CHAPTER 1
INTRODUCTION

In this era, most of the population is having smart devices with digital cameras in them. Photographs captured by these devices are an important source of information. These photographs play a vital role in different ways. For example, photos are used in the courtroom as evidence, pictures clicked by reporters are used in news to telecast or to publish in the magazine/journals and medical images are used to detect and diagnose the diseases. An image editing tool changes the semantics of such photographs. This practice usually comes into the category of forgery and forgery in images is a matter of concern. This chapter gives an overview of a digital image, digital image forgery including its types, how forgery is done in the image, and what are the consequences of the forgery in a digital image? This chapter also focuses on research findings that are the motivation behind the research work. Further, the chapter lists the objectives of the research and contributions to the thesis followed by a brief discussion on the organization of the thesis. The main objective of this chapter is to set a base for the thesis and its role in the research.

1.1 Background

Millions of images are being captured every day either by smartphones or scanning devices. According to Business Insider India [1], more than 1 trillion photos were taken in 2016 and 85% of them were taken from smartphones. These images are being stored on cloud storage to share, view, and edit them. Rather than that these images are also being used for scientific reports, evidence in courtrooms, news to broadcast over electronic media, and diagnosis of diseases. Google is also on a mission to digitize the world's books that are ever printed [2]. Hence, images can be interpreted as the

information currency of this era. So, what is a digital image? How to define it? A digital image can be defined as a 2D signal that varies over spatial coordinates *x* and *y*, and can be mathematically expressed as:

$$I = f(x, y) \tag{1.1}$$

Here, *f* at any pair of coordinates *(x,y)* is called the intensity of that image at that point. This point with the intensity value is known as pixel or picture element. Image manipulation is performed keeping the various mixed intension in the mind. Some of them are– beautifying the image, creating awareness in society, creating MEMEs just for enjoyment and defaming various personalities. Apart from these, image manipulation is done in an undesirable manner, mostly for libeling individuals from various sectors of society and creating MEMEs of them. This is very popular on social media platforms these days. Beautifying an image doesn't change the semantic of the image and is not harmful as manipulating the content of the image turns semantic. Thus, the latter comes into the category of forgery.

1.2 Digital Image Forgery

With the advancement of smart devices, graphic editing applications are easily available on these devices. Using these applications, manipulation of images gets easier and cheaper. The availability of applications on the fingertip in handheld devices has made it more convenient to manipulate computerized pictures. An individual with zero professional skill can manipulate the photos according to his/her desire. Excessive development of such editing tools like Adobe Photoshop, Sensi [3], and FacApp [4] can be used to alter original image and alteration can be done in such a way that a bare human eyes cannot differentiate between the altered and original image. The only change in the intensity of pixels without altering the content of an image (i.e., beautifying an

image/image retouching), is mild processing while altering the content of an image changes the semantic meaning of the image. Thus, just enhancing an image is not the case of forgery while manipulating the content of an image is known as forging/morphing an image, such an act is known as digital image forgery and manipulated images are called forged/fake/tampered or morphed images. The image forgery can be done in different ways, some of them are:

- Erasing the region of an image.
- Replacing a region of an image with another region of the same image.
- Replacing a region of an image with a region of another image.
- Resizing (rescaling) of the replaced object.

Similarly, the following points define how forgery can be done in reports and scanned documents:

- Addition or alteration of handwritten entries in cheques, medical certificates, IOUs (I owe you), etc.
- Addition of printed text to a document that has already been signed.
- Alteration to the pages or contents in printed documents.
- Manipulations of the signature(s) in the documents

(a) (b) (c)

Figure 1.1: Example of editing of an image with mild processing (a) Original Lenna Image (b) Color processed Lenna image (c) Image with noise addition

If there are *n* number of non-overlapped regions in an image and represented by $\{R_1, R_2 \ldots R_n\}$, the original image I_o can be given by:

$$I_o = \bigcup_{i=1}^{n} (R_i) \tag{1.2}$$

Here, region R_i is the collection of pixels and $R_i \cap R_j = \emptyset$ for all i and j where $i \neq j$. If the erased regions from the original image are $R = \{\cup R_i : i \leq n\}$ then the forged image can be represented as:

$$I_F = I_o - R \tag{1.3}$$

Erasing the region of an image defines that pixels of the region are replaced by either maximum value or minimum value of intensity. If a region R_i is replaced by R_j from the original image I_o then the forged image will be represented as:

$$I_F = \{R_1 \cup R_2 \dots R_j \cup R_{i+1} \dots R_{j-1} \cup R_j \dots R_n\} \tag{1.4}$$

Similarly, if the region of the original image R_i is replaced by a region of another original image S_i then the forged image will be defined as:

$$I_F = \{R_1 \cup R_2 \dots S_i \cup R_{i+1} \dots R_n\} \tag{1.5}$$

1.2.1 Types of Digital Image Forgery

Considering different manipulation of an image, image forgery can be classified into two different classes: one is a copy-move forgery and another is image splicing.

(a) (b) (c) (d)

Figure 1.2: Examples of digital image forgery (region alteration) (a) Original Image (b) Image Splicing (c) Original Image (d) Copy-move forgery

1.2.1.1 Copy Move Forgery

Copy-move forgery (CMF) is one of the most common types of forgery techniques. In CMF, part of an image is copied and being pasted onto the same image

intentionally, the purpose is to conceal the area/object in the original image with some other part of the same image [5]. It can be done using basic image editing tools. As shown in figure 1.2(c) is an original image- there is only one scooter and in the tampered image shown in figure 1.2(d)- the same scooter is copied and pasted.

1.2.1.2 Image Splicing

It is a composition technique. Image splicing is the act of cropping regions of an image and pasting it into a different image to create a new forged picture [6]. Thus, it is a combination of two images, resulting in fake images, as in Figure 1.2(a-b). This forged image was posted on Downing Street's Facebook page (social media) in 2015, after which British Prime Minister David Cameron was criticized for wearing a Remembrance Day poppy [7]. The posted photo was spliced using some editing software. The photo was later removed from its official page.

1.2.2 Need of the Digital Image Forgery Detection

The floating images on the web and social media platforms can influence public opinions. In that case, forged images may change the actions of the community. These fake images have the competence to change the mindset of an individual, deceiving and emotionally distressing people [8]. There are cases of digital image manipulation in academic papers. As an instance, in a survey conducted by [9], 15% of the respondents admitted that they are engaged in scientific misconduct such as fabricating, falsifying, plagiarizing, or manipulating data during the year 2011 to 2014. Another study states that approximately 20% of accepted manuscripts in the Journal of Cell Biology contain manipulated figures and at least 1% of them have fraudulent manipulations [10]. Even political parties have been using forged images to claim false achievements to gain more votes. Modification of identity documents takes a few seconds using editing software. In

the field of medicine, patient reports are highly confidential and always supposed to be authentic. Scanned copies of medical documents are used as proof for the claim of disease. Since medical documents are dealing with a huge amount of money, people can get lured to tamper images for claiming medical insurance. Also, medical documents are generally placed as proof or alternatives for avoiding punishments in courts. Hence tampering may disturb the security of individuals. Sometimes pictures are being used as evidence in the courtrooms. These digital pictures work as visual evidence in some cases. But then again, they are smoothly morphed to trick the court and legal working. Alteration in images is a question mark on the authenticity and integrity of images. It is important to pay attention to such types of problems. Thus, the authenticity of images is a major concern. In this way, it is important to answer the following questions:

- How to determine the authenticity of digital images?
- What are the techniques to detect and localize the tampered area in digital Images?

In the experiment conducted, samples of participants were collected, and it was found that there was no significant impact on participant's internet skills, knowledge about images, photo-editing experience and social media use [8]. Numerous examples of fake images are given in the news article [11] which shows the extent to which fake images pose threats for individuals, organizations and society. Hence, it has become the need of the hour to design such a structure that can filter and identify the morphed images. Thus preventing them from any kind of misuse and going viral on social platforms.

1.2.3 Digital Image Forgery Detection Techniques

Researchers have been reported many image authentication techniques which can be categorized into two classes. One is active protection schemes, and another is passive detection techniques.

1.2.3.1 Active Protection Schemes

In active protection schemes, image authentication is done with the help of content that is attached to the image at the time of the image acquisition process. Digital signature and watermarks are attached with the image at the time of acquisition by digital cameras. Digital signatures are attached as meta-data and are used to authenticate the digital image during the forgery detection. The signature relies on standard cryptographic primitives. In this technique hash value of raw pixels of the image, contents are calculated using the hash function family (such as SHA). Hash is then encrypted with the private key of an asymmetric cipher. The encrypted value is then stored in the metadata of the image additionally. The digital watermark is used to embed side information directly into image content instead of metadata. A general framework for digital watermark consists of two components one is an encoder, and another is the decoder. To embed information into an image content encoder is used. To extract information from the watermarked image, restoring the original image and tampering detection (localization) decoder is used. Based on authentication capability and functionality different watermarking techniques are used.

1.2.3.2 Passive Detection Techniques

Active protection schemes of the digital image are excessively restrictive and impractical in many cases, such as for cryptography schemes one should have the key. To address such types of issues passive detection techniques are there which find the intrinsic traces of an image. An image is processed through various camera components after capturing it and before the final image is produced [12]. The captured image is modified by a processing algorithm each time when it passes through any component. These processing algorithms may leave some intrinsic fingerprint clues to detect the manipulated regions. Some of them are as below:

- Lens/Shutter (Chromatic Aberration, Radial Distortion, Motion Blur, Depth of Field), Sensors (Sensor Pattern Noise)
- Demosaicing traces (Periodic Interpolation, filter configuration)
- JPEG Traces (Blocking Grid, AC coefficient statistics, first digit Statistics)
- Post Processing Traces (Copied Region Features, Resampling Features, Histogram Equalization)

1.2.4 Image Authentication Challenges

Active protection schemes are sensitive to change in pixel values, such as brightness or contrast adjustment. Moreover, the image transmitted through the channel requires compression of the image, in such case resaving of images, changes the pixel values, which is undesirable. Minor changes, like contrast and brightness adjustment, don't change the semantic content of an image. Hence, generic signatures are not robust during mild processing of an image and the image may be detected as forged. Robust hash functions are specially designed for image search applications, not for security purposes, they may be a poor choice for authentication purposes. In many cases, the hash is designed to tolerate only a small number of operations and the impact of others is not investigated at all. For example, if the hash allowed a specific structure of one image format (e.g. the blocking structure of JPEG), it is unlikely to work well with another (e.g. wavelet-based JPEG2000). One more important challenge with the cryptography-system-based image authentication techniques is that the digital signatures are stored in metadata, which can be easily removed by an attacker. Challenges with watermark-based authentication schemes are – need for prior knowledge about the embedded watermark, degradation of image quality due to watermark insertion. Considering the challenges of active protection schemes, a lot of research have been done on passive detection techniques. These techniques are based on intrinsic footprints (traces/evidence) left by the process at a different phase of the image acquisition pipeline during the formation

process of the image. These are mathematical or statistical models on assumptions that forged images may leave traces during the editing process. These traces are in the form of added heterogeneous noise [13]–[16] by sensors, light intensity variation due to lens aberration [17]–[19], an inconsistent pattern of color filter array [20]–[22], artifacts during JPEG compression [23]–[25] and many more. These footprints are quite effective for the detection of forged regions in an image but have several shortcomings and challenges. A very important challenge among them is a single scope of application with a single footprint. Other challenges are that these systems either do not have any sequence of morphological operations to localize forged regions or they don't produce the result in efficient time. A system that always gives perfect results but takes a long time for the output is not useful. During CMF, several post-processing techniques act as hurdles towards its detection. Several techniques like contrast adjustment, brightness change, blurring, noise addition, JPEG and other compression and transformation techniques foil the efficient process of CMFD. Block matching techniques based on discrete cosine transform can handle such post-processing techniques but is not invariant to scaling, rotation and other major geometric transformation [26]. Most CMFD techniques fail to detect multiple image forgeries which have undergone such transformations on a single image. Most of the existing techniques used for forgery detection (i.e. CMF and splicing) have been applied over natural scene images that are acquired from digital cameras only and not over scanned reports (digital documents). Thus, a series of state-of-the-art methods have been implemented, and experiments have been carried out over digital documents and found many false-positive and false-negative pixels. The reason behind this worse result is the intrinsic features of digital documents. Authentic content of the document may have similar-looking features as the forged content of the document. Also,

some letters that are not identical but have similar shape features (i.e. letter ‘c’ and ‘e’ have) may confuse existing methods between forged and non-forged regions.

1.3 Problem Statement

A lot of literature has been reported for the authentication of the image using passive detection techniques. This thesis addresses some of the challenges and issues arising from the passive detection techniques which is the main objective of the thesis. The problem statement of the research can be defined as-

Design and development of some digital image forgery detection techniques — copy-move, spliced image and forged scanned document centered— to address various challenges with existing image forgery detection methods.

1.4 Motivation of the Research

A lot of techniques have already been reported by various researchers in literature in the past decade. But there are still some research challenges as well as gaps that need to be overcome. This forms the motivation of the research. From the literature survey given in chapter 2 of this thesis, identified research issues are highlighted as follow:

Copy-Move Forgery Detection: Based on the literature survey of CMFD in chapter 2 and section 2.1, the major limitations of the existing state-of-the-art techniques are the geometrical transformation of the forged region in the image and computation cost of the techniques. So, the detection of CMF is still an open problem.

Image Splicing Detection: Spliced image forgery detection is another type of digital image forgery. Based on the literature survey of image splicing detection in section 2.2, major challenges of reported techniques are- non-suitable features in the case of machine learning detection technique which leads to false positives, estimation of non-qualified sensor noise pattern, sequence of morphological operations in case of noise as

a footprint for image splicing detection. These limitations make image splicing detection an open problem.

Bling Forgery Detection: Except these, there is a limited number of works of literature reported for the forgery detection in digital documents and a generalized model for the detection of digital image forgery whose type is not known i.e. blind forgery detection scheme. Generally, the type of forgery in manipulated images is never defined. These gaps and open problems motivated us to research in this area.

1.5 Objectives of the Research

The research made in this thesis is related to the development of image authentication using passive detection techniques. As discussed above, there is a need for such a system that can do the following tasks-

- Verification for the authenticity of digital images or scanned reports
- Detection of forged images or scanned reports
- Distinguish between forged and non-forged regions in a forged image which will be called here as localization.

To perform these tasks, numerous techniques were developed during the past two decades. Considering the gaps (discussed in the motivation) among the reported state-of-the-art techniques, the objective of the research is to provide efficient approaches of CMFD, image spliced detection and approaches that can blindly detect the forged region in a manipulated image. Objectives of the research are as follows:

i. Comprehensive literature review and comparative study of various CMFD based on hand-crafted features as well as data-driven techniques, analyzing their merits and demerits.
ii. Further, the design and development of some CMFD using intrinsic features of an image and data-driven techniques considering the gaps of state-of-the-art techniques.

iii. Study and implementation of various image splicing detection techniques based on identified clues and data-driven techniques. Further, design and implementation of some spliced image detection based on the inconsistent pattern as an identified clue from the forged image.
iv. The design of a spliced image detection technique using hand-crafted features and logistic regression.
v. To design some efficient data-driven technique for localization of forged region in the manipulated image whose forgery type is not defined viz blind forgery detection.

1.6 Contributions to the Thesis

This section provides the important contributions made in this thesis. The key contributions to the thesis include design, development, implementation and comparative analysis of the following proposed methods for addressing the problems of digital image forgery detection:

i. A literature review on copy-move forgery and spliced image detection: In the past two decades a lot of literature has been detailed for both types of digital image forgeries. In this thesis, issues related to those techniques, challenges and gaps are discussed. Various research problems are identified using this discussion.

ii. Copy-Move Image Forgery Detection using DCT and ORB Feature Set: Considering the research issues and challenges discussed in chapter 2 (literature review of CMFD), an approach for detection and localization of CMF has been developed. This approach takes advantage of handcrafted features and locates the pasted duplicate region from the forged image.

iii. Detection of copy-move forgery in digital image using multi-scale, multi-stage deep learning model: A deep learning-based approach is developed for CMFD. This technique uses multiple scales of an image at multiple levels to extract features. This tackles the challenges of the geometric transformation of copied region.

iv. A technique for image splicing detection using hybrid feature set: A spliced image detection and localization technique has been designed and developed using higher-order statistics. State-of-the-art techniques are suffering from the challenges like a sequence of morphological operators for localization of spliced regions and estimation of non-gaussian noise patterns.

v. Spliced Image Detection using Inconsistent Noise Pattern: A machine learning and handcrafted features-based image splicing detection technique have been contributed to this thesis. This technique uses some hand-crafted features which are helpful in the case of spliced images and a logistic regression classifier to classify an image into forged or authentic classes.

vi. Modified U-Net Model for Detection of Forged Region in Images Acquired from Various Sources: A blind forgery detection and localization technique have been developed using a modified u-net deep learning model. In case of the type of forgery is not known then this method is much useful. The issues of the U-Net model with the dataset of forged images have been taken care of in this technique. Identity block is used in the modified U-Net model to save the important feature before the max-pooling layer. This reduces the chance of information loss during dimensionality reduction.

vii. An investigation and analysis of forged digital documents using a deep inception network: A lot of techniques have been developed for image forgery detection during the last decade. These all are for natural images, which are captured from digital cameras only. Here a deep learning technique has been developed for scanned documents forgery detection. The most important challenge was the unavailability of a publicly available dataset. In this contribution, a dataset of the forged scanned document is developed. This dataset has been used to train a deep learning model developed for the detection and localization of forged scanned documents.

1.7 Thesis Organization

Throughout the research work, various challenges are identified in existing state-of-the-art techniques. Based on these challenges various models are proposed and published in research articles. For better understanding and clear view, works of this thesis are divided into three chapters based on types of digital image forgery and its detection techniques. These chapters are arranged as chapter 3 for CMFD using statistical and data-driven techniques, chapter 4 for spliced image forgery detection using intrinsic footprints of image and chapter 5 for some data-driven techniques for detection and localization of blind image forgery. An outline of the thesis is shown in Figure 1.3. The flow of the chapter and color defines its importance in the outline.

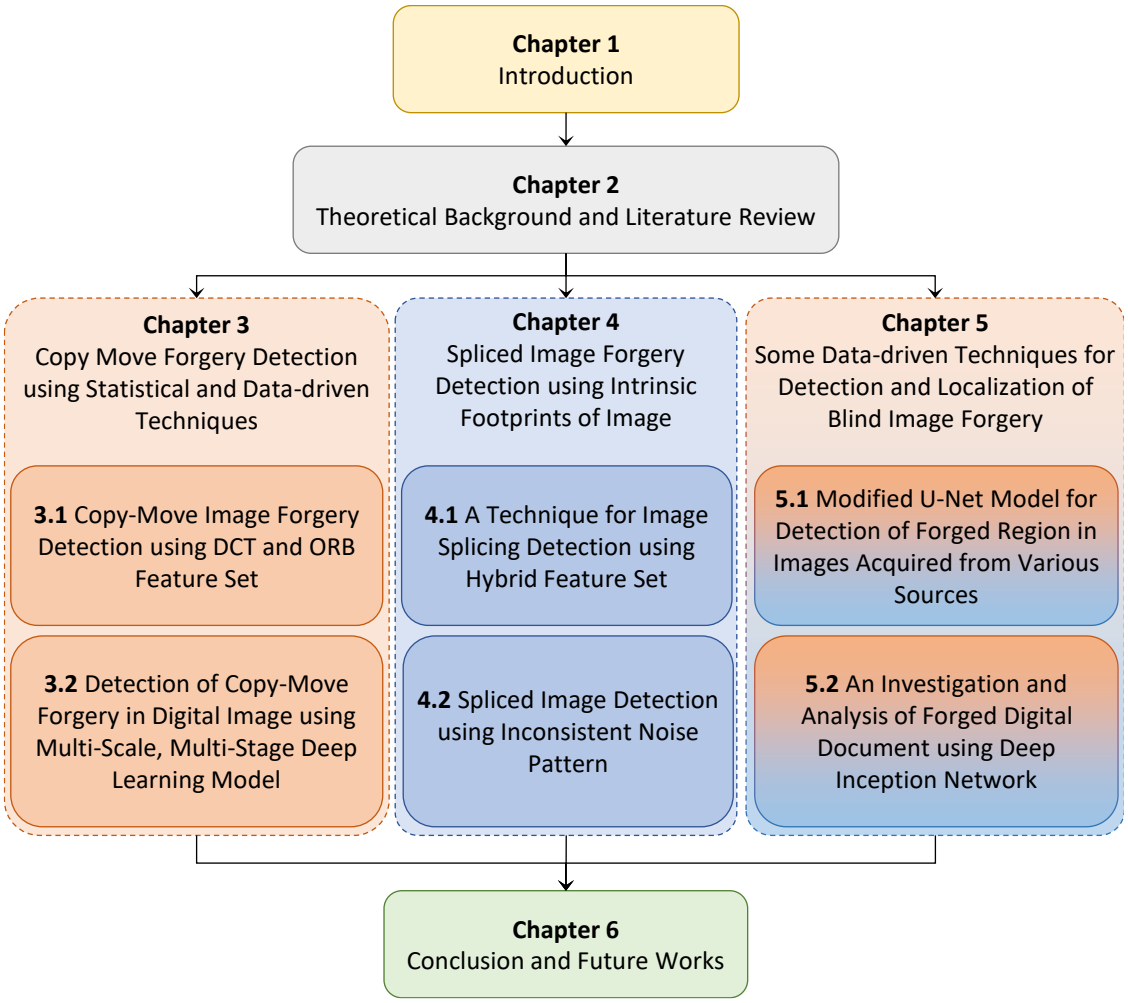

Figure 1.3: Outline of the thesis

The organization of the thesis is as follows:

Chapter 1 briefs about the background knowledge on image and its importance. This chapter also discusses digital image forgery, types of digital image forgery, the need for image authentication and image authentication techniques. Further, challenges in the existing image authentication technique, motivation of the research and problem statement are also given in this chapter. This chapter focuses objective of the research, contribution to the thesis and concludes with the organization of the thesis.

Chapter 2 presents the theoretical background and literature review related to the identified research problem. This chapter also presents the description of datasets and evaluation metrics used for the experimental and comparative study of the proposed methods and models in the thesis.

Chapter 3 titled "Copy Move Forgery Detection using Statistical and Data-driven Techniques" presents the two methods namely "Copy-Move Image Forgery Detection using DCT and ORB Feature Set" and "Detection of Copy-Move Forgery in Digital Image using Multi-Scale, Multi-Stage Deep Learning Model" for detection of copy-move forgery in an image. Experimental analysis and comparative study show that the proposed methods perform better in comparison to other methods available in the literature.

Chapter 4 titled "Spliced Image Forgery Detection using Intrinsic Footprints of Image" presents two spliced image detection techniques namely "A Technique for Image Splicing Detection using Hybrid Feature Set" and "Spliced Image Detection using Inconsistent Noise Pattern". One is a detection technique based on handcrafted features of the image and machine learning classifier logistic regression and another is a localization technique based on the statistical approach i.e., a clue left during the formation process of the image. Experimental analysis and comparative study show that

the proposed approaches perform better in comparison to the state-of-the-art techniques given in the literature.

Chapter 5 titled "Some Data-driven Techniques for Detection and Localization of Blind Image Forgery" presents two different data-driven techniques using deep learning approaches namely "Modified U-Net Model for Detection of Forged Region in Images Acquired from Various Sources" and "An Investigation and Analysis of Forged Digital Document using Deep Inception Network" to detect and forgery whose type is not known. One method detects forgery in natural images while another detects forgery in scanned documents. The experiment result of the first proposed method shows that the method works better in the case of images acquired from different sources. For the scanned document analysis, a forged document dataset is also generated and described in this chapter. Experiment analysis and the comparative result of the proposed method on the generated dataset, as well as the publicly available dataset, show that the method performs better in comparison to state-of-the-art techniques available in the literature.

Chapter 6 concludes the research work and summarizes the main findings of the thesis. This chapter also proposes some possible future directions for the research.