Chapter 1

Introduction and Background

1.1 Introduction

Digital image forgery is not new to the human being but a very old issue. Previously, it was restricted to art and literature although did not affect the common people. Nowadays the rapid growth of internet, image processing software plus sophisticated editing tools make this task pretty easy where a digital image could be effortlessly modified or forged [1]. Further, it is almost impossible for human vision system to recognize visually either the image is original or doctored with naked eye. The rapid improvement have been found in the digital forgeries in mainstream media as well as on the internet and in social media [2]. This trend shows grave susceptibility as well as decreases the trustworthiness of the digital images. Consequently, developing better algorithms to authenticate the honesty as well as genuineness of digital images is essential, specifically taking into consideration that images can be conferred as an evidence in a court of law, as a part of a medical records, as news item and as financial documents. So, detecting forgery in a image is one of the prime objective of digital image forensics. The classification of image forgery is shown in figure 1.1.
1.1.1 Pixel-Based Image Forgery Detection

Pixel based approaches emphasis to pixels of the image. Pixel-based approaches are also known as passive image tampering detection techniques. Further, this method is classify into four types. In this work, our focus is on copy-move image forgery. This technique is one of the most trivial method for image forgery. Figure 1.2 display the classification of pixel based image forgery method.
1.1.2 Copy-Move (Cloning)

Copy-move is one of the widely used as well as trivial method of image forgery and it is also known as cloning. In this type of forgery, the area or object of image is copied and then pasted into someplace within the image. Figure 1.3 depicts the original image with its doctored version. The original image is having six balloons and copy-move image with nine balloons.
1.1.3 Resampling (Resize, Stretch, Rotation)

For combining two objects or people into a single, it is likely to perform various operations such as we have to resize as well as stretch one person or object to match with the other object or people. Additionally, in this process we have to resample original image into a new sampling lattice.

1.1.4 Splicing

This is a different type and widely used technique of image forgery. In this approach, two or more than two images will be converted into a single composite image. Suppose we have two images shown in Figure 1.4. We have made a composite of these two into a single image. If this is done carefully than the border between spliced are impossible to identify visually.
1.1.5 Statistical

The statistical model is basically used to detect all things from basic image alterations such as resizing as well as filtering to perceptive photographic from computer generated photo and finding the hidden messages.

1.2 Related Work

Various algorithms have been proposed for detecting copy-move region by various researchers, few algorithms are efficient in term of detection of actual forgery region but taking too much execution time. Some algorithms are not efficient detecting forgery but having less execution time. However, very few algorithms are efficient in term of detecting forgery with less execution time but not robust in term of various attacks such as rotation, scaling, blurring, multiple copy-paste attack etc.
The detection of digital image forgery algorithms are divided into active and passive techniques. In the active technique, digital image verb needs preprocessing of image namely signature generation as well as embedding of watermark, which restricts their application or usefulness in systems. Contrasting, watermarking and signature based techniques; the passive techniques do not require the generation of digital signature or embedding of watermark. Further, passive approaches of detecting image forgery are separated into five types as display in Figure 1.1 Additionally, pixel based approaches mainly identify the statistical anomalies applied at the pixel level; on the other hand, format based approaches control the statistical correlations employed by a specific lossy compression system; Further, camera based approaches utilize artifacts introduced by the camera lens or sensor as well as on-chip post-processing; In physical environment based approaches, we unambiguously model and notice anomalies in the three-dimensional interaction among physical objects or light as well as camera; Lastly, geometry based approaches formulate dimensions of objects in the world and their locations reciprocal to the camera.

a) Pixel Based Techniques are mainly emphasized on the detecting pixel irregularities that were introduced at the time of forgery process. These are the most popular technique in image forensics, further categorize in three categories i.e. Cloning (copy-move), Splicing and Retouching.

b) Format Based Techniques are mainly depend on image formats as well as work in the JPEG format, this techniques are further classify into three categories i.e. JPEG Quantization, Double JPEG and JPEG Blocking.

c) Camera Based Approaches are focus on identifying the clues of forgery by exploiting the artifacts applied by various step of the image capturing process. Further divided in four categories i.e. Chromatic Aberration, Color Filter Array, Camera Response and Sensor Noise.
d) Physics Bases Technique are depend on calculating the lighting directions and differences in lighting betwixt image area in the image as a telltale sign of image doctoring, further divides in three types i.e. Light Direction 2D, Light Direction 3D and Light Environment.

e) Geometric Based Technique is depending on calculating principal point of image areas crosswise a image, and the discrepancy between principal points. This technique is further categories in two category i.e. Principal point and metric measurement.

The copy-move (Cloning) image tempering is most common approach practice to create a image tampering, in which a particular block or object of image is copied and then pasted it into some other place of the similar image to accomplish information hiding. As the copied block arrive from the similar image, its significant characteristics namely noise texture and color palette will be reconcilable with the remaining part of the image and hence it will leads to a great threat whenever we are going to detect it as well as in locating the doctored region. The detection of copy-move (cloning) image forgery various approaches have been developed that are mainly depend on either block based technique or key point matching techniques are shown in figure 1.5[3, 4, 9, 12, 18, 24, 26].
1.2.1 Key-point based Approaches

The key point based approaches are mainly reckon on the extracting local interest points. These points are also known as key-points. Further, extracting the local points with high entropy without any image sub-blocking. The best key-points are able to identify distinct locations in a image areas are considered as efficient key points. They should be robust in terms of detecting noise, geometric transformations, illumination changes and other distortions. The major benefits of key-point approaches are that the detecting tampered region with high rate, which illustrate a rich structure namely image regions, though struggling to decrease the false matches in the flat regions such as sky and ocean.

Huang et al. [15] developed copy move forgery detection using scale invariant feature transform (SIFT) technique in 2009. Firstly, the authors have used SIFT technique to find the duplicate region with scale as well as rotation. Further, best
bin first search (BBF) techniques have been used for finding possible duplicate key-points. Additionally, nearest neighbor distance ratio (NNDR) is applied to increase the detection rate or accuracy. This technique is able to find key-points even if image is noisy or compressed. Similar methods have been developed by various authors using SIFT and SURF algorithm such as, Amerini et al. [22] and Battiato et al. [53].

1.2.2 Block Based Methods

Block based approaches are very popular and able to detect forgery regions accurately. First image is separated into a overlapping sub blocks. Further, efficient features (feature vector) are extracted from every block with the help various feature extraction and dimension reduction methods (DWT, DCT, SVD and PCA etc.) as shown in figure 1.6. Compared these feature vectors to find the possible forgery regions.

Figure 1.6: Block based image forgery detection techniques
The first block based method is introduced by Fridrich et al. [1] for detecting image tampering in 2003. This technique have divided the image into overlapping blocks (16 × 16) for extracting features. Further, extracted DCT coefficients are used as feature vector. Moreover, lexicographically sort the DCT coefficients of each blocks. After lexicographically sorting, identical blocks are nearby and forgery region are detected. Authors have perform retouching operations But any other robustness test have not performed. This method is taking too much computational time and not able to detect tampered region if attack are applied on image like rotation and scaling.

Next, Popescu et al. [2] initiated a technique for exposing digital forgeries by detecting duplicated image regions in 2004. Principal component analysis (PCA) is applied on fixed size image blocks (16 × 16, 32 × 32). Further, eigenvalues as well as eigenvectors have been calculated of every block. Moreover, lexicographical sort is applied and duplicated regions have been detected. This technique provides better results compare to fridrich methods. This technique is capable of detecting tampered region even if the image is compressed as well as noisy.

Gouhui Li et al. [7] introduced a sorted neighborhood technique for the detection of duplicate region with the help of DWT and SVD in 2007. First, DWT is used to decompose image into four sub-bands. Further, low frequency sub band is chosen for further processing. Moreover, singular value decomposition (SVD) is applied to extract feature vector on reduced dimension representation. Lexicographical sort is applied on singular value vector and similar vectors are nearby. These vectors are matched and forged region detected. They have used gray scale as well as color images for detecting duplicate region.

Mehdi Ghorbani et al. [8] developed DWT-DCT (QCD) method for detecting copy-move image forgery in 2011. Initially, authors have applied DWT to get low, high frequency sub bands of image. Further, DCT-QCD (Quantization Coefficient Decomposition) is employed in row vectors to decrease vector
length. Then, lexicographically sort is applied to the row vectors and shift vector is calculated. Finally, the comparison of shift vector with the preset threshold is performed and the tampered region is located.

Jing Zhang et al. [13] introduced a new technique for copy-move image forgery detection from digital images in 2008. Firstly, authors have applied DWT, the image is splitted into low frequency four sub bands. Further, low frequency sub band is chosen and divided into non-overlapping blocks. Moreover, the phase correlation utilize to calculate the spatial offset betwixt the copy-move areas. Finally, pixel matching is employed for detecting tampered area. developed technique provides better results even if the image is highly compressed and also considered as very effective technique which is taking less computational time comparatively.

Li kang et al. [15] designed the algorithm for detecting tampering from digital image in 2010. Firstly, the image is divided into small blocks as well as improved singular value decomposition (SVD) is applied for feature extraction. Further, lexicographically sort is applied on SV vectors, similarity matching is employed to located forged region from the input image.

Zhouchen Lin et al. [17] developed a fast as well as automatic technique and fine-grained forgery region detection with the help of DCT coefficient in 2009. First of all DCT coefficient have applied for extracting feature from image and then bayesian method is employed for locating possible forgery. Finally, the forgery region is location successfully.

Further, Wang et al. [43] developed hybrid approach, used DWT and DCT for detecting copy-move forgery region. Similarly, distinct techniques have been developed for detecting copy move image forgery. [4, 5, 6, 11, 12, 15, 17, 18, 19, 20, 23, 24, 25, 26, 45, 46, 55, 56, 57]
1.3 Feature Extraction Techniques

The most common features available in the image include color, texture and Shape etc. Feature extraction is mainly dependent on these three types of features and performance of any desired task is also dependent on these extracted features. Generally, feature representation methods are divided in three categories namely region-based, global based and block-based features [44, 101]. Additionally, less concentration has been given to image feature extraction related to a meaningful research on annotation as well as retrieval model itself developed. In this present work, our attention is only on texture based feature extraction. we have tested our algorithm on various medical images i.e. X-Ray, thyroid and Brain CT scan, and image processing images i.e. Lena image and JUIT logo.

A number of textural feature extraction methods were developed [62, 63]. The local binary pattern (LBP) method [63] is working on the idea of binary patterns for illustration of texture. It is extensively accepted due to simplicity of LBP and effective in representing the local spatial structure of an image. Further, the LBP techniques were enlarged as well as joined with different techniques. In results, the wide range of texture demonstration algorithm are convenient for various image analysis assignments. Conventional examples contain LBP expansion featuring scale invariance [66] as well as rotation invariance [66, 67] Further, the combination of both inter plus intra spatial structure of the LBP patterns [68] as well as fusion of micro LBP and macro Gabor features [69].

A very first study on visual inspection [73] has demonstrated that the LBP features were efficiently adopted in surface defect detection. Afterwards, BP-based features [74] have also adopted for wood quality discrimination. Moreover, more recently these features have been employed on automatic defect detection [75, 76] as well as in remote sensing [77]. Additionally, a diversified inspection has presents, the extraction of features with the help of BP approaches are found to be useful for content based image retrieval [78, 79]. Though, recently the LBP
technique has been utilized in a discriminative model for image ranking from text queries [80]. In addition to that, texture representation technique is also considered as highly efficient and effective in the area of face recognition. Afterwards, it is proficiently employed in invariant face recognition [81, 82], recognition of facial expressions [84] and face authentication [83]. Wonderful results are achieved from its various application of biomedical imaging including classification of protein images [86], video endoscopy [85], computer aided neuroblastoma prognosis system [87]. Further, it is also successfully used in various area of motion analysis such as underwater image matching [88], object tracking [90], modeling and detection of moving objects [89].

The research community has lot of interest on LBP texture representation, various approaches have been proposed with the help of BP model. The technique was developed for the assessment of local contrast measure [64]. Later, the LBP/C technique was establish by using the joint distribution of LBP codes as well as local contrast measures, which shows support to diversity of the illumination. This is also employed to improve the differentiation capacity of the original LBP technique. In addition to that, other version of LBP is Local edge patterns (LEP) technique which was designed for image segmentation [70]. This technique explain the spatial structure of local texture through the spatial orientation of edge pixels. Afterwards, similar method median binary pattern (MBP) was developed by Hafiane et al.[71], which is intensity-shift invariant. It is works on the texture primitives are resolved with localized thresholding contrary to local median. Following this analysis, a hashed variant of MBP to a binary chain has been figure out, in results another resolution as well as rotation invariant MBP (MBP-ROT) texture descriptor found [72].

Fuzzy sets provide a adaptable framework for dealing with indeterminacy characterizing real world problems, originating mainly from the unprecise as well as imperfect nature of information. However, fuzzy sets do not deal with the hesitancy (intuitionistic index) in images originated out of distinct factors. In which
their majority are caused by intrinsic vulnerability of the acquisition and imaging mechanisms. Further, distortions arises as a result of the restraint of acquisition chain namely the non-linear nature of mapping system, quantization noise, affect certainty with respect to the “brightness” or “edginess” of a pixel, the suppression of dynamic range. Hence, introduce a degree of hesitancy connected with the corresponding pixel.

Next, fuzzy sets theory introduced by Zadeh [96] by extracting the texture spectrum features [91] as well as their proficient successors. Additionally, the LBP features are able to improve their robustness to noise [30, 92, 93, 94, 95]. Though, these practice can only be treated as preliminary because they incorporate only a restricted experimental assessment. Further, Keramidas, Iakovidis et al [30, 95] proposed a generic as well as uncertainty aware technique for the derivation of fuzzy local binary pattern (FLBP) texture models. Additionally, intuitionistic fuzzy set theory proposed by Atanassov [97] provides a impressionable mathematical structure to deal with uncertainty as well as the hesitancy originating from imperfect as well as imprecise information. A extrusive property of IFS is that it appoint to each element a membership degree as well as a non membership degree with certain amount of hesitation degree.

1.4 Performance Measures

The performance of the forgery detection techniques can be observe by calculating Accuracy, True Positive Rate (TPR) and False Positive Rate (FPR). They can be estimated as follows:

True Positive (TP): Tempered image detected as tempered
False Positive (FP): Original image detected as tempered
True Negative (TN): Original image detected as original
False Negative (FN): Tempered image detected as original
From these above measures, we can define various performance evolution metrics: Accuracy, True Positive Rate (TPR) and False Positive Rate (FPR) as follows:

\[
\text{Accuracy} = \frac{\text{Number of identified images}}{\text{Number of forged images}} \times 100
\]

\[
\text{True Positive Rate(TPR)} = \frac{\text{Number of forged images identified as forged}}{\text{Number of forged images}}
\]

\[
\text{False Positive Rate(FPR)} = \frac{\text{Number of original images identified as original}}{\text{Number of original images}}
\]

1.5 Problem Identification

In this thesis, we have focused to design robust algorithms which are able to detect forgery with less execution time and also able to detect forgery on images subjected to scaling, rotation, blurring, and multiple copy-paste attacks. We have focused on the following issues:

1. In the literature survey of image forgery, we have found that the number of existing approaches, which are not able to detect actual forgery region. So, the false matches are the major limitation. Detecting actual region with good accuracy rate is the challenging tasks. We have addressed this issue and proposed an algorithm based on projection profiling.

2. We have processed the image block by block and extracted the feature vector for each block then compared similar the feature vector to find the possible duplication. The extraction process will take lot of computational time so improving computational time is other major challenge of this research domain. We have suggested a hybrid algorithm based on direct fuzzy transform and ring projection which reduces the execution time as well as improve the accuracy.
1.6 Objectives of Thesis

Image processing software’s, editing tools and internet makes image forgery process quite easy. Anyone can doctor images without leaving any visual clues. Therefore, there is necessity of some effective algorithm which can detect image forgery automatically with good accuracy rate. Objective of the thesis are given as follows:

1. To propose a robust and efficient forgery detection algorithm, which is able to detect forgery region successfully. Also reduce the false matches and suggest new improvements in the accuracy rate.

2. To develop a lightweight and fast technique for detecting copy-move image forgery. The algorithm will take less execution time for detecting copy-move region compare to existing approaches.

3. To introduce a hybrid scheme which provide better result compare to other reported algorithms if various attacks are applied. And also able to detect copy-move forgery region accurately with less execution time.

4. To propose an efficient scheme for feature extraction from digital image, these extracted features can be applied in many application areas of image processing including image forgery detection.

We design a forgery detection technique with less execution time and robust to various forgery attacks. Proposed algorithms obtain the several objectives and identified number of problems in existing forgery detection techniques and their solutions.
1.7 Organization of the Thesis

The thesis has been organized into six chapters as follows:
chapter 1 provides the introductory part of the thesis as well as literature review and background. In chapter 2, we have presented an approach for identification of copy-move image forgery based on projection profiling for reducing the execution time. In chapter 3, a hybrid scheme for copy-move image forgery detection using ring projection and modified fast discrete haar wavelet transform is discussed. Chapter 4 presents a copy-move image forgery detection using direct fuzzy and ring projection transform. This algorithm is efficient in term of accuracy of detecting forgery as well as reducing the execution time. Further, chapter 5 demonstrates a texture features extraction technique using intuitionistic fuzzy local binary pattern. Finally, the conclusions and future scope are discussed in chapter 6. List of publications and references are depicted at the end.