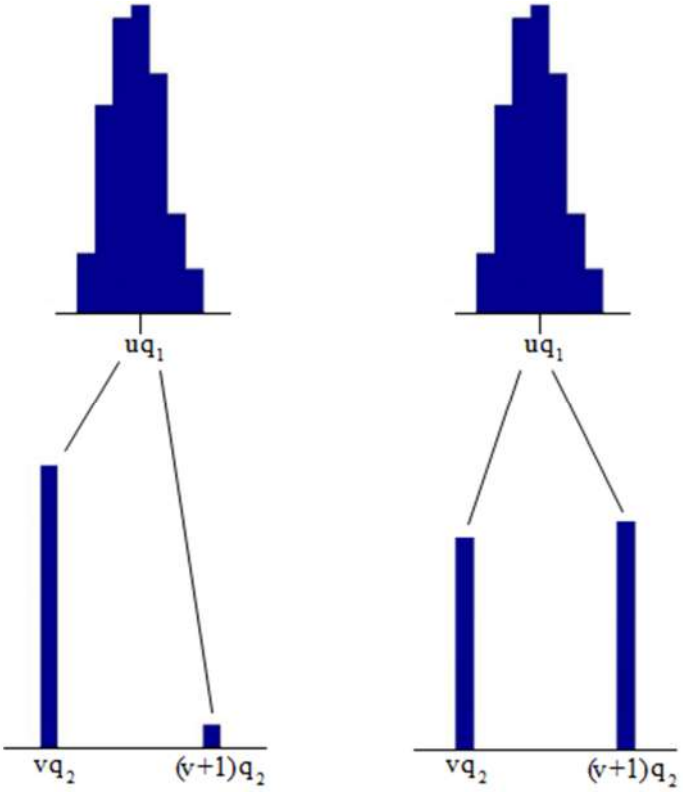
2.3.2 Double Image Compression

A JPEG image is said to be double compressed when a JPEG image is decompressed and then is again compressed with another quantization table. Now, in digital image forensics, the study of double compressed JPEG image becomes important because these images result from various manipulations. The basic ideology here is that an image is manipulated by replacing a portion of the image with another image and then resaving it through compression. Thus, the manipulated portion will exhibit the properties of single compression whereas the whole image would be double compressed. Thus, the main motivation is to estimate first quantization matrix from image that has undergone double JPEG compression. The portion that do not follow the estimated primary quantization matrix would be replaced one. These observations may lead to the digital manipulations in the JPEG image.

The algorithm presented by Lukáš and Fridrich in [38] to detect the presence of double JPEG compression, observes the periodic artifacts introduced in the histogram of DCT coefficients of the image. The peaks of histogram take different configurations corresponding to the relationship between quantization steps of first and second quantization tables. The special attention should be provided to the double peaks and missing peaks.

Thus, the method is developed in [4] to estimate the primary quantization steps only for the scenarios where the second quantization is lower than the first. This is because it is quite possible to estimate in this particular case as the double compressed image still hold some traces of its first quantization when the second quantization is lighter than first. If the second quantization is more than the first, it would then become difficult as the traces of first quantization becomes less prominent in this case. This method deals with the problem of double peaks and missing peaks faced by Lukáš and Fridrich in their approach [38] by employing a filtering strategy to remove the uneven shape of the histogram. This type of filtering is known as DCT histogram filtering. The filtering is done by setting a specific

threshold for every histogram bin. The uneven histogram is viewed as to be corrupted by residue noise and split noise.



(a) (b)

Figure 2.2: Histogram depicting DCT histograms (a) Residual Noise, and (b) Split Noise [4].

A new method to identify regions which have been double JPEG compressed is proposed in [39]. The method applies similar coding technique on the image under examination. This would direct to an output image which is highly correlated to the test image. This correlation is then used to develop the quantization table.

Weiqi Luo *et al.* [40] reported that the main errors of JPEG comprise rounding errors, truncation errors, and quantization errors. Through considering these errors on single and double compressed JPEG images, three techniques for image forensics have been developed. It has been used to cater three problems, i) whether a bitmap image has been formerly been JPEG compressed, ii) approximating quantization steps of a quantization

table in a JPEG image, and iii) identifying the quantization table of JPEG image. The theoretical examination and experimental results are done for grey-scale images. The research can be protracted to examine color images in the similar way. The approach was extended to two copy-paste scenarios, i) JPEG images, copy-paste together and saved in a lossless format, and ii) JPEG images, copy-paste together and saves in JPEG format. To detect the tampered region, sum of absolute difference (ASD) was computed by Zhulong *et al.* [41] computed between the tampered image and the resaved JPEG compressed image at different quality factors. The proposed method is accurate even for small tampered regions. Tampered region can be detected even if the image is rotated. It is computationally simple and effective. The proposed method is not very effective, if the Quality factor (Q-factor) of the tampered region and original image is same or very close. The proposed method is also ineffective, if the image is resaved with Q-factor lower than the Q-factor of both regions.

2.4 Image Editing

In most general scenarios, image is edited to enhance the perception of the image. It can be done to improve the quality of the image or to change the semantic content. The main purpose of image editing is to make the information of image more useful. But, this step is sometimes misused to hide or change the original content of the image. This type of editing is known to be malicious.

The most concerning malicious attacks on the image are the cut-paste scenarios and copy-move scenarios. In copy-move attacks, a small portion of an image of random shape is pasted on another position of the same image. This procedure is helpful when the counterfeiter is trying to conceal some content of image, by pasting portion of the same image onto it. In cut-paste attacks, a slice of an image of random size or shape is pasted onto another image. This attack is also known as splicing. Splicing is more reliable as it has flexibility to create a wide range of photorealistic images. The discussion about the detection of the forgery is similar to previous approaches, i.e. the analysis of the traces left by the editing operators.

The basic inspiration for the work in this direction is taken from block based matching method provided by Fridrich *et al.* in [42]. The basic ideology was to analyze the image by segmenting the whole image into overlapping square blocks instead of analyzing the whole image. It is assumed that the forged region is bigger than the block size assumed. It is suggested to employ the block DCT coefficients. Lou *et al.* in [43] also used the color-based features with block DCT. In [44], Popescu *et al.* proposed a method in which a Principal Component Analysis (PCA) was employed to speed up the search and classification.

Gallagher in [15] witnessed that the variance of second derivative of the interpolated signal is periodic. It was then used by Popescu who took the Fourier Transform of the whole image to determine its periodicity. It is well collaborated and discussed by Kirchner in [45, 46]. The authors in [47-51] studied the periodicity in interpolated signal that was postulated by Gallagher [15].

A perception restraint established scheme to calculate the presence of spliced objects is presented in [52] by Wang *et al.* It is based on the assumption that despite the fact pasting an object onto another image, it is challenging to perfectly size the said object. Thus, the ratio of its height is evaluated in accordance to the original image. The inconsistencies are reported to reveal any forgery.

A new approach established on scale-invariant feature transform (SIFT) is discussed in [53] by Hailing *et al.* The main ideology is to employ SIFT descriptors [54] to locate matching regions in the same particular image. The SIFT descriptors are also used in [55, 56]. The copy-move forgeries have always been challenging problems. The performance parameters and the proper localization are two important aspects that the detection algorithms have to cater.

2.5 Gaps in Study

Several approaches have been proposed in the literature, which take advantage of the inconsistencies. These techniques can be classified into pixel based, format based, camera based and geometric based [57]. The previous approaches, which comprise in turn a very

large and ever growing number of individual detection techniques, testify both the interest towards this problem and its complexity [58]. The following problems have been encountered.

- Each digital fingerprint has been examined in isolation from the other processing stages, thus there is no relation between the various stages of the digital life cycle.

  The techniques of forgery detection, by extracting various fingerprints of the digital image are not compatible with each other. Besides, the implementation of the individual techniques, concern the interpretation of their results in terms of homogeneous and meaningful performance measures [59].

- Tools based on individual stage traces require image to be captured under controlled conditions.

  It is noticed that some techniques require some special conditions to be met when the image is being captured. If those parameters are not met, then these techniques might fail to deliver the results [1].

- Trace detectors often give uncertain results as their performance is not that robust.

  The performance of the detectors is also an issue. The performance of detectors used are very sensitive in nature. Their performance degrade gradually if the image parameters are changed even slightly. This means the methods and techniques are not capable to cater a wider range of image settings [60].

2.6 Objectives of the Thesis

The objectives of this dissertation are:

- To detect and localize the tampered regions of the image by analyzing the fingerprints left during the image acquisition phase.
- To analyze the artifacts left during the image interpolation. The green channel is extracted and prediction error is computed between the acquired and interpolated pixels. This prediction error can be used to develop a probability map that defines

the presence or absence of CFA artifacts in a region, whose existence has been altered due to forgery.

- To formulate an approach to reveal forgery attacks even when the image is compressed. The detection of forgery becomes difficult when the compression or decompression ratios are high.

2.7 Methodology

Generally, a characteristic fingerprint is left in the image while image interpolation. This fingerprint is due to the demosaicing algorithm which develops a full color image. Demosaicing algorithm basically creates incomplete pixel values in correlation to the pixels in its vicinity. At a small block level of the image, this fingerprint can be observed as an artifact, also known as CFA artifact. When a forgery is introduced in an image, these artifacts are removed or altered in that specific region. A feature can be developed which computes the probability of the presence or absence of the CFA artifacts throughout the image at local 2×2 pixel block. This probability map can reveal the introduced forgeries.

2.8 Chapter Summary

It has been observed in this chapter that digital image forensics finds its significance in today's scenarios where a bulk of information is being shared in the form of digital images. This chapter deals with various techniques that can be employed to detect the forgery in an image and to classify the source camera of the image. The techniques are discussed according to the digital image life cycle, i.e. step where forgery has been introduced, corresponding techniques to tackle or identify the forgery has been discussed there only.

Also it can be observed that the reconstruction of the digital image life cycle is mandatory for the detection of the forgery. Through reconstruction of digital image life cycle, various fingerprints left in the image can be extracted and can be tested for inconsistencies. These inconsistencies would ultimately help for the detection as well as localization of forgery in the image.

Chapter 3

Feature development based on CFA artifacts for Image Forgery Detection

3.1 Introduction

The basic ideology behind this research is to analyze the CFA artifacts left in the image during the image interpolation. These artifacts are left during the image interpolation or image reconstruction. Generally, the main process in CFA interpolation is to reconstruct the full-color image from the incomplete color samples. This process is known as a demosaicing process. A certain algorithm is involved in the demosaicing process, thus leaving a pattern in the image. This digital fingerprint or trace can be studied while accessing the quality of the image. When a tampering is introduced into a digital image, the structure of this fingerprint is somewhat hindered. The tampering will remove the CFA artifacts of the image in that particular region where it is introduced. Thus, while evaluating the CFA artifacts, its presence or absence in a certain area would reveal forgery.

3.2 Analysis of CFA artifacts

A color filter array (CFA) is a mosaic of color filters used in front of the image sensor. The basic idea here is that only one color is captured for each pixel. The most commercial and widely popular CFA composition is a Bayer filter, as portrayed in figure 3.1. The bayer filter utilizes the combination of three colors, red (R), green (G) and blue (B), placed alternatively for different rows for red and blue filters. The number of green filters is twice that of red and blue filters because of the fact that human eye is more sensitive to green color and thus is acquired more.

For each pixel, the intensity combination of the three color filters, red (R), green (G) and blue (B) is usually used to provide the color for one pixel. In this research, the only green

color filter is acquired and other pixels are interpolated, to generate a green color channel image.

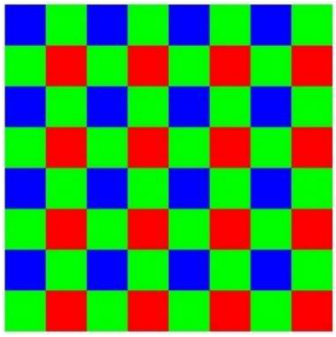


Figure 3.1: Bayer filter of 8×8 block size.

3.2.1 Image Interpolation and Demosaicing

Image Interpolation is a very important step in a digital image life cycle. It finds its way during zooming or shrinking or rotating the image. It refers to assigning values to new pixel locations based on the information of the known values of original pixel values. Thus, the identification of artifacts left during the image interpolation due to CFA demosaicing can be viewed as a specific case of the evaluation of interpolation artifacts [15].

Interpolation refers to the process of estimating the missing values from the knowledge of known values. For example, while resizing the image, zooming per se, there would be some creation of new pixel locations. Thus, the values of these new pixels can be estimated through the known pixel values of the original image. This process is known as image interpolation. Basically, image interpolation is used while remapping the image, i.e. resizing (zooming or shrinking), rotating, or distorting etc.

Similarly, demosaicing is a process to develop a full-color image from the sampled color channel output of the CFA. The received light is projected on CFA to form three color channels of red, green, and blue, in the case of RGB images. The intensity of each color channel for a pixel is combined together to form a particular color for that specific pixel. The main attributes to be possessed by a demosaicing algorithm are:

- It should have low computational complexity so that the in-camera operation of the development of full-color image is performed efficiently.
- It should possess the quality to reduce noise in the image.
- The resolution of the image should be preserved.
- The aliasing effect, abrupt color changes in the neighboring pixels etc., should be avoided.

In simple words, the reconstruction of a full-color image from the samples obtained after filtering by CFA can be done through finding the missing pixel values. The process of finding the missing pixel values from the known pixel values is referred to as image interpolation. The process of providing color to the pixels during interpolation can be achieved by employing a demosaicing algorithm.

The demosaicing algorithm follows a particular pattern while providing a filtered image a full color, this pattern can be seen as a digital fingerprint. This pattern would be present throughout the whole image. Any introduction of a forgery into the image would disrupt the overall structure of this fingerprint. While analyzing the fingerprint present in the image, any inconsistencies would reveal the fact that the image is tampered with.

3.2.2 Feature development and extraction

In [45], Kirchner concluded that the variance $var[e(x)]$ is periodic with a period equal to the original sampling rate; where $e(x)$ is the prediction error of resampled, stationary and non-constant signal, with $x \in \mathrm{Z}$. Thus, if an image is resampled in accordance to image interpolation factor r, then

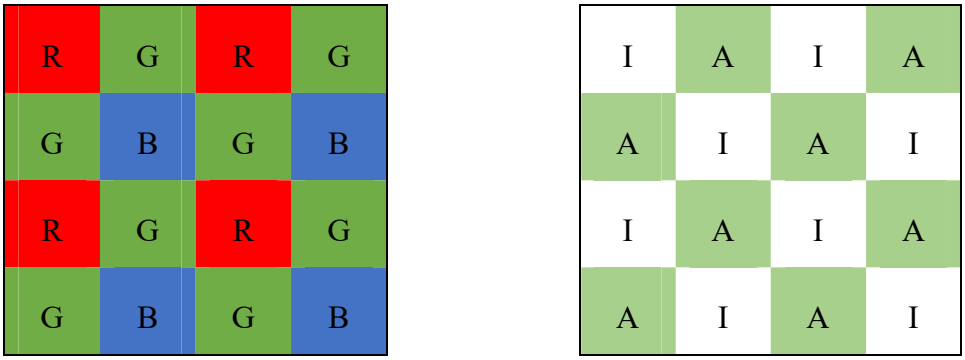
$$var[e(x)] = var[e(x + r)] \tag{3.1}$$

since the r samples of the resampled image corresponds to the original sampling rate.

The variance of the prediction error can assume only two values, one for odd and one for even positions. Thus, (1) can be written as:

$$var[e(x)] = var[e(x + 2)] \tag{3.2}$$

A novel idea is proposed in [18] based on this concept to localize the image forgery at a local level, i.e minimum up to 2×2 block size. According to the model proposed in [15], the green channel is generally considered because it is upsampled by 2, as compared red and blue channels, like in Bayer's filter mosaic as shown in figure 3.2 (a). Thus, in this one-dimensional case, the whole image lattice of odd/even positions can be depicted by acquired/interpolated green values as shown in figure 3.2 (b).



(a) (b)

Figure 3.2: The demonstration of (a) Bayer's filter mosaic; (b) the mosaic of acquired green channel 'A' and interpolated green channel 'I'.

The prediction error has zero mean and variance proportional to the variance of the acquired signal. In the presence of CFA interpolation, the variance of the prediction error of the acquired A lattice is assumed higher than the variance of the prediction error of the interpolated I lattice. Also, in the absence of demosaicing, the variance of the prediction error of both lattices is assumed to be similar. In order to detect the image forgery, all that is required is to detect the presence/absence of the demosaicing artifacts. It can be done by analyzing the imbalance between the variance of the prediction error of the two lattices [1].

The approach provided in [18] has been extended to evaluate the standard deviation (second norm) and skewness (third norm) of the prediction error instead of the variance. The standard deviation and skewness of prediction error $e(x)$ is locally evaluated pixel-by-pixel for each position, interpolated (I) or acquired (A).

The standard deviation of the distribution provides the spread or dispersion of any probability distribution. It is also the square root of the variance. The variance is most often used because of the fact it can be easily applied when the statistical model is to be expressed

mathematically. It can also be used to model various uncorrelated distributions together. In this paper, the standard deviation is used because pixel-to-pixel variability can be more aptly expressed using SD. This is because that the changes in the values of interpolated pixels due to the presence of forgery can be more correctly collected using SD than variance. The feature extracted for generation of the forgery map is modeled as Gaussian Mixture Model. The SD would be more suitable to provide the spread as compared to the variance. The margin of error can be reduced and can be represented in the multiples of SD. Also, the value of SD is same as the values of distribution and is easy to represent as well as interpret.

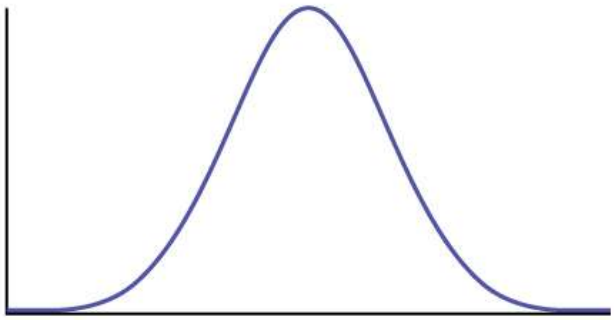


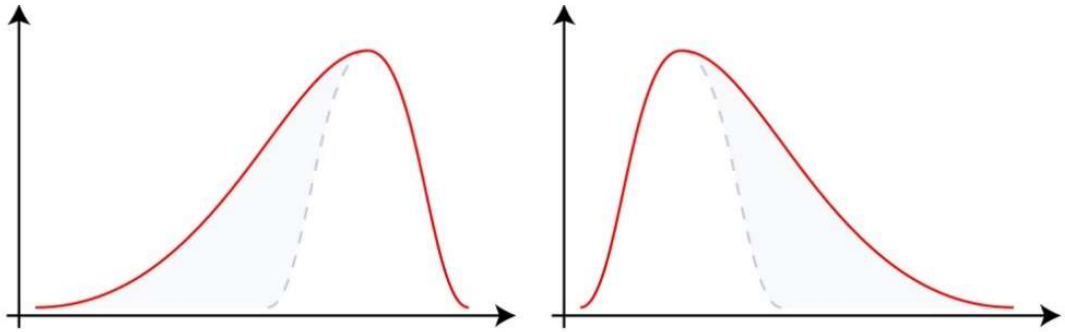
Figure 3.3: A simple Gaussian Curve.

The feature is extracted through the calculation of prediction error of each block of the image. Now, the presence of any tampering would disturb the structure of the fingerprints left in the image during interpolation. This is because the traces or artifacts are removed by inclusion of any alien portion in the image.

Thus, the distribution of the model would not be purely Gaussian. It then becomes very convenient to employ skewness (third norm) to evaluate the asymmetry of the Gaussian Mixture model that arise due to the absence of the demosaicing artifacts.

The detailed workflow of the algorithm is provided in figure 3.5. The proposed feature **M** is to evaluate the inconsistencies in the local standard deviation of prediction errors when an image is demosaiced. It is assumed that the local standard deviation of the prediction error of acquired pixels is higher than that of interpolated pixels. Also, if the image is not

demosaiced, the difference between the standard deviation of the prediction errors of acquired and interpolated pixels approaches to zero.



(a) Negative Skew (b) Positive Skew

Figure 3.4: The distribution curves demonstrating skewness

Now let us assume that the image has undergone some processing and a forgery has been introduced. This forgery would conclusively destroy the demosaicing traces and artifacts in the forged region. Thus, in the untampered region, the local standard deviation of prediction error would yield the value of feature **M** significantly greater than zero. Whereas in the tampered regions, the absence of demosaicing traces would lead to a difference in the standard deviation of prediction errors of acquired and interpolated pixels tends to zero, ultimately making the feature **M** close to zero.

The probability of the presence/absence of CFA artifacts in each block can be observed using the *Bayesian approach* on the values of **M**. Let P_1 and P_2 be two probable for presence and absence of CFA artifacts, respectively. In order to simplify the problem for detection of demosaicing artifacts, the feature **M** is taken to be Gaussian distributed. Thus, for a pixel of a block $B_{k,l}$, the feature **M** can be characterized using *conditional probability density functions*:

$$Pr\{M(k,l)|P_1\} = \mathcal{N}(\mu_1, \sigma_1^2) \tag{3.3}$$

where $\mu_1 > 0$, and

$$Pr\{M(k,l)|P_1\} = \mathcal{N}(0, \sigma_1^2) \tag{3.4}$$

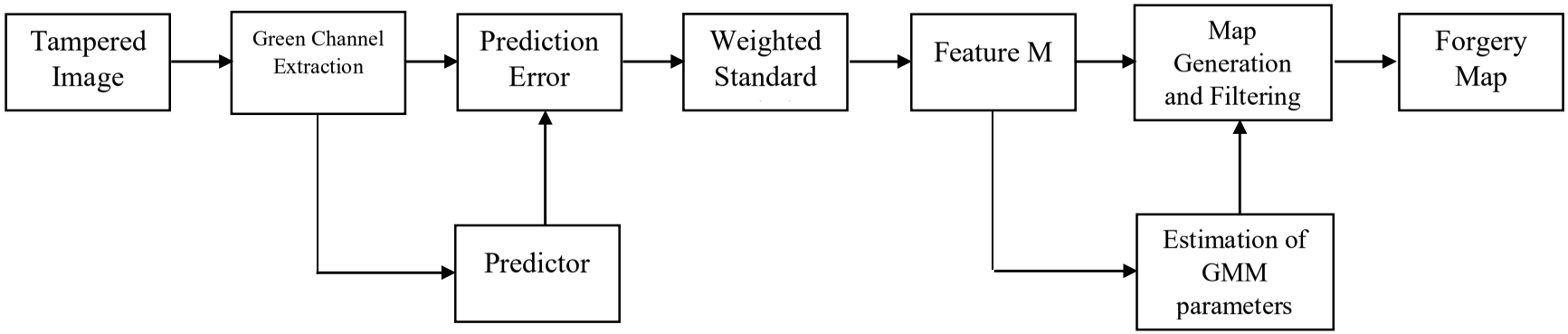


Figure 3.5: The basic block diagram of the algorithm.

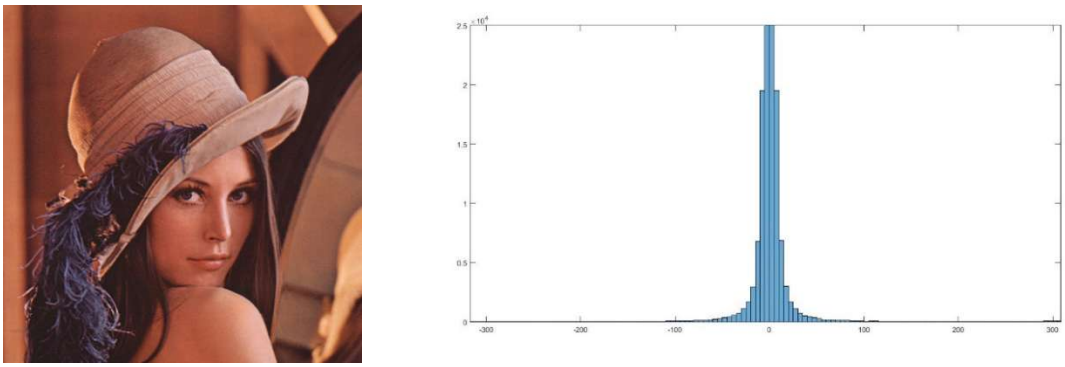
Thus, the whole feature can be modeled as mixture of Gaussian distribution of two hypotheses $\boldsymbol{P_1}$ and $\boldsymbol{P_2}$, with equation (3.3) for the region where CFA artifacts are present and equation (4) for the region where CFA artifacts are absent. In equation (3.4), μ_2 has been taken to be zero due to removal of CFA artifacts (can be due to some tampering process).

Thus, to evaluate the parameters μ_1, σ_1 and σ_2 of the proposed Gaussian Mixture Model (GMM), the Expectation Maximization (EM) algorithm is employed, which estimates by maximizing the expected values of log likelihood function of feature **M.**

3.2.3 Extension to the compressed image scenarios

JPEG compression is most widely used in image file formats. Generally, an image takes a lot of space while transmitting or storing. An image also contains a lot of redundancies that can be discarded without hampering the important content of the image. Generally, image compression is carried after the demosaicing process.

But recently, various methods had been proposed that compress the image before the CFA interpolation is performed [60]. The scenario where compression is performed after the demosaicing process, the CFA artifacts are intact as each color channel is compressed separately. In the other case, the CFA structure of the image is heavily disturbed. The JPEG compression can be explained by taking an example. The process of compression comprises of a transformation followed by quantization.



(a) (b)

Figure 3.6: (a) A JPEG image with corresponding (b) histogram of DCT coefficients.

The image and its original DCT histogram is demonstrated in figure 3.6. Now, if the image is quantized with the help of a quantization table, the compressed image is obtained, whose histogram of DCT coefficients is depicted in figure 3.7.

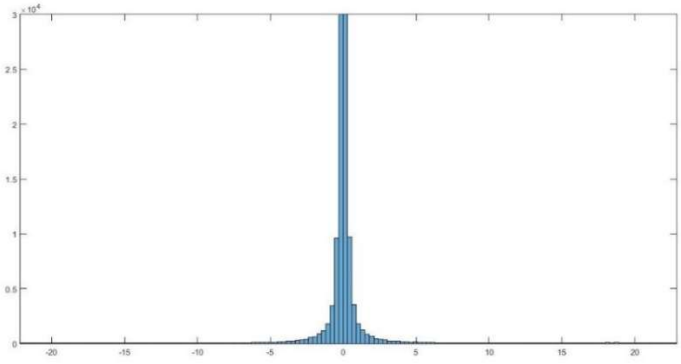


Figure 3.7: A histogram plot of DCT coefficients after quantization.

It can be clearly observed that the peaks of the DCT coefficients as in figure 3.6 (b) are quantized into a low concentration in figure 3.7. If the image is now decompressed with the same quantization table, still the image would not be the same, though appearing to be similar. The histogram of DCT coefficients of the decompressed image is shown in figure 3.8. The difference between the histograms in figure 3.6 (b) and figure 3.8 can be easily seen. Though the image would appear to be same, there would be some difference.

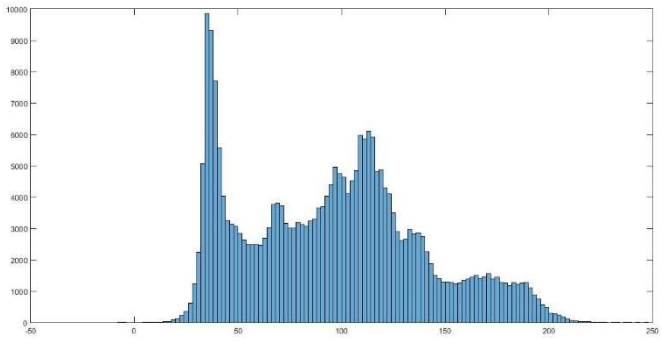
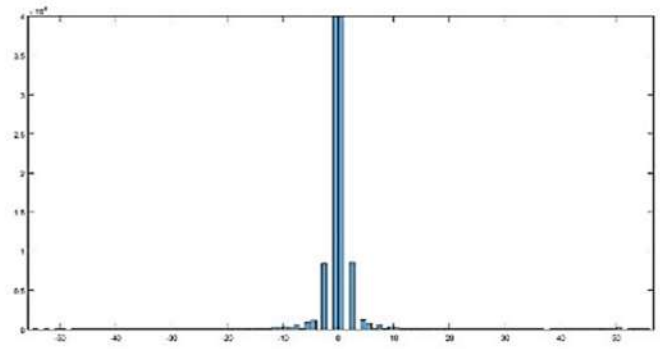
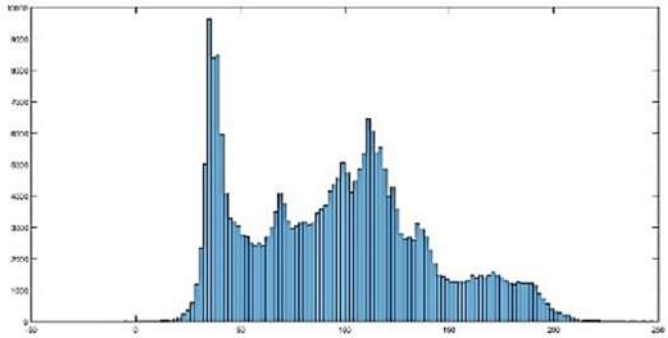


Figure 3.8: A histogram of DCT coefficients of decompressed image.

If the decompressed image is further compressed using a different quantization table, it would be a double compressed image. The histograms of DCT coefficients of double compressed image and image obtained after its decompression are shown in figure 3.9.



(a)

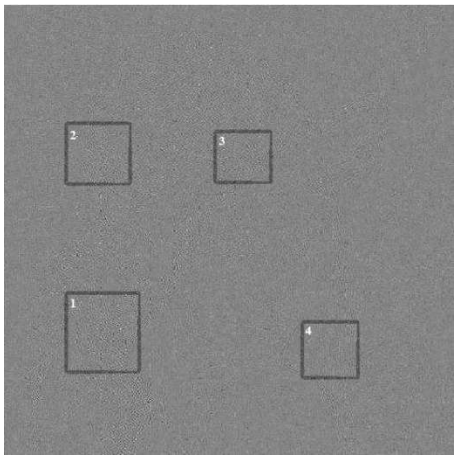


(b)

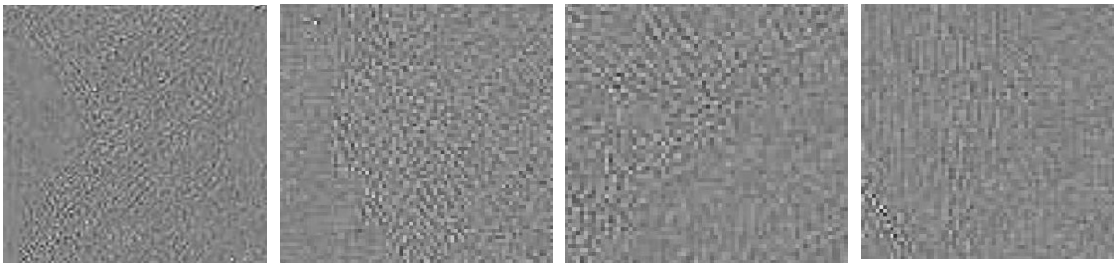
Figure 3.9: (a) A histogram of DCT coefficients of a double compressed image; (b) a histogram of DCT coefficients after decompressing a double compressed image.

It can be clearly observed that the image obtained after decompressing a compressed image is different from the image from the acquisition, although they both look very similar. Thus, the traces left by demosaicing process upon acquisition are somewhat altered through each compression. This can be explained through the following example. The figure 3.10 shows the difference image of the original image, 3.6 (a) and the reconstructed image after first compression.

Though the difference image obtained is not self-explanatory as the difference is not clearly visible. Thus, small blocks are segmented from the image at random to portray the aberrations observed as shown in figure 3.10. The artifacts left after compression are visible in latter images of figure 3.10 (b), 3.10 (c), 3.10 (d) and 3.10 (e). These artifacts are observed on the edges of the object, region possessing high frequency components.



(a)



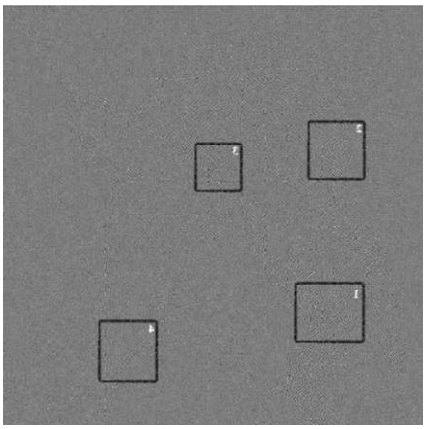
(b) (c) (d) (e)

Figure 3.10: The difference image obtained among the original image and the reconstructed image after the first compression.

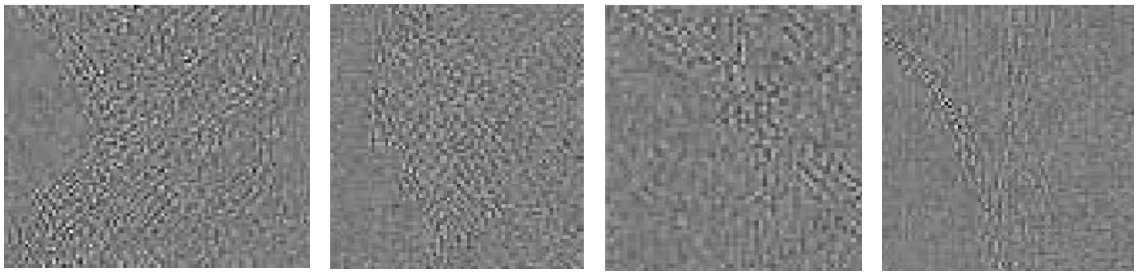
These type of artifacts is also visible if the image is double compressed too, as shown in figure 3.11. The difference image is closely observed at some segmented blocks as shown in figure, 3.11 (b), 3.11 (c), 3.10 (d), and 3.11 (d). The blocks portray the variations in the original and reconstructed image after double compression.

3.2.4 Forgery Map generation

The last step is the generation of a map indicating the tampered and untampered regions of the image. The map is generally based on the probability of presence or absence of CFA artifacts. The *apriori* probabilities of the two cases are assumed to be 0.5, i.e. $Pr[P_1] = Pr[P_2] = 0.5$, and from these *apriori* probabilities, the *posteriori* probability for being an authentic region is obtained.



(a)



(b) (c) (d) (e)

Figure 3.11: The difference image obtained among the original image and the reconstructed image after the second compression.

For estimation of *posteriori* probability, Bayesian approach is applied.

$$Pr\{P_1|M(k,l)\} = \frac{Pr\{M(k,l)|P_1\}}{Pr\{M(k,l)|P_1\} + Pr\{M(k,l)|P_2\}} \tag{3.5}$$

The equation (3.5) can be expressed as,

$$Pr\{P_1|M(k,l)\} = \frac{1}{1 + \mathcal{L}\{M(k,l)\}} \tag{3.6}$$

Where $\mathcal{L}$ is the likelihood ratio of probability of $\boldsymbol{M(k,l)}$, defined as:

$$\mathcal{L}\{M(k,l)\} = \frac{Pr\{M(k,l)|P_2\}}{Pr\{M(k,l)|P_1\}} \tag{3.7}$$

By applying equation (3.6) and (3.7) to each test block of the image, a likelihood map can be obtained, where each pixel is associated with the likelihood ratio of the block. The maps obtained are usually noisy itself. This is because the probability maps corresponds single recognition of feature $\boldsymbol{M(k,l)}$, which itself is not absolute. Thus, the feature extraction can be applied to large block values, to provide the probability map in a broader impression. But, by doing this the detection accuracy of the tampered region is affected. Thus, a proper trade-off is required to achieve a proper forgery map.

A suitable filtering strategy can be further applied to improve the localization performance of the algorithm. In general, the tampered region of the image is usually connected. Thus, by applying a low-pass spatial filter, like a mean or median filter, it is possible to highlight the connected forged portion.

3.2.5 Complete System Model

The complete system model is illustrated in the figure 3.6, where a forgery map is obtained based on probability corresponding to the tampered image. Each pixel in the forgery map resembles the probability to each image block (i.e. 2x2 in this case) to contain a CFA artifact, and other values amount to the forged regions.

Firstly, green channel is extracted from the image and then, the prediction error is computed. The in-camera processing is unknown, thus, the predictor is assumed. The weighted local standard deviation and skewness is calculated to obtain the feature $\boldsymbol{M(k,l)}$ for each 2x2 block. The feature **M** is then mapped to estimate GMM parameters and EM algorithm is applied to obtain the forgery map. Additionally, a proper filtering technique, either mean or median or any other suitable, can be applied to clear out the noise patterns in the forgery map.

3.3 Chapter Summary

The proposed scheme is an extended from the approach provided by Ferrara *et al.* in [15] which computed the variance of the prediction error to create the probability map of the presence or absence of CFA artifacts. In the proposed scheme prediction error is calculated between the acquired and interpolated pixels. Then the standard deviation and skewness is computed of this prediction error, instead of previous approach which evaluated variance. A feature **M** is postulated to generate the probability map that calculates the probability of presence or absence of CFA artifacts that have been altered during inclusion of forgery. A median filtering is also performed on a 2×2 block of map and forgery map is created depicting real and forged portions clearly.

Chapter 4

Results and Discussions

4.1 Introduction

The established algorithm is further tested on few datasets to provide the performance analysis. The algorithm proves fruitful even for the scenarios when the image is compressed at a certain ratio. In these cases, even the information about compression ratio of the image is not required. The various forgery techniques use processes like stretching, edge smoothing, filtering, rotating and image enhancing etc. that makes the forged image to look more authentic or original. But, with these processes, the CFA artifacts of the tampered region are significantly removed making it easier to localize the tampered region. These feature of the technique affirms its efficiency for its application in a broader sense. The suspected images are thus obtained from various social networking websites, like Twitter, Facebook, Instagram etc., and the technique is applied to test their authenticity. The algorithm is also compared with previously established methods, which justifies its prestige in recent times.

4.2 Comparative Analysis

The comparative compatibility of the proposed algorithm can be affirmed through an example. Here, an image is taken where forgery is introduced through splicing an object into the host image. The algorithm presented is compared with previously established methods. The example in figure 4.1 demonstrates the comparison between the proposed algorithm and the algorithms provided by Ferrara *et al.* (FBRP) [18], Dirik and Memon (DM) [61], and by Gallagher and Chen (GC-B and GC-L) [16]. The test is performed on JPEG image with bilinear interpolation and Median filtering is applied on the likelihood map for construction of the forgery map. For the fair scope of comparison, all the algorithms are applied to 8×8 block size whereas GC-L is computed on 7×7 blocks but is assumed to yield similar results. The proposed algorithm clearly outperforms the existing

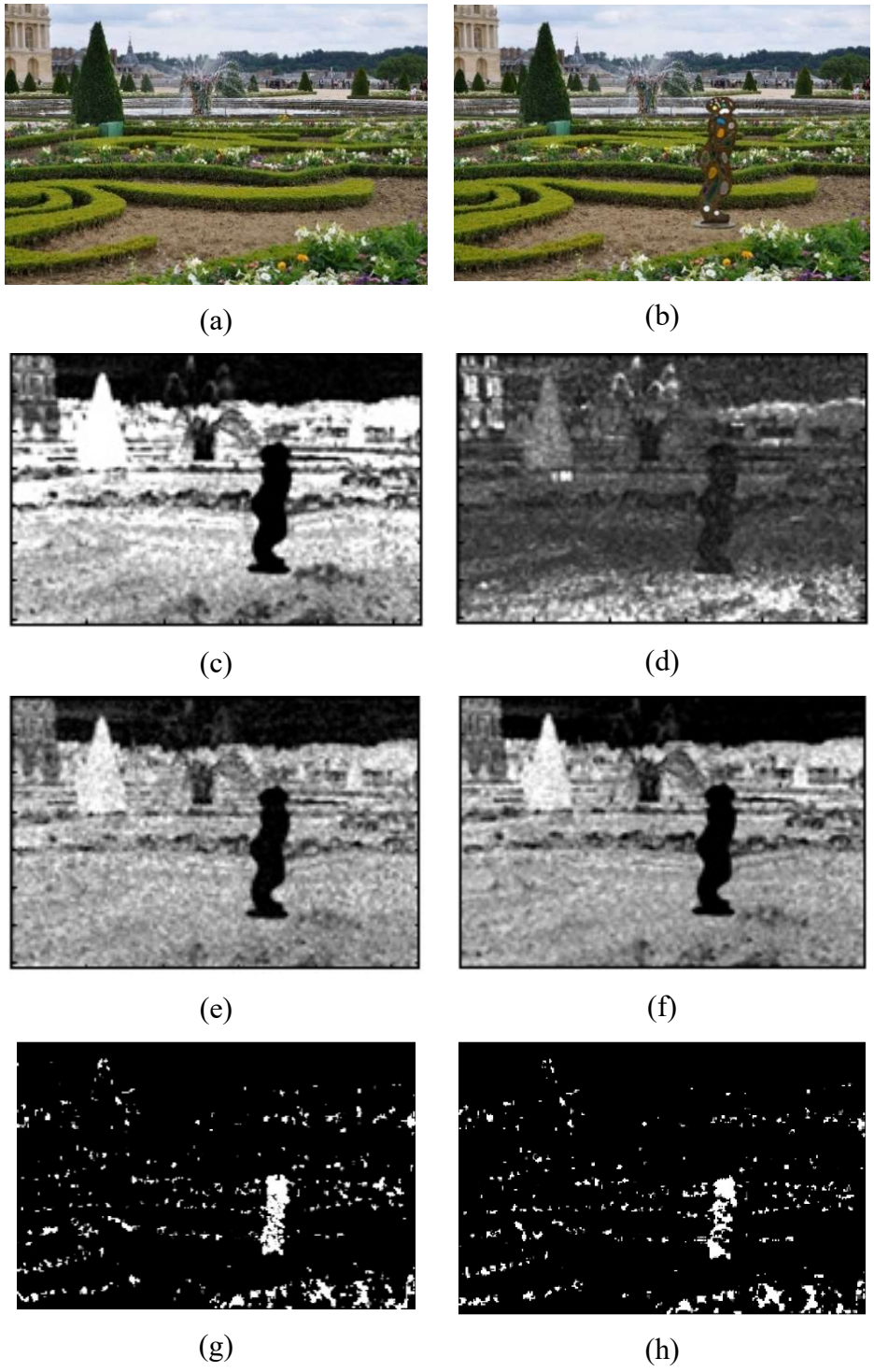


Figure 4.1: An example demonstrating tampering through splicing on an image: (a) Original image; (b) Tampered image; forgery maps localizing the tampered regions obtained using (c) FBRP algorithm; (d) DM algorithm; (e) GC-B algorithm; (f) GC-L algorithm; and the proposed algorithm considering (g) standard deviation, and (h) skewness of the prediction error.

algorithms, demonstrating significantly better localization of the tampered regions in the image.

The proper analysis of the forgery maps provides false positive results due to the presence of uniform or very sharp regions. In order to detect the tampered regions perfectly, there is a need for proper interpretation as solely accepting the forgery map to be perfect would be an understatement.

The forgery map can be analyzed on a local level through studying the CFA artifacts at as small as a 2×2 block. Thus, providing a fine-grained localization of the tampered region. The main drawback of the previous methods was the detection of the tampering was highly influenced by JPEG compression [18]. The results deteriorate with the high rates of compression or decompression. Thus, the proposed approach is extended to the JPEG compression scenarios.

In figure 4.1, it can be clearly observed that the localization of the tampered region, i.e. the object included, is very finely depicted in the forgery map of the proposed algorithm. The forgery map demonstrated in figure 4.1 (c) is also astounding but a slight pitfall in the result can be observed. If it is to be established that black part is inferred for tampered region and a white portion for actual image regions, then the sky region is wrongly depicted in the forgery map. This may be because that the sky region consists of high spatial frequencies. These high spatial frequencies are overall low in number and thus provides inconsistency in the calculation of prediction error and conclusively wrongly identified as tampered region. This shortcoming is also shared by other algorithms too, clearly visible in 4.1 (d), 4.1 (e) and 4.1 (f). In the proposed methods, this issue seems to have resolved as shown in figure 4.1 (g) and 4.1 (h).

4.3 Experimental Results

The remarkable feature of the proposed algorithm is that it shows performs equally well even when the image is compressed. Therefore, the algorithm is tested on a few images that were posted on social media. It is assumed that the images undergo some kind of compression while they are shared on the social networking websites. Though the reference

image is not known, thus it becomes very difficult to analyze the percentage of compression that an image has undergone. The results of the test of the algorithm on the compressed image are discussed further.

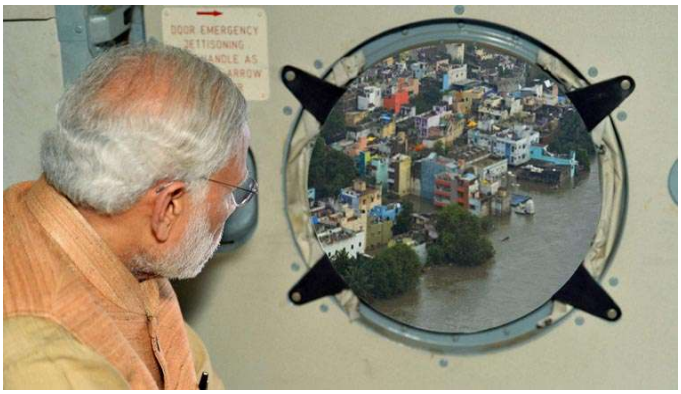
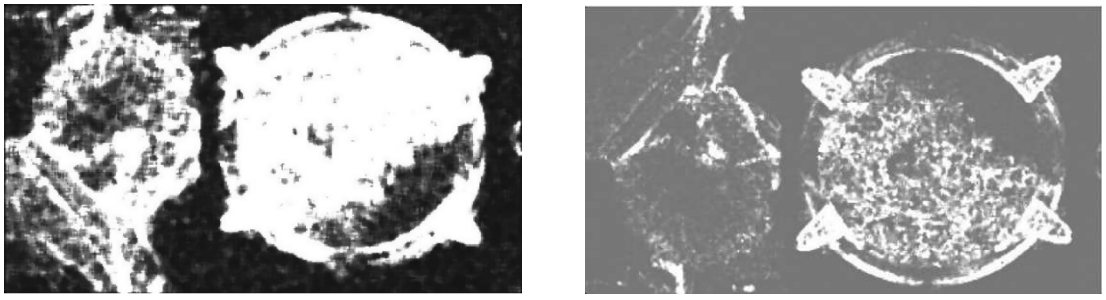


Figure 4.2: A doctored image of Indian Prime Minister Mr. Narendra Modi.

Figure 4.2 shows a photograph of Honorable Prime Minister of India, Mr. Narendra Modi, doing an aerial survey of the flood-hit areas of Chennai somewhere between 8th November 2015 to 14th December 2015. This photograph was posted by Press Information Bureau (PIB) on their website, and it took twitter by storm. This photograph was actually doctored by PIB and was conclusively removed.

The image was tested with the discussed algorithm in the previous section, and the results obtained are shown in figure 4.3.



(a) (b)

Figure 4.3: Forgery maps of fig. 4.2 using (a) standard Deviation and (b) skewness of the prediction error.

The map shown in figure 4.3 (a) is when the standard deviation of the prediction error is evaluated and figure 4.3 (b) is when skewness of prediction error is calculated. It can be observed that by applying standard deviation the tampered regions can be distinguished properly. As in the case, where skewness is employed, the edges of the tampered region boundary is specifically extracted. Here, it can be clearly observed that the tampered portion is very specifically depicted in the forgery map. This is because it shows the absence of the CFA artifacts which were actually left during the interpolation process. The introduction of forgery in the image has changed or removed the CFA artifacts, thus, depicting the forgery.

The images shown here are from various social networking sites. Also, the images are compressed at least once because the size of the image varies while uploading to a website according to the websites capacity. The previous algorithm in [18], showed somewhat unsatisfactory results in scenarios when the image was compressed or uncompressed at high-quality factor. That limitation is removed in this algorithm by taking standard deviation and skewness into account. The algorithm shows similar results for detection even when the image is compressed or not, also the information of compression ratio is not required.

The proposed algorithm is also employed on few more images of social media and their results are too shown in figure 4.4.

4.4 Performance Analysis

The basic fundamental requirement of the obtained forgery map based on the probability of the presence or absence of the CFA artifacts is its accuracy to clearly differentiate between the tampered region(s) and the original region(s) of the image, also known as localization property. This generally defines the quality of the forgery map obtained and can be used as a parameter to define its acceptability as a proper detection map. The doctored images cannot be used alone to test the accuracy of the map obtained.

This can be done by making a forged image. Thus, a digiimage is taken and its map is obtained by applying the proposed scheme. Then, a forgery is introduced in that particular image through ‘PhotoShop’, ‘Microsoft Paint’ etc., and its forgery map is accomplished

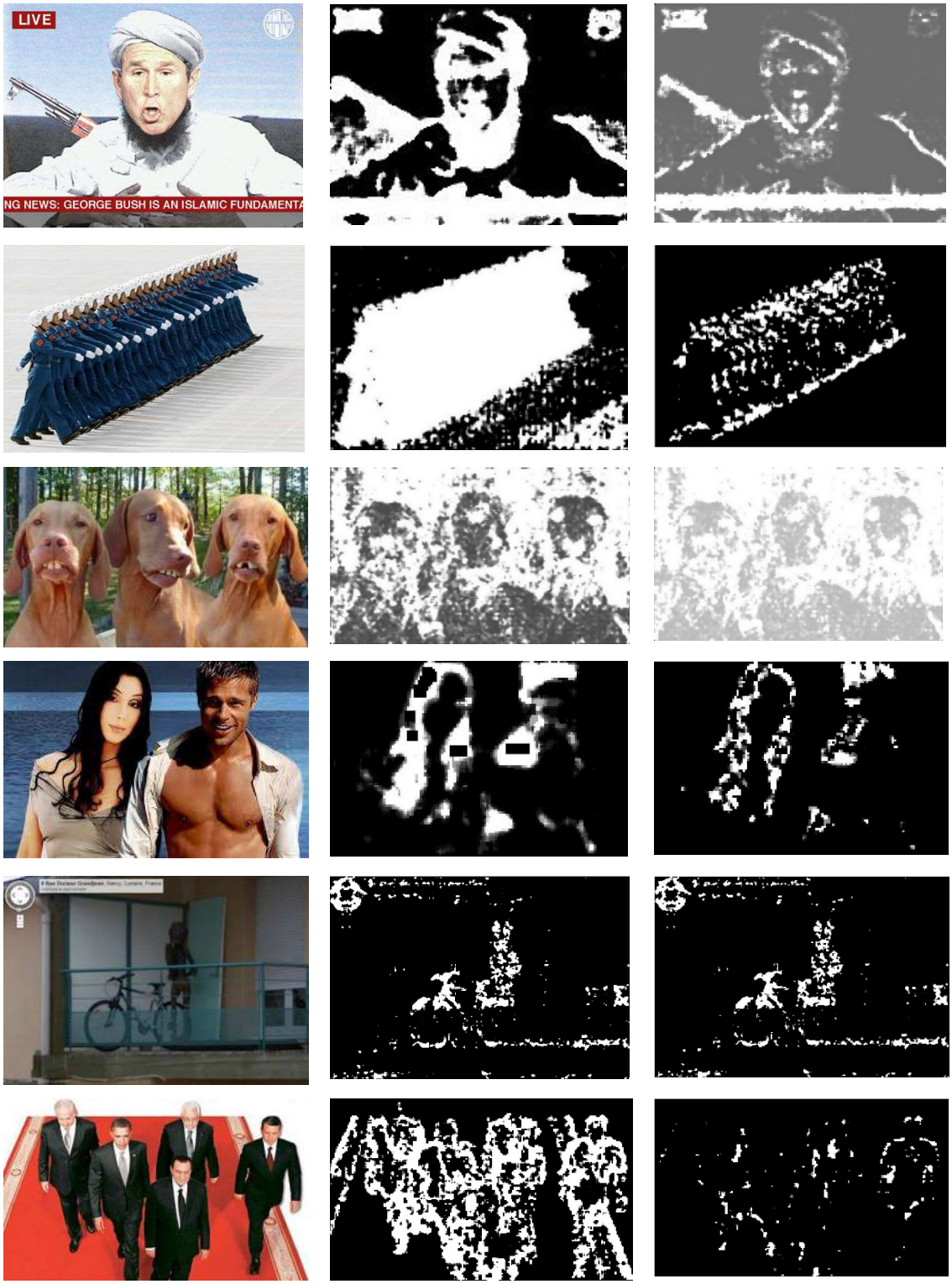


Figure 4.4: The experimental results with first column of doctored images, second column representing the forgery map using standard deviation, and third column depicting forgery maps using skewness of the prediction error.

using the same established algorithm. The maps obtained through both the images, the original one and the tampered one, are accessed together to evaluate the quality of the map. In this, it has to make sure that the algorithm is somehow unaffected to the amount of forgery introduced. The parameters used to evaluate the forgery maps rather only consider the fact to properly identify the forgery.

For this consideration, Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index (SSIM) are used as parameters. SSIM provides the similarity between the two images, whereas PSNR defines the actual quality of the map. Mean Square Error (MSE) of the image has also been calculated, defining the total change in both the maps.

The algorithm is tested on 10 images each of three datasets, namely, UCID containing '.tif' images, and datasets of 'Nikon D50' and 'Nikon D7000', both containing '.jpg' images. A PSNR of value between 30dB and 50dB is percieved as good quality image. If the forgery map obtained has PSNR lying in this range, would conclusively mean that the map is of good quality.Thus, it can be easily demonstrated with ten images only. The following results for standard deviation and skewness has been noted.

Tiff Image	PSNR	SSIM	MSE
01.tif	31.4265	0.9743	2.4501
02.tif	61.1640	0.9993	0.0733
03.tif	61.1100	0.9994	0.0273
04.tif	60.5778	0.9998	0.0088
05.tif	41.6905	0.9969	0.0860
06.tif	32.3719	0.4374	9.2472
07.tif	33.9983	0.9681	1.0183
08.tif	23.7863	0.8858	3.0549
09.tif	30.4216	0.9400	2.6965
10.tif	33.6192	0.8861	5.8646

(a)

Tiff Image	PSNR	SSIM	MSE
01.tif	41.8801	0.9010	40.8815
02.tif	36.0718	0.9100	08.8655
03.tif	35.7773	0.9228	28.2610
04.tif	37.5953	0.9086	25.6785
05.tif	32.1237	0.9102	07.2232
06.tif	31.6197	0.8585	01.0630
07.tif	41.4963	0.9438	79.1374
08.tif	28.2561	0.8733	09.1160
09.tif	34.4360	0.9276	14.8534
10.tif	25.7861	0.5330	05.2123

(b)

Table 4.1: The parameters of the propose scheme when performed on *dataset* UCID with (a) standard deviation, and (b) skewness.

JPEG Image	PSNR	SSIM	MSE
01.jpg	39.1427	0.8376	2.1686
02.jpg	37.8635	0.8135	3.8052
03.jpg	39.1448	0.8662	8.3662
04.jpg	43.0910	0.8852	2.5283
05.jpg	35.9364	0.8450	2.3724
06.jpg	27.6323	0.1364	2.6823
07.jpg	27.4392	0.3441	3.3440
08.jpg	31.5778	0.5922	3.5259
09.jpg	36.5213	0.4578	4.6243
10.jpg	29.4456	0.6334	1.0575

(a)

JPEG Image	PSNR	SSIM	MSE
01.jpg	36.4767	0.9126	27.6000
02.jpg	37.8034	0.9238	47.6987
03.jpg	44.5103	0.9549	39.4192
04.jpg	36.0432	0.9655	43.8299
05.jpg	37.9270	0.9591	43.5828
06.jpg	35.5892	0.8660	33.8585
07.jpg	37.7691	0.9158	48.0767
08.jpg	44.5496	0.9567	38.1616
09.jpg	42.4369	0.9361	39.8543
10.jpg	37.9559	0.9616	43.2942

(b)

Table 4.2: The parameters of the propose scheme when performed on *dataset* Nikon D50 with (a) standard deviation, and (b) skewness.

JPEG Image	PSNR	SSIM	MMSE
01.jpg	31.4624	0.8089	1.3227
02.jpg	34.7566	0.8130	5.9102
03.jpg	33.7739	0.7591	9.2142
04.jpg	32.0725	0.7266	1.5226
05.jpg	40.6737	0.8248	2.6901
06.jpg	24.0277	0.6383	2.4023
07.jpg	27.7026	0.5077	1.2323
08.jpg	23.9476	0.3411	9.8874
09.jpg	32.1991	0.6221	1.7361
10.jpg	36.5953	0.4683	8.8259

(a)

JPEG Image	PSNR	SSIM	MSE
01.jpg	40.2436	0.9243	47.0220
02.jpg	32.2709	0.9340	19.7076
03.jpg	33.0426	0.9503	21.0210
04.jpg	29.6283	0.8989	15.3553
05.jpg	33.4119	0.9382	33.1508
06.jpg	32.0392	0.9215	20.7875
07.jpg	33.0480	0.9511	20.9950
08.jpg	29.5065	0.8941	15.7921
09.jpg	33.3515	0.9343	33.6155
10.jpg	40.0248	0.9160	10.2034

(b)

Table 4.3: The parameters of the propose scheme when performed on *dataset* Nikon D7000 with (a) standard deviation, and (b) skewness.

It can be noted that the PSNR in all the cases is around the desired range. Thus, it can be verified that the forgery map obtained is of a good quality such that the tampered and actual regions in the image are easily distinguished. The proposed scheme is then employed with a Support Vector Machine (SVM) to determine the accuracy of the algorithm. In this

evaluation, a total of 50 images are used of UCID dataset and forgery is introduced in these images. Thus, a total of 100 images are tested upon, to evaluate the performance of the algorithm. An SVM classifier is a binary classifier that in this case classifies the images into two classes: real and forged. The algorithm under test is one that uses standard deviation of the prediction error which is calculated through bilinear interpolation. The map is generated by applying median filtering on a 2×2 block.

On the basis of the inputs and functioning of the classifier, two parameters are calculated, namely True Positive Rate (TPR) and False Positive Rate (FPR). TPR refers to the total number of forged images that are properly classified under forged class, whereas, FPR provides the number of real images falsely classified under forged class. The basic ratios of the TPR and FPR can be expressed as:

$$TPR = \frac{N_{TD}}{N_{TT}} \qquad FPR = \frac{N_{FD}}{N_{TT}} \tag{4.1}$$

where N_{TD}, N_{FD}, and N_{TT} refers to truly detected, falsely detected, and total truly detected images to class forged. The algorithm is tested and TPR and FPR are calculated for various threshold values to create a Receiver operating characteristic (ROC) curve shown in figure 4.5.

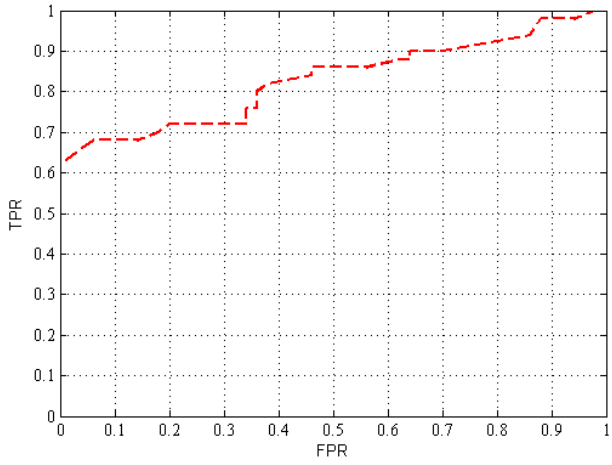


Figure 4.5: ROC curve considering 50 images of data set UCID and 50 forged images. The algorithm has calculates standard deviation of the prediction error.

4.5 Chapter Summary

The established algorithm is tested upon on various images to evaluate its significance. The algorithm is compared with a few previously established algorithms and results are obtained. The results obtained show that the proposed algorithm is better than the previous methods and can be easily applied to a variety of images.

The algorithm is tested on various images taken from social networking websites as well. The main idea was to manifest that the technique performs well even when the image is in compressed form and the information of the amount of compression is still unknown. The results obtained through tests are also provided in this chapter.

To evaluate the performance of the scheme, it is also tested on a few image datasets, with and without forgery, and quality determining parameters are calculated and provided in a tabular form. SVM classifier is also employed to credit the scheme of its accuracy to determine if the image is forged or not. The accuracy of the scheme to correctly identify forged image is 80%. The ROC curve obtained provides the results in favor of TPR, when calculated at different threshold values.

Chapter 5

Conclusions and Future Scope

5.1 Prologue

It can now be established that the proposed scheme performs well for the detection of forgery in the image and its tampered region localization capability is also very good. The algorithm is performed for both standard deviation and skewness and results in both the cases are astonishing. The test of the scheme on the image datasets and their respective results obtained provide satisfactory results.

5.2 Conclusions

The method discussed in this dissertation, localizes the forged region of the digital image provided that there is no prior information about the location of the tampered part(s). Also, the images used for validation are compressed at random compression factor and still the results are valid while distinguishing between the tampered and original portions of the image.

The consideration of standard deviation and skewness of the prediction error instead of the variance in [18], has altogether improved the quality of forgery map, as the tampered objects or regions are localized very accurately. The feature extracted is performed at 2×2 size block, providing a fine-grained tampering detection. The proposed scheme outperforms the existing detection techniques because the difference between the forged and actual regions can be clearly observed.

The existing techniques have a tendency to provide incorrect results when the image is compressed or decompressed at high ratio. This shortcoming is also improved by the proposed scheme. The algorithm is employed on a wide range of social media images where the images are in compressed form, and the compression rate is often unknown. The algorithm proves to be successful in these cases too as the images on which experimental results have been obtained, are all from social networking websites. The information about

the compression ratio or format is unknown in these cases. The proposed algorithm thus caters two concerns: the detection on the basis of existence of CFA artifacts in the image, and the forgery detection in scenarios even when the image is compressed.
The algorithm is tested on a few datasets to evaluate its performance. An SVM classifier is employed with the algorithm, which demonstrates that the algorithm is 80% accurate to correctly classify a forged image. The forgery map obtained is of a good quality and can be verified through the obtained PSNRs.

5.3 Future Scope

The main problem in image forensics nowadays is that forgery is added into an image with a combination of various tools. Thus, while analyzing the traces, only one type of attack would be exposed which would not be reliable as a lot of the image would be left out of testing. It is a need to incorporate various tools together with this method to reveal forgery.

- The main drawback of this algorithm is the forgery map is small in size as compared to the test image in accordance with the block size. In simple words, if the block size is taken to be 2×2 pixels for calculation of prediction error, the size of the forgery map is the half the size of the test image. Thus, it would be more convenient if the forgery map is of the same size of the test image.
- Sometimes due to the presence of uniform regions in the image, the results can yield slight inconsistencies. A proper segmentation algorithm employed with this algorithm can reduce these inconsistencies.

REFERENCES

[1] A. Piva, "An Overview of Image Forensics", *ISRN Signal Processing*, vol. 496701, pp. 1-22, 2013.

[2] *Photo tampering throughout history* [Online], 2012. Available: http://www.fourandsix.com/photo-tampering-history/.

[3] S. Bayram, H. T. Sencar, N. Memon, and I. Avcibas, "Source camera identification based on CFA interpolation," in *Proc. IEEE International Conference on Image Processing 2005* (*ICIP '05*), pp. 69–72, September 2005.

[4] F. Galvan, G. Puglisi, A. R. Bruna, and S. Battiato, "First Quantization Matrix Estimation from Double compressed JPEG Images," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 8, 2014.

[5] K. Kaur. "Feature Extraction Method based on Various Scanning Techniques in Iris Recognition System." M.E. thesis, Thapar University, Patiala, 2015.

[6] X. Wu and N. Memon. "Context-based, adaptive, lossless image coding." *IEEE transactions on Communications* 45.4 (1997): 437-444.

[7] A. Swaminathan, M. Wu, and K. J. R. Liu, "Nonintrusive component forensics of visual sensors using output images," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 1, pp. 91–105, 2007.

[8] P. D. Pandit and M. Rajput, "Survey on Anti-forensic Operations in Image Forensics," *International Journal of Computer Science and Information Technologies*, vol. 5, no. 2, pp. 1570-1573, 2014.

[9] M. Barni and A. Costanzo, "A fussy approach to deal with uncertainty in Image Forensics," *Signal Processing: Image Communication*, vol. 27, no. 9, pp. 935-1048, 2012.

[10] S. Dehnie, "Digital Image Forensics for identifying Computer generated and Digital camera images," in *Proc. IEEE International Conference on Image Processing*, pp. 2313-2316, 2006.

[11] S. Bayram, H. T. Sencar, and N. Memon, "Classification of digital camera-models based on demosaicing artifacts," *Digital Investigation*, vol. 5, no. 1-2, pp. 49–59, 2008.

[12] C. McKay, A. Swaminathan, H. Gou, and M. Wu, "Image acquisition forensics: forensic analysis to identify imaging source," in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing* (*ICASSP '08*), pp. 1657–1660, 2008.

[13] A. Swaminathan, M. Wu, and K. J. R. Liu, "Digital image forensics via intrinsic fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 101–117, 2008.

[14] A. C. Popescu and H. Farid, "Exposing digital forgeries in color filter array interpolated images," *IEEE Transactions on Signal Processing*, vol. 53, no. 10, pp. 3948–3959, 2005.

[15] A. C. Gallagher, "Detection of linear and cubic interpolation in JPEG compressed images," in *Proc. Canadian Conference on Computer and Robot Vision*, pp. 65–72, 2005.

[16] A. C. Gallagher, and T. Chen, "Image authentication by detecting traces of demosaicing," in *Proc. IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops* (*CVPRW '08*), pp. 1–8, 2008.

[17] A. E. Dirik, and N. Memon, "Image tamper detection based on demosaicing artifacts," in *Proc. International Conference on Image Processing (ICIP '09)*, pp. 1497–1500, 2009.

[18] P. Ferrara, T. Bianchi, A. De Rosa, and A. Piva, "Image Forgery Localization via Fine-Grained Analysis of CFA Artifacts," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 5, pp. 1566-1577, 2012.

[19] J. Janesick, *Scientific Charge-Coupled Devices*, 1st edition, vol. 117, Bellingham Washington: SPIE Press, 2001.

[20] I. Amerini, R. Caldelli, V. Cappellini, F. Picchioni, and A. Piva, "Estimate of PRNU noise based on different noise models for source camera Identification," *International Journal of Digital Crime and Forensics*, vol. 2, no. 2, pp. 21–33, 2010.

[21] M. Chen, J. Fridrich, M. Goljan, and J. Lukáš, "Determining image origin and integrity using sensor noise," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 74–90, 2008.

[22] S. Lin and L. Zhang, "Determining the radiometric response function from a single grayscale image," in *Proc. IEEE Computer Society Conference on Computer Vision and Pattern Recognition* (*CVPR '05*), vol. 2, pp. 66–73, 2005.

[23] T. T. Ng, S. F. Chang, and M. P. Tsui, "Using geometry invariants for camera response function estimation," in *Proc. IEEE Computer Society Conference on Computer Vision and Pattern Recognition* (*CVPR '07*), pp. 1–8, 2007.

[24] T.-T. Ng, S.-F. Chang, J. Hsu, L. Xie, and M.-P. Tsui, "Physicsmotivated features for distinguishing photographic images and computer graphics," in *Proc. 13th Annual ACM International Conference on Multimedia*, H. Zhang, T.-S. Chua, R. Steinmetz, M. S. Kankanhalli, and L. Wilcox, Eds., pp. 239–248, ACM, 2005.

[25] Y. F. Hsu and S. F. Chang, "Camera response functions for image forensics: an automatic algorithm for splicing detection," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 816–825, 2010.

[26] H. Gou, A. Swaminathan, and M. Wu, "Intrinsic sensor noise features for forensic analysis on scanners and scanned images," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 3, pp. 476–491, 2009.

[27] C.-H. Choi, M. J. Lee, and H. K. Lee, "Scanner identification using spectral noise in the frequency domain," in *Proc. International Conference on Image Processing (ICIP '10)*, pp. 2121–2124, 2010.

[28] N. Khanna and E. J. Delp, "Intrinsic signatures for scanned documents forensics: effect of font shape and size," in *Proc. International Symposium on Circuits and Systems* (*ISCAS '10*), pp. 3060–3063, 2010.

[29] S. Saha and M. Jangid, "Forensic Approach of detection of Digital Image tampering using Watermarking embedding and Extraction," in *Proc. 4th SARC-IRF International Conference*, 2014.

[30] K. M. Kumar, "A novelty approach on Forgery Digital Image Detection based Image Source Identification ANN," *International Journal on Computational Sciences & Applications* (*IJCSA*), vol. 5, no.1, 2015.

[31] Z. Fan and R. de Queiroz, "Maximum likelihood estimation of JPEG quantization table in the identification of bitmap compression history," in *Proc. International Conference on Image Processing* (*ICIP '00*), pp. 948–951, 2000.

[32] Z. Fan and R. L. de Queiroz, "Identification of bitmap compression history: JPEG detection and quantizer estimation," *IEEE Transactions on Image Processing*, vol. 12, no. 2, pp. 230–235, 2003.

[33] Z. Wang, A. C. Bovik, and B. L. Evans, "Blind measurement of blocking artifacts in images," in *Proc. International Conference on Image Processing* (*ICIP '00*), vol. 3, pp. 981–984, 2000.

[34] H. Liu and I. Heynderickx, "A no-reference perceptual blockiness metric," in *Proc. IEEE International Conference on Acoustics, Speech and Signal Processing* (*ICASSP '08*), pp. 865–868, 2008.

[35] S. Tjoa, W. S. Lin, H. V. Zhao, and K. J. R. Liu, "Block size forensic analysis in digital images," in *Proc. IEEE International Conference on Acoustics, Speech and Signal Processing* (*ICASSP '07*), pp. 1633–1636, 2007.

[36] W. Luo, J. Huang, and G. Qiu, "JPEG error analysis and its applications to digital image forensics," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 480–491, 2010.

[37] R. Neelamani, R. de Queiroz, Z. Fan, S. Dash, and R. G. Baraniuk, "JPEG compression history estimation for color images," *IEEE Transactions on Image Processing*, vol. 15, no. 6, pp. 1365–1378, 2006.

[38] J. Lukáš and J. Fridrich, "Estimation of primary quantization matrix in double compressed JPEG images," in *Proc. Digital Forensics Research Conference* (*DFRWS '03*), 2003.

[39] H. Farid, "Exposing digital forgeries from JPEG ghosts," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 1, pp. 154–160, 2009.

[40] W. Luo, J. Huang, and G. Qiu, "JPEG error analysis and its application to Digital Image Forensics," *IEEE Transactions on Image Forensics and Security*, vol. 5, no. 3, pp. 480-491, 2010.

[41] L. Zhulong, L. Xianghua, and Z. Yuqian, “Passive Detection of Copy-Paste tampering for Digital Image Forensics,” in *Proc. IEEE International Conference on Intelligent Computation and Automation*, pp. 649-652, 2011.

[42] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, “Detection of copy-move forgery in digital images,” in *Proc. Digital Forensic Research Workshop*, 2003.

[43] W. Q. Luo, J. W. Huang, and G. P. Qiu, “Robust detection of region duplication forgery in digital image,” in *Proc. International Conference on Pattern Recognition* (*ICPR ’061*), pp. 746–749, 2006.

[44] A. C. Popescu and H. Farid, “Exposing digital forgeries by detecting duplicated image regions,” Tech. Rep. TR2004-515, Dartmouth College, Computer Science, Hanover, NH, USA, 2004.

[45] M. Kirchner, “Fast and reliable resampling detection by spectral analysis of fixed linear predictor residue,” in *Proc. 10th ACM Workshop on Multimedia and Security* (*MM&Sec ’08*), A. D. Ker, J. Dittmann, and J. J. Fridrich, Eds., pp. 11–20, ACM, 2008.

[46] M. Kirchner and T. Gloe, “On resampling detection in recompressed images,” in *Proc. 1st IEEE International Workshop on Information Forensics and Security* (*WIFS ’09*), pp. 21–25, 2009.

[47] S. Prasad and K. R. Ramakrishnan, “On resampling detection and its application to detect image tampering,” in *Proc. IEEE International Conference on Multimedia and Expo* (*ICME ’06*), pp. 1325–1328, 2006.

[48] B. Mahdian and S. Saic, “On periodic properties of interpolation and their application to image authentication,” in *Proc. International Symposium on Information Assurance and Security*, pp. 439–446, 2007.

[49] W. Weimin, W. Shuozhong, and T. Zhenjun, “Estimation of rescaling factor and detection of image splicing,” in *Proc. 11th IEEE International Conference on Communication Technology* (*ICCT ’08*), pp. 676–679, 2008.

[50] N. Dalgaard, C. Mosquera, and F. Pérez-González, “On the role of differentiation for resampling detection,” in *Proc. International Conference on Image Processing* (*ICIP ’10*), pp. 1753–1756, 2010.

[51] G. S. Song, Y. I. Yun, and W. H. Lee, "A new estimation approach of resampling factors using threshold-based peak detection," in *Proc. IEEE International Conference on Consumer Electronics* (*ICCE '11*), pp. 731–732, 2011.

[52] H. Yao, S. Wang, Y. Zhao, and X. Zhang, "Detecting image forgery using perspective constraints," *IEEE Signal Processing Letters*, vol. 19, pp. 123–1126, 2012.

[53] H. Hailing, G. Weiqiang, and Z. Yu, "Detection of copy-move forgery in digital images using sift algorithm," in *Proc. Pacific-Asia Workshop on Computational Intelligence and Industrial Application (PACIIA '08)*, vol. 2 of *IEEE Computer Society*, pp. 272–276, 2008.

[54] D. G. Lowe, "Object recognition from local scale-invariant features," in *Proc. International Conference on Computer Vision (ICCV '99)*, pp. 1150–1157, 1999.

[55] I. Amerini, L. Ballan, R. Caldelli, A. del Bimbo, and G. Serra, "Geometric tampering estimation by means of a sift-based forensic analysis," in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing* (*ICASSP '10*), pp. 1702–1705, 2010.

[56] X. Pan and S. Lyu, "Detecting image region duplication using sift features," in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing* (*ICASSP '10*), pp. 1706–1709, IEEE, March 2010.

[57] H. Farid, "Image Forgery Detection," *IEEE Signal Processing Magazine*, vol. 26, no. 2, pp. 16-25, 2009.

[58] D. Cozzolino, G. Poggi, C. Sansone, L. Verdoliva, "A Comparative Analysis of Forgery Detection Algorithms," in *Proc. Joint IAPR International Workshop on Structural, Syntactic and Statistical Pattern Recognition*, vol. 7626, pp. 693-700, 2013.

[59] M. Kharrazi, H. T. Sencar, N. Memon, "Improving steganalysis by fusion techniques: a case study with image steganography," *Transactions on Data Hiding and Multimedia Security*, vol. 4300, pp. 123–137, 2006.

[60] S. H. Park and A. No, 2009, *Analysis on Color Filter Array Image Compression Methods* [Online]. Available: https://scholar.google.co.in/scholar?oi=bibs&hl=en&cluster=3754062411869037504.

[61] A. E. Dirik and N. Memon, "Image tamper detection based on demosaicing artifacts," in *Proc.16th IEEE International Conference on Image Processing* (*ICIP '09*), pp. 11-20, 2009.

LIST OF PUBLICATIONS

1. "A review on Digital Image Forensics," in *International Conference on Signal Processing*, Samrat Ashok Technological Institute (SATI), Vidisha (M.P.) – *Communicated*, 2016.
2. "Digital Image Forgery Detection in Social Network domain," *Forensics Science International – Communicated*, 2016. (*SCI Indexed*).

Amneet_Thesis

by Amnnet Singh

Amneet_Thesis

ORIGINALITY REPORT

17%	16%	10%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.cosy.sbg.ac.at Internet Source	5%
2	millib.rtarf.mi.th Internet Source	1%
3	profs.info.uaic.ro Internet Source	1%
4	Submitted to Sardar Vallabhbhai National Inst. of Tech.Surat Student Paper	1%
5	www.cs.dartmouth.edu Internet Source	1%
6	www.shahidulnews.com Internet Source	1%
7	en.wikipedia.org Internet Source	1%
8	dspace.thapar.edu:8080 Internet Source	1%
9	Submitted to University of Derby	