REGION DUPLICATION FORGERY DETECTION TECHNIQUE BASED ON KEYPOINT MATCHING

DIAA MOHAMMED HASSAN ULIYAN

FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR

2016

REGION DUPLICATION FORGERY DETECTION TECHNIQUE BASED ON KEYPOINT MATCHING

DIAA MOHAMMED HASSAN ULIYAN

DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR

2016

UNIVERSITI MALAYA
ORIGINAL LITERARY WORK DECLARATION

Name of Candidate: **DIAA MOHAMMED HASSAN ULIYAN**

Registration/Matrix No: **WHA120005**

Name of Degree: **DOCTOR OF PHILOSOPHY**

Title of Project Paper/Research Report/Dissertation/Thesis ("this Work):

REGION DUPLICATION FORGERY DETECTION TECHNIQUE BASED ON KEYPOINT MATCHING

Field of Study: **Digital Image Forensic – Computer Science**

I do solemnly and sincerely declare that:

(1) I am the sole author/writer of this Work;
(2) This work is original;
(3) Any use of any work in which copyright exists was done by way of fair dealing and for permitted purposes and any excerpt or extract from, or reference to or reproduction of any copyright work has been disclosed expressly and sufficiently and the title of the Work and its authorship have been acknowledged in this Work;
(4) I do not have any actual knowledge nor do I ought reasonably to know that the making of this work constitutes an infringement of any copyright work;
(5) I hereby assign all and every right in the copyright to this Work to the University of Malaya ("UM"), who henceforth shall be the owner of the copyright in this Work and that any reproduction or use in any form or by any means whatsoever is prohibited without the written consent of UM having been first had and obtained;
(6) I am fully aware that if in the course of making this Work, I have infringed any copyright whether intentionally or otherwise, I may be subject to legal action or any other action as may be determined by UM.

Candidate's Signature Date:

Subscribed and solemnly declared before,

Witness's Signature Date:

Name:

Designation:

ABSTRACT

Manipulation of digital images is not considered a new thing nowadays. For as long as cameras have existed, photographers have been staged and images have been forged and passed off for more nefarious purposes. Region duplication is regarded as an efficient and simple operation for image forgeries, where a part of the image itself is copied and pasted into a different part of the same image grid. The detection of duplicated regions can be a challenging task in digital image forensic (DIF) when images are used as evidence to influence the judgment, such as in court of law. Existing methods have been developed in the literature to reveal duplicated regions. These methods are classified into block-based and key point-based methods. Most prior block based methods rely on exhaustive block matching on image contents and suffer from their inability to localize this type of forgery when the duplicated regions have gone through some geometric transformation operations and post-processing operations.

In this research, we propose three novel approaches for detecting duplicate regions in forged images that are robust to common geometric transformations and post processing operations.

In the first approach, we propose a novel method for detecting uniform and non-uniform duplicated regions with small size in forged images that is robust to geometric transformation operations such as rotation and scaling. The proposed method have adopted statistical region merging (SRM) algorithm to detect small regions, and then Harris interest points are localized in angular radial partition (ARP) of a circular region which are invariant to rotation and scale transformations. Moreover, feature vectors for a circular

patch around Harris points are extracted using Hölder estimation regularity based descriptor (HGP-2) to reduce false positives.

In the second approach, we therefore proposed a forensic algorithm to recognize the blurred duplicate regions in a synthesized forged image efficiently, especially when the forged region in the images is small. The method is based on blur metric evaluation (BME) and phase congruency (PCy).

In the third approach, we proposed a detection method to reveal the forgery under illumination variations. The proposed method used Hessian to detect the keypoints and their corresponding features are represented by robust descriptor known as Center symmetric local binary pattern (CSLBP).

The proposed methods be evaluated on two benchmark datasets. The first one is MICC-F220 which contains 220 JPEG images. The second dataset is an image manipulation dataset which includes 48 PNG true color. The experimental results illustrate that the proposed algorithms are robust against several geometric changes, such as JPEG compression, rotation, noise, blurring, illumination variations, and scaling. Furthermore, the proposed methods are resistant to forgery where small up to 8*8 pixels and flat regions are involved, with little visual structures. The average detection rate of our algorithm maintained 96 % true positive rate and 7 % false positive rate which outperform several current detection methods.

ABSTRAK

Manipulasi imej digital bukan sesuatu yang baru di abad ini. Semenjak ciptaan camera, imej telah ditiru untuk kegunaan yang tidak elok. Penduaan ruangan diterima sebagai satu operasi yang effisien dan ringkas dalam proses peniruan imej di mana sebahagian daripada imej itu disalin dan dilekatkan pada bahagian yang berlainan pada grid imej yang sama. Pengesanan ruangan pendua adalah mencabarkan dalam forensik imej digital (DIF) apabila imej digunakan sebagai bukti dalam mempengaruhi proses penghakiman di mahkamah. Beberapa cara untuk menonjolkan ruangan pendua telah dikaji di dalam literasi dan boleh diklasifikasikan ke dalam "block based" dan "keypoint based". Kebanyakan cara "block based" bergantung kepada "exhausting block matching" pada kandungan imej dan tetapi tidak cekap dalam menentukan peniruan jenis ini apabila ruangan yang disalin telah diproses secara transformasi geometrik dan pasca process.

Dalam kajian ini, kami telah mencadangkan 3 cara untuk mengesan ruangan pendua dalam peniruan imej tanpa dijejaskan oleh operasi transformasi secara geometrik dan pasca operasinya.

Dalam cara pertama, kami mencadangkan satu cara untuk mengesan ruangan pendua yang seragam dan tidak seragam yang bersaiz kecil dalam imej yang ditiru tanpa dijejaskan oleh operasi transformasi geometrik seperti putaran dan skala. Cara yang dicadangkan ini menggunakan "statistical region merging (SRM) algorith" untuk mengesan ruangan yang kecil dan kemudian "Harris interest point" ditentukan di dalam "angular radial partition (ARP)" dalam ruangan bulatan yang tidak berubah oleh transformasi putaran dan berskala. Tambahan, ciri-ciri vektor untuk ruangan bulatan di sekeliling "Harris points" diekstrakkan menggunakan "Holder estimation regularity based descriptor (HGP-2) "untuk mengurangkan kepalsuan positif.

Dalam cara yang kedua, kami mencadangkan satu algoritma forensik untuk mengenalpasti ruangan pendua yang kabur pada imej tiruan yang disintesis secara effisien, terutamanya apabila ruangan yang ditiru itu kecil. Cara ini adalah berdasarkan “blur metric evaluation (BME) dan “Phase congruency (PCy)”.

Dalam cara yang ketiga, kita mencadangkan cara pengesanan untuk mendedahkan tiruan apabila diiluminasikan secara berubah-ubah. Cara yang dicadangkan ini menggunakan “Hessian” untuk mengesan “keypoints” dan ciri-ciri mereka yang sepadan diwakili oleh “descriptor” yang teguh yang dikenali sebagai “Center symmetric local binary pattern (CSLBP)”.

Cara yang dicadangkan ini akan diuji berdasarkan dua “benchmark datasets”. Yang pertama adalah MICC-F220 yang mengandungi 220 imej JPEG. Dataset yang kedua adalah manipulasi imej yang mengandungi 48 PNG dengan warna sebenar. Hasil experiment ini menunjukkan bahawa algoritma yang dicadangkan boleh mengatasi beberapa perubahan geometrik seperti pemampatan JPEG, putaran, “noise”, pengkaburan, variasi iluminasi dan pengskalaan. Tambahan, cadangan ini tidak dipengaruhi oleh peniruan melibatkan saiz pixel sekecil 8*8 dan ruangan rata . Purata kadar pengesanan menggunakan algoritma kami mengekalkan 96% positif sebenar dan 7% positif palsu , sekali gus mengatasi beberapa cara pengesanan yang sedia ada.

ACKNOWLEDGEMENTS

In the name of Allah, Most Gracious, Most Merciful. I thank Allah S.W.T for granting me perseverance and strength I needed to complete this thesis.

I would like to express a great thankfulness to my supervisor, Dr. Hamid Abdulla Jalab as well as my co-supervisor, Dr. Ainuddin Wahid Abdul Wahab for their support, guidance, suggestions and encouragement over the past years of this research. My supervisor gave me the opportunity to carry out my research with little obstacles. The comments from him had a significant impact on this thesis. His help and support in several ways have always been in my mind.

I would like to thank the Faculty of Computer Science and Information Technology, University of Malaya, HIR, and UMRG for providing me a great academic environment.

I would like to express a special word of thanks to my parents for their faith, support and encouragement. A special thanks to my wife who supported me throughout the writing of this thesis patiently assisting, with words of assurance.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AHL	Agglomerative hierarchical linkage
ARP	Angular radial partitioning
BACM	Blocking artifact characteristics matrix
BME	Blur metric evaluation
CA	Chromatic aberration
CCD	Charged coupled device
CFA	Color filter array
CMFD	Copy move forgery detection
CMOS	Complementary metal oxide semiconductor
CN	Coarseness and contrast
CSLBP	Center symmetric local binary pattern
DCT	Discrete cosine transform
DFT	Discrete Fourier Transform
DIF	Digital image forensic
DWT	Discrete wavelet transform
EM	Expectation maximization
FFT	Fast fourier transform
FMT	Fourier mallin transform
FPR	False positive rate
G2NN	Generalized nearest neighbor
GM	Gradient magnitude
HGP-2	Hölder estimation regularity based descriptor
HH	High frequency
HH1	High frequency at scale 1
LBP	Local binary pattern
LL	Low frequency

LL1	Low frequency at scale 1
LOG	Laplacian of Gaussian
LPFFT	Log-polar fast Fourier transforms
LPM	Log polar mapping
LSH	Locality sensitive hashing
MAD	Median absolute deviation
MLBP	Multiresolution local binary pattern
Ncut	Normalized cut
PCA	Principal component analysis
PCA-EVD	Principal component analysis eigenvalue decomposition
PCT	Polar cosine transform
Pcy	Phase congruency
PRNU	Photo response non uniformity noise
RANSAC	Random sample consensus algorithm
RGB	Red,Green and Blue
SIFT	Scale invariant feature transform
SPN	Sensor pattern noise
SRM	Statistical region merging
SURF	Speed up robust feature
SVD	Singular value decomposition
TPR	True positive rate
UDWT	Undecimated dyadic wavelet transform
WLD	Weber law descriptor
ZM	Zernike moments

LIST OF APPENDICES

CHAPTER ONE

INTRODUCTION

1.1 Research motivation

It's all so easy to manipulate images with Photoshop (Szeliski, 2011). In today's digital age, most of digital images are produced by a variety of high resolution digital cameras and distributed in media channels such as newspapers, websites, social networks and TVs. In all of these channels, digital images have been integrated into various aspects of our daily lives. For instance, digital images on TV news and digital newspapers validate the veracity of events. And they are perceived as a piece of truth. Unfortunately, they are vulnerable to malicious activities. This is mainly due to the development of a wide range of image editing softwares which makes them relatively simple to produce digital image forgeries (Fridrich et al., 2003). Image forgery may cause trouble on many occasions; for example, a large number of forged images have recently been published in digital newspapers to deceive the public about the truth (Figure 1.1 (a)). Furthermore, an important object may be duplicated or removed from images that serve as evidence to induce miscarriages of justice (Figure 1.1 (b)). Similarly, medical images can be tempered to hide or pretend pathology for insurance purposes (Figure 1.1 (c)).

(a) (b) (c)

Figure 1.1: Examples of image tampering throughout History: (a) Composite image includes hurricane sandy combining with a photo of New York city; (b) Fake magazine cover includes duplicated aircrafts; (c) Forged pathology (right).

To understand whether an image is authentic or not by carefully looking at it is no more a viable choice, as sometimes legitimate images may appear as fakes at first glance and vice versa. As a consequence, more sophisticated methods to restore the credibility of digital images are needed. As a result, We cannot examine the trustworthiness of such images visually (Bayram et al., 2008b; Gloe et al., 2007; Sencar & Memon, 2013).

To tackle this crisis of confidence, digital image forensics (Farid, 2009; Mahdian & Saic, 2010; Piva, 2013; Poisel & Tjoa, 2011; Redi et al., 2011) have begun to develop robust image forgery detection methods to authenticate digital images and restore some of the lost credibility of digital images. In particular, this task is fulfilled by providing an answer to questions like the following: What is the history of an image that was being processed after acquisition? What parts of the image have undergone post-processing and up to what extent? Was an image acquired by the device it is claimed to be captured by? One of the advantages of digital image forensics consists in its blind approach of verification of integrity and authenticity of images. Image Forensics is based on the observation that any processing carried out during any stage of an image's life cycle leaves specific abstruse

traces whose presence can be imposed by forensic image analysts to reveal the malicious manipulation (Farid, 2009). It goes without saying that most of the times, examining the complete history of an image is no small effort, especially if we consider that every processing step carried out on the image tends to weaken the clues left by previous manipulations.

1.2 Research background

To understand the principal ideas of digital image forensics, it is necessary to have at least a rough working definition of how different image formation processes (Section 1.2.1) may affect the trustworthiness of digital images (Section 1.2.2). We then detail our notion of passive digital image forensics (Section 1.2.3), which is based on analyzing image characteristics and identifying traces of the respective image formation process.

1.2.1 The image formation process

In image capturing process, different processing stages are carried out to define the life cycle of a digital image as shown in Figure 1.2. Every stage leaves subtle traces as an intrinsic signature the image content. Forensic techniques aim to exploit information on the history of an image by looking at specific artifacts left by different processing steps (Nguyen & Katzenbeisser, 2011; Piva, 2013) . In an imaging system, the light passes the imaging devices through the optical lens, and is focused to a single point on the imaging sensor. The imaging sensor is the heart of a digital camera, and is consisted of an array of detectors. Each of them is corresponding to a pixel of the final image. Each pixel converts the light passing it into a voltage that is proportional to the intensity of the light. At this stage, the produced digital signal does not convey color information, because the sensors react exclusively to brightness. Most of digital cameras, however, are equipped with a

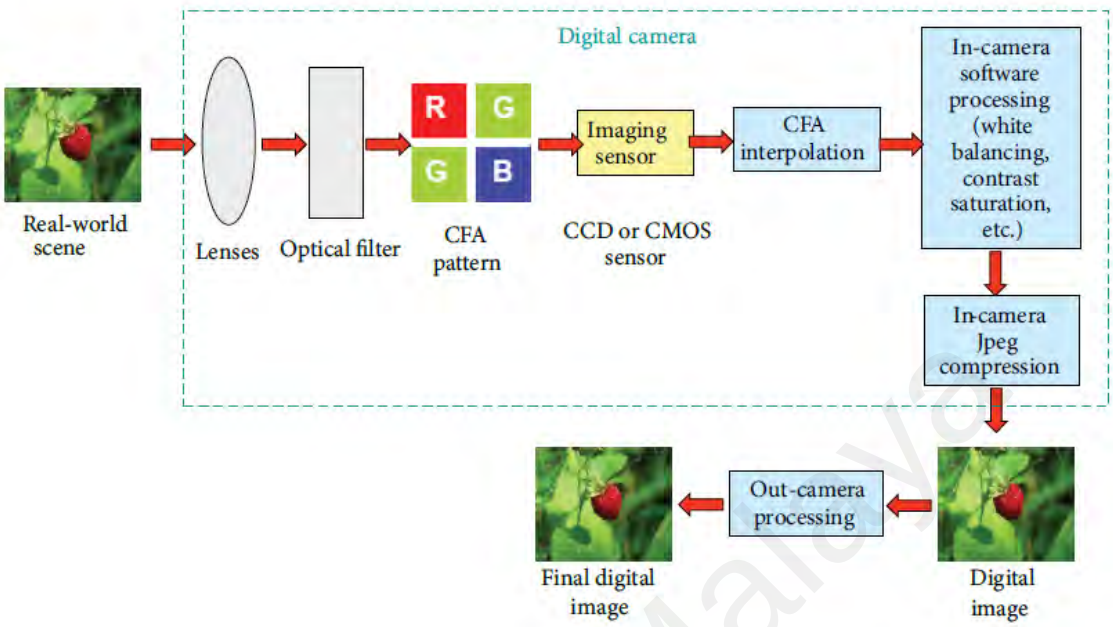


Figure 1.2: A scheme representing the following steps composing the life cycle a digital image undergoes (Piva, 2013).

single CCD (Charged Coupled Device) or CMOS (Complementary Metal Oxide Semiconductor) sensor. And capture color images using a color filter array (CFA)) (Popescu & Farid, 2005). Therefore, CFA is located in front of the sensor in order to render the color. CFA filters are designed in such a way that only a particular color (red, green or blue) rather than all three is captured by each pixel. The effect of CFA is to create a single mosaic channel of red, green and blue pixels which needs to be transformed to the three-channel output by estimating the missing pixel values based on their sensed neighbors (demosaicing). Once the RGB is generated, digital cameras usually achieve various numbers of processing to enhance its quality and to reduce its size for storage purposes, commonly by means of JPEG compression. The stored image can then undergo additional out camera processing aimed at further improving its quality or at manipulating its semantic meaning, such as rotation, scaling, blurring and illumination changes.

According to the previous representation of the image life cycle, the intrinsic fingerprints that can be examined with forensic methods are classified to acquisition, coding and editing fingerprints.

i. Acquisition

Each stage of the acquisition process produces interesting cues in digital images. Even though the pipeline in Figure 1.2 is common to the most of cameras, the in-camera hardware and software introduce intrinsic image features according to the specific manufacturer options. As a consequence, these features are used as traces to discriminate between different kinds of camera brands or revealing the presence of image tampering.

The first fingerprint introduced into an image by any camera is due to lens aberration which deforms the captured image.

There exist several types of aberrations caused by lens, each of which has distinctive features on the image that can be used to link between images with a specific camera called source camera identification. For example, chromatic aberration (CA) is responsible for colored edges along boundaries separating bright and dark regions of the image. Many methods assist on such artifacts for source camera identification and for tampering detection (Yerushalmy & Hel-Or, 2011) .

The second fingerprint is sensor noise caused by imperfections of the image sensor leads a slight variance between the perceived scene and the captured image. The dominant component of sensor noise is the photo response non uniformity noise (PRNU) noise (M. Chen et al., 2008). The PRNU is a noise pattern generated by the irregularity in pixel response over the CCD sensor under illumination changes. While PRNU is caused by the physical aspects of the sensor itself, it is almost impossible to eliminate it completely and is usually considered to be a normal characteristic of the sensor. As a consequence, PRNU

can be utilized for source camera identification according to the technical imperfections of their sensors (C.-T. Li, 2010).

The third fingerprints are CFA demosaicing can be categorized into two main types:

1. Techniques try to estimate the parameters of the color interpolation algorithm (Gallagher, 2005) and the structure of the pattern filter to classify different source cameras.
2. Techniques try to evaluate the presence and absence of demosaicing artifacts (Bayram et al., 2008a). For example, an image coming from a digital camera, in the absence of any successive processing, will exhibit demosaicing traces; moreover, demosaicing irregularities between various regions of the image, as well as their absence in the analyzed image, will put the image integrity in suspicion.

ii. Coding fingerprints

Most of the digital cameras encode the images with high quality JPEG format for efficient storage purposes. In fact, JPEG compression leaves various kinds of clues including blocking artifacts and quantization artifacts. Blocking artifacts are caused by block based coding approach (Y.-L. Chen & Hsu, 2011). Quantization artifacts are caused by quality factor or quantization tables. The underlying idea of forensic techniques is that block based image coding, like JPEG compression, leaves artifacts compression traces in the pixel domain or in the transform domain that can be exposed (Sutthiwan & Shi, 2012).

iii. Editing fingerprints

Following the acquisition and in camera processing steps, the captured image may go through different kinds of processing tools. Editing tools such as Photoshop can be utilized in a legal way which is called “innocent” to improve the quality of an image in an

illegitimate way or in an illegal way to change its semantic meaning. Unfortunately, forgers usually add or hide something in the image content followed by geometric transformations (rotation and scaling) (Christlein et al., 2010) and some post processing operations such as illumination changes and blurring to make the forgery undetectable in such a way that our naked eyes are unable to detect any irregularity caused by the forgery (Mahdian & Saic, 2007). Hence, we refer to this kind of manipulation as "malicious" attacks.

Figure 1.3 introduces three main types of editing operators, along with some examples for each identified type: some operators are likely to be utilized only for innocent editing, like image enhancement operators, while others are clearly intended for malicious attacks. In the middle, there are geometrical transformation (e.g. rotation, scaling) that may be applied either for slight editing or for changing the semantic meaning. Concerning malicious image editing attacks, the most important is copy move forgery.

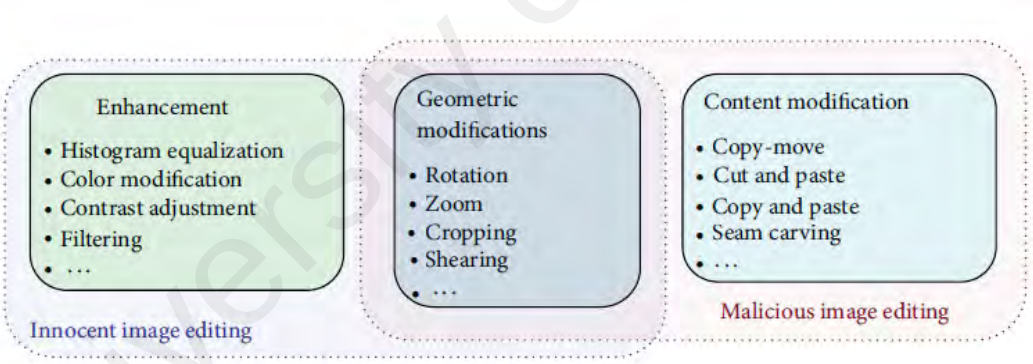


Figure 1.3: Main types of possible image editing tools applied to an image.

1.2.2 Trustworthiness of Digital Images

Whenever digital image is accepted as a piece of occurrence of depicted event, it is to examine the trustworthiness of image. This means specifically that the image has to be authentic to ensure that the image content has not been modified and the depicted scene is a valid representation of the real world. However, it is not only the depicted scene that is

regarded to convey information, but also the image's origin led to the respective image. For instance, consider a photograph is published in a reputable digital newspaper. The responsible editor cannot make a decision whether the image has been tampered with or not. However, this decision may also depend on authentication methods of digital image forensic (Al-Qershi & Khoo, 2013).

- **Digital image authentication methods**

Two main types of authentication methods in digital image forensic have been explored in the research: active methods (Cheddad et al., 2010; Guojuan & Dianji, 2011; Huo et al., 2013; B. Li et al., 2011; X.-Y. Luo et al., 2008; Singh & Ranade, 2013), and passive methods (Birajdar & Mankar, 2013; W. Luo, Qu, Huang, et al., 2007; Piva, 2013; Poisel & Tjoa, 2011; W. Wang et al., 2009). In active methods, mainly watermarking and steganography techniques are used to embed the digital authentication information into the original image. The authentication information may be used as a verification for forensic investigation when the image has been falsified, and even point out if the image has been tampered with or not (Hsieh et al., 2006; Rawat & Raman, 2011; Singh & Ranade, 2013; Li Zhang & Zhou, 2010). These techniques are restricted, because authentication information could be embedded either at the time of recording, or later by authorized person. The limitation of this technique is that it needs special cameras or subsequent processing of the digital image. Furthermore, some watermarks may distort the quality of the original image. Due to these restrictions, the researchers tend to develop passive techniques for digital image forensic. These techniques inspect the images without embedding authentication information, such as signatures or watermarks.

In active methods, the image formation process is purposely modified in which digital authentication information is embedded into an original image at the acquisition step. This information is extracted during the authentication step for comparison with reference authentication data. The authentication information may be used to verify whether an image has been forged in forensic investigations. There are two types of techniques in active approach: a cryptographic signature and imperceptibly embed digital watermark directly into the image.

I. **Cryptographic signature**

Mainly focus on detecting the existence of secret messages, but some paid more attention to identifying the data hiding domain and the type of steganography algorithm. Steganography techniques aim to select features from the image to generate content signature, by assuming that those features are secured from passive or active attacks and also it should be imperciptable (Cheddad et al., 2010).

II. **Fragile watermark**

Is applied to the cover image and it gets destroyed at a tampering attempt. But one major difficulty here is to make the distinction between malicious and naive modifications (tampering versus fair compression) (Rawat & Raman, 2011).

III. **Semi-fragile digital watermark**

Is utilized for image authentication and integrity verification. It can tolerate image content preserving manipulations for both malicious and non malicious manipulations. It is more focused on detecting intentional attacks than validating the originality of the image (Hsieh & Wu, 2006) (Huo et al., 2013) (Bao et al., 2011).

The above techniques as shown in Figure 1.4 are designed to relate the resulting image to its origin, or to be sensitive "fragile" to image post processing attacks.

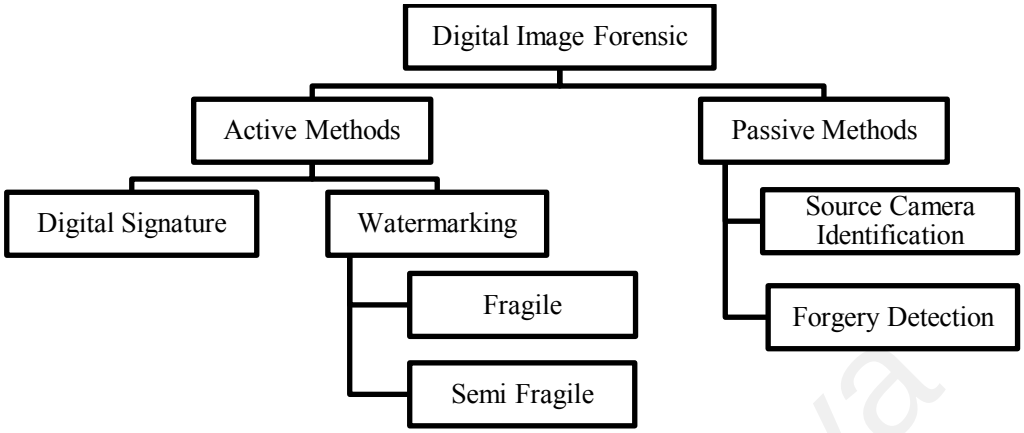


Figure 1.4: Authentication methods in digital image forensics.

In the past few years, digital watermarking has been applied to authenticate and localize tampered regions within images (Li Zhang & Zhou, 2010) (Huo et al., 2013) (Singh & Ranade, 2013) (Hsieh & Wu, 2006) (Rawat & Raman, 2011). Fragile and semi fragile digital watermarking techniques are often utilized for image content authentication. Fragile watermarking is appropriately named because of its sensitivity to any form of attack whilst semi-fragile watermarking is more robust against editing attacks. It can be used to verify tampered content within images for both malicious and non malicious manipulations. In addition, semi-fragile schemes make it possible to verify the content of the original image, as well as permitting alterations caused by non malicious "unintentional" modifications such as image formation processes. Moreover, semi fragile watermarking is more focused on detecting intentional attacks than validating the originality of the image(Huo et al., 2013) (Bao et al., 2011) (Guojuan & Dianji, 2011). Digital signature methods mainly focus on detecting the existence of secret messages, but some paid more attention to identifying the data hiding domain and the type of steganography algorithm.

On other hand, digital image forensic is called passive if the detection process cannot interfere with the image formation process and control the appearance and type of forgery traces. The image formation process is regarded as a read only mechanism and the image forensic inspectors have to analyze the image characteristics that are caused by this process. Exposing forgery in passive approach is made by analyzing device characteristics and post-processing fingerprints that caused by out-camera processing step.

1. **Device characteristics**

   Each component in the acquisition camera may affect the captured image and leaves the inherent fingerprints. Such variations of fingerprints may exist, because manufacturers use different parameter settings in each component for different cameras. This difference can be utilized to infer the source camera of an image. The process of detecting this type of traces can be defined as source camera identification (C.-T. Li, 2010).

2. **Post-processing fingerprints**

   Each processing applied out camera to digital image manipulates their characteristics (e.g. Geometric transformation (rotation, scaling), blurring, illumination changes, additive noise, etc.) producing subtle traces according to the processing itself. The process of revealing this type of traces can be defined as forgery detection (Birajdar & Mankar, 2013).

The main difference between passive methods and active methods is that the former does not require the referenced image, nor additional information about it or the acquisition device. Thus, this type of method is accomplishing a blind analysis. Furthermore, such an analysis is also passive, in the sense that conversely to watermarking techniques no specific

hardware such as trusted cameras should be utilized to make the techniques practically feasible. Such passive methods will be introduced in the following Section 1.2.3.

1.2.3 Passive forensic methods

Passive methods were inspired by image steganalysis which examines the stego image content and measures its statistical properties, for example, first order statistics (histograms) or second order statistics (correlations between pixels, distance, direction). It consists of three major steps: image preprocessing, feature extraction and classification which make it similar to passive methods. But there is a little bit difference between passive digital image forensic and image steganalysis is classify feature vectors of different regions in the same image not between stego and cover image(Guojuan & Dianji, 2011).

Passive methods are regarded as the new direction of forged region detection in an image without requiring explicit prior information. They also expose image tampering by analyzing pixel-level correlations (Al-Qershi & Khoo, 2013; Birajdar & Mankar, 2013; Farid, 2009).

Passive image forensics approaches have been classified into five categories by (Farid, 2009), as shown in Figure 1.5 :

i) **Pixel based techniques** are based on detecting the statistical irregularity or pixel level correlations, introduced at the pixel level during the forgery process (Al-Qershi & Khoo, 2013). Pixel-based approaches are the most popular in image forgery.

ii) **Format based techniques** are based on detecting the transformation of image forgery via analysis of JPEG compression artifacts (Y.-L. Chen & Hsu, 2011; Sutthiwan & Shi, 2012).

iii) **Camera based techniques** concentrate on detecting the clues of image forgery by exploiting the artifacts introduced by different stages of the image capturing process (C.-T. Li, 2010; Van Lanh et al., 2007) as show in Figure 1.5.

iv) **Physics-based techniques** are based on estimating the lighting directions and differences in lighting between objects in the image as a telltale sign of image tampering (Johnson & Farid, 2005).

v) **Geometric based techniques** are based on estimating the principal point of objects across the image, and the inconsistency between principal points, can be used as evidence of image forgery (Johnson & Farid, 2008).

In the pixel-based techniques, the key idea is exposing image tampering by analyzing pixel level correlations as shown in Figure 1.6. Based on the operation used to create a tampered image, pixel based image forgery techniques can be categorized into three groups: image splicing (Avidan & Shamir, 2007; I.-C. Chang & Hsieh, 2011; Ye et al., 2007), image retouching and copy-move forgery. These methods aim to detect forgery as shown in Figure 1.7.

1. **Image splicing** adds a part of an image into another image in order to hide or change the content of the second image.
2. **Image retouching** manipulates an image by enhancing or reducing certain features of the image without making significant changes on image content (Granty et al., 2010).
3. **Copy-move forgery** is copying a region of an image and pasting it in another location of the same image. The forgers perform duplicate region with different geometric and post processing operations to hide traces and make consistency

with surrounding area (Al-Qershi & Khoo, 2013; Bayram et al., 2008b; Christlein et al., 2012; Y. Sheng et al., 2013; Shivakumar & Santhosh Baboo, 2010).

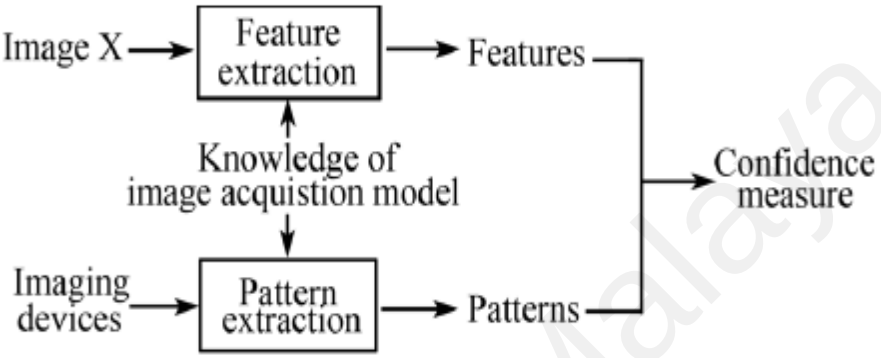


Figure 1.5: Generic Image source camera identification model (W. Luo, Qu, Pan, et al., 2007).

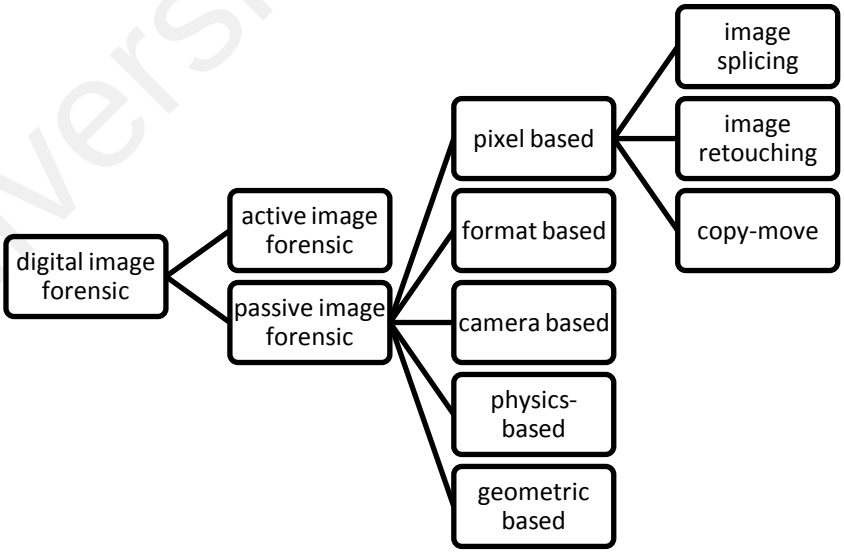


Figure 1.6: The Taxonomy of passive image forensic approaches.

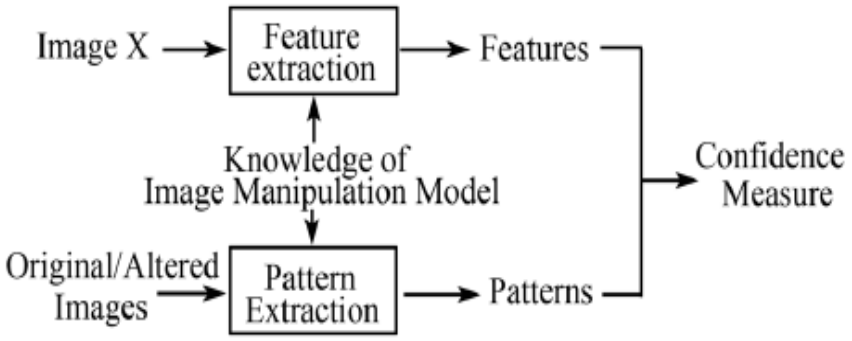


Figure 1.7: Generic Image forgery detection model (W. Luo, Qu, Pan, et al., 2007).

The copy-move forgery is becoming one of the most popular image operations in image tampering, especially with the power and ease of use of image editing software. The key characteristic of the duplicated regions is that they have the same noise components, texture, color patterns, homogeneity condition and internal structure (Devi Mahalakshmi et al., 2012).

i. Definition of copy move forgery detection:

A technique which is used for revealing the duplicated regions in the forged image. However, duplicated regions are not always exactly the similar, because they may be rotated, scaled, blurred or illuminated by changing contrast for a better forgery. Copy-Move forgery detection(CMFD) is defined mathematically as: $g\ (x,y) = T[f(x,y)] + n(x,y)$. Where $f(x,y)$ denotes the original region, and T denotes geometric transformations including translation, rotation, or scaling. $n(x,y)$ denotes such operations including lossy compression, blurring or noise addition. Hence, a good copy-move forgery detection

technique should be robust to all such operations (Y. Sheng et al., 2013). Figure 1.8 gives a typical example and depicts a copy–move forgery in an image of an Iranian missile test.

Figure 1.8: A typical copy move forgery, applied to a press photograph of an Iranian missile test. The original image with three missiles (shown on the left). The forged image with four missile using copy move attack (shown on the middle). The right image shows the detection results.

1.3 Problem Statement and open issues

The most common way to change the semantic meaning of an image is copy move forgery. The purpose of such forgery is hiding authentic region or introducing a fake region into the image. A copy move forgery can be done by duplicating region of any size and shape once or multiple times elsewhere into the same image. The key characteristics of duplicated regions, such as noise components, color patterns, homogeneous textures, and internal structures, are similar and compatible with the rest of image (Devi Mahalakshmi et al., 2012; Mahdian & Saic, 2009; G. Muhammad et al., 2012). Such similarity makes the exposition of duplicate regions in forged images is possible. Thus, they will not be perceptible using methods that search for inconsistencies in statistical measures in different part of the image. To create a convincing forgery, the duplicated regions often are manipulated by geometric transformations and some post processing operations. As a consequence, reliable copy move forgery detection should be robust to geometric

transformations such as rotation, scaling and also post processing operations, including blurring, illumination changes, additive noise and JPEG compression. The main idea of CMFD is to find corresponding points between duplicated regions and spatially link them in such a way that a certain distance measure between their descriptors is minimized.

We will highlight the main geometric transformations and post processing operations that make the CMFD is a challenging task for forensic analysis as follows:

I. Geometric transformations

Is a linear coordinate transformation that includes elementary transformations translations, rotation and scaling.

1. **Translation:** shifts a duplicated region by a specified number of pixels in either the *x* or *y* coordinates or both.
2. **Rotation:** in practice, we found the most of block based CMFD methods have a limited performance for detecting duplicate regions under rotation angles up to 30 degrees.
3. **Scaling:** duplicated regions might have different sizes due to different scaling factors. Scaling can performed by interpolating between pixel values in local neighborhoods.

II. Post processing operations

1. **Blurring**: is used as a retouching tool to hide traces of forgery, especially in the edges of forged region.
2. **Lighting conditions:** varying illumination between duplicated regions is made by changing intensity of their pixels which makes the forgery is difficult.

3. **JPEG compression:** After tampering an image, resaving can be done by the forger by saving the image using a lossy JPEG compression with different quality factor.
4. **Additive noise:** The duplicated regions are modified by applying noise addition, in order to adjust the patch with respect to the image area where it has to be located.

Furthermore, we need to regard the internal structure and texture of duplicated regions in CMFD. The duplicated regions are classified into two classes based on geometric primitives:

1. **Uniform region:** is a flat region in the image does not contain any primitives like edges and corners, mostly contains much less details to represent textured regions in the image for example: Sky and Ocean etc.
2. **Non uniform region:** represents a globa**l** image and more details contain texture primitives like corners, edges and lines.

In this research, we propose to develop an efficient copy move forgery detection algorithm that is able to detect and locate different duplicated regions under various geometric transformations and post processing operations. As a result, the big question is: How would a copy-move forgery detection algorithm is able to efficiently detect, locate the tampered regions with a detection rate in reasonable time and with a capability of robustness to rotation, scale, JPEG compression, Noise, Rotation, blurring and illumination variations?.

Figure 1.9 introduces all the following features have to be carefully investigated in order to develop an efficient copy move forgery detection scheme as follows

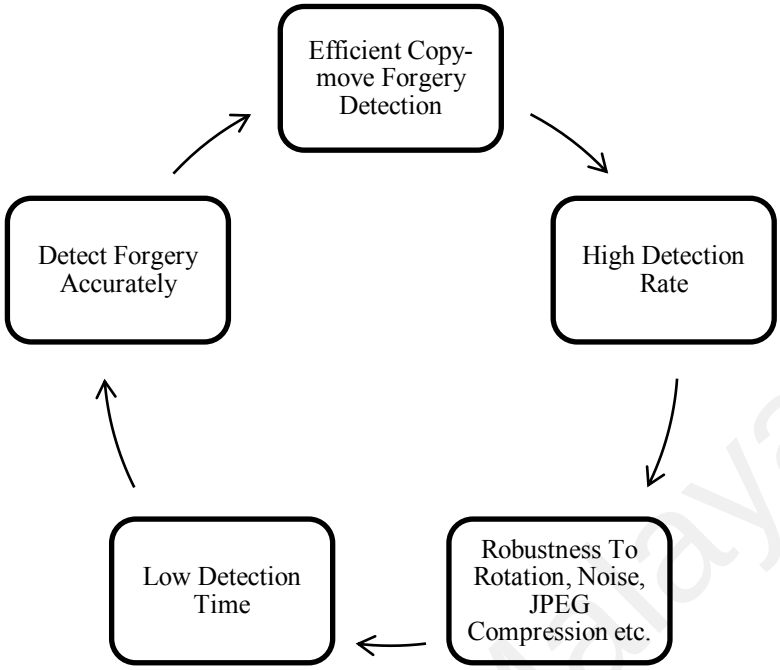


Figure 1.9: The main features of CMFD methods.

1. **Effectiveness:** a reliable CMFD should detect small duplicated regions and multiple regions.
2. **Robustness:** extracted features should be robust to geometric transformations and post processing operations.
3. **Detection Rate:** some of the block based CMFD have high False Positive Rate (FPR) in uniform regions with the small size. The keypoint based CMFD methods struggle to detect non uniform duplicated regions.
4. **Time complexity:** the high computational time of CMFD method due to large number of instances, high dimension of feature vector and exhaustive block matching algorithm.

In the process of development of CMFD method, many open issues for detecting duplicated regions are highlighted as follows

1. The detection of this kind of attack remains a challenging problem such as understanding which is the original patch, between two copies.
2. Improving performance in detecting copied regions with small size is a challenging task and making detection techniques more content independent (attacks on very smooth regions, e.g., depicting the sky, are usually considered false positives) (Piva, 2013).
3. As a suggestion for the potential future work, it can be mentioned here that there is a need to generate a common test images database. And evaluate our method much easier. Furthermore, there is a need to develop further novel and sophisticated analyzing methods allowing for detection of forgery from different points of view.
4. Another challenging task will be improving the reliability and robustness issues of methods (Mahdian & Saic, 2010). Furthermore, block matching methods are not applicable when copies are processed by geometrical transformations, we suggest to concentrate on texture descriptors, with those obtained using other image features (color, shape), and to combine them within a single framework (Ardizzone et al., 2010).
5. One of the biggest issues these techniques had to deal with was, being able to detect the duplicated image regions without getting affected by the common image processing operations, e.g. compression, noise addition, rotation. The other challenge was computational time, which becomes important considering the large databases, these techniques would be used on(Bayram et al., 2008b).

6. Some of the algorithms strongly depend on several thresholds or initial values, and setting these thresholds and values requires a large number of experiments and optimization.

1.4 Research Aim And Objectives

The aim of this research is to develop a reliable copy move forgery detection system that is capable to expose a duplicate region or multiple regions with various block sizes from forged images efficiently and accurately. The proposed method should be robust to the geometric transformations and regarding post processing operations. Based on the findings of the literature review that is discussed in (chapter 2), we need to make improvements in terms of accuracy and/or computational cost. This research is motivated by main goal with specific objectives as set:

1. To investigate different copy-move forgery detection methods.
2. To propose an efficient copy move forgery detection method that is robust to noise, rotation, scale, blurring and JPEG compression with low computational time.
3. To propose a new copy move forgery detection method that can reveal duplicate regions or multiple regions with small sized up to 8 * 8 pixels.
4. To test and evaluate the proposed algorithms by measuring the detection rate using MICC-F220 and Image Manipulation datasets, and evaluate using true positive and false positive rate.

1.5 Research Questions

Several research questions have been formulated to serve as a guideline to conduct this research and to achieve the research objectives at various stages:

Q1. How to reveal the location of region duplication forgery in digital images?

Q2. How to develop an efficient copy move forgery detection method to detect duplicated regions accurately?

Q3. How to develop an efficient Region duplication forgery detection method to expose two types of regions: uniform and non-uniform regions in the forged image?

Q4. How the proposed method can locate small duplicated regions under copy move forgery?

Q5. How can the copy move detector be superior to the existing ones in terms of detection rate and computational time?

1.6 Scope Of Research

This research is mainly focused on the development of state-of-the-art passive image forensic systems for copy move forgery. This research comprises a number of stages:

1) Research finding: Based on the findings of the literature review, the limitations of current CMFD methods are identified. Information is gathered from publications including journals, conference papers and thesis both locally and abroad. Then, the decision was made on which approaches need improvements in terms of accuracy and computational cost.
2) Methodology: The design and implementation of the proposed CMFD system integrate three different methods within its structure. These components are: key

point based detection method, blur forensic scheme and illumination invariant detector (Section 1.7).

3) Data collection: The data collection at the stage keypoint based detection method is conducted using two image datasets:
    i. **MICC-F220 Dataset** (Amerini et al., 2011), a well known benchmark in CMFD research community. Is composed by 220 JPEG images; 110 are forged and 110 originals. Furthermore, MICC-F2000 dataset includes 2000 images; 700 are tampered and 1300 originals.
    ii. **Image Manipulation Dataset** (Christlein et al., 2012), which includes 48 PNG true-color images.
4) Conducting experiments: Qualitative and quantitative results on the above mentioned datasets have been obtained. Generally, when proposing a system with composite steps, it is interesting to evaluate each step separately. The performance evaluation of keypoint based CMFD method is conducted under rotation and scaling conditions, artificial blur and illumination variation. The proposed CMFD system is compared with the state-of-the-art detection methods in terms of accuracy and robustness.
5) Documentation: Some of the research ideas and findings are reported in publications (See Appendix-A). The whole research is documented in this thesis.

1.7 Research Methodology

In practice the problems associated with copy move forgery detection, especially detecting two kinds of duplicate regions: uniform and non uniform regions in the same image can rarely be successfully solved through the application of just one methodology. This makes copy move detection is a challenging task in image forensics. The implementation of geometric invariant methodologies in a reliable CMFD system is considered. Where keypoint based method is adapted with segmentation based method to detect uniform and non-uniform regions with small sizes under rotation and scale attacks. The blur and illumination invariant methods can resolve the problem of detecting duplicate regions under blur and illumination changes. The general architecture of the proposed CMFD system consists of three main phases as shown in Figure 1.10. The proposed methods are:

1. Key point based method based on Harris corners and angular radial partitioning (ARP).
2. Blur forensic scheme based on Blur metric evaluation (BME) and phase congruency (PC).
3. Illumination invariant detector based on Hessian interest points and center symmetric local binary transforms (CSLBP).

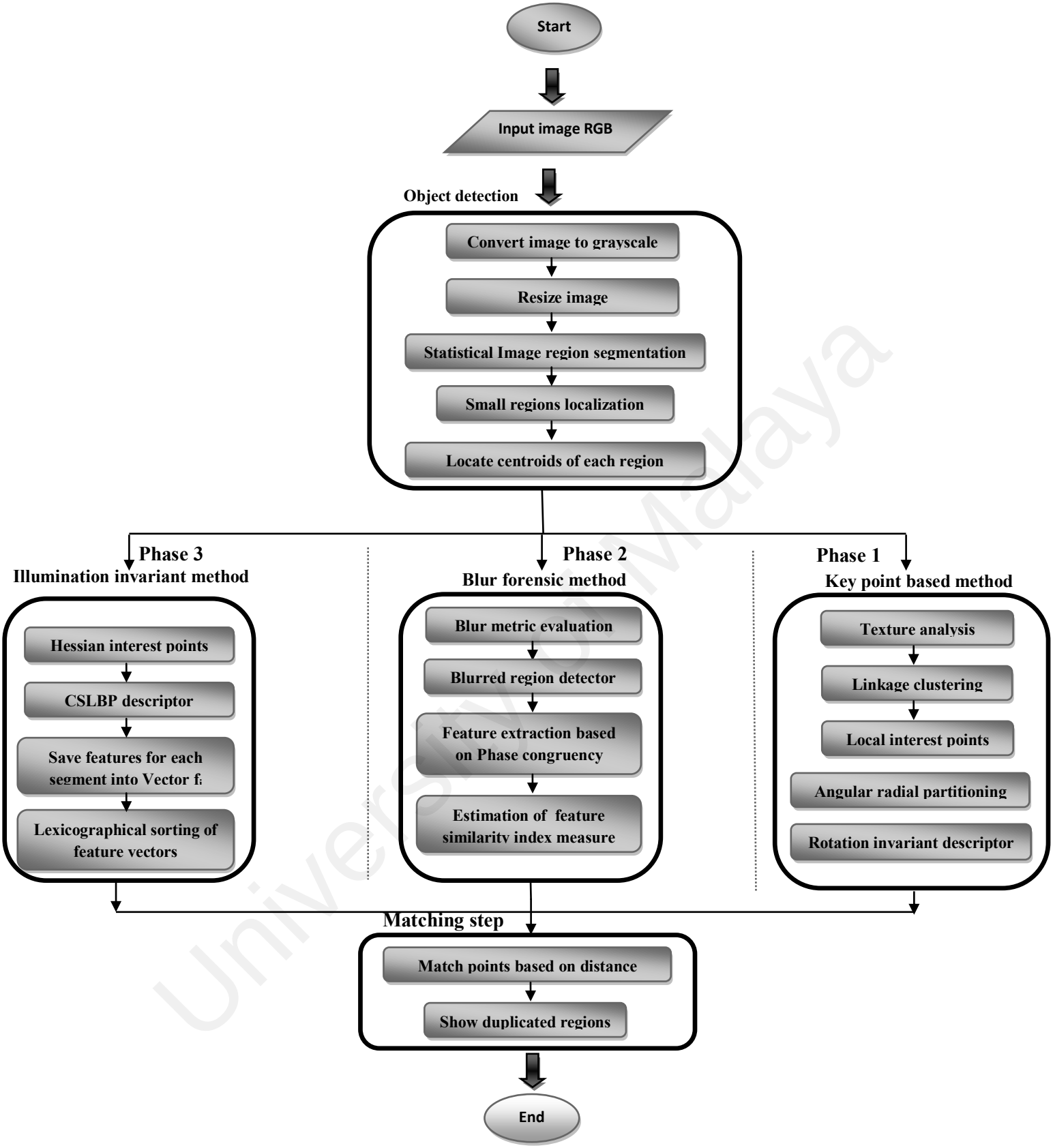


Figure 1.10: Methodological flow of CMFD system.

1.8 Research Contributions

This research introduced a CMFD framework based on image segmentation and key point based method. Although, the duplicated regions have been exposed mainly by comparing the Harris key points extracted from the image. Our main contributions can be concluded to the following aspects:

1. **Proposing a new algorithm for copy-move forgery detection.** The key contribution of this thesis is presenting an efficient copy-move forgery detection scheme. This approach proposes an algorithm to authenticate digital images with the capability of locating copy-move forgery regions. Detection rate, which is a very important factor for forgery detection methods, is increased. The proposed tamper detection algorithm conducts comprehensive comparisons, to ensure the accuracy of the results. As the results illustrated, the proposed efficient tamper detection algorithm detection rate is much better compare to existing methods. The proposed copy move forgery detection scheme maintained 96 % true positive rate and 3 % false positive rate.
2. **We propose to segment the image as a preprocessing step in copy move forgery detection method to detect small duplicated regions.** We consider that duplicate regions have the certain meaning in images. The statistical region merging segmentation divides the image into independent regions based on homogeneity condition. Such that, CMFD problem has been solved by partial matching among these segmented regions.
3. **Finding a suitable feature extraction technique which is able to extract robust features of the image.** A new copy-move forgery detection method based on Harris is proposed. The proposed method can overcome the problem of robustness against

different copy-move attacks such as rotation, scale, blurring, and addition of noise or JPEG compression. An important challenge for copy-move forgery detection approaches is their robustness against rotation with different rotation angles ($R=45^0,90^0,180^0$etc.). One main contribution of our work is the analysis of all existing feature extraction techniques to identify which one produces features with the highest robustness to post processing attacks. Features extracted by Harris are invariant with regard to rotation, scale, addition of noise and are mostly robust to JPEG compression. It is shown that because of the robustness of the features extracted by Harris, the true positive and false positive rates of our scheme are improved.

4. **A new matching similarity measurement to compute similarity between features extracted from the image.** The feature matching process between segmented regions consists of two steps. In the first stage, an accurate estimation of noise pattern can be obtained from Tamura texture features. In the second stage, the linkage clustering algorithm concerned the improvement of computational complexity of our scheme. Segmented regions are clustered with similar noise patterns to quickly and efficiently select a reasonable number of similar candidate regions. In particular, the performance of CMFD and computational complexity depend on the number of instances and the size of candidate regions. While, the most of block based methods does not regard the small sized copied regions, the duplicate regions with small size block are detected by scanning an image horizontally and vertically. Then, small candidate regions are selected and labeled using the least frequent method.

1.9 Thesis outline

The rest of the thesis is organized as follows:

Chapter 2 describes the related works in the CMFD. The main characteristics of different approaches are also presented. These approaches have been developed at different stages. This chapter discus the pipeline of each approach and major issues faced in copy move forgery research and compare them among different parameters at each stage.

Chapter 3 presents the background of key point based CMFD methods according to local interest points and their robustness to rotation and scale.

Chapter 4 is concerned with the methodology of the proposed schemes in each phase of the research. In this chapter, the methodologies of the three different phases (Phase1: rotation invariant copy move forgery detection method; Phase2: blur forensic scheme for copy-move forgery detection ; and Phase 3: illumination invariant method for CMFD) are described.

Chapter 5 details out the proposed geometric invariant CMFD methods in phase1, phase 2 and phase 3 to reveal duplicate regions in digital images. The implementation of each Phase is described in detail.

Chapter 6 presents the findings of the copy-move forgery detection, focusing on the result of the proposed algorithm in both phases against different attacks such as JPEG compression, rotation, Gaussian noise and scale. This chapter analyses the results of the

algorithm against the mentioned attacks and evaluates them compared with other copy-move forgerydetection schemes.

Chapter 7 provides a brief summary of the proposed scheme. It concludes the thesis with highlights of the findings, overall research conclusion and future research direction.

CHAPTER TWO

REGION DUPLICATION FORGERY DETECTION TECHNIQUES – LITERATURE REVIEW

2.1 Introduction

In this chapter, we review the existing techniques for automatic region duplication detection under copy move forgery. It gives a good insight into the problem and a general idea about the different approaches used in attempting to solve the problem. Then, existing geometric invariant methods are reviewed due to the high importance of this step to improve the detection rate. Some terminologies (image forgery detection, image feature consistencies, pixel based detection and region duplication detection) that are closely related to the copy move forgery detection are defined as follows:

- **Image forgery detection:** an image can be forged in many ways with no visual artifacts. This process affects the statistics of the image while has undergone malicious post processing operations. As a result, forged images will exhibit variations due to these operations. Image forgery detection aims to determine whether the image has been manipulated after it has been captured.
- **Image feature consistencies:** detect the image forgery based on consistent features which are extracted from local interest regions in the suspected image. Such consistent features from different regions are based on local interest points (see Section 3.1) or texture features.
- **Pixel based detection:** is to detect statistical regularity introduced at the pixel level where the underlying divided block of a digital image has been

analyzed. The pixel correlations that appeared in a specific form to search similarities.

- **Region duplication forgery detection:** is to localize similar regions in the single image that have the same inherent fingerprints. This process focuses on analysis of the internal structure and texture of image regions according to their geometric and post processing invariance properties such as rotation, scale, blur and illumination changes. This type of image forgery is famous because detecting it is more complicated. It is straightforward to realize that this kind of forgery is harder because of some image features such as noise and color are the same as the rest of image content. Furthermore, the source image and destination are the same which makes a convenient forgery.

  Figure 2.1 shows an example of region duplication forgery detection. This copy move operation was applied on the original image to replicate the object or hide the original content in the moved region as shown in Figure 2.2.

Figure 2.1: From left to right: The image Beachwood (first image) is forged with a green patch to conceal a building in second image. A ground truth map (third image) is generated where copy-moved regions are white.

Figure 2.2: From left to right: first image is forged with replicate girl appeared in the second image. A detection result mentioned in the third image.

The detection of region duplication forgery has started by (Fridrich et al., 2003), and many research works have been published in various conferences and journals about it. Figure 2.3 illustrates the number of papers published in conferences and journals as indexed by Web of Science and SCOPUS since 2007. The data were collected from the Web of Science and SCOPUS websites.

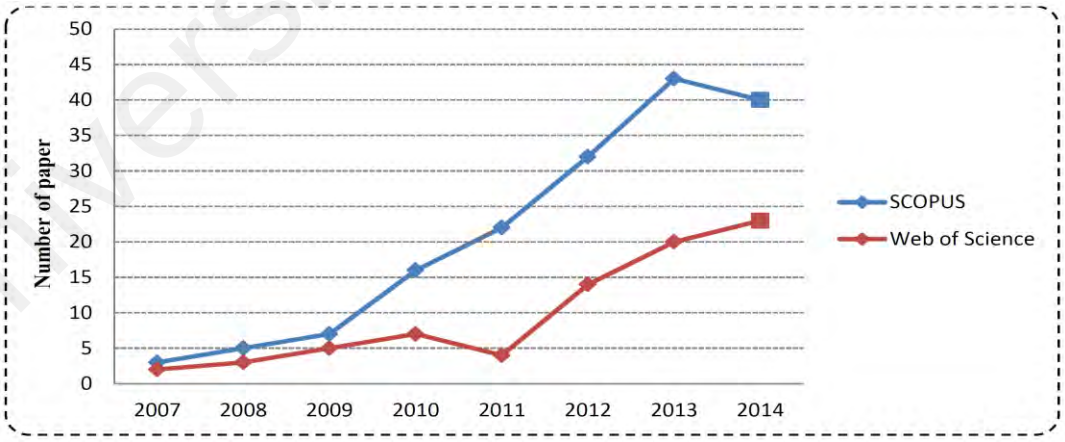


Figure 2.3: Copy move forgery detection papers indexed by Web of Science and Scopus.

In the following Section 2.2, various aspects of digital imaging along with image features which are employed for copy move forgery detection are explored.

2.2 Digital image features used for Forgery detection

When a copy move forgery has been performed to alter the content of the digital image and change the meaning of the represented scene. Some traces of this operation are left somehow over the new forged image. These traces, although unperceivable, can result in the modification of the image intrinsic structure. We need to investigate such pixel values inside image via consistency analysis of features within the image content itself to detect duplicated regions.

Most of copy move forgery detection methods deal with two kinds of images: grayscale images (single dimensional array) and RGB images (three-channeled bi-dimensional array).

i) Grayscale image

The range of pixel values in the grayscale image changes from 0 to 255 conceivable distinctive shades of gray. The value of 0 represents dark color with the weakest intensity while 255 shows the white color with the strongest intensity. The grayscale intensity is usually encoded as an 8-bit integer which gives 256 possible different shades from 0 to 255 which is black to white. Most of copy move forgery detection methods deal with this type of image where the image is converted to grayscale for extracting features such as local descriptors and texture. Figure 2.4 illustrates a sample

of grayscale digital image which contains highly contrasting shades (Gonzalez et al., 2009).

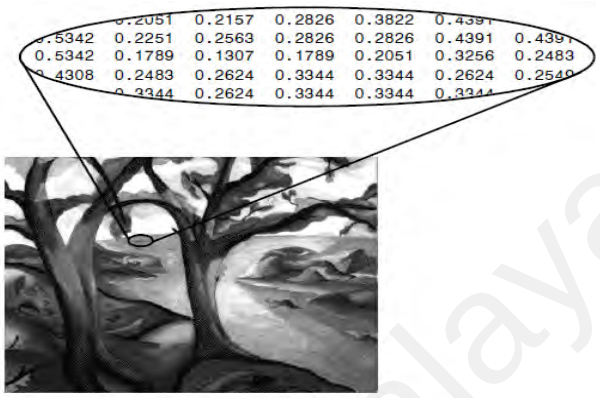


Figure 2.4: Grayscale image.

ii) RGB image

Is a complement model which is an extension of the grayscale model, where each pixel in the RGB model consists of the three primary colors: Red, Green and Blue. These colors are combined in various ways to produce other colors. RGB is a regional color model, which means numerous devices from different organizations produce RGB value in their own way. Indeed, the shade parts like colors or phosphors respond to individual R, G, and B levels in a different way. However, a red RGB model is a number value representing the red module of the next shade, and its pixel intensity lies between 0 and 255. The other two channels are in the same range as red channel. Figure 2.5 illustrates an RGB image (Solomon & Breckon, 2011). Some copy move forgery detection methods used this type of image to detect forgery (Hussain et al., 2012).

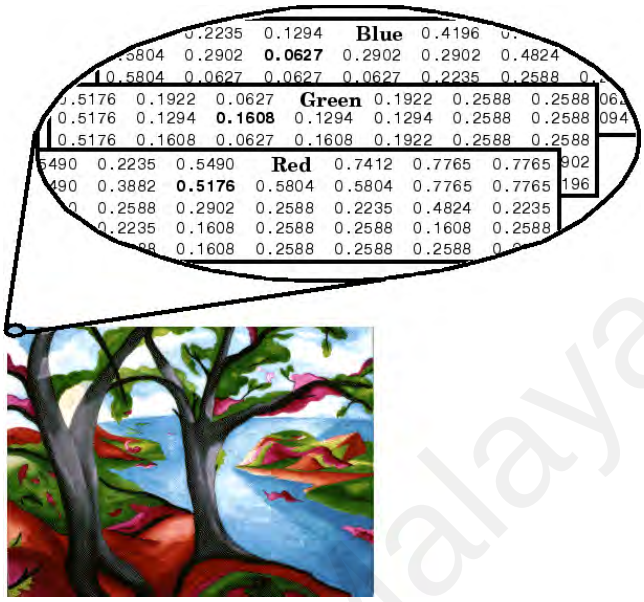


Figure 2.5: RGB image.

2.3 Copy move forgery attacks

An attacker creates his fake image by duplicating a region of the image onto another area. He is often obliged to employ a geometric transformation or some post processing operations to achieve his purpose. In this research, this issue is investigated, if the copy move forgery has taken a place, according to geometric transformations such as scaling and rotation. And also regarding some post processing operations such as blurring, illumination changes, JPEG compression and noise addition.

i) **Geometric transformation** is often used by forgers to perform a spatial transformation of the image coordinate system to achieve special effects. In spatial transformation each point (x, y) of image A is mapped to a point (u,

v) in a new coordinate system $u = f_1(x, y), v = f_2(x, y)$. A rotation is produced by θ by

$$u = x * \cos\theta + y * \sin\theta \quad 2.1$$

$$v = -x \sin\theta + y \cos\theta \quad 2.2$$

As a result, the copied region is rotated by θ in range 5^0 to 345^0 before being moved. Scale transformation is applied to change the size of the object based on the scaling factor by following linear equation

$$u = x * S_x, v = y * S_y \quad 2.3$$

Where S_x, S_y are scaling factors in x, y coordinates respectively.

ii) **Post processing operations**: such as blurring by Gaussian noise which is a statistical noise that uses the probability density function for a normal distribution. Blurring is the process of filtering pixels within the set blur radius with windowed filter function, whose foundational is neighborhood grayscale averaging of pixels within the blur radius (Zhou et al., 2007).

JPEG compression is a method generally used for the data compression of digital images. The degree of compression, which is the quality factor, can be adjusted. Storage size and image quality are traded off by a range of 5 to 100. When an image is compressed using JPEG, it uses a lossy form of compression file based on a discrete cosine transform, and it will affect image quality because some original image information is lost and cannot be restored (Yang & Li, 2012). Figure 2.6 illustrates the rotation operation from different angles and demonstrates the different scale factors applied to a sample image (Amerini et al., 2011). Figure 2.7 illustrates the JPEG

compression to image with different quality factors. Figure 2.8 shows the blur operation to image using different window size.

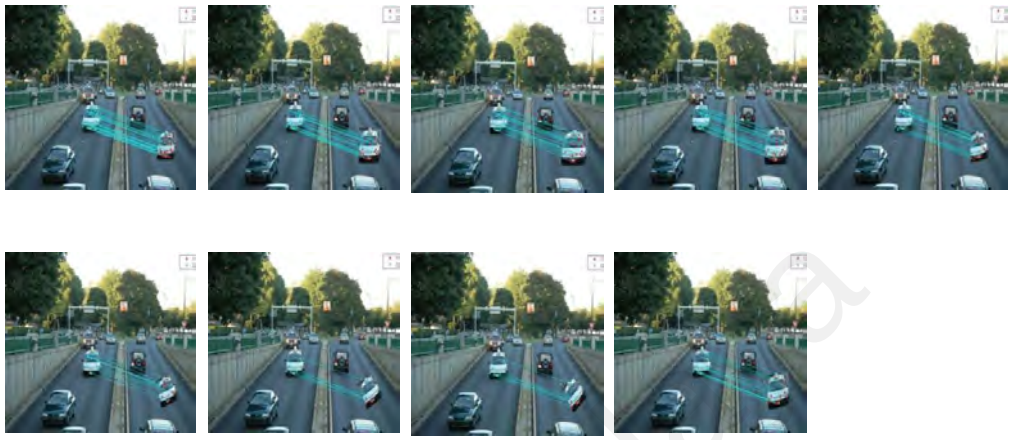
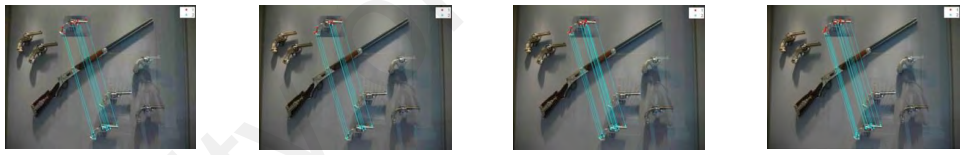


Figure 2.6: Copy move detection results in the presence of 9 different rotation and scaling attacks applied on the image.



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

Figure 2.7: Copy move detection results for compression: (a) JPEG image quality factor 20, (b) JPEG image quality factor 40, (c) JPEG image quality factor 60, and (d) JPEG image quality factor 80.

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

Figure 2.8: Copy move detection results in blurring: (a) window size 5×5, σ = 0.5, (b) window size 5×5, σ = 1, (c) window size 7×7, σ = 0.5, and (d) window size 7 × 7, σ = 1.

2.4 Copy move forgery detection methods

Nowadays, with the availability of high resolution cameras and the popularity of the internet and smart phones, digital images are playing an important role in our daily life. However, due to the powerful image editing software such as Adobe Photoshop, images can be easily tampered with. A large number of tampered images have recently been published by major newspapers to deceive the public about the truth (Bayram et al., 2008b; Gloe et al., 2007; Sencar & Memon, 2013). Therefore, we cannot believe what we are seeing. In other words, the public society has lost its confidence in digital images, especially when it comes in significant situations such as medical records, news items, evidence in court of law, and political propaganda. We need to think about the authenticity of the images. To tackle this crisis of confidence, digital image forensics has begun to develop robust image forgery detection methods to authenticate digital images and restore the lost credibility of digital images. Verifying the originality of the digital image alone is not enough; locating the tampered regions makes the authentication procedure more complete, by separating the parts of the image that are reliable from the parts that are forged.

Due to the growing popularity of copy-move forgery in recent years, many existing methods of region duplication forgery detection have been proposed to detect this type of forgery can be explored in literature. The first method proposed by (Fridrich et al., 2003). It was based on block wise analysis, followed by a similarity ordering of features extracted from each block and comparing them to each other in order to determine which blocks match.

The main steps of copy move forgery detection schemes are: image preprocessing, feature extractions, features matching, match pair connection and outlier removal. However, the type and size of the features in feature extraction step are the main differences among the existing methods. For this reason, as pointed out in (Nathalie Diane et al., 2014) based on partitioning the image and matching subdivisions or features extracted from subdivisions rather than pixels, the detection of region duplication forgery can be categorized into: block based methods (Cao et al., 2012; B. Li et al., 2011; Popescu & Farid, 2004; Zimba & Xingming, 2011) and key point based methods (Amerini et al., 2011; L. Chen et al., 2013; Kakar & Sudha, 2012; Pan & Lyu, 2010).

2.4.1 Block based methods

Due to the fact that in the copy move forgery, the duplicated regions are located in the same image, the tampered image should exhibit two matched regions in internal structure and texture properties. The detection method basically searches for large similar regions in the forged image. This can be done by block wise generation. First, an image is segmented divided into overlapping sub blocks. Then, some features are extracted from each block, and compared with other blocks, to find the most similar blocks. At last, results are analyzed and decision is made only if there are several pairs of similar image blocks

within the similar distance. Most of block based methods consist of the following steps in the common framework as shown in Figure 2.9 are described as follows:

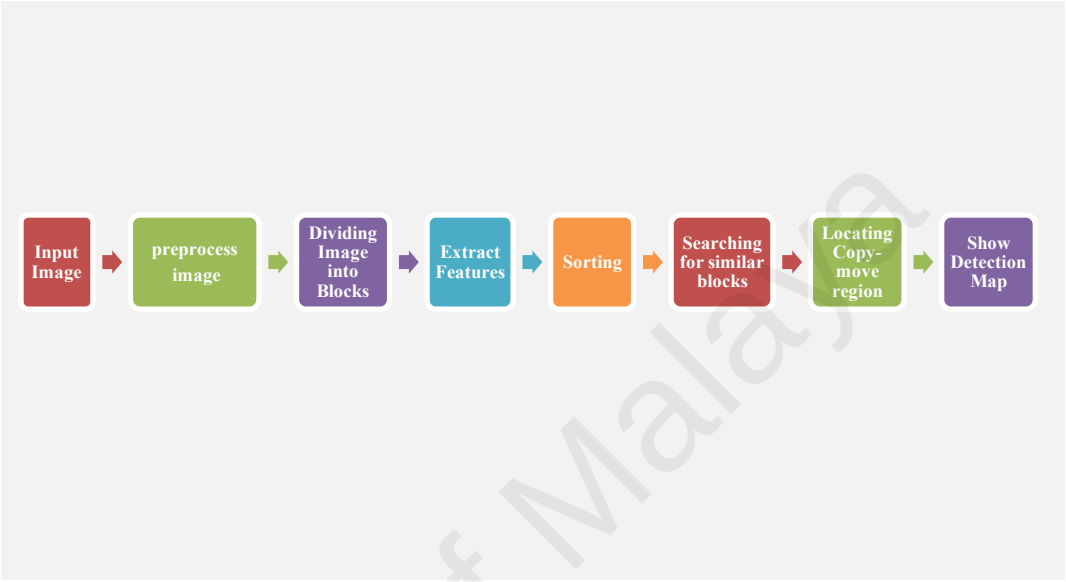


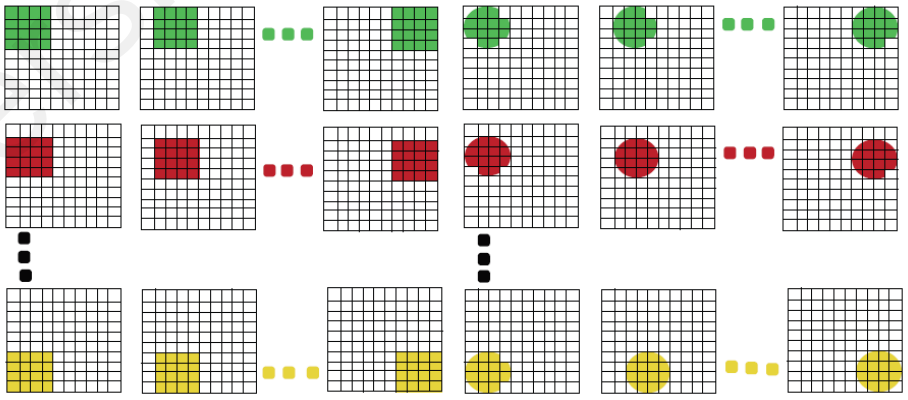
Figure 2.9: The common framework of block based CMFD method.

I. Preprocessing image

Color conversion is one of the most common preprocessing operations used to convert the RGB image to grayscale image or convert the image from RGB (Red, Green, Blue) color model to YC_bC_r color model. Most of block based methods operate on the grayscale images; some methods require the RGB color information from the image to extract features. Other methods deals with the luminance information (Y) from YC_bC_r color image as in (Hussain et al., 2012) .

II. Block tilling

The easiest way to detect such forgery is to segment the image into overlapping or non overlapping blocks of the same size as shown in Figure 2.10. The divided blocks can be square blocks or circle blocks. The similarity check is done at the block level. The block size varies for different detection methods. While the size of the block is BxB and the size of the image is, the total blocks in the image are $(M-B+1)*(N-B+1)$. Instead of exhaustive search between divided blocks, to detect duplicate region makes the total time complexity of sorting algorithm is $O(MN)^2$. The main drawback of block based algorithm is the high computational complexity due to the high dimensionality of blocks. And it is inefficiency against some geometric transformations and post processing operations such as rotation, scaling, blurring and illumination.



(A) **(B)**

Figure 2.10: Overlapping square 4 × 4 block division and corresponding overlapping circular block division with radius r=4 (Nathalie Diane et al., 2014) .

III. **Feature extraction**

The extraction of robust features from each block is applied in order to make the detection method faster and more efficient in case of further post processing of the copied region.

IV. **Dimensionality reduction**

Representing each divided block from the image by proper extracted features, leads to the high dimensionality of feature vectors. Most researchers try to apply dimensionality reduction approaches to improve the time complexity of detection method, such as PCA (principal component analysis) methods and SVD (singular value decomposition) methods.

V. **Sorting feature vectors based on lexicographical sorting or radix sorting algorithm.**

VI. **Matching** each pair of sub blocks to check if they are similar. The Euclidean distance between two corresponding blocks is calculated by $d = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$. Where x_i, x_j and y_i,y_j are the coordinates of matched blocks.

VII. **Show duplicated regions visually** based on morphological operations to threshold the matched regions. The duplicated regions marked with a special color and other unrelated regions are marked with black color.

According to these previous steps, many of block based methods have been proposed depending on the characteristics of divided blocks such as type of extracting features and a dimensionality reduction used to resize feature vector. For instance, different features are extracted by, such as discrete cosine transform

(DCT) (Cao et al., 2012; B. Li et al., 2011), discrete wavelet transform (G. Muhammad et al., 2012), discrete Fourier transform (DFT) (Mahdian & Saic, 2008), principal component analysis (PCA) (Popescu & Farid, 2004; Zimba & Xingming, 2011), singular value decomposition (SVD) (D.-Y. Huang et al., 2014), intensity (W. Luo, Qu, Huang, et al., 2007), and Zernike moments (Zm) (S-J Ryu et al., 2013) as shown in Figure 2.11. These methods are described in details as follows:

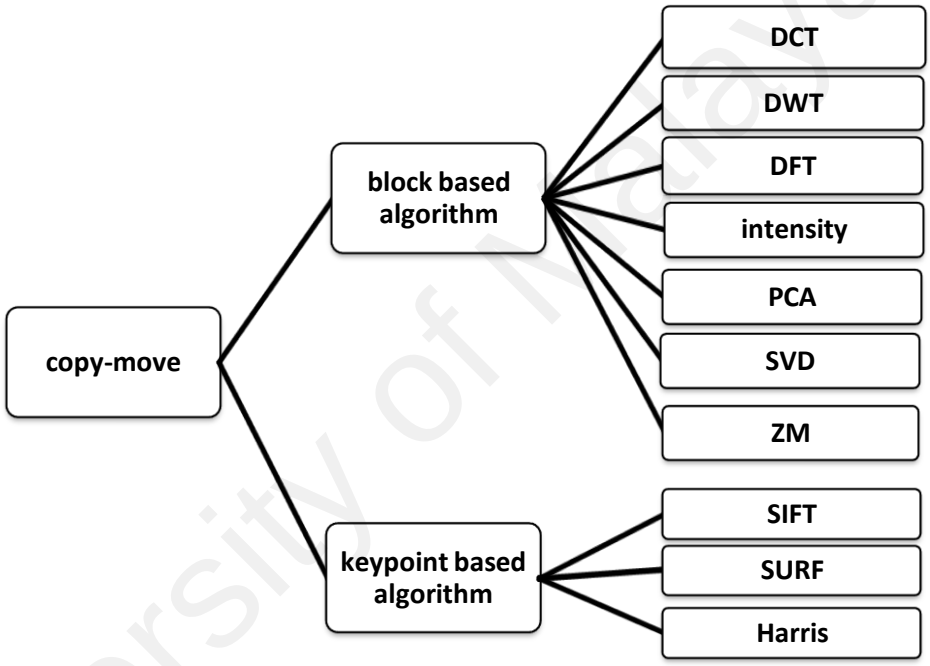


Figure 2.11: Classification of copy move forgery detection methods (Nathalie Diane et al., 2014).

i. **Discrete cosine transform (DCT) based method:** In (Fridrich et al., 2003), the image is divided into overlapping blocks. They applied DCT on each block and store the quantized DCT coefficients into feature vector. A lexicographical sorting of feature vector is employed. Finally, find the

matched pairs between two corresponding blocks and label them as forged regions. This method is the first block based method was developed. The main advantage of this method is that it is suitable for uniform region detection. These regions generally represent image textures such as the sky and the ocean in minimal detail. The common assumption regarding this method is that the forged duplicate regions have not been subject to geometric transformation or post-processing operations such as blurring and illumination changes.

(Cao et al., 2012) proposed copy move tampering detection algorithm based on DCT and circle blocking to extract features. Each circle block was divided into four sectors; a feature vector was computed based on the mean value of DCT coefficients in these sectors.

In (B. Li et al., 2011) DCT is applied to every blocks of the entire image for extracting features. The DCT coefficients are reshaped into a row vector in the zigzag order. And dimensionality reduction was made by truncating the higher frequency coefficients and save only the first lower frequency coefficients because they represent the energy of DCT coefficients better than higher frequencies. All vectors are sorted lexicographically; finally calculate the distance between two corresponding blocks to find similarity.

ii. Discrete wavelet transform (DWT) based method

(Mahdian & Saic, 2009) proposed copy move forgery detection based on DWT to decompose the image into high frequency HH sub bands at scale 1 which give the diagonal details of the image the highest resolution. They are divided into square blocks and compute median absolute deviation (MAD) as a noise estimation of each block. Block merging technique is applied

based on MAD similarity of each block and neighboring blocks to segment the matched regions.

In (Zimba & Xingming, 2011), the DWT was applied in the image to extract low frequency sub bands LL1 at scale 1. DWT coefficients are selected as features from divided blocks. And principal component analysis eigen value decomposition (PCA-EVD) is performed as a dimensionality reduction of feature vector. Only eight features are extracted for each divided block and saved into feature vectors and sorted lexicographically to detect region duplication forgery.

Muhammad et. al. proposed blind CMFD method based on undecimated dyadic wavelet transform (UDWT) to extract features from low frequency sub bands (LL1) and high frequency sub bands (HH1). The similarity measurement is computed between copied and moved blocks in LL1 and dissimilarity in HH1 (G. Muhammad et al., 2012).

iii. Fourier Transform (FT) based method

(Mahdian & Saic, 2008) detected the traces of copied regions in the tampered image based on analyzing periodic properties of interpolated signals of Image. The image is divided into blocks with size 128*128. The periodicity is simply analyzed by applying the discrete Fourier transform (DFT) of an averaged signal obtained from the second derivative of the divided blocks. And plot the magnitude of FFT of these blocks to find peaks that represent to the forged region and can estimate the rotation angle and scale factor. The advantage of this method is that can estimate the resampling rate and interpolation factor caused by rotation and scale attacks.

(Bravo-Solorio & Nandi, 2011) proposed a duplicate region detection algorithm based on log polar mapping (LPM) of image blocks and Fourier transform to build 1 D descriptor with four features length. Where f1, f2, f3 represent the average of red green and blue of color image in one hand and f4 is the entropy of the luminance pixels within each block on the other hand. All features saved into feature vector and applied lexicographical sorting to find the Euclidean distance. The correlation coefficient between these descriptors and its FT magnitude is computed to improve matching decision. Log polar mapping with FT method yields to rotation and scale invariance.

In (Wu et al., 2011), the log-polar fast Fourier transform (LPFFT) of each divided block is applied by first calculating the Fourier transform (FFT) followed by polar mapping with 8 concentric circles and 16 angles to achieve rotation invariance. The method is tolerant to scaling and rotation.

(Bayram et al., 2009) proposed a copy-move forgery detection scheme based on applying a Fourier Mellin transform to the blocks in the image. The image is segmented into square blocks. The magnitude of FT of each block is computed. These values are resampled into log polar girds. Finally, these features are retained onto one dimensional descriptor.

However, the method is robust slightly simple to scaling attack by 10% and it works only with rotation angles less than 10^0.

Among the remaining frequency domain techniques, we provide a comparison Table shows the performance evaluation between these methods according to their detection steps as illustrated in Table 2.1.

Table 2.1: The performance evaluations of frequency based methods.

Literature	Feature extraction	Feature dimension	Detection accuracy	False positives
(Cao et al., 2012)	DCT with circle blocking	4	0.80	0.13
(B. Li et al., 2011)	Improved DCT with low frequency coefficients	16	0.99	0.027
(Mahdian & Saic, 2009)	DWT with HH sub band at scale 1	256	81.18	10.03
(Zimba & Xingming, 2011),	DWT with PCA	8	91.03	9.65
(G. Muhammad et al., 2012).	UDWT	NA	95.90	4.54
(Bayram et al., 2009)	FMT	45	90.75	NA

iv. **Intensity based methods**

Use the color information for blocks as features and build the discriminate statistical color descriptor. These features are used to represent image blocks in spatial domain in order to distinguish them from each other.

(W. Luo et al., 2006) divided an image into small overlapping blocks and each block was divided into two equal parts in four directions (horizontal, vertical and diagonal directions). Then, the average of the color channels RGB is computed and saved into feature vector of length 7. This method showed that such features are not significantly affected by JPEG compression or additive white Gaussian noise and Blurring. Furthermore, it gives high detection rate in case of copy move forgery without malicious modification of copied regions. time complexity for this method was reduced to O(7k lgk) compared to the previous method (Fridrich et al., 2003) with time complexity $O(MN^2)$. but it is highly sensitive to any geometric transformation Because it is based on block of pixels in the spatial domain, (Nguyen & Katzenbeisser, 2011).

Another improvement in (H.-J. Lin et al., 2009) where the image was divided into overlapping blocks and each block was divided into 4 equal sub block to build descriptor based on average of color channel in each block. The radix sort of feature vector is used to improve time complexity to O (9k).

In (W. Luo, Qu, Huang, et al., 2007) identified the similarity between the blocking artifact characteristics matrix (BACM) of the copied and pasted region in the same image. The symmetry of BACM was calculated by dividing image into 7 * 7 square blocks. Each block is divided to represent 4 regions. Finally, BACM feature is computed by sum of energy of differences between the values in each block. This method cans effectively detecting cropping and JPEG recompression operations in JPEG images.

(J. Wang et al., 2009) proposed algorithm for detection of region duplication forgery based on circle blocking. Instead of square blocking, the circle regions exhibit the rotation effects between duplicated regions. The image dimension is reduced by Gaussian pyramid, and four features (mean of each circle area) are calculated and saved into feature vectors. The feature vectors are lexicographically sorted. Then similar vectors will be matched by a certain threshold value. Finally, the area threshold is proposed to remove the wrong similar blocks. This method is robust to pre-processing operations as well as to JPEG compression and the addition of Gaussian white noise.

(Peng et al., 2011) proposed a passive copy move forgery scheme based on denoising the suspected image using Wiener filter in the wavelet domain. The image is converted into grayscale and divided into sub blocks. Sensor pattern noise (SPN) of each block is calculated as features. Finally, forged regions have been located by analyzing the correlations of the features between the

divided blocks in the image. The method is robust to robust against JPEG compression, noise, rotation, scaling and blurring.

(Hussain et al., 2012) transformed the image from RGB to YC_bC_r to extract features from Chrominance components: C_b and C_r to provide some features that human eyes can't see. These components C_b and C_r can be formed by subtracting luminance from red $(Cr = R - Y)$ and by subtracting luminance from blue $(Cb = B - Y)$ respectively. They proposed a copy move forgery detection method based on Weber law descriptor (WLD). This descriptor is a texture descriptor based on the difference of image stimulus intensity. Finally, to find the similarity between duplicated regions, they used a support vector machine to classify matched points. The main advantage of this method is its ability to reach a WLD descriptor with up to 91% accuracy using C_b component of the images. It is also robust to noise and illumination and has the capability of edge detection. Naked eyes are less sensitive to Hue component than brightness. Thus, even though forged images appear normal, several altered traces remain in hue channels.

v. PCA based methods

There are several factors affect to the computational time of block based methods such as number of blocks, sorting techniques and the number of extracted features. Some researchers try to reduce the size of extracted features using dimensionality reduction techniques such as Principal component analysis (PCA) techniques. PCA belongs to linear transform based on statistical techniques used in signal processing for the data dimension

reduction or for the data decorrelation. Some authors applied PCA that takes advantage of eigenvectors properties of divided block in the entire image for determination of duplicated regions forgery. For instance, (Popescu & Farid, 2004) employed a principle component analysis (PCA) on divided blocks in the image after resize it into small fixed size, to reduce the dimension of DCT blocks. Each block was reshaped as 16x16. The DCT coefficients in each block were saved in a matrix and the corresponding covariance matrix was computed. The eigenvectors of the covariance matrix are determined as features saved into feature vector. Finally, duplicated regions are exposed by lexicographically sorting features vector. Their method was robust to compression up to JPEG quality factor 50 and the time complexity of this method was improved to time O(32× k log k). (Zimba & Xingming, 2011) computed covariance matrix of each block .The eigen vectors and eigen values are determined as features to represent each block inserted into feature vectors and sorted lexicographically to detect copy moved regions.

vi. SVD based method

SVD is a method taking a high dimensional, highly variable set of data points and reducing it to a lower dimensional space that exposes the substructure of the original data more clearly and orders it from most variation to the least. Copy move forgery detection method takes an advantage of the SVD method applied to each block by following equation

$$A_{mn} = U_{mn} S_{mn} V_{mn} \qquad 2.4$$

Where A is an image matrix of size mxn can be broken down into the product of three matrices - an orthogonal matrix U, a diagonal matrix S, and the transpose of an orthogonal matrix V. Then, U and V values are reshaped into n-dimensional feature vectors u and v as $u = (U_1, U_2, .., U_n)$, $v = (V_1, V_2, ..., Vn)$ .The Euclidean distance between these vectors is determined to localize duplicated regions. The method is robust to JPEG compression up to the quality level 90 , Gaussian blur filter with radius 0.3 pixels, and Gaussian white noise contamination SNR=38, respectively.

(C.-C. Chang et al., 2007) applied The singular value decomposition (SVD) on divided blocks of low frequency sub bands LL1 at scale 1. S and V values are reshaped into feature vectors. The SV features vector was lexicographically ordered to search matched regions. The method is robust to JPEG compression up to JPEG quality factor 70 and additive noise.

vii. Moments based methods

Mahdian *et al.* proposed a direct approach to detect blurred duplicated regions (Mahdian & Saic, 2007). Specifically, they proposed a CMFD method based on the central moments of an image up to the seventh order. A color image was divided into overlapping blocks. Twenty-four blur-invariant moments were extracted from each block for each red–green–blue (RGB) color channel. Therefore, the feature vector of length 72 was reduced as per PCA. Finally, a k-dimensional tree was used as a nearest neighbor searching algorithm to locate matched block pairs. This method

was proved to be robust not only against blur, but also against lossy JPEG compression and noise addition in the forged region.

Tao *et al.* (T. Wang et al., 2013) detected blurred duplicate regions by using combined blur-affine moment invariants to extract features from image blocks. Block pairs were matched according to correlation coefficients and relative error was utilized as a measure of the stability of invariant features distorted by blurs.

In (S-J Ryu et al., 2013), the Zernike moments are extracted from overlapping blocks and their magnitudes are used as feature representation. Locality sensitive hashing (LSH) is employed for block matching, and falsely matched block pairs are removed by inspecting phase differences of corresponding Zernike moments. These features are robust to rotation attack, JPEG compression and additive white Gaussian noise.

(G. Sheng et al., 2012) divided image into overlapping sub blocks. The ridegelet transform for each sub block is performed and HU moments obtained to represent each block. HU features are saved into feature vectors. The search of similar features is done using Euclidean distance. These moments, like the Hu moments and the circularly orthogonal invariant moments, such as the Zernike moments (ZMs), pseudo-Zernike moments possess the property of being invariant to rotation and can be made invariant to translation and scale after geometric transformations.

viii. **Polar mapping methods**

Feature extraction is a prerequisite step for CMFD and crucial to detection accuracy. It is desired that the regions in a copy-move pair can be mapped to similar features even in the presence of post processing such as rotation. At the same time, the features should correctly distinguish distinct regions in the image. To accomplish these goals, the polar mapping is used to generate rotation-invariant and orthogonal features for CMFD. (Bayram et al., 2009) applied radial projection on the log-polar coordinate Fourier transformation of image blocks to build 1 D descriptor contains 45 features under different orientations range from 0 -180^0. Then, save these feature descriptors into Matrix and applied lexicographical sorting. To improve the detection decision he used counting bloom filter to hash these descriptors in which the matched descriptors have the same hashing value. Finally, they calculated the Euclidean distance between the two blocks that are detected to be the duplicated pairs.

(Wu et al., 2011) computed log-polar fast Fourier transform (LPFFT) on image blocks to produce a rotation invariant features. These features are save into feature vectors. The similarity of features can be measured with the normalized cross power spectrum of feature vectors. The main advantage of the proposed method is that the log-polar fast Fourier transform can produce high detection rate with much lower computation complexity than the FMT and ZM based approach as shown in Table 2.2. And also works well with images that have rich contents such as objects.

Table 2.2: Performance analysis of different rotation invariant block based features.

	FMT	LPFFT	ZM
Complexity	$O(N^4)$	$O(n^2 \log n)$	$O(m_{moments})+O(n\times m_{moments}\times L2)+$ $O(m_{moments}\times n\times \log n)$.
Rotation invariance	Yes, less than 10^0	Yes,5^0,45^0,90^0	Yes, 0^0 to 90^0
Scale invariance	Yes	Yes	No
Features length	45	NA	12

Another method to detect region duplication forgery under rotation attacks is employed such as polar harmonic transform. (L. Li et al., 2013) proposed a method to detect the forged regions based on circle blocking of low pass filtered image region. And they extracted features from these blocks using polar sine transform (PST) to build 9 dimensional feature vectors. The block matching was done by estimating the Euclidean distance of the lexicographical sorted feature vectors. Finally morphological processing is employed to obtain the final detection map, where the order of PST is 3 and the similarity threshold=2.1.The proposed method is rotation invariant under 15^0, 30^0 and 90^0 degrees.

(Y. Li, 2012) proposed copy move forgery detection algorithm based on orthogonal polar cosine transform (PCT) of image blocks which has rotational invariant property and more efficient than ZMs in computational complexity. The color image tilled into square blocks and applied PCT to extract PCT coefficients. And saved into feature vectors. They applied local sensitive hashing (LSH) to hash features and to perform a probabilistic dimensionality reduction of features which map similar features to the same bucket with high probability to maximize the portability of collision rather than avoid collision of similar items. To decrease the false matching, the similar features with low variance are discarded. This

technique is different from other block based techniques where the hashing method LSH is employed as an alternative approach to lexicographical sorting. As shown in Table 2.3, the LSH method to find similar regions shows significant detection rate over the lexicographical sorting method, since the approximate nearest neighbors of LSH make it more robust against post processing operations such as additive Gaussian noise. For instance, when the duplicated regions are post processed by the Gaussian noise with variance 10^{-3}, 93% of the duplicated region pairs have been correctly identified by the LSH approach, while the percentage corresponding to lexicographical sorting is 4%.

Table 2.3: Percentages of the region duplication pairs detected by different approaches.

	Variance of Gaussian noise			
	0.001	**0.003**	**0.005**	**0.007**
LSH	93%	86%	78%	70%
Lexicographical sort	4%	2%	1%	1%

ix. Texture based methods

The aim of copy move forgery is to add or hide an object by duplicating regions. Since duplicated regions came from the same image, these regions have the similar intrinsic properties such as texture. A forgery can apply the geometric transformation to the copied region with additive noise or recompress the forged image. But still the textures of duplicated regions are quite similar. Some researchers have focused on texture analysis for detecting copy move forgery (Ardizzone et al., 2010; Davarzani et al., 2013; Gharibi et al., 2011; Hsu & Wang, 2012; Quan & Zhang, 2012).

(Quan & Zhang, 2012) proposed region duplication forgery detection method based on image blocks with similar textures. Their algorithm first applies local dimension estimation for divided blocks in the image using KNN algorithm and saved into feature vector. Then segment the image based on local dimension estimator into different regions. Finally, similar blocks are connected with each other to produce the duplicated regions using morphological operations. the method is robust JPEG compression, additive white Gaussian noise (AWGN) and blurring.

In (Davarzani et al., 2013), the image is divided into blocks and each block is first filtered with an edge-preserving adaptive low-pass filter. for instance, the Wiener filter. Then, the multiresolution local binary patterns (MLBP) have been extracted from each block by combining the features from multiple local binary pattern (LBP) operators on the blocks. Their method is robust to JPEG compression, white Gaussian noise addition scaling, rotation and Gaussian blurring.

In the recent years, another type of block based methods (Mahdian & Saic, 2009; N. Muhammad et al., 2011) have been proposed which partitioned the image into segments based on homogeneity condition. As a result, a single segment fully contains an object, and the segment is relatively homogeneous as shown in Figure 2.12. The noise estimation is performed for each segment. Finally, histograms of the extracted noise segments are compared for matching similarities (Mahdian & Saic, 2009; N. Muhammad et al., 2011).

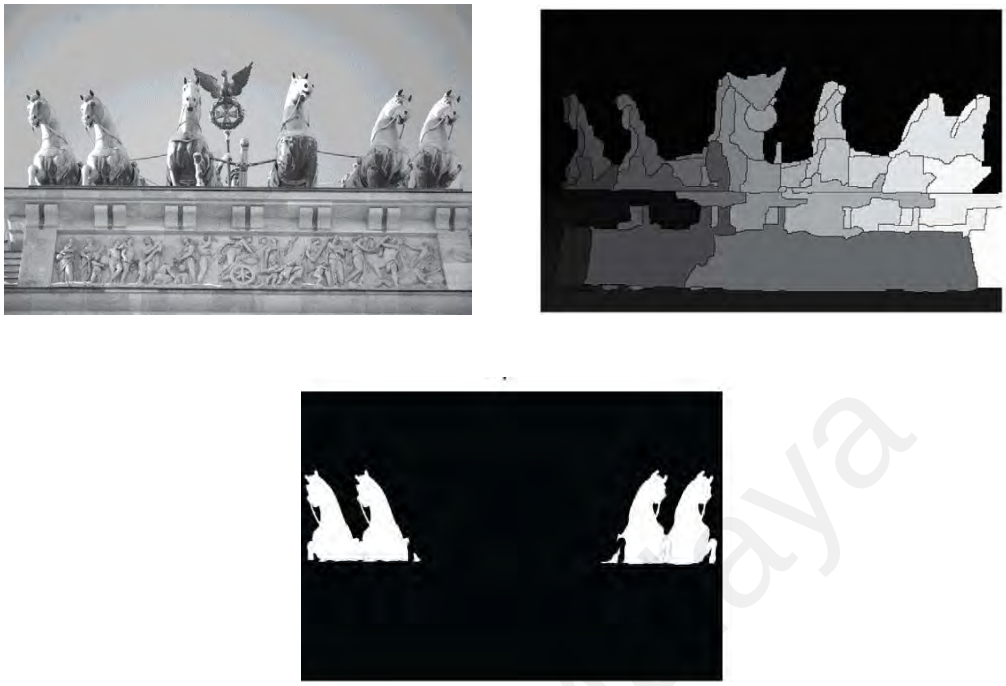


Figure 2.12: Shows (a) forged image, (b) segmented image and (c) the detection results of block based detection method.

2.4.2 key point based methods

The keypoint based methods depend on the extraction of local interest points (keypoints) from local interest regions with high entropy, without any image sub-blocking. Good keypoints should be efficient to compute, identify distinct locations in the image regions, and robust to geometric transformations, illumination changes, noise and other distortions (Mokhtarian & Suomela, 1998). The main advantage of keypoint based methods is that they give high detection rate in duplicated regions, which exhibit a rich structure such as objects. but still struggle to reduce the false matches in the flat regions in the image which do not contain any primitives like edges and corners, mostly

contains much less detail to represent textured regions in the image for example: Sky and Ocean etc.

In general, the performance of keypoint based CMFD algorithm depends on the first step of this algorithm called local interest point detection. Two good surveys explore the general performance of local interest point detection algorithms against affine transformations (Mikolajczyk et al., 2005), (J. Li & Allinson, 2008). Recently, significant research has been performed on extracting keypoints with application to CMFD (Christlein et al., 2012), (Pan & Lyu, 2010), (Amerini et al., 2011), (L. Chen et al., 2013).

These keypoints are detected from an image by using scale invariant feature transform (SIFT) (Amerini et al., 2011; Pan & Lyu, 2010), the speeded-up robust feature (SURF) (Bo et al., 2010; Mokhtarian & Suomela, 1998; Pandey et al., 2015), Harris (L. Chen et al., 2013) and Hessian (Leutenegger et al., 2011; Ling et al., 2011). The general framework of forgery detection in keypoint based methods is shown in Figure 2.13.

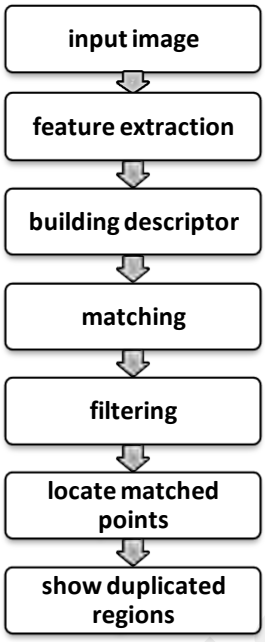


Figure 2.13: The general framework of copy move forgery detection in key point based.

The procedure of keypoint based approach differs from block based approach. According to processing steps in Table 2.4, we can provide the characteristics of each approach.

Table 2.4: Comparison Table between block based and keypoint based method based on their processing steps.

Characteristics	Block based approach	Keypoint based approach
Block tilling	Subdivide image into blocks	Without image subdivision
Type of region	Uniform regions	Non uniform region
Feature extraction	Compute feature vector from block	Compute feature vector from image region on high entropy
Descriptor size	Memory requirement more	Memory requirement less
Dimensionality reduction	Mandatory	Optional

Show matching	Morphological operations	Line linker between matching pairs in region
	Limit consideration to:	
Robustness to geometric transformations	-Rotation invariant: less than 10^0 -Scale: not scale invariant	-Rotation invariant -Scale invariant
Robustness to post processing operations	JPEG, additive noise, blurring and illumination	JPEG, additive noise and partially to illumination and blurring.

1. **SIFT based method**

Huang, Guo et al. proposed a SIFT based detection method to identify duplicate region with scale and rotation, then used the best bin first search (BBF) method to find the nearest neighbors with high probability which returns the matched key points (inliers) as a possible duplicate region. To increase the accuracy of detection method, nearest neighbor distance ratio (NNDR) is applied for matched keypoints (H. Huang et al., 2008).

In (Pan & Lyu, 2010) the duplicated regions in the forged image are identified by finding the matching key points based on SIFT algorithm. Random sample consensus algorithm (RANSAC) is employed to search the inliers in the duplicated region. The proposed method avoided searching from close adjacency between duplicated regions by searching far from 11 × 11 square block whose center is at the detected keypoint in the image.

(Amerini et al., 2011) detected multiple duplicated regions based on SIFT features, then employed generalized nearest neighbor (G2NN) to improve the similarity match between key points. The agglomerative hierarchical linkage (AHL) clustering method has been employed to group the similar keypoints into the same cluster and merge closest pair of clusters into single cluster to represent the cloned regions. The estimation of affine transformation parameters is computed between duplicated regions.

(Battiato et al., 2012) proposed a framework for detection of duplicated region based on SIFT. Hashing method is applied to the feature vectors, and then saved into hash table which used for comparing the hash code of corresponding feature vectors after image alignment. The alignment process of the hash is used to estimate the geometric transformation parameters.

In (Christlein et al., 2010) , the rotation and scaling parameters have been estimated from a few blocks of duplicated regions, and expressed by affine transformation matrix. Recently, In (Jian et al., 2015) the image is segmented into different regions. SIFT features are extracted to find the matched keypoints in the first stage. The transform matrix between duplicated regions is estimated based on expectation maximization (EM) algorithm. EM is an iterative method for finding the maximum log likelihood between duplicated regions. Then repeat these steps again to find other matched pairs. The method is robust to different attacks as shown in Table 2.5

Table 2.5: Setting of attacks.

Attacks	Parameters
Additive noise	Deviation (20:20:100)
JPEG	Quality factor(20:10:100)
Rotation	Angle(2^0:2^0:10^0)
Scale	Sacle ratio(0.9:0.02:1.09)

All above techniques share in common the use of the SIFT keypoint detection. Hence, they commonly inherit the limitations of lacking keypoints in flat/smooth areas where little structure is exhibited. This led researchers to utilize other keypoints detectors to overcome these limitations. Other techniques are proposed to detect the region duplication forgery in the image by using other keypoints detectors such as Harris corners, SURF, Hessian and Laplacian of Gaussians (LOG) detector.

2. **SURF based method**

It is a keypoint-based method that is used to extract features in copy-move forgery detection methods much faster than SIFT. (Bo et al., 2010) presented a copy move forgery detection method based on SURF features and KD tree method to find forged duplicated regions. The integral image is employed in SURF to reduce the size of feature vector into 64 feature length. The procedure improves the time complexity of detection method.

(Mishra et al., 2013) presented a copy move detection method based on SURF keypoints and hierarchical agglomerative clustering (HAC). Euclidean distance is

calculated between pairs of SURF keypoints in the image. And hierarchical clustering is applied on basis of distance to improve the time complexity of detection method compared with SIFT based method as shown in Table 2.6.

Table 2.6: TPR, FPR values (%) and processing time (average per image) for each method

Method	FPR%	TPR%	Time
(Fridrich et al., 2003)	84	89	294.96
DCT(Popescu & Farid, 2004)	86	87	70.97
SIFT(Amerini et al., 2011)	8	100	4.94
SURF(Mishra et al., 2013)	3.64	73.64	2.85

The proposed method is immune to various transformations like rotation, scaling and illumination with gamma values [1.2:1.8] as shown in Figure 2.14.

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

Figure 2.14: Copy move detection results for: (a) gamma value = 1.2, (b) gamma value = 1.4, (c) gamma value = 1.6, and (d) gamma value = 1.8.

3. Harris based method

In (Kakar & Sudha, 2012), local interest points were detected through the modified scale Laplacian of Gaussian. A Harris corner detector renders features invariant to geometric transformations. The feature descriptor was built using MPEG-7 signature tools to detect duplicated regions under copy move forgery. The global trace transform

method is used to extract a binary “feature signature “from circular regions centered at Harris feature points. Finally, the Euclidean distance was used to find true matches between feature descriptors of duplicated regions. Best bin first search is employed to improve the detection rate. The performance of proposed algorithm was tested on MICC F220 database (Amerini et al., 2011) and Kodak database(Franzen, 1999).

(L. Chen et al., 2013) Proposed duplicate region detection algorithm based on local interest points in the image which detected by Harris corner detector and apply circular region around each interest points. Then, they divided the circular region into 36 sector extracted as features and calculate the mean and standard deviation for each sector to build a 72 dimensional feature descriptor. Euclidean distance matches done between feature vector elements. Their method is robust to rotation and scale attacks under copy move forgery. The results indicate that the proposed method detects copy-move forgery efficiently. The Figure 2.15 , shows high resolution tampered images in top row, the Harris keypoints extracted for the tampered image in the middle row and the detection results in bottom row.

Figure 2.15: Illustrates the detection results of Harris based detection method. From left to right: Acropolis (large copied region), Beachwood (large copied region) and Building (small region with two forged area).

4. Hessian based method

(Leutenegger et al., 2011) proposed novel method for region matching based key points detection like fast hessian detector and build the BRISK descriptor which relies on relatively small number of intensity difference tests to encode an image patch as a binary string to produce 512 dimensional descriptor, That makes the descriptor much faster than surf and sift and invariant to illumination variations. Finally, they used Hamming distance as the metric for matching.

(S. D. Lin & Wu, 2011) proposed a forgery detection technique based on Hessian features and DCT to located copy move regions. the image is converted from RGB to YC_bC_r. Only Y channel is investigated in the image. Hessian matrix approximation is used to extract Hessian interest points in the image. DCT is employed for each keypoint

and save the low frequency DCT coefficients into feature vector. The DCT coefficients of all blocks around keypoints are presented by histogram to locate the forged regions. The main advantage of this method is that can detect multiple copy move regions with detection time 235.4 seconds in image of size 2272×1704 as shown in Figure 2.16.

a) Original image b) Tampered image c) Detection results

Figure 2.16: The detection results of the multiple forged regions on copy-move forgery images

2.5 An overview of region duplication detection under copy move forgery

Many methods have been proposed over the past years for exposing image forgeries by detecting cloned regions based on content similarity. Region duplication forgery detection is still a challenging problem because of illumination inconsistencies, scaling and rotations of cloned regions. However, duplicated regions are not necessarily identical, because they may altered by some post processing operations such as illumination changes and blurring to make the forgery undetectable in such a way that our naked eyes are unable to detect any irregularity caused by the forgery. The existing Region duplication forgery detection methods are based on the fact that, the suspected image will have relatively similar cloned regions since these regions come from the same image. And they have the same lighting condition, noise components, texture, color patterns, homogeneity condition and internal

structure (Mahdian & Saic, 2009; G. Muhammad et al., 2012; N. Muhammad et al., 2011). Some additional Geometric transformations and post processing operations are often applied either on the cloned region before moving it or on the whole tampered image, in order to hide the traces of forgery. Among them, we found scaling (Amerini et al., 2011; Pan & Lyu, 2010), rotation (L. Chen et al., 2013; Liu et al., 2011), translation(Bayram et al., 2008b), flipping (Guo & Cao, 2010), lossy compression(B. Li et al., 2011; Y. Sheng et al., 2013), noise addition(Cao et al., 2012; Fridrich et al., 2003), blurring on edge regions (Liu et al., 2013; J. Wang et al., 2010; L. Zheng et al., 2012; Zhou et al., 2007) or the whole forged region (Mahdian & Saic, 2007; T. Wang et al., 2013) and illumination (Davarzani et al., 2013; de Carvalho et al., 2013; Fan et al., 2012; Z. Wang et al., 2011) changes as shown in Figure 2.17. A key issue of successful detection of copy move forgery lies in the design of robust image region descriptors that are invariant to theses post processing operations (L. Zheng et al., 2012).

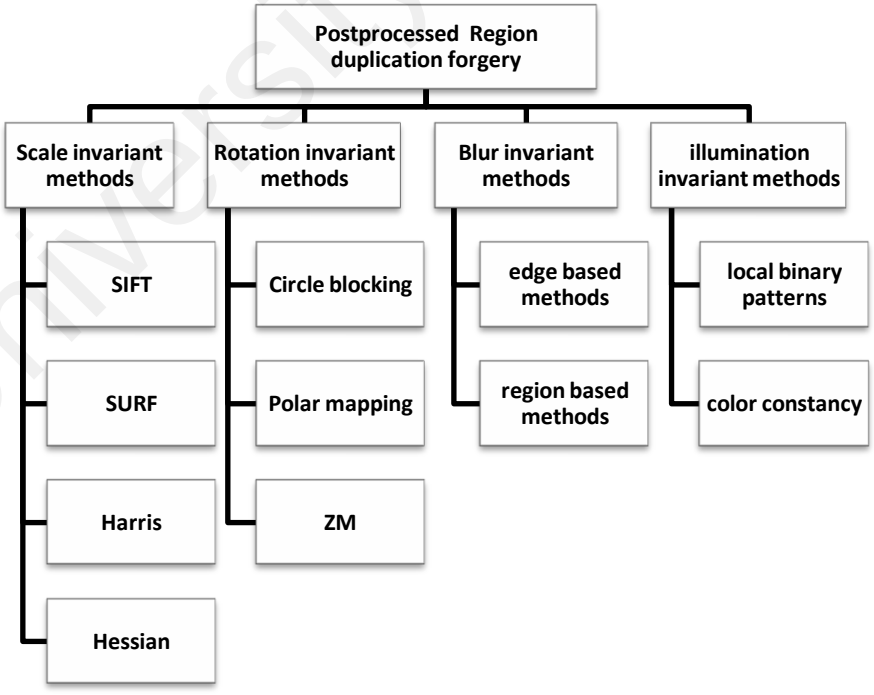


Figure 2.17: Taxonomy of post processed region duplication forgery detection methods under various types of attacks.

However, these methods are not perfect and have some weakness should be eliminated to acquire efficiency and robustness in their detection results. Different methods have been evaluated with various detection algorithms based on two main criteria: keypoint-based and block based method. Each of these categories has its own advantages and drawbacks.

Common limitations of block-based method contain:

1) Direct using of Frquency; quantized or intensity based features from divided blocks for matching.

2) The block tilling step makes the size of features vector is quite high, which force the researchers to employ the dimension reduction step to reduce the time complexity of detection method. For instance, the computational complexity in the first block based method (Fridrich et al., 2003) was $O(MN^2)$. The issue of high computational complexity of their method, has been improved by authors in (G. Li et al., 2007; H.-J. Lin et al., 2009; W. Luo et al., 2006; Popescu & Farid, 2004).

(Popescu & Farid, 2004) employed a principal component analysis (PCA) on divided image blocks as a dimensionality reduction representation. Then lexicographical sorting algorithm is applied on extracted features to locate duplicated region. The time complexity of sorting algorithm was reduced to $O(32\times (\sqrt{MN}-B+1)^2 \log(\sqrt{MN}-B+1)^2)$. The time complexity for sorting was reduced by G. Li et al. (G. Li et al., 2007) to $O(8\times(\sqrt{MN}-B+1)^2 \log(\sqrt{MN}-B+1)^2))$ by the use of singular value decomposition (SVD). Lin, Wang et al. improved the time complexity of detection method to $O(9 \times (\sqrt{MN}-B+1)^2)$. The radix sort is applied for sorting the 9 dimension feature vectors of the divided sub-blocks. As an alternative to lexicographic sorting, which is commonly used by the existing copy-move

forgery detection schemes(H.-J. Lin et al., 2009). Another improvements in have been made by reducing the size feature vector (Cao et al., 2012) as shown in Table 2.7.

Table 2.7: computational complexity comparison.

Method	Feature extraction	Feature dimension
(Fridrich et al., 2003)	DCT	64
(Popescu & Farid, 2004)	PCA	32
(B. Li et al., 2011)	Improved DCT	16
(Cao et al., 2012)	Block representation	4

Detection time for a 256 x 256 color image was improved in (Kang & Wei, 2008) when compared with the proposed method in (Mahdian & Saic, 2007). However, the computational time remained high compared to other methods. Their method improved forgery detection in case of forgery with uniform areas, such as when the sky or ocean is manipulated. The computational complexity is also lower and noise robustness is increased compared to ;(Fridrich et al., 2003; W. Luo et al., 2006; Mahdian & Saic, 2007; Popescu & Farid, 2004). In (Mahdian & Saic, 2007), the detection time is high because lexicographical sorting has been used for sorting Singular Values Feature Vectors. While their detection time was 40 min per image for detecting blurred regions, (Kang & Wei, 2008) reduced the detection time into 120 seconds for the same test images.

3) The detection procedure rarely considers geometric transformation operations such as scaling and rotation. Rotation attack is considered as the most difficult geometric transformation to deal with copy move tampering. Three key approaches were introduced to achieve a rotation invariant CMFD; polar mapping (Bayram et al., 2009; Bravo-Solorio

& Nandi, 2009; L. Li et al., 2013; Y. Li, 2012), circle blocking (Liu et al., 2011; Shao et al., 2012) and image moments such as Zernike moments (Zm) (S-J Ryu et al., 2013; Seung-Jin Ryu et al., 2010).Unfortunately, these methods still partially invariant to rotation attacks. Thus, the block based method can detect flat regions that contain less detail to represent texture in the image. Forgers usually used these uniform regions for better hiding forgery.

To overcome these issues in block based method, an alternative approach used for copy move tampering detection, which is the keypoint based method. Keypoint based techniques perform well in terms of memory utilization and computation time. Although the feature size and the number of extracted keypoints is large, they are less than the number of image blocks used in block based methods. Thus, the detection procedure is very lightweight. Keypoint based method deals with non uniform regions such as objects that have texture primitives like corners, edges and lines. Where forgers often use this type of region to apply region duplication forgery in the image. In terms of speed and robustness to large amounts of rotation and scaling methods: SIFT, SURF, Harris and Hessian methods are remarkable and are better techniques for forgery detection, but they may fail to detect very small tampered regions and cannot overcome blur retouching and illumination variations.

Some of region duplication forgery detection schemes are reviewed in Tables 2.8. Several aspects of the detection schemes such as robustness and detection rate are investigated. The robustness of the existing methods in Tables 2.8 were determined based on the following geometric transformations and post processing operations:

i. Robustness to rotation attack (R).

ii. Robustness to scale attack (S).

iii. Robustness to JPEG Compression attack.

iv. Robustness to additive noise attack.

v. Robustness to blurring (B).

vi. Robustness to illumination (I).

Table 2.8: A comparison between reviewed region duplication detection methods.

Literature	Feature extraction	Robustness						Detection rate (%)
		R	S	JPEG	Noise	B	I	
Block based methods								
(Fridrich et al., 2003)	DCT	×	×	✓	✓	×	×	89
(Popescu & Farid, 2004)	Intensity+PCA	×	×	✓	✓	×	×	87
(Cao et al., 2012)	DCT	×	×	✓	✓	×	×	90
(B. Li et al., 2011)	DCT	×	×	✓	✓	×	×	99.8
(Mahdian & Saic, 2009)	DWT	×	×	✓	✓	×	×	NA
(G. Muhammad et al., 2012)	DYWT	×	×	✓	✓	×	×	95.9
(Zimba & Xingming, 2011)	DWT+PCA	×	×	✓	✓	×	×	98
(Bayram et al., 2009)	FMT	✓	×	✓	✓	×	×	90.75
(Kang & Wei, 2008)	SVD	×	×	✓	✓	×	×	NA
(Y. Li, 2012)	PCT	✓	×	✓	✓	×	×	98
(Mahdian & Saic, 2007)	Blur moments	×	×	✓	✓	✓	×	NA
(S-J Ryu et al., 2013)	ZM	✓	✓	✓	✓	✓	×	99.4
(N. Muhammad et al., 2011)	noise estimation	×	×	✓	✓	×	×	98

(Davarzani et al., 2013)	MLBP	✓	✓	✓	✓	✓	×	90.9
Key point methods								
(Amerini et al., 2011)	SIFT	✓	✓	✓	✓	×	×	100
(Pan & Lyu, 2010)	SIFT	✓	✓	✓	✓	×	×	94.6
(Pandey et al., 2015)	SURF	✓	✓	✓	✓	×	×	NA
(Mishra et al., 2013)	SURF+HAC	✓	✓	✓	✓	×	✓	73.64
(Kakar & Sudha, 2012)	LOG+MPEG7	✓	✓	✓	✓	✓	✓	90
(L. Chen et al., 2013)	Harris	✓	✓	✓	✓	×	×	92.15
(S. D. Lin & Wu, 2011)	Hessian	✓	✓	✓	✓	×	×	NA
(Jian et al., 2015)	SIFT+EM	✓	✓	✓	✓	×	×	86

2.6 Summary

Throughout this chapter, state-of-the-art region duplication forgery detection schemes are presented. In this chapter, a comprehensive research into existing forgery detection schemes is discussed. Moreover, different aspects of the existing algorithms, such as detection rate, robustness and detection time, are investigated. Tables 2.8 shows a comprehensive study of several region duplication detection methods. Finally, several current issues, such as type of detected regions, feature extraction and detection rate, along with the robustness of existing methods, have been identified. As a result, we found that keypoint based methods are more robust than block based methods in case of detecting copy move forgery under geometric transformations and post processing operations. Keypoint based methods rely on extracting local interest points that help to represent the internal structure of duplicated regions in the image. We need to find

similarity between duplicated regions based on their internal structure to achieve the aim of detection method discussed in chapter 3. Thus, we can take the advantage of the segmentation method to detect small flat regions which are hard to detect by keypoints method. We propose a novel method that employs image segmentation techniques and accurate match using the keypoint based method to detect copied and moved regions introduced in Chapter 5.

CHAPTER THREE

LOCAL INTEREST POINTS

3.1 Introduction

The main aim of this chapter is to provide a detailed description of local interest points that are invariant to geometric transformations such as scale and rotation. These points are used as features to represent the internal structure of non uniform regions in an image such as corners, blobs and edges that have been applied in image matching. Interest points simply can be defined as image pixels that are unique when compared with surrounding pixels. These features are widely used in modern computer vision applications. Traditionally, extracting interest points from the image can be done by detector. The main goal of detector is to localize ideal points features in the image that are more rotational and scale invariant are described in Section 3.2.

3.2 Interest point detectors

Is responsible to find locations in the image where we can reliably search correspondences with other images for matching. For instance, good features to track which their detector response insensitive to image geometric transformations. Good features should have the underlying characteristics:

i) **Repeatability**: Given two images I_1 and I_2 of the same scene, taken under different Geometric transformations: scales or rotation angles, the total number of detected interest points in I_1 should be repeated in the transformed image I_1.

ii) **Distinctiveness**: the local interest points should give a clear variation of their intensity patterns, such that features can be matched.

iii) **Quantity**: The total number of detected points in the image should be sufficiently large, such that a reasonable number of interest points are localized on small regions or objects to represent their ideal internal structure.

iv) **Accuracy**: The detected features should be accurately localized, both in image spatial coordinates.

v) **Efficiency**: local interest points in the image should be detected in a reasonable time.

vi) Invariance: the detector should extract interest points under geometric transformations including translation, rotation and scale operations.

There are four major feature detectors have been used to detect local interest points described in the following:

1. **Scale invariant feature transform (SIFT)**

   SIFT is an approach of extracting keypoint features from the image used for object recognition. It is regarded as one of the most successful algorithms in recent years for keypoint detection due to strong matching ability and stability in noise, rotation and variety of different scales. It proposed by (Lowe, 2004). The main concept of this algorithm is the scale space representation for detecting keypoints (Koenderink, 1984; Lindeberg, 1994).

   SIFT consists of four major steps for feature extraction, which are: (a) scale-space extreme detection, (b) key point localization, (c) orientation assignment and (d) key point descriptor generation. The explanation of each step is introduced as follows

   a) **Scale space extreme detection**

      The first step of SIFT searches for extreme over all scales in the image. Given an input image I (x, y), then scale space of an image is computed (Lowe, 2004) as follows

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y, \sigma) \quad 3.1$$

Where $G(x, y, \sigma) = \frac{1}{2\pi\sigma^2} e^{\frac{x^2+y^2}{\sigma^2}}$ is a Gaussian kernel which is convolved with input image $I(x, y)$ in x and y at a scale factor σ in scale space. In order to detect a robust interest points that are invariant to scale and rotation, the scale-space extrema is defined by the difference of Gaussian (DoG) operator convolved with the image, $D(x, y, \sigma)$, which can be computed from the difference of two nearby scales separated by a constant multiplicative scale factor k:

$$\begin{aligned} D(x, y, \sigma) &= (G(x, y, k\sigma) - G(x, y, \sigma)) * I(x, y) \\ &= L(x, y, k\sigma) - L(x, y, \sigma) \end{aligned} \quad 3.2$$

As shown in Figure 3.1, for each octave of scale space, the input image is convolved repeatedly with a Gaussian filter to construct sets of scale space images. Adjacent Filtered images are subtracted to obtain DOG images. After each octave, the Gaussian image is down sampled. Then local interest key points are determined as local maxima of the DoG images across various scales. This can be made by comparing each pixel (marked with x) in the DoG images to its eight neighbors (marked with a circle) at the current scale and nine corresponding neighboring pixels in each of the neighboring scales. If the pixel value is larger than all of these neighbors, it is selected as a local interest key point shown in Figure 3.2.

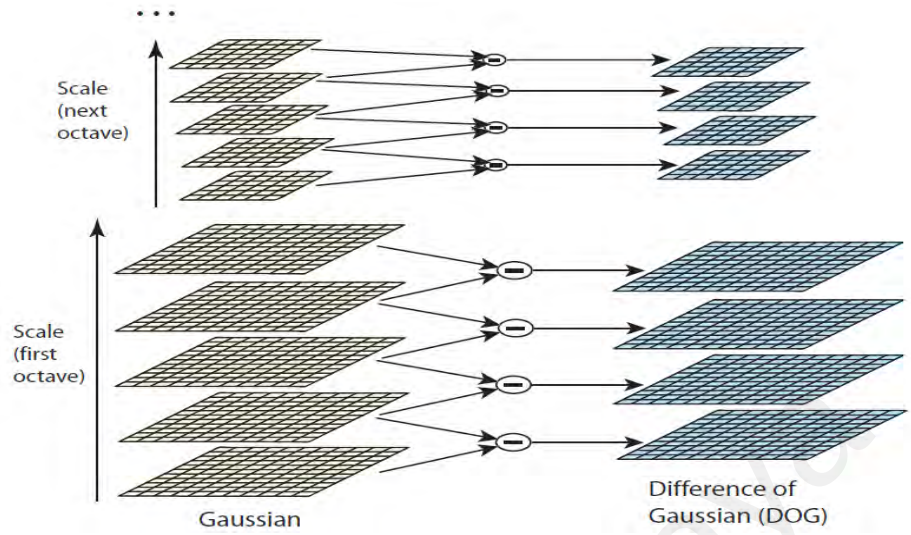


Figure 3.1: Constructing Difference of Gaussian in the scale space.

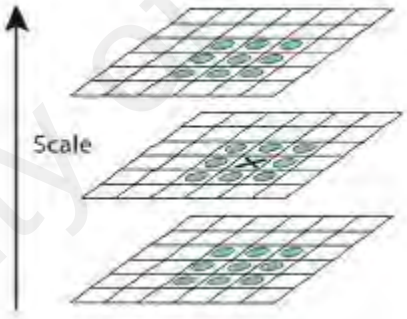


Figure 3.2: Local maxima point of Difference of Gaussian detected by comparing.

b) Keypoint localization

Too many keypoint candidates are detected in the scale space extrema. Some of them are unstable. In this stage, keypoints are filtered and identified to select stable ones by performing a detailed fit to the closest data for accurate location,

scale and ratio of principal curvatures. This information helps to discard key points that have low contrast and are weakly identified along an edge.

c) Orientation assignment

In the previous stage useful key points are determined and best key points are selected that are scaled invariance. Moreover, to achieve the rotation invariance, each selected key point is assigned one or more orientation using image gradient directions.

The key point orientation is computed from an orientation histogram of local gradients from the nearest Gaussian filtered image $L(x, y,\sigma)$. Given image $L(x, y)$ at the key point's scale σ, the gradient magnitude $m(x, y)$ and orientation $\theta(x, y)$ are calculated as follows:

$$m(x,y)=\sqrt{(L(x+1,y,\sigma)-L(x-1,y,\sigma))^2+(L(x,y+1,\sigma)-L(x,y-1,\sigma))^2}. \quad 3.3$$

$$\theta(x,y)=\arctan((L(x,y+1,\sigma)-L(x,y-1,\sigma))/(L(x+1,y,\sigma)-L(x-1,y,\sigma))) \quad 3.4$$

An orientation histogram is constructed with 36 bins, each bin covering 10 degrees, is formed from the gradient orientations of sample points within a region around the keypoint. Then the maximum orientation is assigned to this keypoint.

d) Keypoint descriptor

For each keypoint, the feature descriptor is constructed as a set of orientation histograms of 4 x 4 pixel neighborhoods. The orientation histograms are relative to the key point orientation and the orientation data comes from the Gaussian image closest in scale to the keypoint's scale. Histograms contain 8 bins each, and each descriptor contains a 4x4 array of 16 histograms around the keypoint.

This leads to a SIFT feature vector with (4 x 4 x 8 =) 128 length as shown in Figure 3.3.

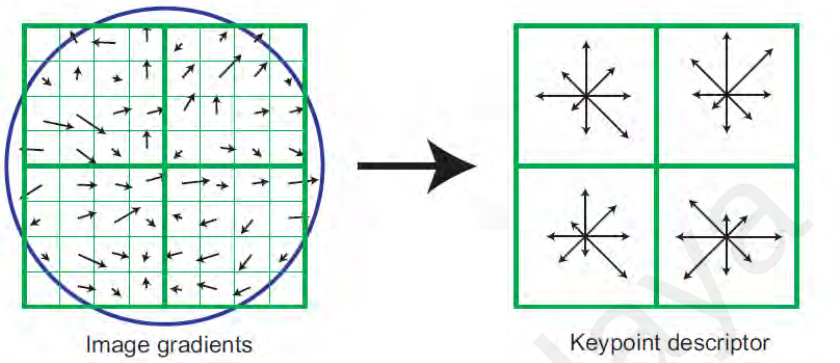


Figure 3.3: Generating SIFT keypoint descriptors.

2. Speed up robust feature (SURF)

SURF is an approach lies in its fast computation of approximate differential operators in the scale space based on integral image representation and box filters. It has been proposed by (Bay et al., 2006). In contrast to SIFT method, which approximates Laplacian of Gaussian (LOG) with difference of Gaussian (DOG), SURF approximates second order derivatives of Gaussian with box filters (See Figure 3.4). SURF keypoints are detected in the following steps:

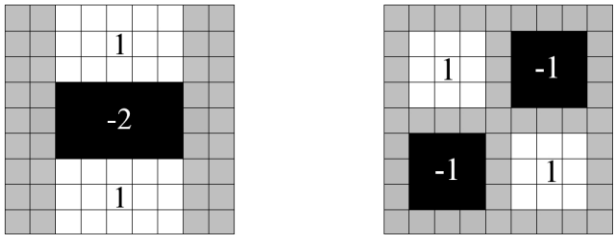


Figure 3.4: SURF's 9 x 9 box-filter approximation for the second order Gaussian partial derivative in y-direction and xy-direction. The gray regions are equal to zero.

1. **Computation of integral image**

The Integral image $I_{\sum}$ (x) at location x=(x, y) represents the sum of all pixels in the input image I of the rectangular region formed by origin and point x, described in Equation

$$I_{\sum}(x) = \sum_{i=0}^{i<=x} \sum_{j=0}^{j<=y} I(i,j) \qquad 3.5$$

Once, the integral image is computed, it takes four additions to compute the sum of all intensities on rectangular region as shown in Figure 3.5.

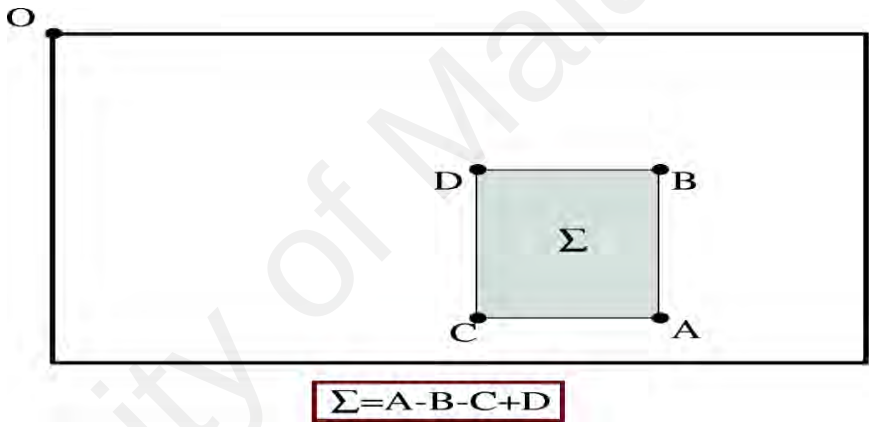


Figure 3.5: Integral image calculation by rectangular region of any size.

2. **Interest points detection**

In this step, the input image I with Laplacian of Gaussian, which is approximated by 9 x 9 box filters with $\sigma = 1.2$ for creating scale space. The location and scale of interest points are selected by computing the scale normalized determinant of Hessian Matrix. The determinant of the Hessian represents the blob response in the input image I at location x when it is positive. These responses were saved in a blob response map.

Finally, local maxima points are detected using a non maxima suppression algorithm. Hessian matrix is defined by

$$H(x,\sigma)=\begin{bmatrix} L_{xx}(x,\sigma) & L_{xy}(x,\sigma) \\ L_{xy}(x,\sigma) & L_{yy}(x,\sigma) \end{bmatrix} \quad 3.6$$

Where L_{xx}, L_{yy}, L_{xy} are second order derivatives of Laplacian of Gaussian. The determinant of Hessian can be calculated by

$$\det(H_{approx}) = L_{xx}L_{yy} - (0.9 * L_{xy})^2 \quad 3.7$$

3. Local descriptor generation

To build the descriptor around each detected keypoint, first select a square block around interest keypoint. This square region has been divided into 4 × 4 sub blocks. For each of these blocks, Haar wavelet response is computed. Here, d_x refers to horizontal response and d_y refers to a vertical response. For each of these sub regions, 4 responses are formulated in a vector as follows

$$v_{subregion} = \left[\sum d_x, \sum d_y, \sum |d_x|, \sum |d_y|\right] \quad 3.8$$

The SURF descriptor for all 4 by 4 sub-regions is 64 dimensional vector. SURF has been reported that is faster than SIFT method five times but less accurate.

3. Harris corner detector

Is a corner detector approach proposed by (Harris & Stephens, 1988), is based on second moment auto correlation matrix. This matrix describes the Gradient distribution of input image at point x, weighted by Gaussian G(x,σ) as following:

$$M = G(x,\sigma) * \begin{bmatrix} I_x^2(x,\sigma) & I_x I_y(x,\sigma) \\ I_x I_y(x,\sigma) & I_y^2(x,\sigma) \end{bmatrix} \quad 3.9$$

Where $I_x^2, I_y^2, I_x I_y$ are square derivatives of input image I. These derivatives are smoothed with Gaussian kernel of scale σ. While the eigenvalues of Matrix M represent the signal changes along both orthogonal directions, Harris have used the two eigenvalues to measure the cornerness in the image defined as

$$cornerness = Det(M) - \lambda_1 Trace(M)^2 \quad 3.10$$

Where Det (M) is the determinant $= I_x^2 I_y^2 - I_{xy}^2$ and Trace(M) $= I_x^2 + I_y^2$ is trace of auto correlation Matrix M. The typical value of λ_1 =[0.04-0.06]. The corners are located by computing the local maxima of cornerness measure as show in Figure 3.6.

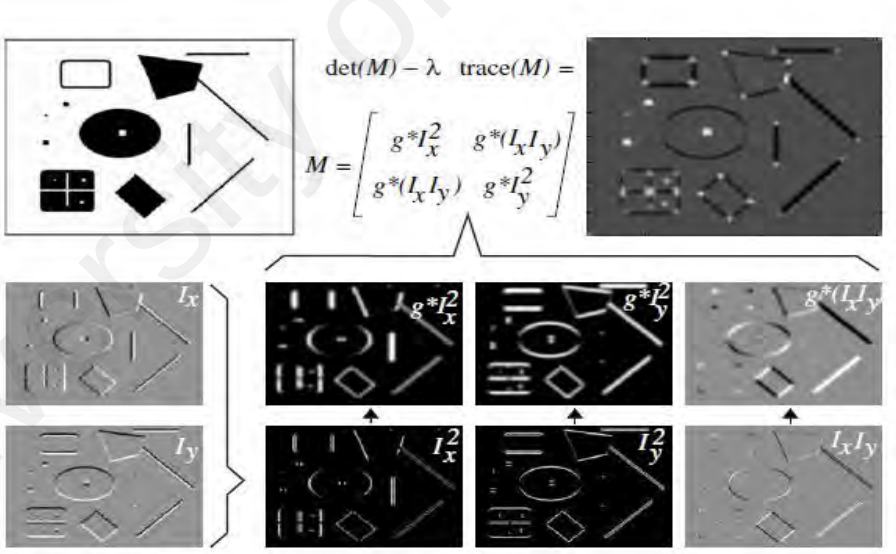


Figure 3.6: illustration of auto correlation matrix M and cornerness measure.

4. Hessian points detector

Is an intensity based detector proposed by (Beaudet, 1978), which is rotation invariant. It searches for interest points in image which exhibit strong derivatives in along both orthogonal directions. It is based on Hessian Matrix defined above in Equation 3.6. The Hessian detector calculates the second derivatives I_{xx},I_{yy} and I_{xy} for input image I. Then, find the points where the determinant and trace of Hessian become maximal. The trace and Determinant of Hessian can be defined as follows

$$Trace(H_{approx}) = L_{xx} + L_{yy} \quad 3.11$$

$$\det(H_{approx}) = L_{xx}L_{yy} - L_{xy}^{2} \quad 3.12$$

The search procedure applies non maximum suppression using 3 x 3 window, considering only points whose value is larger than its 8 neighbors. Inside the window. The detector gives good responses located on corners and strongly texture regions in the image (Mikolajczyk & Schmid, 2005).

3.3 Summary on local interest point detectors

An overview of the most characteristics for local interest point detectors is introduced in Table 3.1. These detectors are organized according to their invariance and localization ability. For rotation invariant properties, the highest accuracy of localization and repeatability has been prevailed by Harris corner detector. The hessian detector search blobs which are not well localized like Harris. Both of them are suitable for applications where such depend on the spatial location of features as object recognition and no large scaling are considered. As show in Table 3.1, SIFT (Scale Invariant Transformation Feature) can detect corners and Blobs. Moreover, it

is robust for matching features with regarding spatial localization and scale changes. SURF (Speed Up Robust Feature) detector was designed for efficiency to speed up detection time compared with SIFT.

Table 3.1: Overview of interest point detectors.

Detector	Corner	Blob	Rotation	Scale	Repeatability	Localization	Efficiency
SIFT	✓	✓	✓	✓	✦✦	✦✦	✦✦
SURF	✓	✓	✓	✓	✦✦	✦✦	✦✦✦
Harris	✓		✓		✦✦✦	✦✦✦	✦✦
Hessian		✓	✓		✦✦	✦✦	✦

CHAPTER FOUR

RESEARCH METHODOLOGY

4.1 Introduction

The research methodology in this chapter contains four main phases. Phase 1 presents the requirement and analysis, while the other three phases are the design and implementation of three proposed algorithms for detection copy move forgery. Each algorithm was implemented with the purpose of improving the tamper detection rate and robustness. The description of each phase is in the following subsections.

4.2 Research phases

As illustrated in Figure 4.1, the design and implementation phase consists of three approaches. The first proposed algorithm consists of an efficient copy-move forgery detection method. This keypoint based algorithm has the capability to authenticate and locate region duplication forgery accurately under rotation attacks. The details of the proposed algorithm are discussed in the implementation and design chapter. The proposed copy-move forgery detection algorithm is keypoint based algorithm which is designed based on Harris and angular radial partition.

In the implementation of the second approach, we therefore proposed a forensic algorithm to recognize the blurred duplicate regions in a synthesized forged image efficiently, especially when the forged region in the images is small. The method is based on blur metric evaluation (BME) and phase congruency (PCy).

In the third approach, a detection method is proposed to reveal the forgery under illumination variations. The proposed method consists of four steps: object detection based on normalized cut segmentation (Ncut), detection of hessian interest points in illuminated

objects, extracting illumination invariant features using Center symmetric local binary based method (CSLBP) and feature matching.

The performance of the proposed algorithms is analyzed based on detection rate, robustness to pre-processing operations. The experimental results confirm the efficiency of the proposed technique in terms of high tamper detection rate and robustness against copy-move forgery attacks (which are rotation, scale, blur, noise and JPEG compression.

As demonstrated in Figure 4.1, the proposed algorithms explore different approaches for feature extraction and feature matching. While the first proposed method based on Harris points achieves rotation invariance, the different feature matching scheme in algorithm two is applied to have a good performance in terms of tamper detection rate under blurring attack.

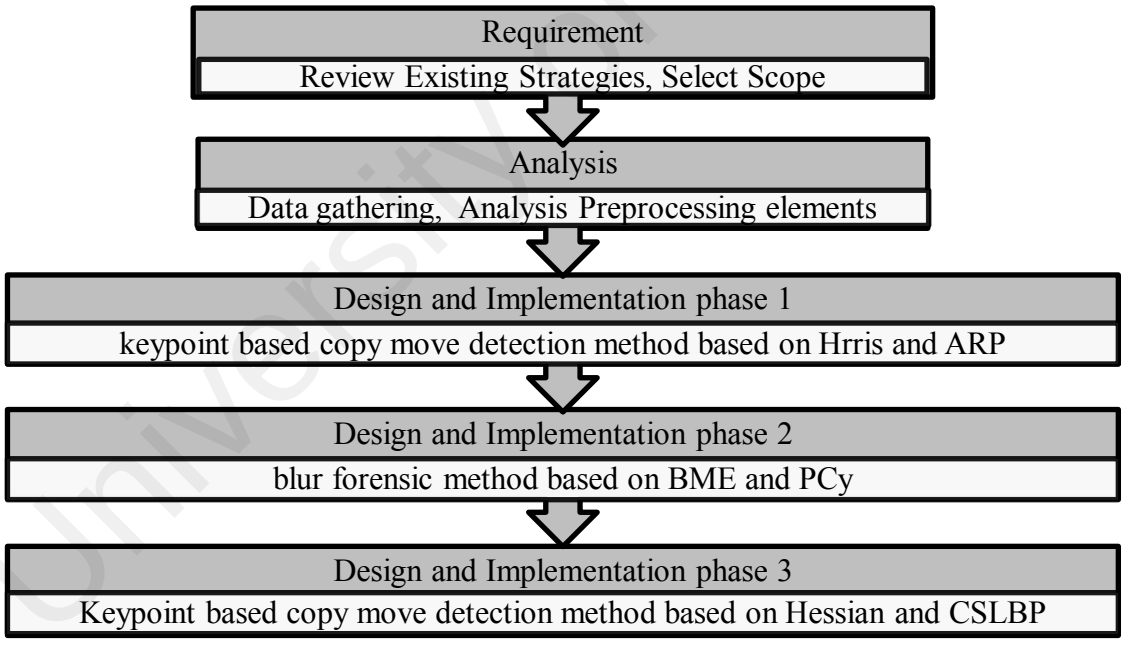


Figure 4.1: General development flowchart.

The general stages of the research methodology are research requirements, system analysis, design, implementation and lastly, certifying the proposed algorithm by testing different

methodologies. However, some fundamental stages of any developed scheme are formed within the first two steps of the methodology structure. The proposed algorithms are evaluated by testing each proposed scheme against different copy-move attacks such as rotation, scale, blur, illumination, noise and JPEG compression. Moreover, the scope of the proposed algorithm will be simplified in the requirement phase. Every step of the proposed phases will be described in detail in the following chapters. In the design and implementation phase, the major structure of the proposed copy-move forgery detection will be constructed, and the designed structure will be converted to machine language. Finally, in the last stage of the research, the effectiveness of the proposed algorithm will be evaluated against copy-move attacks and the results will be analyzed. Every step of the proposed algorithms are explained in detail in the following chapters. In the pre-processing stage, different challenges of copy-move forgery detectors are identified. The problems and issues related to detectors are clarified as an objective. Images are converted to grayscale images, ready to be tested with the proposed methods. Then, features which have been extracted will be compared together to recognize similar features. At this stage, finding a suitable feature extraction technique is essential, because if the features extracted from image are robust against pre-processing attacks, then the copy-move forgery detector will be robust against pre-processing operations. Subsequently, features are extracted from the images, and it becomes necessary to find a proper way to identify similar features while reducing false matches. By clustering the features and searching for similar clusters, the number of false matched is reduced. Finally, a line will connect the matched clusters in order to locate the tampered areas in the image. In the last stage, the proposed methods in both algorithms are evaluated based on standard evaluation criteria. Table 4.1 illustrates the general steps of the proposed method briefly, and addresses the objectives and contributions of this study.

Table 4.1: The general steps of the proposed method

Steps	Activities	Contributions	Objectives
Image Preprocessing	Identify different challenges to improve detection rate	-----	Identify different challenges of copy move forgery detection to improve detection rate
	Convert image to grayscale and resize it to suitable size.	-----	-----
Dividing Image	Segment an image into homogenous texture regions	Selection of small regions with 8*8 and 16 *16 pixels size	Detecting small objects in the forged image
Feature Extraction	Feature extraction based on Harris	Finding a suitable feature extraction techniques which are able to extract robust features of the image	Proposing an efficient copy move forgery detection that is robust to rotation, scale, noise and JPEG.
	Feature extraction based on Phase congruency		Proposing a new copy move forgery detection that is robust to blurring attack
	Feature extraction based on Hessian and CSLBP		Proposing an efficient copy move forgery detection that is robust to scale and illumination attack
Similarity Matching	Similarity condition	A new matching similarity measurement using Harris chain code of detected regions	To detect duplicated regions or multiple duplicated regions under copy move forgery

Locate Duplicated Regions	Connect matched regions together	-----	----
System Evaluation	Evaluation based on TPR and FPR	----	Test proposed methods using MICC-F220, F2000 and Image manipulation datasets with the evaluation analysis based on TPR and FPR

4.2.1 Requirements stage

As described in the previous section, in order to develop the proposed algorithms for each phase, all the research approaches have to be completed in an organized manner. This means the first three steps of the research methodology (which are: requirement, system analysis and system design) will be done respectively before developing the proposed algorithm. The first step of the proposed copy-move forgery detection system is the requirement phase. The requirement phase is the primary stage of each proposed phase. This step comprises the following activities:

a. **Review and Compare the Existing Schemes:** The requirement stage of the proposed scheme is a very important phase of the research study. A comprehensive literature review is focused to discover problems of the past copy-move forgery detection schemes. The result of the literature review, which is provided in chapter 2, assists in identifying the problem statement, checking the drawbacks and advantages of each technique, and helps in identifying the research objectives.

b. **Scope Selection for Proposed Copy-move Forgery Detection:** At this stage of the research, the scope of the research is determined in accordance with the literature explanations and the structure of the copy-move forgery detection

algorithm proposed by this research. For implementation of the proposed algorithm, a suitable programming language is required; therefore MATLAB language is chosen. MATLAB is frequently considered as a high level technical computing language and interactive environment for algorithm development, data analysis and data visualization. MATLAB is a correct choice for the implementation of proposed copy move forgery detection schemes, because of its numerous toolboxes, such as image processing. By considering the problem statement of this research, the scope of the proposed algorithm is identified as the following:

1. The copy-move forgery detection algorithm proposed by this research can support grayscale and RGB image.
2. The detection algorithm can work on images with different dimensions.
3. The forgery detection algorithm can accurately detect and locate the copy pasted areas.
4. The copy-move forgery detection method is keypoint based which is robust to rotation, noise, scale and JPEG compression.

4.3 Analysis stage

The next stage of the proposed algorithm is the declaration of various hypotheses related to the way the copy-move forgery detection algorithm works. In this stage of the research, the perfect solutions for satisfying the requirement stage are recognized and certified. The outcome of the analysis phase helps to construct the most effective algorithm in order to achieve the objectives identified by this research. In this section, the data collection for the proposed copy-move forgery detection algorithm will be described. However, the analysis carried out in this phase depends on the outcome of the proposed forgery detection algorithm. To complete the analysis phase, an evaluation of the results of existing copy-move forgery detection algorithms is an essential element. To confirm the result of the analysis stage, numerous experiments are carried out in the last step of the research.

4.3.1 Data Collection

The data for this study are collected from numerous academic and research sources. Except well known datasets, a dataset created which consist of 100 images with various topics from different sources for evaluation purpose. The idea of creating this dataset is to create different forged images with various tampered areas. Images come from personal collection with various attacks applied on them. Four other databases which published in valuable journals and are regularly used for experimental result comparison in image processing and forensic researches are utilized for evaluation. Currently, most of copy move forgery detection methods use these four databases, which are named MICC (F220, F2000 and F8multi) and Image manipulation dataset, for evaluation.

The following will describe the nature of four digital image databases selected for this research. The first digital image database is MICC-F220 (Amerini et al., 2011) which

consists of images with various contents and comes from the Columbia photographic image repository (Ng et al., 2005) and their personal collection. MICCF220 consists of 220 images: 110 are originals images and 110 are tampered. The image resolutions vary from 722 x 480 to 800 x 600 pixels and the size of the forged patch covers, on the average, 1.2% of the whole image. The forged images are created by randomly selecting an image area and duplicating it over the image by applying various attacks like rotation, noise, scale, JPEG compression or a composition of them. Table 4.2 shows the geometrical transformations for the attack used in the MICC-F220 dataset (10 attacks, from A to J). Where q presents rotation degrees, Sx and S_y are scaling factors applied to the x and y axis of the tampered image part.

Table 4.2: Attacks applied in the MICC-F220 dataset

Attack	θ	S_x	S_y
A	0	1	1
B	10	1	1
C	20	1	1
D	30	1	1
E	40	1	1
F	0	1.2	1.2
G	0	1.3	1.3
H	0	1.4	1.2
I	10	1.2	1.2
J	20	1.4	1.2

The second digital image database is MICC-F2000 (Amerini et al., 2011) which consists of images with various content, and comes from the Columbia photographic image repository (Ng et al., 2005) and their personal collection. MICC-F2000 is a large dataset which contains 2000 images of 2048 x 1536 pixels: 700 are tampered whereas 1300 are original.

The altered images are achieved by implementing different attacks like noise, scale, rotation, translation or a composition of them. The size of the forged patch covers, on average 1.12% of the total image (Amerini et al., 2011) .

The third digital image database is MICC-F8multi (Amerini et al., 2011) which consists of 8 high resolution tampered images with realistic multiple copy-move forgeries. This dataset is utilized for the evaluation of the proposed method in cases of multiple forgeries in one image.

The fourth digital image database is Image manipulation dataset (Christlein et al., 2012) which includes 48 PNG true color images. The forged images are obtained in both datasets based on having a different type of post processing operations such as rotation, scaling, JPEG compression and Additive White Gaussian noise (AWGN). Large images are resized to either 800 x 533 pixels or 500 x 333 pixels. The content of those images includes objects like human, buildings, animals.

Figures 4.2 and 4.3 illustrates a few samples from MICC-F220 and Image manipulation dataset to show the structure of the images in this dataset. Samples are under different copy-move attacks such as rotation, scale, etc.

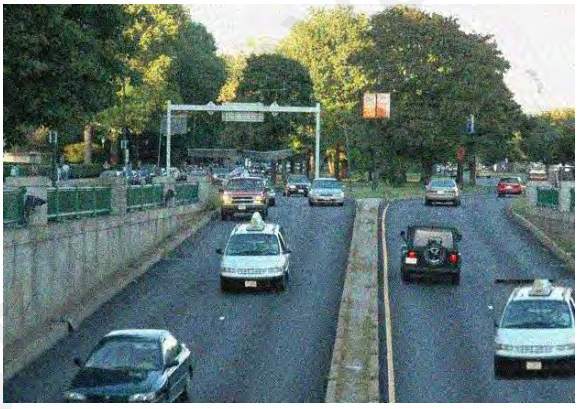
(a)

(b)

(c)

(d)

(e)



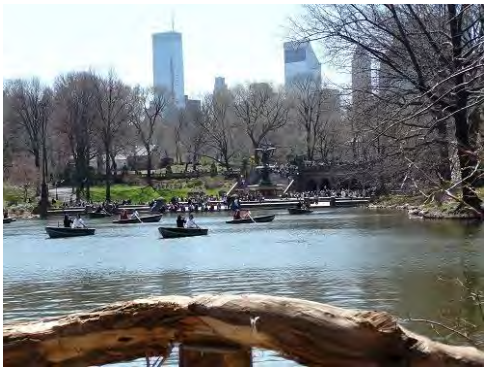
(f)

Figure 4.2: (a) Tampered image under scale attack from MICC-F220 dataset, (b) Tampered image under rotation attack, (c) Tampered image under scale and rotation attack, (d)Tampered image without attack, (e) Tampered image under JPEG compression, (f) Tampered image under noise attack,

(a)

(b)

(c)



(d)

Figure 4.3: (a)-(d) Samples of copy move forgery images from Image manipulation dataset.

4.4 The structure of research phases

The overall design flow of the proposed phases is explained. As explained in previous sections, this research proposes three algorithms for copy-move forgery detection. However, the first proposed algorithm is improved in terms of detection rate and detection time. The following subsections describe the general structure of the proposed algorithms.

4.4.1 Approach 1: Keypoint-based copy-move Forgery Detection-Algorithm

In this approach, the proposed keypoint-based algorithm for copy-move forgery detection is presented. The primary method of the proposed algorithm begins with converting an RGB image to a grayscale image. As illustrated in Figure 1.10, the statistical region merging segmentation is applied to the tampered image to divide the whole image into homogenous regions. Small regions are labeled based on least frequent method. Each region has given a centroid. Then, Harris detector is used to extract the keypoints in angular radial partition of a circle region for each centroids in order to obtain a scale and rotation invariance. And then unique keypoints are compared to each other to find matched keypoints for locating duplicated areas in

the image. This process continues until every single keypoint is checked with all other keypoint descriptors in the image to find exact match keypoints. If there is any pair of keypoints which match each other, it shows that the image is not original. Euclidean distance is computed between descriptors; if the two nearest neighbors have a ratio of less than a specific threshold it shows those tested descriptors are suspected as being matched. Finally, the duplicated areas are localized.

4.4.2 Approach 2: Blur forensic copy-move Forgery Detection-Algorithm

In this approach, the design structure of the proposed copy-move forgery detection algorithm is described. As mentioned before in Figure 1.10, the second proposed algorithm utilizes blur metric evaluation to detect blurred regions, and applied phase congruency to achieve blur invariance. The primary design of the proposed algorithm starts with the image segmentation using the statistical region merging method. Then, a blur degree is estimated for each region detected based on BME. The blurred regions are detected by examining the histogram of the BMEs of detected regions. Finally, PCy features are extracted from the regions for similarity matching. However, given the inherently blurred invariant feature of the PCy method, blurred copy–move forgeries with different blur radius parameters can be detected successfully.

4.4.3 Approach 3:Illumination invariant method for copy move forgery detection-Algorithm

In this approach, we present a robust keypoint based scheme to detect such specific artifact. The design structure of the proposed method has the following step: Firstly, the original image is segmented into small homogenous regions based NCut algorithm. And then, Hessian features are extracted for each segment, thus, the Hessian local interest points represent each segment. Secondly, each segment is represented by a center with square block and center symmetric local binary pattern (CSLBP) for local interest points are constructed as descriptors of each segment. Finally, the feature vectors are lexicographically sorted, and duplicated image blocks will be matched by a preset threshold value.

4.5 Summary

The methodology of the proposed method in each phase for copy-move forgery detection was explained through this chapter, and the main structure of each proposed phases are described. Furthermore, the key progress flows of this research, which contains the requirement, an analysis, the primary design, and implementation, are explained. However, the details of the proposed copy-move forgery detection algorithms are stated in the design and implementation chapter.

CHAPTER FIVE

RESEARCH DESIGN AND IMPLEMENTATION

5.1 Introduction

The structural design and detailed description of the proposed methods for exposing region duplication forgery under copy move attack are introduced in this chapter. The first proposed method is robust to Geometric transformations such as rotation and scaling. The second method is blur invariant. And the third proposed method is robust to illumination changes. All of these methods rely on Keypoint based method and Segmentation method which are able to authenticate the originality of the image with the capability of detecting region duplication forgery in the tampered image. The ultimate goal of the proposed methods is to detect small regions in the image using segmentation based technique and analyze the internal structure of these regions based on their keypoint features to find region duplication forgery. These methods improved the detection rate in terms of TPR and FPR to achieve robustness and efficiency.

This chapter proceeds as follows. In section 5.2 Approach 1: rotation invariant method on Harris points for detecting region duplication forgery is introduced. In section 5.3 Approach 2: blur invariant scheme for exposing blurred duplicated regions is presented. In section 5.4 we regard the illumination changes in the forged image to reveal the copy move forgery presented in approach 3.

5.2 Approach 1: Rotation Invariant Method on Harris Interest Points for Exposing Region Duplication Forgery.

I. Introduction

For as long as cameras have existed, photographers have been staged and images have been forged for more nefarious purposes. Region duplication is regarded as an efficient and simple operation for image forgeries. The detection of duplicated regions can be a challenging task in digital image forensic. Most current methods to expose this forgery are based on an exhaustive block matching of image contents and it may not be easy to detect this type of forgery when the duplicated regions have gone through some geometric transformation operations before being pasted. Here, we propose a novel method for detecting duplicated regions in forged images that is robust to common post processing operations and geometric transformation operations such as rotation and scaling. First, the image is segmented with statistical region merging (SRM). Harris points are employed in angular radial partition (ARP) of a circle region for each detected object in order to obtain a scale and rotation invariant feature points. Feature vectors for a circle patch are extracted using Hölder estimation regularity based descriptor (HGP-2). Finally, the circle patches are matched using the Nearest Neighbor (NN) to expose duplicated regions.

The proposed method is a combination of both existing techniques: keypoint features matching and circle blocking technique inside segmented regions. Our method depends on statistical region merging segmentation technique (SRM) of image as a preprocessing step to detect homogenous objects and has an advantage to detect small flat regions with little structure in the entire image, and a linkage

clustering based on Tamura texture features of detected objects is employed to improve the time complexity of detection algorithm.

To achieve good performance with rotation attacks, we represent every object by a chain code. Chain code is created as a sequence of total number of corner points based on accumulation of Harris corners in the image partition defined by ARP. Fast, reliable regularity based descriptor is developed to locate the duplicate regions in the tampered images. The results show that the chain code of corner points with a regularity based descriptor gives a good performance, and preserves a powerful discriminator metric for detecting duplicate regions. The significance of this work is providing a rotation invariant method that can detect duplicate regions in copy-move image forgery with high accuracy, especially when the size of the duplicate region is small. Moreover, we improved the time complexity of detection by using linkage clustering the detected regions in the image based on their texture features. The importance of our work comprises a forensic investigation of copy-move forgery in depth by exploiting the critical internal structure and texture in images.

The rest of section 5.2 can be organized as follows. The detailed description of the proposed method is presented in section II. Time complexity analysis of the proposed methods is defined in section III.

II. The proposed method

The main aim of our proposed is to recognize copy-move forgery in suspected images that were subjected to geometric transformations. The objectives include; (1) classify images as tampered or non tampered, (2) to accurately identify the duplicated regions in forged images, and (3) to improve the time complexity of the

detection method. According to these objectives, the proposed detection method consists of the following steps, as shown in Figure 5.1:

1. Input the suspicious color image.
2. Segment the input image of size MxN pixels into small image regions using Statistical Region Merging Segmentation (SRM.).
3. Locate centroid of each image regions.
4. Crop each image region to 11 x 11 pixels square image block around the centroid of detected region.
5. Apply Tamura texture on each square image block.
6. Cluster similar image regions by texture.
7. Apply Angular radial partitioning (ARP) on each image region indexed by its centroid coordinates in the same cluster.
8. Convert input image into grayscale and extract key points with Harris detector.
9. Calculate the total number of Harris corners in each sector of a circle image region in the same cluster.
10. Represent the total number of Harris corners by a chain code, and search for closely one to one matching between two images regions in the same cluster.
11. Extract regularity-based features the centroid and around each Harris corners of the image regions that have the same chain code by using Hölder estimation regularity based descriptor (HGP-2).
12. Compute median absolute deviation (MAD) for all HGP-2 of the two matched image regions, and save it in feature vector fv.
13. Find the Euclidean distance between two corresponding final feature vectors fv and fv'.

14. Detect and localize the tampered regions.

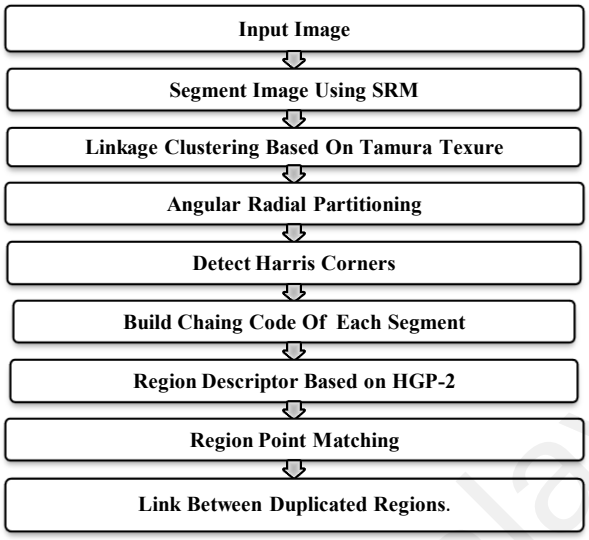


Figure 5.1: The main steps of rotation invariant CMFD method.

1. **Statistical Region Merging Segmentation (SRM)**

The duplicated regions in forged images have the same homogeneity condition and internal structure (Mahdian & Saic, 2009; N. Muhammad et al., 2011). Based on this idea, the input image is segmented into homogenous regions, which is a preprocessing step toward higher level image analysis. Segmentation of the image is carried out using SRM algorithm (Nock & Nielsen, 2004). SRM algorithm has an excellent performance to capture the main structural objects of images using effective statistical image analysis. SRM has the ability to deal with significant noise distortions, handle occlusions with the sort function. SRM is a multiscale segmentation method; formulate image segmentation as an inference problem. It is the reconstruction of regions of the observed image, based on an unknown theoretical (true) image. The SRM depends on two steps: the merging predicate and the testing order to test the merging of regions in the image.

1.1 The Merging Predicate

The merging predicate can be introduced as the following:

$$P(R,R') = \begin{cases} true, if \forall a \in \{R,G,B\}, |\bar{R}'_a - \bar{R}_a| \leq \sqrt{b^2(R) + b^2(R')} \\ false, otherwise \end{cases} \quad 5.1$$

Where, the notation $||$ stands for cardinal. The observed image I contains $|I|$ pixels, each containing Red-Green-Blue (RGB) values, each of the three belonging to the set {1,2,…,m}. In 8 bit images, *m* takes 256. Each color channel is replaced by a set of exactly Q independent random variables, taking positive values in $[0, m/Q]$. It is to be noted that the Q parameter can be used to quantify the statistical complexity of mapped image, the generality of the model, and the statistical difficulty of the problem. Higher values of Q result in finer segmentation and thus the generation of more regions, $R \text{ and } R'$ are adjacent regions, $\bar{R}_a$ stands for the perceived average for channel α in region R, and *b(R)* is a predicate function for merging regions.

$$b(R) = m\sqrt{\frac{1}{2Q|R|}(In\frac{|S_{|R|}|}{\delta})} \quad 5.2$$

Where $S_{|R|}$ Denotes the set of regions with $|R|$ pixels, and Q=[1-256]. δ is the maximum probability when $P(R,R')=false$, which is usually set with small values. In short, if the $P(R,R')$ returns true, the R and R` can merge to be a bigger region.

1.2 Testing Order

Each pixel with its 4-neighbor connectivity form pixel couples. There are $N<2|I|$ couples in all. Each pixel couple is weighted by the difference of adjacent pixels, called Dissimilarity, which is calculated as follows:

$$d(p,p') = \max_{a \in \{R,G,B\}} \left| p_a' - p_a \right| \qquad 5.3$$

Where, p_a and p_a' are 4-neighbor connectivity on the channel a. A radix sorting algorithm sorts the couples in ascending order according to their Dissimilarity. Then, The SRM traverses the couples. As a result, the segmented regions of the observed image are saved into mapped image, then the mapped image is scanned horizontally and vertically to find the least frequently occurring values in the mapped image plane. These values are retained to detect the small regions such as objects and flat areas (sky, grass, ocean, etc.) in the image, we assumed that duplicate region forgery with small size for better tampering. This procedure reduces the number of instances of detected objects. Finally, the centroids of the detected objects are located, as shown in Figure 5.2.

Figure 5.2: Results of segmentation with the SRM. (a) The initial image. (b) Detected objects. (c) Centroids. of small objects.

2. Linkage Clustering of Objects Based on Tamura Texture Analysis

The main reason behind the high time complexity in block based methods is that the lexicographical sorting algorithm is blindly search for all features extracted from divided blocks without considering the type of regions. For example, there is no need to compare the grass region with sky region in the image. The centroids of least frequently occurring regions are obtained in the mapped image from step 2. In order to improve the computational complexity, the detected regions are grouped into clusters, according to their texture features. We applied a straightforward linkage block clustering algorithm for classifying the blocks into clusters (Akbarpour Sekeh et al., 2013). Hence, a square image block of size 11 x 11 is employed for each centroid of detected object. An improved Tamura texture features (Tamura et al., 1978) are defined as a new criterion to find similar clusters in the block-clustering step. An improved Tamura features consider only coarseness and contrast (CN) as features to create a two dimensional feature vector. After extracting Tamura features, Ward's linkage clustering method (Rokach & Maimon, 2005) is performed on spatial locations $(i.e., x, y\ coordinates)$ of the centroids. Ward's linkage clustering creates a hierarchy of clusters which can be described by a tree structure. In (Akbarpour Sekeh et al., 2013) three different linkage methods have been evaluated: Single, Centroid, and Ward's linkage on MICC-F220 to detect duplicate regions forgery. Though Ward's linkage looks to be slightly better than others which gives a good detection rates TPR=100 and FPR=8 in their algorithm. We conclude the Ward's linkage clustering method can improve the detection rate of our proposed algorithm.

First the algorithm tries to assign each centroid to a cluster; then determines all the mutual spatial distances among clusters. Then, it finds the nearest pairs of clusters, and

merges them into a single cluster. In Ward's linkage, the distance between two clusters is the increase in the total within a cluster sum of squares as the result of merging two clusters. It is given by the following equation:

$$D_{ward}(\mathrm{X}, \mathrm{Y}) = (2[\mathrm{SS}(\mathrm{X} \cup \mathrm{Y}) - (\mathrm{SS}(\mathrm{X}) + \mathrm{SS}(\mathrm{Y}))])^{1/2} \quad 5.4$$

where X and Y are two clusters of size N_X and, for data points. SS of a set of values is the sum of squared deviations from the centroid of the cluster. For a cluster X with points, the $SS(X)$ is described by the following expression:

$$SS(X) = \sum_{i=1}^{N_X} \left| X_i(d) - \frac{1}{N_x} \sum_{j=1}^{N_X} X_j(d) \right| \quad 5.5$$

where $\| \|$ is Euclidean distance. In the clustering step, all the image regions are clustered based on Tamura texture features.

3. Angular Radial Partitioning (ARP) and Harris Corner Detection

Rotation and scale invariant features are crucial in most recognition tasks and should be considered in the features chosen for efficient CMFD systems. To deal with rotation and scale invariance, a rotation robust region description method based on ARP and Harris corner detector is employed, as described below:

1. Angular Radial Partitioning

The ARP (Chalechale et al., 2004) was originally designed as an edge based descriptor. We proposed a simple modification on the original ARP by selecting corner points in the image regions as features. The image regions are divided into circular

sectors of the surrounding circle. The algorithm defines M is the number of radial divisions and N is the number of angular divisions resulting in $M\,x\,N$ sectors. The angle between adjacent sectors is described as $\theta = 2\pi / N$. The radius of circle region is r , the number of corner points in each sector of an image region I is computed as follows:

$$f(p,i) = \sum_{\theta=\frac{i\,2\pi}{N}}^{\frac{(i+1)2\pi}{N}} (I(r,\theta)) \qquad 5.6$$

where $i = 1,2,\ldots,N$. I is the image region. The Harris region features H are circularly shifted for an image rotation of $\theta = i\,2\pi / N$. As shown in Figure 5.3.

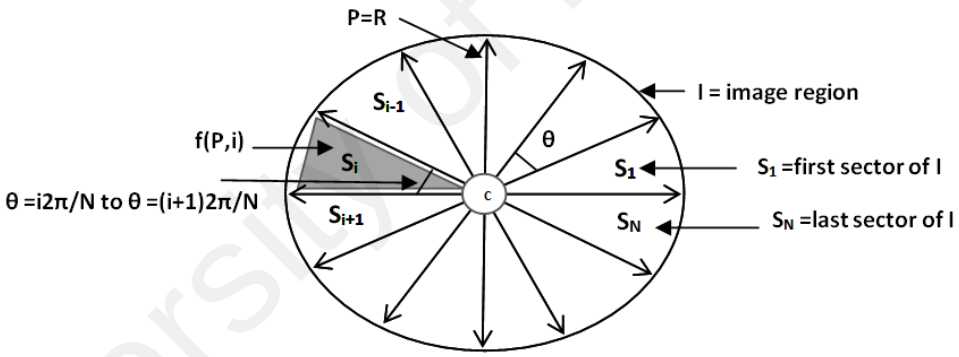


Figure 5.3: Angular radial partitioning of an image region I to N angular sectors.

The created angular radial partitions in practice are shown in Figure 5.4. The radius of the circle region is 10 and number of radial partitions $M = 1$. The radial partition rotates 30° every time, and 12 partition masks $(N = 12)$ labeled as $S1, S2, \ldots, S12$, they will be defined after a whole circle is covered. The corresponding detected image regions in the image are divided into 12 sectors, each sector with angle 30^0 are saved to detect corner interest points based on the Harris corner detector in the next subsection.

Figure 5.4: The angular radial partition masks. (a) The partition in direction of 30°. (b) The partition in the direction of 120^{0}.

2.Harris Corner Detection

Extraction of local interest points from images has been demonstrated to be an efficient paradigm for computer vision tasks, as it provides robustness to some geometrical transforms such as scale and rotation. Various techniques for extracting local interest points have been implemented over the past few years (Mikolajczyk et al., 2005), , such that they satisfy scale and rotation invariance properties. The Harris corner detector (Harris & Stephens, 1988) is a common technique that identifies corners of an image. It was implemented to be invariant to rotation. Harris corner detection (Szeliski, 2011) is employed using the harmonic mean.

The Harris corner algorithm makes use of several linear filtering of an image. For a given an image f , a low pass filtering is expressed as follows :

$$L(p,\sigma)=g(p,\sigma)*f(p) \qquad 5.7$$

Where $g(p,\sigma)$ is a Gaussian function of scale σ, and p is the location in the image grid. Let $L_x(p,\sigma_D),L_y(p,\sigma_D)$ be the respective horizontal and vertical image derivatives at location p, established with Gaussian kernel filter of local scale σ_D (the differentiation scale). Later, these results are composed to create three images

$L_x^2(p,\sigma_D), L_y^2(p,\sigma_D), L_x L_y(p,\sigma_D)$ where the multiplicative operation is accomplished pixel by pixel. These images are then filtered by a Gaussian kernel function $g(p,\sigma_1)$ of scale σ_1 (the integration scale):

$$\mu(p,\sigma_1,\sigma_D) = \sigma_D^2 g(p,\sigma_1) * \begin{bmatrix} L_x^2 & L_x L_y(p,\sigma_D) \\ L_x L_y(p,\sigma_D) & L_y^2(p,\sigma_D) \end{bmatrix} \quad 5.8$$

Where * is the convolution operator. Finally, the Harris corner indicator $H(p,\sigma_1,\sigma_D)$ is given by:

$$H(p,\sigma_1,\sigma_D) = \frac{\det(\mu(p,\sigma_1,\sigma_D))}{k\,tr(\mu(p,\sigma_1,\sigma_D)) + \Psi} \quad 5.9$$

Where k is a trade-off scalar, experimentally lying in the interval $[0.04,0.15]$ and Ψ is Floating-point relative accuracy. As shown in Figure 5.5, Harris corners are detected for each object.

(a) (b)

Figure 5.5: The Harris corners of each object in the same cluster. (a) Centroids of objects in the same cluster (b) Harris corner points around centroids.

4. **Region Description Based on Chain Code and Regularity Based Descriptor**

The chain code is extracted from these objects, as a sequence of total number of detected Harris corners in each sector of a circle image region is expressed as

$$chain_{ci} = \left[f_{S_i}(p,i), f_{S_{i+1}}(p,i+1), \ldots, f_{S_N}(p,N) \right] \quad 5.10$$

where i=1,2,…,N and c_i represent the centroid of image region. In our work, chain code extraction started from sector $_{S1}$ and ended at sector $_{S12}$. The reading direction of chain code is anticlockwise. The chain code is assigned for each region indexed by its centroid coordinates in the image. After chain code assignment, the chain code and its circularly shifted description are overlaid seeking closely matching chain code, and the estimation of rotation angle is computed based on the number of circular shifts between two similar chain codes of regions**.** A local descriptor, based on HGP-2 regularity estimator (Trujillo et al., 2012), is constructed for centroid and corners of the regions that have the same chain code. HGP-2 regularity estimator is simply used to regularize the image data by convolving them with a Gaussian smooth function. We employed the HGP-2 estimator to quantify the singularity, or amount of irregularity contained within image region. The Symbolic expression for HGP-2 estimator is described as follows:

$$HGP-2 = G_1 * |log|G_1 * (k \ .(w - G_1 * w))|| \quad 5.11$$

where *w* is 8 x 8 pixel window, $G1$ is Gaussian kernel at scale 1. k is optimal operator =11.

The main advantages of a HGP-2 descriptor are: (1) gives the fastest estimation compared with other regularity based methods; (2) robust to partial occlusions and to various kinds of geometric transformation operations ; and the main advantage of using

chain code is the total amount of image content is sharply reduced because only a subset of local regions are described and examined by a compact representation for all regions with similar chain codes.

Chain codes are saved into feature vectors to represent the sequence of total number of Harris corners around the centroid of image region. HGP-2 descrpitor is built on centroid and its surrounded Harris corners in the image regions with similar chain codes.

5. Region Duplication Detection Algorithm

We used median absolute deviation MAD (Leys et al., 2013) as a similarity measure for detecting duplicate regions. MAD is the most robust scale estimator in the presence of outliers. We computed MAD of the HGP-2 region descriptor within each centroid c, and Harris corners $H_i \, for \, i = 1,2,\ldots,n$ of each object within same cluster $S_k \, for \, k = 1,2,\ldots,m$, $eg., M_c = MAD(c), M_{H_i} = MAD(H_i)$. A feature vector of each object is denoted as follows

$$fv = \left[M_c, M_{H_i} \right] \tag{5.12}$$

Finally, by iterating over Harris corner points and centroids in detected regions with their corresponding feature vectors, we can obtain the set of matched points using Euclidean distance. The Euclidean distance between two regions R_1, R_2 with corresponding feature vectors fv and fv' is expressed as follows:

$$D(R_1,R_2) = \sqrt{(fv_i - fv_i')^2} \quad ,i = 1,2,\ldots,n \tag{5.13}$$

The region is matched only if this constraint is satisfied: $D(R_1,R_2) \le T$, where $T \, in \, [0.14 - 0.25]$. All the matched points are retained, and displayed with a line

connecting them. The duplicate regions can be revealed through corner points and relation lines. However, the number of matched points will vary among different objects in the same image.

III. Time complexity analysis

The goal of computational complexity is to assess the proposed algorithm according to its performances. The main problem in image region duplication forgery detection is the computational complexity related to block matching. The technical viewpoint of this study is based on three components: SRM segmentation, linkage clustering and Harris corners points.

If we consider the input image having (M x N) pixels, Therefore, the SRM segmentation time will be defined as(Nock & Nielsen, 2004):

$$T1 = O(M\ x\ N) * log(Q) \quad 5.14$$

where Q is independent random variable which taking positive values ranging from 1 to 256 as defined in (Nock & Nielsen, 2004). The Ward's linkage time used for clustering the image regions be represented as: $T2 = O(L^2)$. Where L is the total number of detected image regions, to obtain clustered regions based on their texture features. The time used to find Harris corners points for each image region in the same cluster followed by searching algorithm with sliding search window of size (b x b) would equal to: $T3 = O(K * b^2)$). Where (b x b) << (M x N), and K=12 which is the total number of divided sectors in the image region. Therefore, the computational complexity of proposed algorithm mainly depends on the image size (MxN) and the total number of detected image regions L.

5.3 Approach 2: Exposing Blurred Duplicated Regions nder Copy-Move Forgery in Image Forensic

I. Introduction

The rapid advancement of image technology has improved and enhanced the capability to forge images. The problem of digital image forgery may be serious. Digital images are commonly manipulated through region duplication; nonetheless, most region duplication detection methods are rendered ineffective when the duplicated regions are retouched by blurring operations that remove obvious detectable traces. In the current study, we therefore proposed a forensic algorithm to recognize the blurred duplicate regions in a synthesized forged image efficiently, especially when the forged region in the images is small. The method is based on blur metric evaluation (BME) and phase congruency (PCy). First, the image is segmented using the statistical region merging method. Second, a blur degree is estimated for each region detected based on BME. The blurred regions are detected by examining the histogram of the BMEs of detected regions. Finally, PCy features are extracted from the regions for similarity matching. Given the inherently blurred invariant feature of the PCy method, blurred copy–move forgeries with different blur radius parameters can be detected successfully. Experimental results demonstrate that the proposed method can effectively detect duplicated regions on tampered images obtained from two image databases, namely, MICC-F220 and image data manipulation, even when the image is retouched through a blurring operation.

Region duplication forgery is one of the most common approaches to image forgery, especially given the power and ease of use of image editing software.

Given that the copied region originates from the same image, the key characteristics of duplicated regions, such as noise components, color patterns, homogeneity textures, and internal structures, are similar (Devi Mahalakshmi et al., 2012; G. Muhammad et al., 2012). Such similarity complicates the exposition of duplicate regions in forged images. In the current study, we consider region duplication forgery with blurring to detect copy–move image forgery. The main contributions of this study include:

1) The blurring of entire duplicated regions is estimated through the blur metric evaluation (BME) of copy–move forgery detection (CMFD).
2) Features are extracted from edge regions using the phase congruency (PCy) method. They are blur-invariant.

II. Proposed method

In spite of the fact that keypoint-based methods (discussed in chapter 2) can reveal either rotated or scaled region duplication forgery; these approaches cannot overcome blur retouching. In artful image forgery, forgers usually employ retouching methods such as blurring to eliminate visual distortions on the duplicated region in relation to the surrounding area (Hsiao & Pei, 2005; Mahdian & Saic, 2007). Blurring is a common process in digital image manipulation, and the simple blur operation smoothes the manipulations effectively based on the mathematical averaging of neighbor pixel values in a sliding square window (Zhou et al., 2007). The blurring process is modeled as a convolution of images with a blurring kernel as follows:

$$B(x,y) = \sum_m \sum_n h(m,n) * f(x+m, y+n), \quad 5.14$$

where $f(x, y)$ is the original image with x and y pixel coordinates; $h(m, n)$ is the blur kernel with size $m \times n$; $B(x,y)$ is the blurred image; and * is the convolution operator. Different blur models can be established by varying the filter functions and the size of the moving average sliding window. Three types of blur are common: Gaussian, defocus, and motion blurs (Shan et al., 2008). In practice, the use of the Gaussian blur filter during image forgery is regarded as simple and effective. If the image region is blurred after the copy–move forgery process, then the main intentional features of the blurred region are reduced and details cannot be perceived. These features include the total number of local interest points detected based on either Harris, SIFT, or SURF, gray range, mean, and contrast. As a result, the matched consistencies between the features of copied and blurred regions extracted from the forged image are difficult to recognize (Su et al., 2011; J. Zheng & Liu, 2009). Therefore, we should detect the blurred regions in an image and determine the quality of these regions to identify the consistencies between duplicate regions in a forged image.

Many researchers have recently begun exposing blurred region duplication forgery (Mahdian & Saic, 2007; T. Wang et al., 2013). For instance, Mahdian *et al.* proposed a direct approach to detect blurred duplicated regions (Mahdian & Saic, 2007). Specifically, they proposed a CMFD method based on the central moments of an image up to the seventh order. A color image was divided into overlapping blocks. Twenty-four blur-invariant moments were extracted from each block for each red–green–blue (RGB) color channel. Therefore, the feature vector of length 72 was reduced as per PCA. Finally, a k-dimensional tree was used as a nearest neighbor searching algorithm to locate matched block pairs. Zhou *et al.* (Zhou et al., 2007) developed a scheme for blurred image forgery

detection by exploring the blurred edges of an image region. To detect blurred forged regions, edge preserving–smoothing filters were applied to binary images, followed by a mathematical morphology process based on erosion operation. Tao *et al.* (T. Wang et al., 2013) detected blurred duplicate regions by using combined blur-affine moment invariants to extract features from image blocks. Block pairs were matched according to correlation coefficients, and relative error was utilized as a measure of the stability of invariant features distorted by blurs.

The main aim of our proposed method is to recognize the blurred duplicate region in a synthesized forged image efficiently, especially in a situation where in the forged region is small. Figure 5.6 illustrates the main steps in image forgery detection.

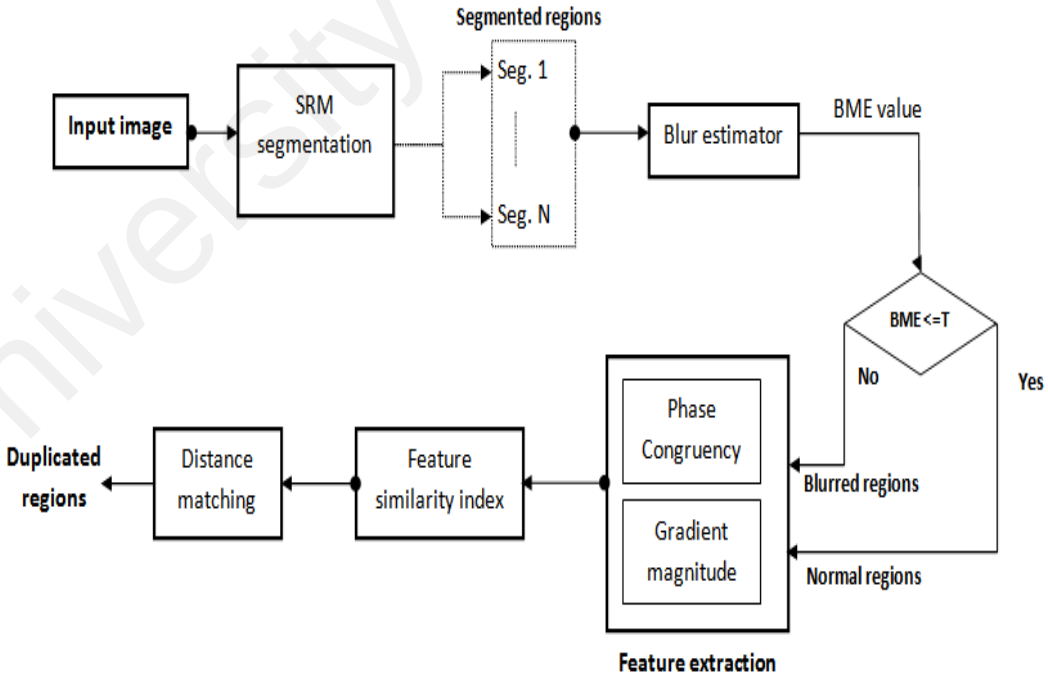


Figure 5.6: The main steps in blurred CMFD algorithm.

1. **Small region detection using Statistical region merging segmentation (SRM)**

Duplicated regions in forged images generally have the same homogenous texture (Abdul Jauwad & Ullah, 2011; Ardizzone et al., 2010) and internal structure (Mahdian & Saic, 2009; N. Muhammad et al., 2011). Based on this idea, our task is detecting segmented regions that share the same intrinsic features. In this section, we will determine the presence of such regions using SRM segmentation algorithm (Nock & Nielsen, 2004) and localize their centroids. The suspected image is segmented into various homogenous regions, which is a preprocessing step toward higher level image analysis. The SRM is applied based on two main steps: merging predicate and testing order to test the merging of regions in the image. Each step is introduced separately in the following sections:

i. Merging predicate

The statistical region merging (SRM) method is a bottom-up process that integrates image pixels into large regions on the basis of the predicate criterion. A common assumption that underlies the merging predicate of an image is that the statistical pixels obtained from the same statistical impose a constant expectation value for any color channel. The expectation values of adjacent regions vary for at least one color channel. Hence, a suitable merging predicate is applied according to these assumptions as described in (Nock & Nielsen, 2004). I is the input image that contains $|I|$ pixels. Each pixel contains RGB values that represent a color channel a. Each of the three values belongs to the set$\{1, 2, \dots, g_n\}$. In an eight-bit image, $g_n = 256$. This value is the number of expected different color values. Each color channel is replaced by a new set of exactly Q independent random variables that

derives the positive values in $[0, g_n/Q]$. The Q parameter can quantify the statistical complexity of a mapped image. High Q values result in a fine segmentation; thus, additional regions are generated. *b(R)* is a predicate function for region R and is defined in (Nock & Nielsen, 2004) as in (5.2).

where $\delta = \frac{1}{(6|I|^2)}$ is a probability error with a small value. It is inversely proportional to the square of the size of image I to limit over segmentation in the mapped image. $S_{|R|}$ denotes the set of regions with $|R|$ pixels, and Q is in the range [1–256]. To merge two adjacent regions R and R' with color averages $|\bar{R}_a|$ and $|\bar{R'}_a|$ for channel a, respectively, the merging predicate can be introduced (Nock & Nielsen, 2004) as in (5.1). If $P(R, R')$ is true, then R and R' can merge into a large region.

ii. Testing order

To merge one pixel with another within a statistical region, the adjacent pixels should be considered. Therefore, the pairs of adjacent pixels are sorted. The testing order and the merging predicate are the basis of the SRM algorithm, and they interact with each other. The order in which the merging tests are conducted follows a simple rule: when a merging test is performed between two true regions, all merging tests have been conducted previously within each region. The testing order is described as follows:

a. For an input image *I*, the number of merging tests $N < 2|I|$ pairs of adjacent pixels in four-neighbor connectivity. S_I denotes the set of all pairs of adjacent pixels. The algorithm first sorts these pairs in ascending order according to the sort function defined in (Nielsen & Nock, 2003) as follows in (5.3).

b. The set of adjacent pixels in S_I is traversed only once; thus, the SRM algorithm is fast due to radix sorting with the S_I values.

c. Any current pair of adjacent pixels $(p, p')\epsilon S_I$ is merged if the predicate criterion $P(R, R')$ is true. R and R' represent the regions of pixels p and p', respectively. The pseudo code of the SRM segmentation algorithm is defined in Figure 5.7 as follows:

Input: a suspected image I

Let S_I be the set of 4 neighbor pairs of adjacent pixels in image I

S_I'=radixsortIncreasing(S_I, d);

For i=1 to $|S_I'|$ do

If ($(R \neq R')$ and $P(R,R')$ == true) then

mergeRegion(R,R');

Output: homogenous regions.

Figure 5.7: Pseudo code of SRM segmentation method.

As a result of the processes in the segmentation step, the segmented regions of the image under observation are saved into a mapped image. This image is scanned horizontally and vertically to locate the least-frequently occurring values in the mapped image plane. These values are then retained to detect small regions in the image. We assume that duplicate region forgery is small for effective tampering. This procedure also reduces the number of instances of object detection. Finally, the centroids of the detected objects are determined, as displayed in Figure 5.8.

(a) (b)

(c)

Figure 5.8: Results of image segmentation with the SRM method. (a) Input image that contains the bird blurred by Gaussian blur with radius = 0. 7. (b) Segmented regions. (c) Centroids of detected small regions.

2. Blur metric evaluation

To differentiate between normal and blurred regions within a single image, we predict the blur degree for each region based on the perceptual blur metric model presented in (Crete et al., 2007). BME is a no-reference blur metric method that is defined in the spatial domain as a measure of the variation in the neighboring pixels of the image region. This method analyzes the behavior of such variations by blurring the image region using a low pass filter. It also compares the original region with its blurred version. As the image region is increasingly blurred, the image region is smoothed and variation intensity decreases. Thus, the blurred region

is detected based on the reduced absolute differences between the original region and its blurred version. The steps are detailed as follows (Crete et al., 2007):

Step 1: Horizontal and vertical low pass filters H_{hor} and H_{ver} are applied to each region I_{reg} with size $m \times n$. Blurred regions B are obtained as follows:

$$B_{ver} = I_{reg} * H_{ver} \ , \ B_{hor} = I_{reg} * H_{hor} \tag{5.15}$$

where | * | denotes the convolution operator.

Step 2: The horizontal and vertical absolute differences between the original region and its blurred vision are computed. These image differences are expressed as follows:

$$D_{I_{ver}}(i,j) = \sum_{i=1}^{m-1} \sum_{j=0}^{n-1} | I_{reg}(i,j) - I_{reg}(i-1,j)|$$

$$D_{I_{hor}}(i,j) = \sum_{i=0}^{m-1} \sum_{j=1}^{n-1} | I_{reg}(i,j) - I_{reg}(i,j-1)|$$

$$D_{B_{ver}}(i,j) = \sum_{i=1}^{m-1} \sum_{j=0}^{n-1} | B_{ver}(i,j) - B_{ver}\,(i-1,j)|$$

$$D_{B_{hor}}(i,j) = \textstyle\sum_{i=0}^{m-1} \sum_{j=1}^{n-1} | B_{hor}(i,j) - B_{hor}\,(i,j-1)| \tag{5.16}$$

Step 3: The variation in the horizontal and vertical absolute difference images is evaluated by the Riemann integral as follows:

$$V_{hor} = \text{Max}(\{f(x), 0\}) = \begin{cases} f(x) = D_{I_{hor}} - D_{B_{hor}} \ , \ f(x) \geq 0 \\ 0 \ , \ otherwise \end{cases} \tag{5.17}$$

where V_{hor} and V_{ver} are the horizontal and vertical absolute difference images, respectively. They are computed in the same manner.

Step 4: The variations in the sum of the intensities of difference images $D_{I_{ver}}, D_{I_{hor}}$, $D_{B_{ver}}$, and $D_{B_{hor}}$ in a defined range [0–1] are normalized to estimate the vertical and horizontal blur measures as follows:

$$Blur_{I_{ver}} = \frac{sum(D_{I_{ver}}) - sum(D_{V_{ver}})}{sum(D_{I_{ver}})} \quad , where\ D_{v_{ver}} = sum(V_{ver})$$

$$Blur_{I_{hor}} = \frac{sum(D_{I_{hor}}) - sum(D_{V_{hor}})}{sum(D_{I_{hor}})} \quad , where\ D_{v_{hor}} = sum(V_{hor}) \qquad 5.18$$

Step 5: The blur measure is selected as the maximum value among the vertical and horizontal measures as follows

$$\text{BME} = \text{Max}(\{Blur_{I_{ver}}, Blur_{I_{hor}}\}) \qquad 5.19$$

where BME is in the range [0–1]; 0 indicates that the image is sharp and 1 suggests that it is blurred. Figure 5.9 shows an array of sample image regions that are rated according to the blur degree estimated by the BME method. Furthermore, blurred regions in a single image have greater BME values than normal regions do. These regions exhibit the most common BME value in the image. Thus, a histogram of the BME values of the image is constructed to depict the total BME distribution in the image and to filter out the blurred regions of the image. A stem chart of the count of each BME in the image region in the image is developed as presented in Figure 5.10. Normal regions generally correspond to the highest peak in the histogram. As a result, the detected blurred regions have BME values greater than that of the highest peak. The constructed histogram with a highest peak since it has BME ranges that appear most often in the image. In a process that is repeated over image regions, we typically expect the blurred regions to have BME value that exceeds the estimated BME with highest peak. The

main advantage of this process is the usage of BME features, as histogram features very quickly and the comparison of these features is computationally fast and efficient to detect blurred regions.

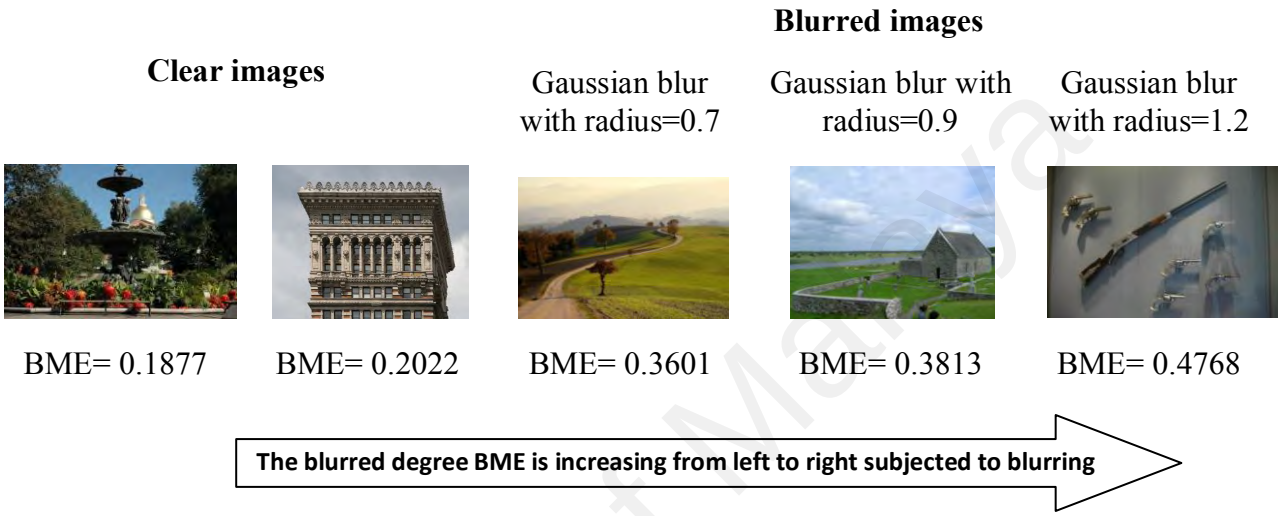


Figure. 5.9: Images from MICC-F220 (Amerini et al., 2011) and image data manipulation (Christlein et al., 2012) datasets rated on the basis of the blur degree estimated through BME. The proposed BME in Equation 5.9 captures the region blur degree appropriately.

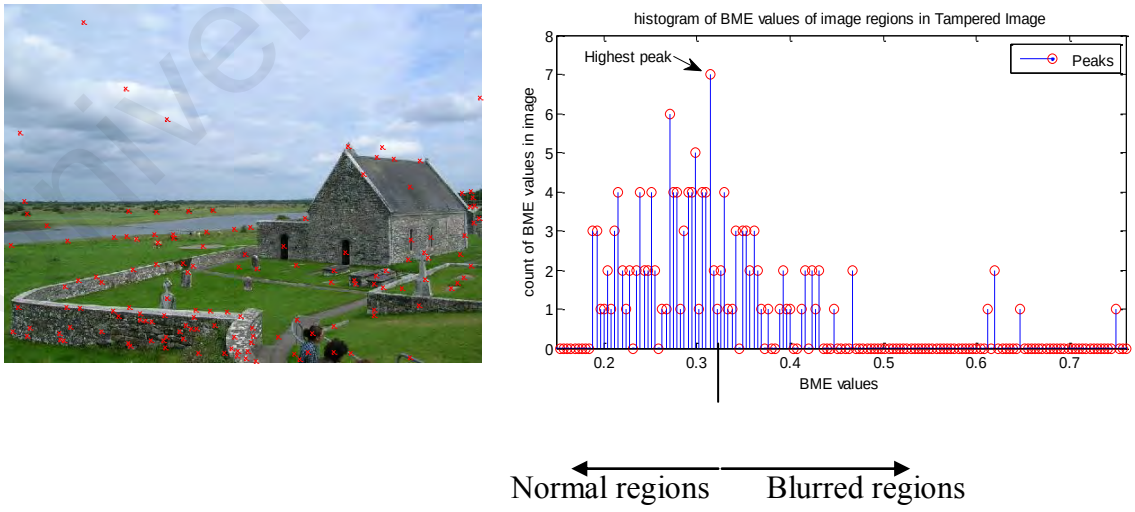


Figure 5.10: Histogram of the detected regions in the image.

3. Feature extraction

Duplicate regions in the forged image typically share an internal structure. However, high-frequency components are reduced when the duplicate region is blurred, and the fine details of the region are lost. To improve the high-frequency components that contain edge information, we first adopt the PCy method proposed in (Lin Zhang et al., 2011) to predict the value of each pixel in the edges of the image region. The gradient-based method (GM) is then used to extract features from the edge region of the PCy image. This process is expected to remove low-frequency components and enhance detection precision.

- **PCy features**

Important image features are perceived at the points in which Fourier components are maximal in phase. The PCy on 2D images was defined by Kvoesi in (Kovesi, 2003) in terms of the Fourier transform of signal f *(x, y)* at point *(x, y)* in the image as follows:

$$PCy(x,y) = \frac{\sum_n \sum_\theta W(x,y)\lfloor A_{n\theta}(x,y)\Delta\psi_{n\theta}(x,y) - T \rfloor}{\sum_n \sum_\theta A_{n\theta}(x,y) + \varepsilon} \quad 5.20$$

where *W(x, y)* is the weight function of the 2D log-Gabor filter at point *f(x,y)*. $\lfloor\ \rfloor$ is a floor function that equalizes the enclosed quantity to itself when its value is positive; otherwise, the value is zero. $A_{n\theta}(x,y)$ is the amplitude of the Fourier component at scale *n* and an orientation angle of filter θ. It is defined as follows:

$$A_{n\theta}(x,y) = \sqrt{e_{n\theta}(x,y)^2 + o_{n\theta}(x,y)^2} \quad 5.21$$

where $e_{n\theta}(x,y)$, $o_{n\theta}(x,y)$ are the responses between image *f(x,y)* and the 2D log-Gabor filter. They are expressed as follows:

$$[e_{n\theta}(x,y), o_{n\theta}(x,y)] = [f(x,y) * M^e_{n\theta}], \quad 5.22$$

where * is the convolution operator. $M_{n\theta}^{e}\ and M_{n\theta}^{o}$ are even and odd symmetric wavelets at scale $n = 4$ and angle $\theta = 6$, respectively. T is the estimated noise energy. $\varepsilon = 0.0001$ is a small constant that prevents division by zero. $\Delta\psi_{n\theta}(x, y)$ is the sensitive measure of phase deviation that is written as follows:

$$\Delta\psi_{n\theta}(x,y) = \cos(\psi_{n\theta}(x,y) - \bar{\psi}_{n\theta}(x,y)) - |\sin(\psi_{n\theta}(x,y) - \bar{\psi}_{n\theta}(x,y))| \quad 5.23$$

A PCy image is constructed for each region in the image. The PCy coefficients are real numbers in the range [0–1]; 0 corresponds to low-frequency components, whereas 1 denotes the highly informative features in the image. The PCy image can detect blurred regions efficiently, as exhibited in Figure 5.11. Specifically, we highlight edge points obtained from the image region whose PCy coefficients are non-zeros. The first three moments, namely, mean (μ), variance (ϖ), and contrast (c), are defined as the features of edge regions and are saved into feature vector F_v=*[μ, ϖ, c]*. This vector is used to detect matched edge regions.

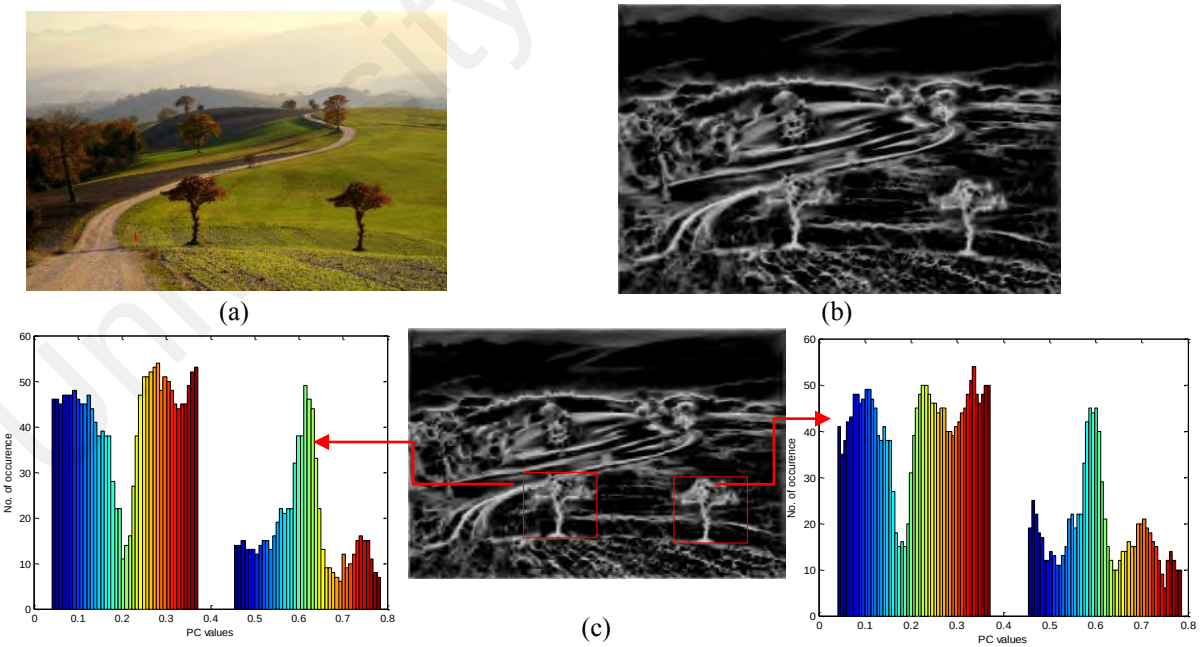


Figure 5.11. Illustrating enhanced image by Fourier coefficients. (a) Image "tree" has blurred copy–move forgery with Gaussian blur (radius = 0.8), (b) PCy map of (a) to obtain a significant mapping of internal structure of foreground objects such as edges. (c) selected ROIs in PC map including normal tree in the left side and blurred cloned tree in the right side and the histograms of selected ROIs in PC map to show robustness to blur.

- **GM features**

An image gradient is defined as a directional transition of intensities in an image (Lowe, 1999). The gradient $\nabla I(x,y) = [\nabla I_x, \nabla I_y]$ is large, and intensity changes as in discontinuous or texture structures. Simple derivatives in the horizontal and vertical directions of image *I* are obtained, namely, $\nabla I_x = \frac{dI(x,y)}{dx}, \nabla I_y = \frac{dI(x,y)}{dx}$.

Gradient magnitude is estimated as the square root of the sum of image directional gradients. That is, $GM = \sqrt{\nabla {I_x}^2 + \nabla {I_y}^2}$. GM features are extracted as secondary features from each image region in the forged image and are then combined with PCy features to estimate a similarity index measure of the image region as described in the following section.

4. Region duplication localization

We detect blurred duplicate regions within a forged image precisely in two stages:

i. **Estimation of a feature similarity index measure**

We measure the feature similarity between the detected blurred regions and another candidate regions based on local similarity for Pcy and GM image as follows:

a. local similarity measure between two regions R_i and R_j for the PCy map is defined as

$$S_{pc}(x) = \frac{2PC_{yi}(x).\, PCy_j(x)+T1}{PCy_i(x)^2.\, PCy_j(x)^2+T1} \quad 5.24$$

where $T1 = 0.85$ (Lin Zhang et al., 2011) is positive stability constant.

b. local similarity measure between two regions R_1 and R_2 for the GM image is similarly expressed as:

$$S_{GM}(x) = \frac{2GM_i(x).GM_j(x)+T2}{GM_i(x)^2.GM_j(x)^2+T2} \quad 5.25$$

Where GM is a gradient magnitude image and $T2$ = 160 is positive stability constant (Lin Zhang et al., 2011).

Finally, the feature similarity index measure is defined as:

$$FSIM = \frac{\sum_{x\in\Omega} S_l(x).PC_{ym}(x)}{\sum_{x\in\Omega} PCy_m(x)} \quad 5.26$$

where Ω is the spatial domain of the entire region. $S_l(x)$ is the relative importance of PCy and GM features and is expressed as $S_l(x) = S_{PC}(x).S_{GM}(x)$. $PCy_m(x)$ is the maximum value of PCy maps and is written as $PCy_m(x)=Max(PCy_i(x), PCy_j(x))$. Thus, duplicate region pairs whose estimated similarity measure satisfies the rule $FSIM > T_{sim}$ are identified. T_{Sim} = 0.92 is the preset threshold.

ii. **The Euclidean distance**

$D(p,q)$ determines the distance between regions p and q. p_i and q_i are the corresponding feature vectors of the matched regions with edge points. They are expressed as follows:

$$D(p_i, q_i) = \sqrt{\sum_{i=1}^{n}(p_i - q_i)^2} \quad 5.27$$

Finally, the duplicate regions are located along with their centroids. The blurred region is highlighted by a circle to visualize the forged region in the image.

5.4 Approach 3: Exposing Small Uniform And Nonuniform Region Duplication Forgery Under Illumination Variations

1. Introduction

With the availability of advanced editing softwares and fully equipped digital cameras, region duplication is becoming more common in image forgery which copying a region of an image and moving it in another location in the same image to conceal undesirable objects. Copied regions may be in uniform and nonuniform areas are perceptible in our method. Most existing block based techniques struggle to detect such tampering under post processing operations such as (scaling and illumination). And they are mainly at the cost of higher computational complexity. Here, we present a robust scheme to detect such specific artifact. Firstly, the original image is segmented into small homogenous regions, and Hessian features are extracted for each segment, thus, the Hessian local interest points represent each segment. Secondly, each segment is represented by a center with square block and center symmetric local binary pattern (CSLBP) for local interest points are constructed as descriptors of each segment. Finally, the feature vectors are lexicographically sorted, and duplicated image blocks will be matched by a preset threshold value. Experiment results show that our scheme is robust to post processed copy move forgery under scaling, illumination changes, JPG compression and additive noise.

We propose a robust copy move image forgery detection method using Hessian features and CSLBP. Copy move is one of the widely used techniques for image forgery. In this technique, a portion of the image is copied and pasted to another region of the same image to hide the original content in the pasted region. While pasting, the duplicated region may post processed using rotation, scaling, blurring or illumination changes. The

proposed method utilizes the similar patterns between the segments. First the input image is segmented based on the color palette. Second, small regions are localized based on the late frequent method. For each segment, centroids and Hessian features are extracted. Hessian interest points are scale and translation invariant. Then illumination invariant CSLBP is applied to the approximation of the Hessian features. The extracted features are thereby translation, scale and illumination invariant. The similarity of features between two segments is measured using Euclidean distance.

2. Proposed method

The task our copy move forgery scheme is to find small similar regions in an image. Since the duplicated regions are unknown both in shape and size, if we compare every possible pairs pixel by pixel, the computational complexity will be higher. Obviously, it is more practical to segment the suspicious image into different homogenous regions for detecting the duplicated regions. The proposed method consists of four steps: object detection based on Normalized cut segmentation (Ncut), identifying small objects based the least frequent method, localizing local interest points of each object based on Hessian method, extracting illumination invariant features based on CSLBP. Figure 5.12 shows the flowchart of the proposed method.

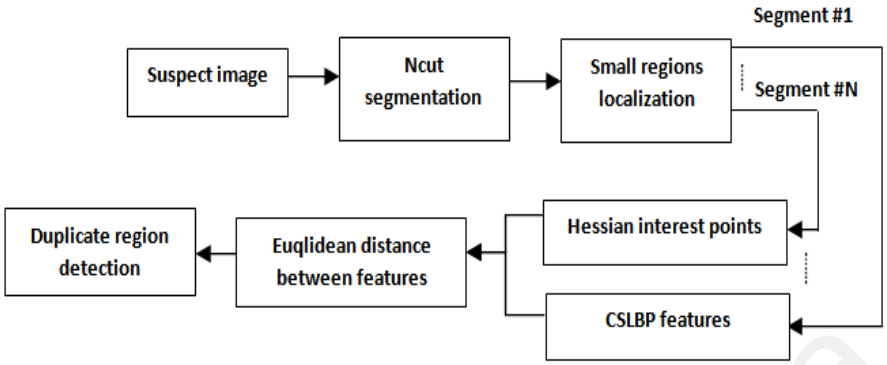


Figure 5.12: Block diagram of the proposed CMFD method using Hessian and CSLBP.

I. Image Segmentation based on Normalized cuts

The input image is segmented into different segments in such a way that an object is fully contained in a single region, and the detected object is almost homogeneous. For this purpose, we use Normalized cut algorithm (Shi & Malik, 2000) which recursively divides a graph of all pixels in the input image based on contour and texture cues, globally minimizing a cost function defined on the edges at the partition boundaries. The image is modeled as a weighted graph G= (V, E). This graph can be subdivided into two sub graphs A and B by presenting the partition as minimizing the *cut* as described below

$$cut(A,B) = \sum_{u\in A, v\in B} w(u,v) \qquad 5.28$$

Where w(i,j), the weight of each edge is the similarity function between nodes i and j. And the minimum cut criteria approves cutting small sets of isolated nodes in the graph via Normalized Cut defined below

$$Ncut(A,B) = \frac{cut(A,B)}{assoc(A,V)} + \frac{cut(A,B)}{assoc(B,V)}, assoc(A,V) = \sum_{u\in A, t\in V} w(u,t) \qquad 5.29$$

Where the assoc(A,V) represents the total connection from nodes A to all nodes in the graph.

As a result of the Ncut segmentation step, An input image I of size $r \times c$ is segmented into k segments $Seg_1, Seg_2, \ldots, Seg_k$. The segmented uniform and non-uniform regions of the image under observation are saved into a mapped image. This image is scanned horizontally and vertically to locate the least frequently occurring values in the mapped image plane is described as follows:

i. For the mapped image $M_{r,c}(r\ row,\ c\ cols)$, there is a set A have the assigned segment values with no repetitions $a_{i,j} \in \text{unique}(M_{r,c})$ *where* $1 \leq i \leq r$ *and* $1 \leq j \leq c$ to detect all objects with different sizes.

ii. Set B is created which denotes to the set of the most frequent values in M *via* row and column wise searching to locate the biggest objects. It is described as follows

$$B=[unique(\ mode_{row}(M_{r,c})) \cup unique(\ mode_{cols}(M_{r,c}))] \quad 5.30$$

Where mode function returns the most frequently occurring value in M by rows and columns.

iii. To identify the small region, the set S denotes to the least frequent values can be calculated via Set difference of two sets $S=A-B$.

These values in the set S are then retained to detect small regions in the image. We assume that duplicate region forgery is small for effective tampering. This procedure also reduces the number of instances of detected objects. Finally, the centroids of the detected objects are determined which locate all uniform and uniform regions.

II. Hessian interest points

The purpose of local interest points (Mikolajczyk & Schmid, 2004) is to provide a representation that allows to efficiently match local structures between uniform

duplicate regions. We want to compute a sparse set of local measurements that capture the essence of the underlying detected regions and build a descriptor in their interesting structure to gain scale invariant features. Local interest points of the small objects are identified based on Hessian matrix that exhibit strong derivatives in two orthogonal directions. Given a point $x= (x, y)$ in the interest region in an image I, the Hessian matrix $H(x, \sigma)$ in x at scale σ described as follows

$$\mathrm{H}(\mathrm{x}, \sigma) = \begin{bmatrix} \mathrm{I}_{\mathrm{xx}}(\mathrm{x}, \sigma) & \mathrm{I}_{\mathrm{xy}}(\mathrm{x}, \sigma) \\ \mathrm{I}_{\mathrm{xy}}(\mathrm{x}, \sigma) & \mathrm{I}_{\mathrm{yy}}(\mathrm{x}, \sigma) \end{bmatrix} \quad 5.31$$

Where $\mathrm{H}(\mathrm{x}, \sigma)$ is a square matrix containing second order derivatives of Gaussian describing surface curvature. I_{xx}, I_{xy}, and I_{yy} are the second derivatives for each point x in the image. The extrema of the determinant of Hessian measure in a local neighborhood was used to detect interest points. This measure can be expressed as

$$Det(H) = I_{xx}I_{yy} - \left(0.9\, I_{xy}\right)^2 \quad 5.32$$

A non maximum suppression using a 3 × 3 neighborhood is applied on the *Det* to ensure that it assumes a maxima along the gradient direction. The local maxima of the measure *Det* was used to localize interest points.

III. Illumination invariant descriptor using CSLBP

In this section we provide details of analyzing the patterns of interest regions of segments for copy move forgery detection. The descriptors f_i for each segment S_i is calculated, which combines the strength of Hessian features and CSLBP texture analysis. The center symmetric local binary pattern can be defined (Xiao et al., 2013) as a modified version of local binary pattern (LBP) such that at each pixel, neighboring pixels that are opposite to each other are compared to produce *16 (2^4)*

binary patterns as illustrated in Figure 5.13. Mathematically, with definitions, the Local Binary Pattern (LBP) is defined as

$$LBP(x_c, y_c) = \sum_{n=0}^{n=7} s(g_n - g_c)2^n \ , s(x) = \begin{cases} 1, x \geq 0 \\ 0, otherwise \end{cases} \quad 5.33$$

Where g_c is the grey value of center pixel (x_c, y_c) , g_n represents eight neighboring pixels. If *gn* is smaller than *gc*, the binary result of the pixel is set to 0, otherwise to 1. All the results are combined with an 4 bit binary string. In CSLBP, instead of comparing the neighboring pixels with the center pixel, the center-symmetric pairs of pixels such as (g_0, g_4), (g_1, g_5), (g_2, g_6), (g_3, g_7) are computed as follows:

$$CSLBP(x_c, y_c) = \sum_{n=0}^{n=3} s(g_n - g_{n+4})2^n \ , s(x) = \begin{cases} 1, x \geq 0 \\ 0, otherwise \end{cases} \quad 5.34$$

T is a small value, and which is used to increase the detection rate on non uniform regions by thresholding the gray level differences. In our experiments, T was given a value of 0.3.

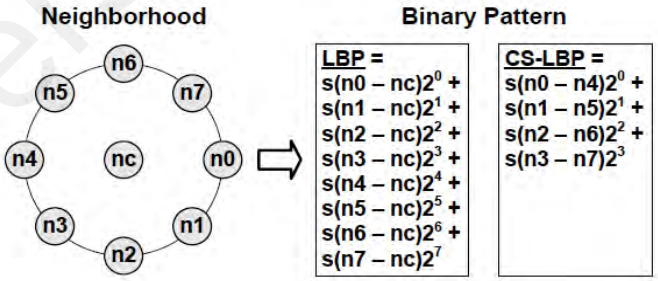


Figure 5.13: LBP and CSLBP descriptors for a neighborhood 3x3 pixels.

IV. Detecting duplicated region forgery

We inspect feature vectors f_i of each segment S_i within the Euclidean distance expressed as follows

$$D(f_i, f_j) = \sqrt{\sum_{i=1}^{n}(f_i - f_j)^2}, i - 1, \dots, r, j = 1, \dots, r, i \neq j \quad 5.35$$

Where $D(f_i, f_j)$ gives the distance between segments *Si* and *Sj*. f_i are corresponding feature vectors of matched regions with edge points. Finally, duplicate regions are located with their centroids and matched features.

5.5 Summary

Throughout this chapter, the structural design of three proposed schemes is described. The design flow of each proposed phase has been described separately step by step. The implementation procedures of the proposed keypoint-based tamper detection schemes are described in detail. In the first approach, an image authentication scheme with a capability of detecting region duplication forgery is proposed, we used Harris keypoints in angular radial partitions to achieve rotation inariance. The importance of the proposed algorithm 1 is its ability to authenticate digital images and accurately locate rotated copied and pasted areas. Therefore, we proposed another forensic algorithm to recognize the blurred duplicate regions in a synthesized forged image, especially when the forged region in the images is small. The proposed method detects blurred regions via blur estimation and then we explored phase congruency features to find similarity between duplicated regions. Finally, we proposed another copy move forgery detection method to reveal the forgery under illumination variations. The proposed method consists of four steps: 1) Object detection

based on normalized cut segmentation (Ncut) which identifies only small regions in the image, 2) Detection of hessian interest points in illuminated objects, 3) Extracting illumination invariant features using Center symmetric local binary based method (CSLBP). 4) Feature matching.

The experimental results in chapter 6 illustrate that the proposed algorithms are robust against several geometric changes, such as JPEG compression, rotation, noise, blurring and scaling. Furthermore, the detection rate of the algorithm is improved by utilizing the proposed clustering procedure. The true and false positive rates achieved by the proposed algorithm outperform several current detection algorithms.

CHAPTER SIX

EXPERIMENT RESULTS

6.1 Introduction

In this chapter, different region duplication forgery will be exposed to determine the robustness, effectiveness and accuracy of the proposed methods. As described in previous chapters, this type of forgery is made by copy move attack under different geometric transformations and post processing operations such as rotation, scale, blur, illumination changes, JPEG compression and additive noise. These operations make the authentication and localization of forged regions more difficult. Furthermore, the proposed region duplication forgery detection schemes are examined against these attacks to evaluate the detection accuracy of the proposed methods.

However, to illustrate the robustness and effectiveness of the proposed region duplication forgery detection methods, various experimental results have been conducted in section 6.4.

To evaluate the accuracy of our methods, we used an evaluation metric based on TPR and FPR. The performance of our methods were evaluated on two image datasets named MICC-F220 (Amerini et al., 2011) and Image Manipulation Dataset (Christlein et al., 2012) as described in the next section. We used the MICC-F220 (Amerini et al., 2011) because it includes many images that have been tampered by copy move forgery under geometric transformations and post processing operations. furthermore, many of exisiting methods regard it as a standard image dataset. Moreover, (Christlein et al., 2012) made an evaluation of poular existing methods using Iamge manipulation Dataset to detect uniform regions and non uniform

regions under JPEG compression, scaling, rotatation and noise addtion. As a result, we need to detect region duplication forgery on the above two iamge datasets as a challenging task and evaluate our method with existing methods.

The organization of this chapter is presented as follows. In Section 6.2, the experimental setup is introduced. Section 6.3 defines the evaluation metric. The experiment result under effectiveness and robustness tests are illustrated in Section 6.4. Finally, comparisons and discussions are debated in Section 6.5.

6.2 Experimental setup

Our experiments were carried out using the MATLAB R2012a software running on a personal computer with Intel Core i5 processor 3.10 GHz and 4 GB memory. 50 experimental images were tested, based on the following two image datasets. The first dataset is MICC-F220 (Amerini et al., 2011) which contains 220 JPG images; 110 are forged images and 110 are originals. The second dataset is an image manipulation dataset (Christlein et al., 2012) which includes 48 PNG true color images. The forged images are obtained in both datasets based on having a different type of post processing operations such as rotation, scaling, JPEG compression and Additive White Gaussian noise (AWGN). Large images are resized to either 800 x 533 pixels or 500 x 333 pixels. The content of those images includes objects like human, buildings, animals. Often, there are two main factors influencing the accuracy of copy move forgery detection methods; the size of the forged region and the post processing operations. In general, there is a direct relationship between the size of the duplicated

region and precision of detection method. On the other hand, a forger usually applies various kinds of post processing operations to hide artifacts of tampering.

To evaluate our proposed methodology, we provide two main kinds of tests: 1) Robustness to rotation, scaling, blurring and illumination. 2) Effectiveness to detect multiple regions. First, we discuss the evaluation metric used in our method. Then we present quantitative results and examples for the detection of copy move forgery subjected to the size of duplicated regions and many post processing operations.

6.3 Evaluation metric

For practical image applications, the most important issue of a detection method is the ability to recognize forged and original images. Thus we adopt the evaluation metric which are defined in (Christlein et al., 2012) to evaluate the performance of our proposed methodology at image level. Due to the need of authenticating an image if the image is forged or not, we need to use statistical measures of performance of a binary classification: normal image or forged image. In each experiment, we record the number of forged images detected as forged T_P (True Positive), the number of images detected as forged being original F_P (False Positive), and the falsely missed forged images F_n (False Negative).

From these measures we define four evaluation metrics: Precision (P), Recall (R), True Positive Rate (T_{PR}) and False Positive Rate (F_{PR}) as follows:

$$P = \frac{T_P}{T_P + F_P}, \qquad R = \frac{T_P}{T_P + F_N}. \tag{6.1}$$

Precision (P) indicates the probability that a detected forgery is truly a forgery, while Recall (R) denotes the probability that a forged image is detected.

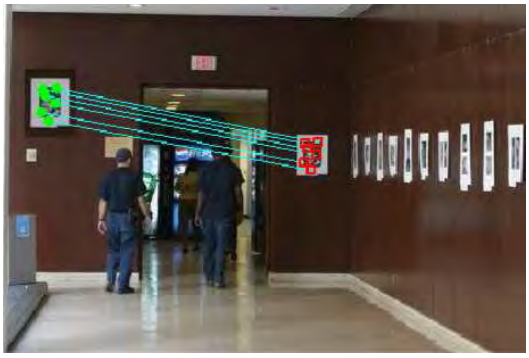
$$T_{PR} = \frac{No.of\ forged\ images\ detected\ as\ forged}{No.of\ forged\ images} \quad 6.2$$

$$F_{PR} = \frac{No.of\ original\ images\ detected\ as\ forged}{No.of\ original\ images} \quad 6.3$$

Where T_{PR} reflects the performance of the detection algorithm in correctly locating the pixels in forged region, while F_{PR} is the fraction of original images that was not correctly detected. The higher T_{PR} (Towards 1) and the lower F_{PR} (Towards 0), the better the detection performance.

6.4 Experiment result

As explained in chapter 2, normal region duplication forgery is defined as creating a forged image by applying copy move attack without using any geometric transformations or post processing operations. We illustrate some samples of region duplication forgery detection with our first proposed method in the following section to test the effectiveness. Figure 6.1 illustrate some examples of copy move forgery and detection results of the first proposed method have been performed on MICC-F220. More experimental results for normal region duplication forgery detection are available in (Appendix B).



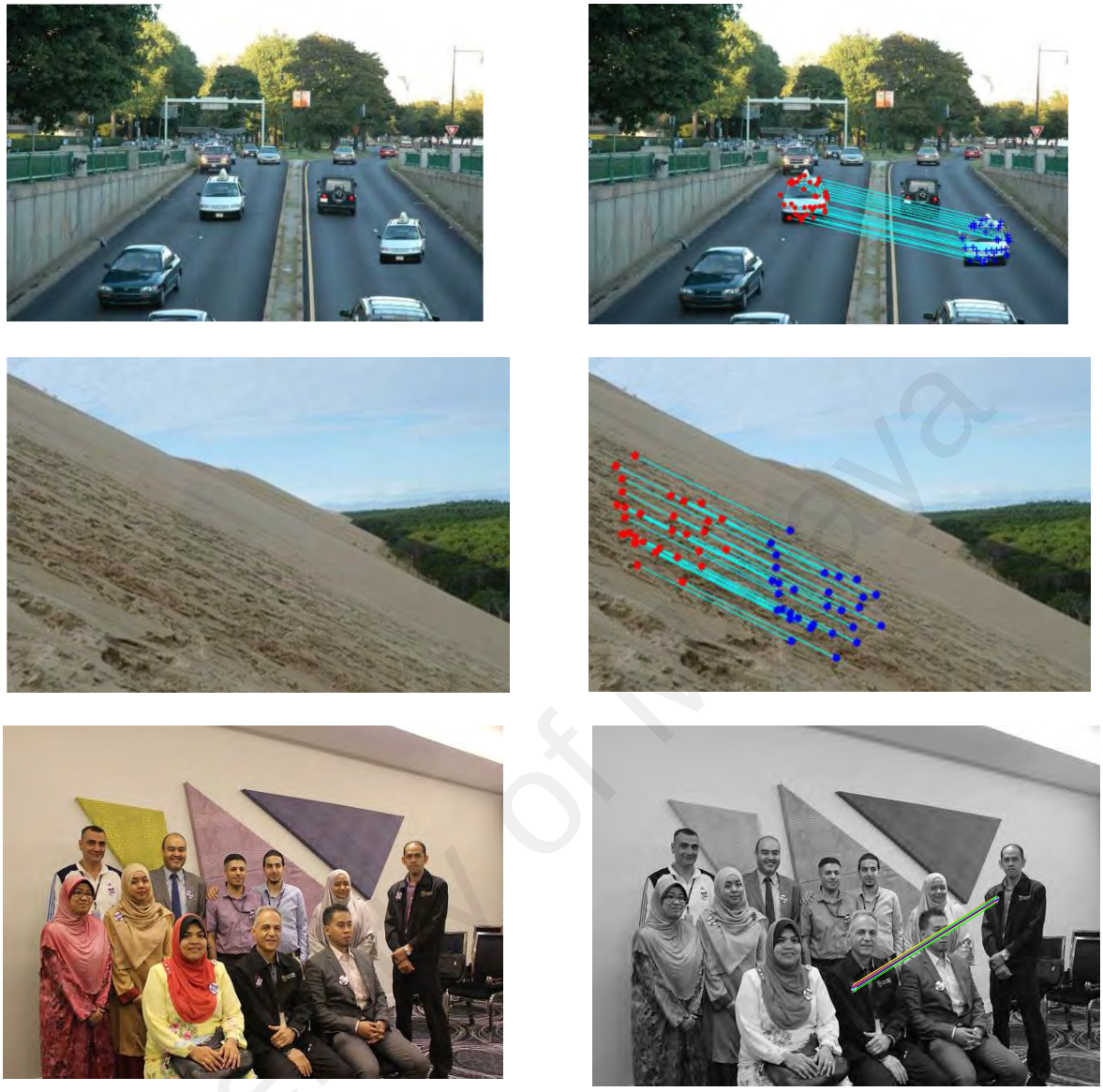


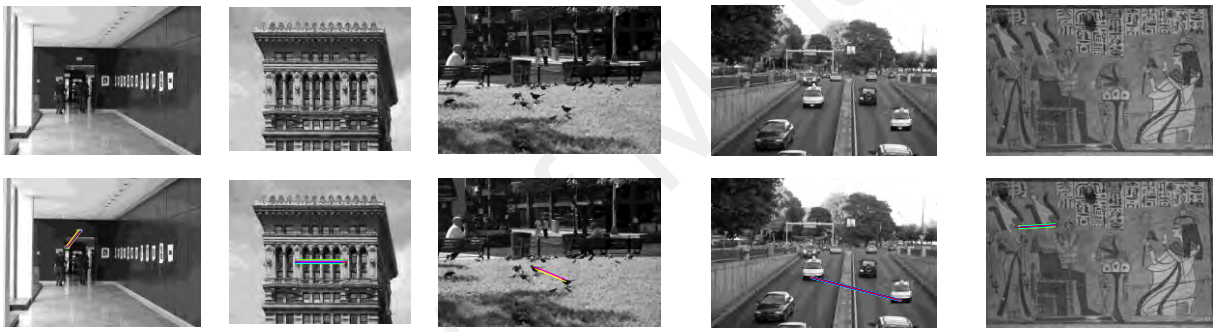
Figure 6.1: Some examples of tampered images are pictured in the first column. The corresponding detection results are reported in the second column.

6.4.1 Effectiveness test

In the following experiment, we choose images from MICC-F220 and Image Data Manipulation datasets to test the effectiveness of our method. These images have duplicate regions that are non regular shapes and meaningful objects with different size of 32 x 32 , 64 x 64 , 96 x 96 and128 x 128 pixels. The images shown in Figure 6.2 are the detection results of simple copy move forgery without any post processing operation.

Another test is given in Figure 6.3. We can see from this Figure that our algorithm can also work well when the forged images contain multiple duplicate regions. More examples of multiple duplicated region detection results in (Appendix C).

A good CMFD method should not only be effective, but also be efficient, which impose the time complexity to be reasonable which the average time for detecting duplicate regions is 90.8 seconds.



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

Figure 6.2: Shown on the top row are five images with duplicated region size of 20 x 20 pixels, 32 x32 pixels, 64x64 pixels 96 x96 pixels and 128 x128. Shown below are the detection results using our algorithm.

a) Forged image: the door is copied and moved into the left side and upper side(rotated one).

b) Detection results of multiple doors in the forged image.

Figure. 6.3: Shown are the detection results for multiple copy-move forgery.

6.4.2 Robustness test

Since forgers usually create an imperceptible forged image, various kinds of post-processing operations are carried out including: rotation, scaling, additive Gaussian noise and JPEG compression. We show a series of experiments to test the robustness of the proposed method.

I. JPEG Compression

In this part, we tested our method for robustness to JPEG compression. The proposed algorithm can locate the duplicated regions under different JPEG compression $(Q = 90;80;70;60;50)$ are shown in Figure 6.4. In our experiments, the forged image was compressed with different quality factors and subjected to the rotation and normal copy move operations. The detection performance of our method for JPEG compression of different qualities is shown in Table 6.1. As the detection results show, even when the quality factor of the distorted image is quite low such as JPEG compression (Q=50), the detection performance of the proposed method is still reliable.

Generally, the detection performance of our proposed method tends to decrease with the decrease of the quality factor of JPEG compression. The main issue is that with low quality JPEG compression images, it becomes more difficult to identify the exact Harris interest points. The matching and linking between these points might be strongly confused. As a result, there may be less or even no matched Harris points at all. However, with such low quality factors, the compressed images are not usually visually good enough anyway. So, those low factors are not usually commonly used.

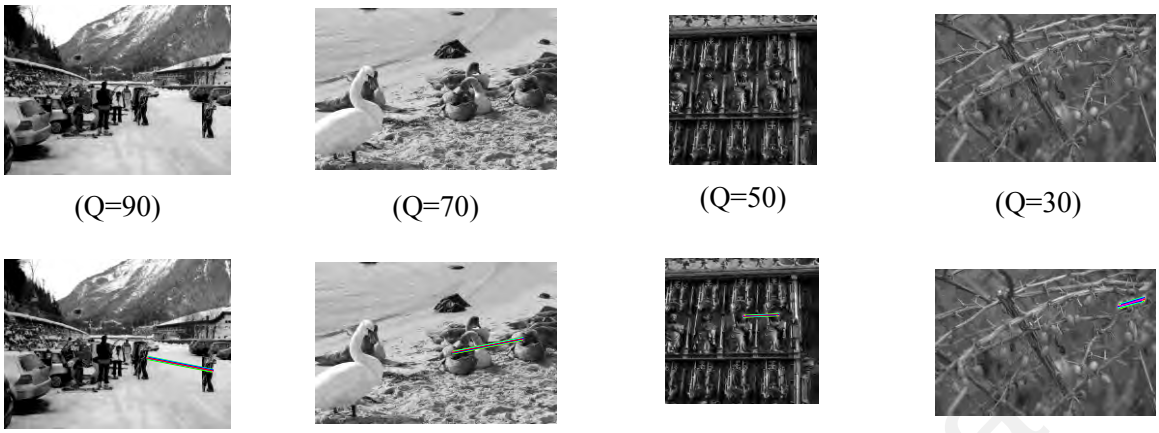


Figure 6.4: The detection results on sample images under different JPEG compression.

Table 6.1: The average detection rate of copy move forgery for JPEG compression based on MICC-F220 .

Operations	Quality factors	90	80	70	60	50
Normal copy move	T_{pr}	0.96	0.90	0.92	0.90	0.90
	F_{pr}	0.06	0.08	0.08	0.10	0.10
Rotation	T_{pr}	0.92	0.92	0.90	0.86	0.80
	F_{pr}	0.08	0.09	0.09	0.1	0.2

II.Additive White Gaussian Noise (AWGN)

The proposed method is tested for robustness to Additive White Gaussian Noise in forged images. The experimental results of our method on the image data sets are shown in Table 6.2. The forged image was invaded by Addition of White Gaussian Noise with different SNRs of 15, 20, 25, 30 and 35 dB. It can be seen that we can locate the duplicate regions very well (see Appendix F).

Table 6.2: The average detection rate of copy move forgery for AWGN on MICC-F220

SNRs (dB)	**35**	**30**	**25**	**20**	**15**
TPR	0.94	0.94	0.96	0.96	0.96
FPR	0.10	0.07	0.07	0.06	0.06

III. Rotation Copy Move Forgery

Often it is necessary to apply a rotation operation to an object before being pasted in order to create convincing forgeries. An example of rotation duplication forgery, as well as the corresponding detection performance, is mentioned in Table 6.3. Figure 6.5 indicates that our algorithm can identify duplicated regions in the cases of different angles of rotation $\left(\theta = 30^{\circ}; 90^{\circ}; 180^{\circ}\right)$. For example in image C the forged region is rotated to 90^{0}, as a result the chain code of duplicated region is circularly shifted 3 times from the original chain code of the copied region. The proposed algorithm finds the total number of circular shifts between matched chain codes of duplicated regions to estimate the rotation angle. See more examples of rotated duplicated regions in (Appendix D).

Table 6.3: The robustness of feature vector under different rotations with estimation of rotation angle.

Image	**Feature Vectors**				**Chain Code**		$\hat{\theta}$
	$Fv_{original}$		$Fv_{postprocessing=rotation}$				
	$Fv_{centroid}$	Fv_{Harris}	$Fv'_{centroid}$	Fv'_{Harris}	C	C'	
A	0.2627	[0.2035 0.2715 0.2556 0.3103 0.3601 0.2984 0.2762 0.2915 …]	0.2575	[0.2552 0.3511 0.2852 0.3285 0.2640 0.2687 0.2468 0.3218 ...]	[221211222222]	[212112222222]	30°

B	0.4525	[0.4445 0.4461 0.4630 0.3921 0.4498 0.4413 0.4099 0.3364…]	0.4308	[0.4340 0.3725 0.3773 0.4117 0.3448 0.3898 0.5114 0.5181 ...]	[112111111211]	[211111121111]	60°
C	0.5845	[0.4823 0.3734 0.4591 0.5906 0.3344 0.4985 0.4306 0.5305 ...]	0.7659	[0.5624 0.6070 0.4253 0.4999 0.4674 0.4236 0.4858 0.4064 ...]	[110011110011]	[011110011110]	90°
D	0.1412	[0.1348 0.2143 0.3836 0.1411 0.5078 0.4310 0.1852 0.2018 …]	0.1443	[0.1170 0.2159 0.1210 0.3742 0.1358 0.4541 0.4186 0.1527 ...]	[222111212211]	[21221122 2111]	180°

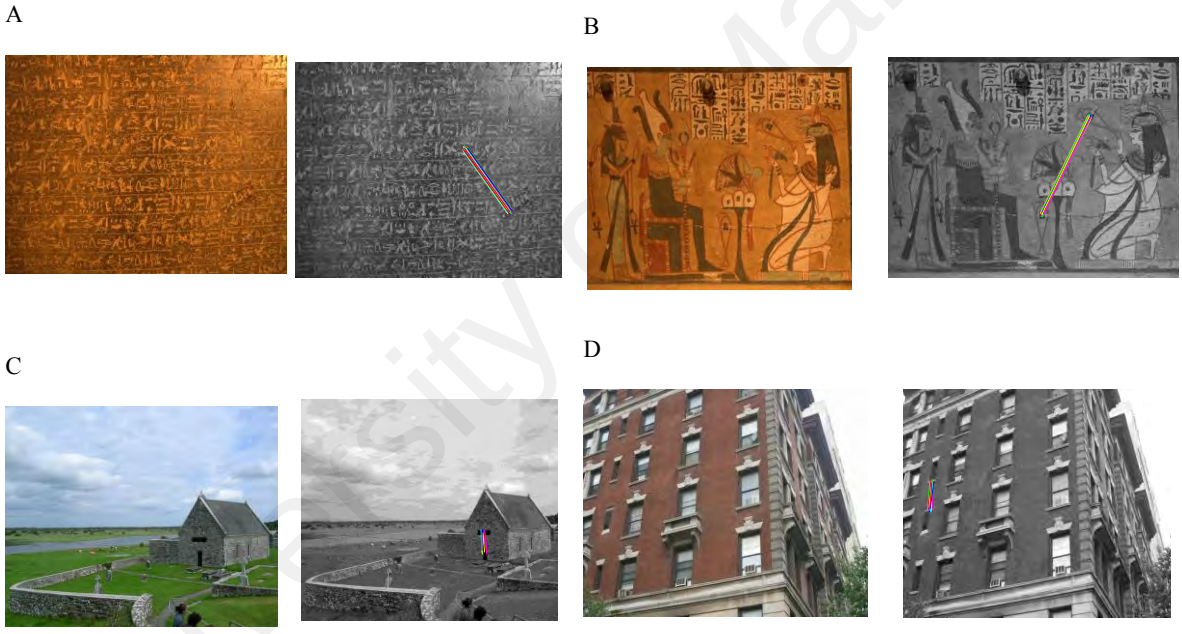
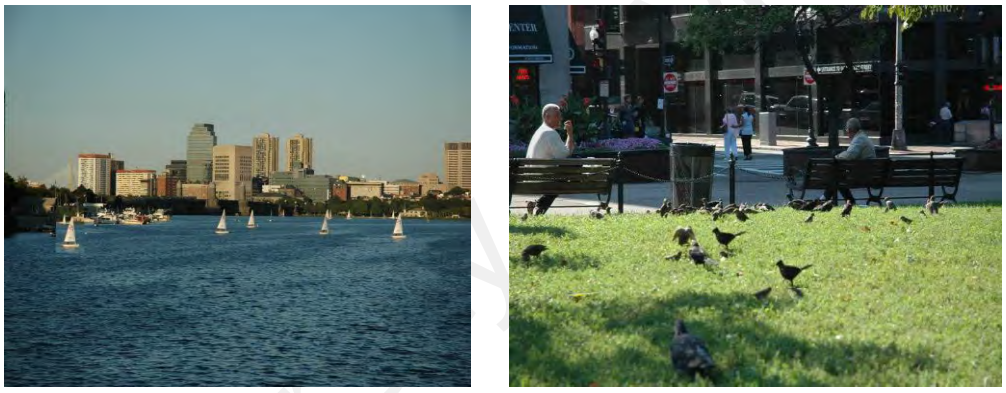


Figure 6.5: Detection results of duplicated regions in the cases of different angles of rotation $(\theta = 30^{\circ}; 90^{\circ}; 180^{\circ})$.

IV. Scaled Copy Move Forgery

To test the robustness of our proposed method for detecting region duplication in the case of scaled duplicated regions, forged regions are scaled up or down with various scaling parameters (s=0.8,0.9,1.1,1.2). One example of visual result is shown in Figure 6.6.

Furthermore, in order to quantitatively evaluate the robustness of our algorithm under different scaling factors, we randomly selected 50 original images from MICC-F220 image dataset (Amerini et al., 2011). For each original image and each duplicate region with a block size 64 x 64 pixels, 96 x 96 pixels and 128 x 128. Pixels, four forged images are created with the scaled up or down duplicated regions by scaling factor s= 0.8, 0.9 1.1 and 1.2. This results in 600 forged images in total, with 50 forged images of one scaling factor for each block size. The detection performances of scaled duplicated regions for each block size are presented in Table 6.4. more examples of scaled duplicated regions detected by our method are shown in (Appendix E).



Scale down with Scaling factor=0.9 Scale up with Scaling factor=1.1

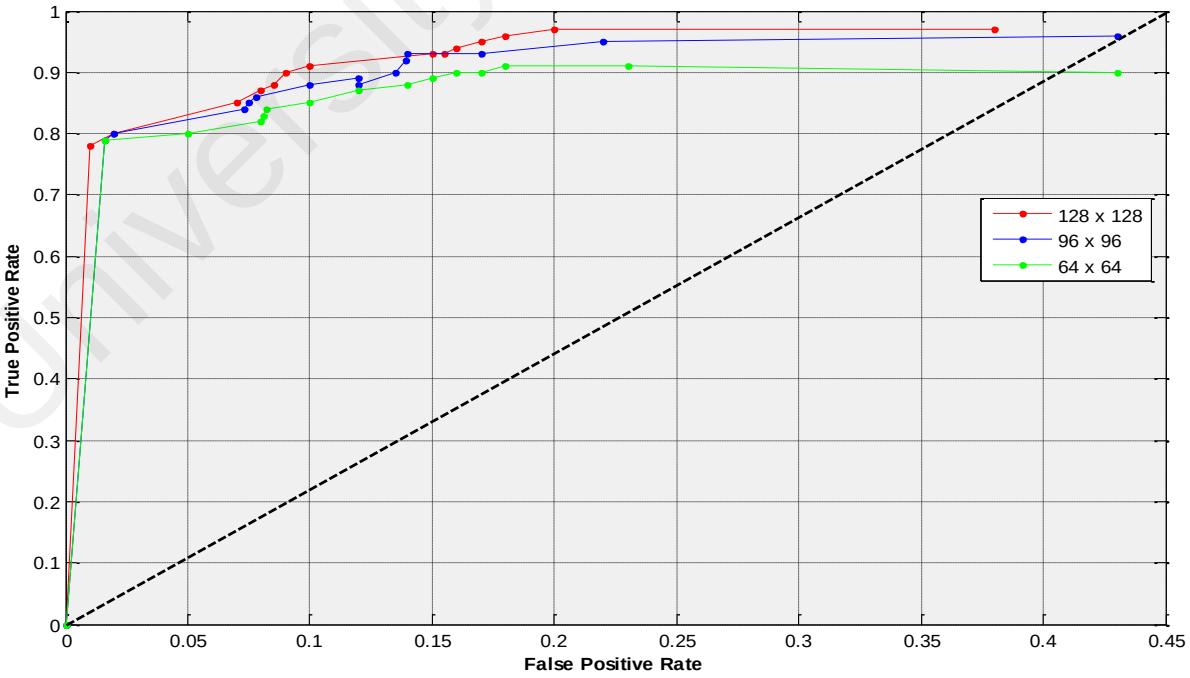
(a) (b)

Figure 6.6: The detection results on sample images (a) and (b) under different scaling factors. Top row: Tampered images; Bottom row: detection results.

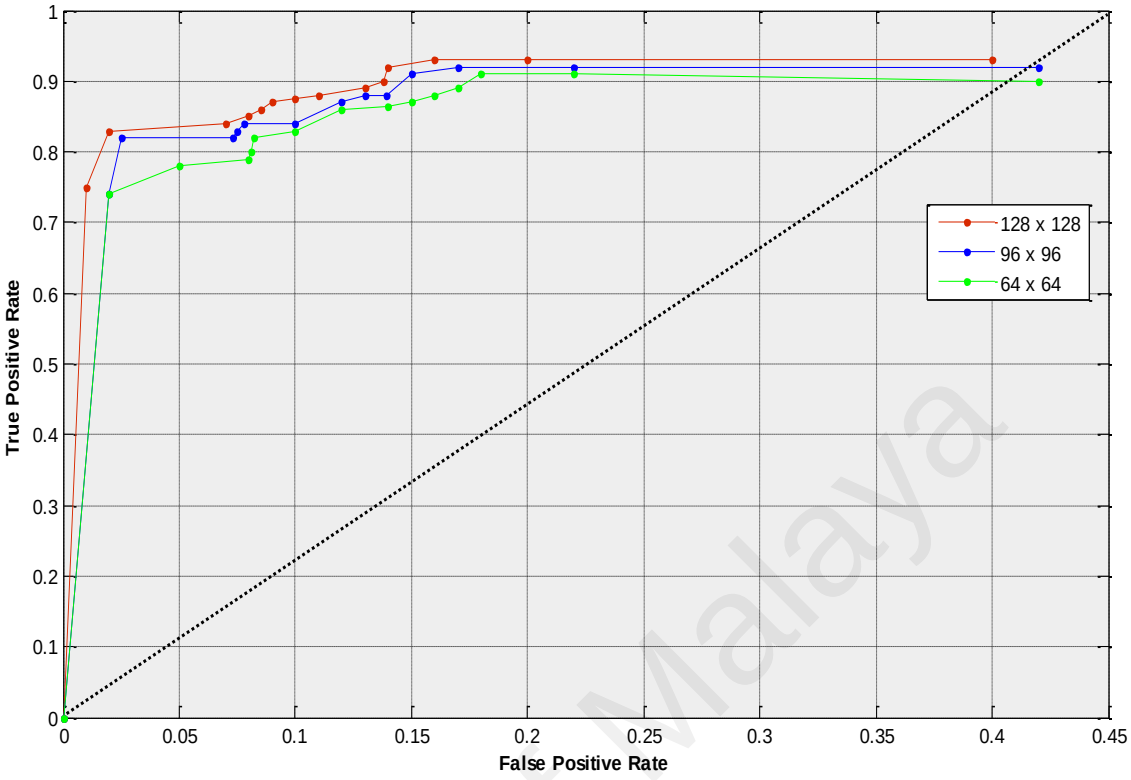
Table 6.4: The detection performance of scaling duplication from 50 forged images on MICC-F220.

Scale	Block size					
	64 x 64		96 x 96		128 x 128	
	T_{PR}	F_{PR}	T_{PR}	F_{PR}	T_{PR}	F_{PR}
0.8	0.90	0.06	0.88	0.07	0.96	0.08
0.9	0.94	0.08	0.96	0.08	0.96	0.08
1.1	0.92	0.08	0.94	0.10	0.92	0.10
1.2	0.92	0.10	0.94	0.10	0.91	0.07

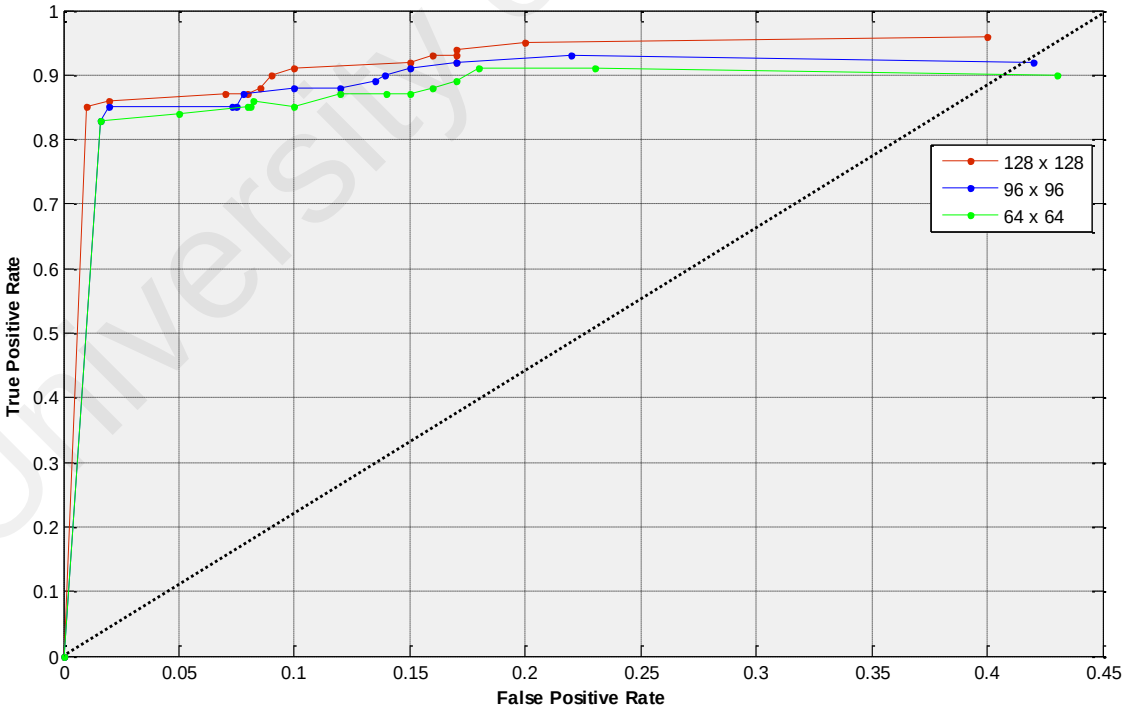
As seen in Figure 6.7, the TPR and FPR rates are combined in a receiver operator characteristics (ROC) curve to show the performance of our method subjected to various kinds of post processing operations and size of duplicated regions. Our method tends to achieve quite high accuracy at low false positive rates with different block sizes of duplicated regions. For block sizes of 96 x 96 and 64 x 64, our method attains a TPR greater than 90% and with FPR around 0.08.



(a) Duplicated region forgery under different block sizes



(b) Rotation attack with different block sizes



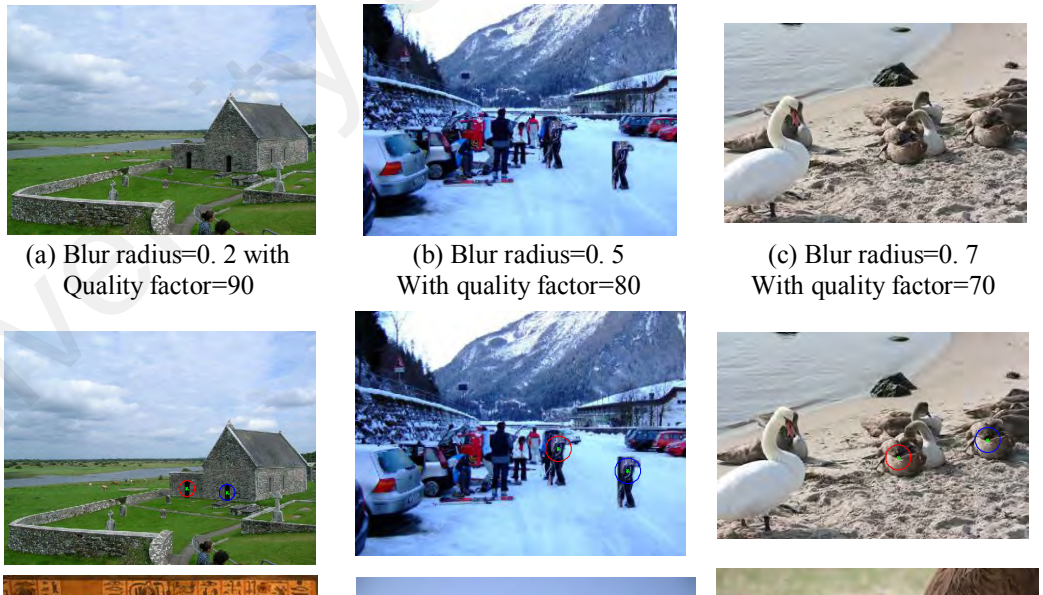
(c) Scaling attack

Figure 6.7: (a-c) ROC curves for different post processing operations and block sizes of duplicate regions.

V. Copy move forgery detection under blurring

Copy–move forgery with a Gaussian blur kernel is performed on every image using Photoshop CS4. The forgery process consists of copying a region in an image, moving it to another location in the same image, and applying the blur tool in the second proposed method to eliminate visual distortion on the duplicated region. The blurring radius is set at [0.2–3] pixels. The parameters of the proposed method are set to T_{sim} = 0.91 (similarity score) and D = 0.3 (threshold of image region distance).

Figure 6.8 shows the detection results of the images forged under a Gaussian blur filter with different radius parameters. The tampered images are saved in JPEG format with various quality factors (Q = 90, 80, 70). The output indicates that the second proposed method can effectively detect blurred duplicate regions under lossy JPEG compression with the increase in Gaussian blur radius.



(a) Blur radius=0. 2 with Quality factor=90

(b) Blur radius=0. 5 With quality factor=80

(c) Blur radius=0. 7 With quality factor=70

(d) Blur radius=0. 9 with Quality factor=90

(e) Blur radius=2 with Quality factor=80

(f) Blur radius=3 with Quality factor=70

Forgery detection

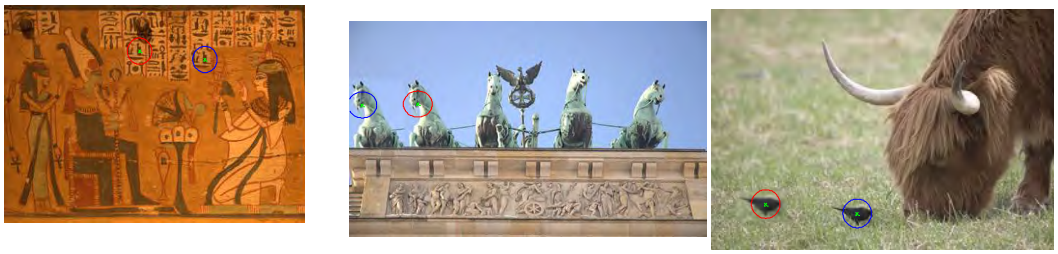
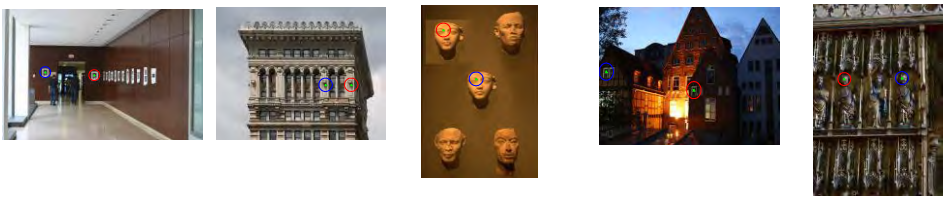


Figure 6.8: Detection results of the copy–move forgery of tampered images (a)–(f) under various Gaussian blurring radii.

Figure 6.9 suggests that forged images A, B, C, D, and E are subject to simple blurring manipulation with different blur radius parameters (0.3, 0.5, 0.9, 2.0, and 3.0). Based on the analysis of blurred duplicate regions in the images mentioned in Table 6.5, we reveal that the blur metric measure increases for the blurred region as the blur radius increases. Moreover, the PCy-based feature vectors in the edge region are blur-invariant features. The feature similarity score based on PCy and GM is robust to blurring.

Table 6.5: Robustness of the proposed method to blurring manipulation.

Forged images	Blur radius	BME of duplicated regions		FSIM	Feature vectors of PCy map	
		$BME_{before\ blur}$	$BME_{after\ blur}$		$Fv_{before\ blur}$	$Fv_{after\ blur}$
A	0.3	0.2301	0.2915	0.9552	[0.2272 0.0139 0.9988]	[0.2508 0.0165 0.9938]
B	0.5	0.2729	0.2735	0.9685	[0.1694 0.0129 1.0000]	[0.1925 0.0132 0.9925]
C	0.9	0.5554	0.5914	0.9648	[0.2350 0.0179 0.9997]	[0.2399 0.0180 0.9991]
D	2	0.2179	0.2325	0.9405	[0.2350 0.0179 0.9997]	[0.2399 0.0180 0.9991]
E	3	0.3569	0.4166	0.9111	[0.2087 0.0275 0.9957]	[0.2159 0.0298 0.9959]



(A) with Blur r=0.3 | (B) with Blur r=0.5 | (C) With blur r=0.9 | (D) With blur r=2 | (E) With blur r=3

Figure 6.9: Detection results of the forged images A–E subject to blurring at various blur radii.

VI. Copy move forgery under Illumination changes

The copied region was moved in the same manner as in the case of translation. And also the intensity of its pixels had changed by the gamma factor in the range [0.5-1.5]. In Figure 6.10, we represent the detection results of the third proposed method in the presence of gamma correction with values 0.5, 1, 1.2 and 1.5. In all these forged images, duplicated regions are localized and a line drawn between two keypoints shows that this interest point matches with each other.

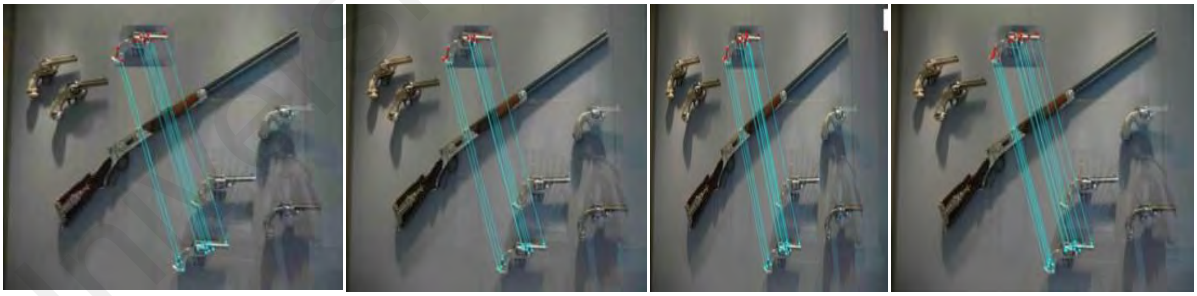
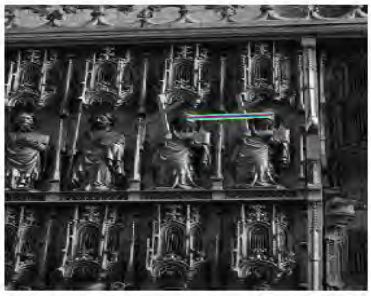


Figure 6.10: Region duplication forgery detection results for: (a) gamma value = 0.5, (b) gamma value = 1, (c) gamma value = 1.2, and (d) gamma value = 1.5.

Another example, in Figure 6.11 illustrates the detection performance for JPEG compression at low quality factors of compression. Furthermore, Figure 6.12 illustrates the detection results of the proposed method for images with block size=8, scaled down with scaling factor=0.9, and for images with block size=16, scaled up with scaling factor=1.1.

JPEG compression(Q=50)

JPEG compression(Q=30)



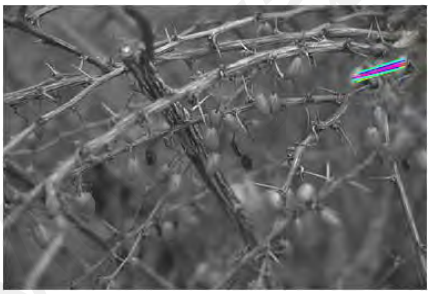


Figure 6.11: Detection performance for JPEG compression.

Non uniform region with block size=8 Scale down with Scaling factor=0.9

A uniform region with block size=16 Scale up with Scaling factor=1.1

(a)

(b)

Figure 6.12: The detection results on sample images (a) and (b) under different scaling factors. First row: Tampered images , second row: Detection results.

6.5 Performance Evaluation

- **Approach 1: Rotation Invariant CMFD Method**

Since our method specifically identify region duplication forgeries that undergo different kinds of post processing operations, we compared our first proposed method with various aspects of the state of the art methods in (Pan & Lyu, 2010), (Amerini et al., 2011). These are typical keypoint based schemes, based on the SIFT keypoints detection and feature matching which is robust to scaling, rotation and some post processing operations including JPEG compression and AWGN. In (Pan & Lyu, 2010), the duplicated region is required to have at least 50 SIFT-keypoints. This is unrealistic in many practical detections since the duplicated region may not guarantee so many SIFT keypoints especially when the copied region exhibits little visual structure. Furthermore, the SIFT method struggle to handle this issue if the copied region exhibits small forgery area, it may happen that the duplicated region is completely missed (Christlein et al., 2012). However, our method performs well in this kind of scenario. The main reason is that our method employs the Harris feature points around centroids of detected objects in image which is superior to SIFT feature points in (Pan & Lyu, 2010), (Amerini et al., 2011). Harris feature points are detected by our rotation invariant CMFD method, where the distribution of feature points is widely divergent around centroids. Consequently, our method can effectively detect the small scaled duplicated regions with visual little structures, such as sky, grass or water area as shown in Figure 6.6 (a). Our method also does not generate any false positives on images containing some repetitive patterns as shown in Figure

6.2 (b). while the method (Pan & Lyu, 2010) gives false matched feature points with no regions detected as forged (Christlein et al., 2012).

In order to compare the performances of our second proposed method with the state of the art, two key approaches were utilized as baselines; keypoint based techniques (Pan & Lyu, 2010) (Amerini et al., 2011) (Kakar & Sudha, 2012) (Mishra et al., 2013) , and block based methods (Popescu & Farid, 2004), (Fridrich et al., 2003). The true positive rates, false positive rates, Precision and Recall are evaluated on the tampered and authentic images from the MICC-F22 and Image data manipulation datasets. As seen from Table 6.6, we achieve a T_{PR} of around 94% and F_{PR} of 7 %. In comparison, Amerini et al. (Amerini et al., 2011) method achieves a T_{PR} of around 100% and F_{PR} of 8 %. Pan and Lyu's method (Pan & Lyu, 2010) achieves a T_{PR} of around 89.96% and F_{PR} of 1.25 %.

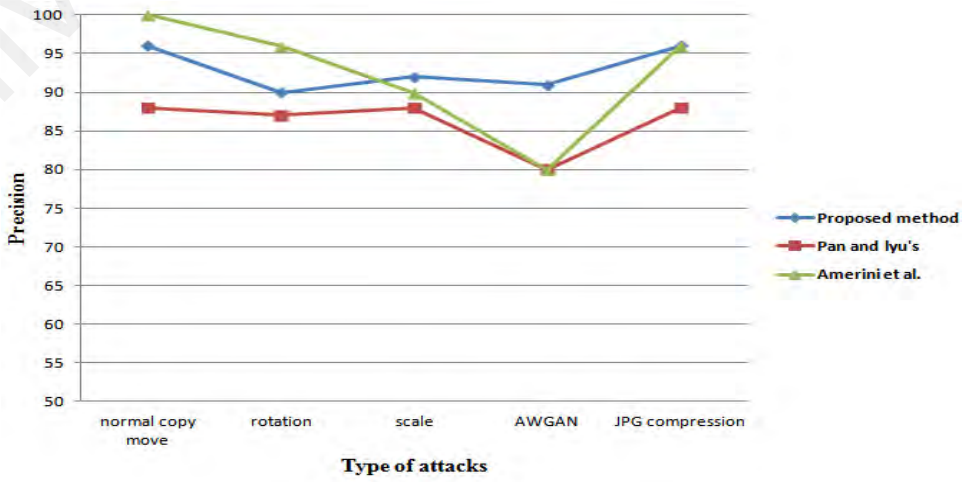
The proposed rotation inavariant CMFD method reduces the false positive rate while still maintaining a high true positive rate, as shown in Table 6.6. Here, we can see that TPR of our method is greator than some keypoint based methods:(Pan & Lyu, 2010), (Kakar & Sudha, 2012) and (Mishra et al., 2013) method. In case of FPR, we reduced the false positives 1% less than (Amerini et al., 2011) method to achieve robustness and reliability of detecting forged images. As seen from Table 6.6, the execution time for block based methods: Fridirch et al. (Fridrich et al., 2003) and Popescu and Farid (Popescu & Farid, 2005) are high compared with keypoint based methods: (Pan & Lyu, 2010), (Amerini et al., 2011), (Mishra et al., 2013) and our method. The time required to detect forgery in our method is faster than Pan and Lyu's method (Pan & Lyu,

2010) and Amerini et al. (Amerini et al., 2011). However, Mishra et al.(Mishra et al., 2013) method is quite faster than our method due to SURF features.

Table 6.6. Average TPR and FPR values in (%) and processing time (sec) for each method compared with rotation invariant CMFD method using MICC-F220 image dataset.

Methods	TPR	FPR	Time
Pan and Lyu's method (Pan & Lyu, 2010)	89.96	1.25	10
Amerini et al. (Amerini et al., 2011)	100	8	4.94
Fridirch et al. (Fridrich et al., 2003)	89	84	294.96
Popescu and Farid (Popescu & Farid, 2004)	87	86	70.97
Kakar et al. (Kakar & Sudha, 2012)	90	3	NA
Mishra et al.(Mishra et al., 2013)	73.64	3.64	2.85
The proposed method	96	2.89	4

Furthermore, precision and recall are evaluated on the tampered and authentic images from the MICC-F220 as shown in Fig. 6.13.



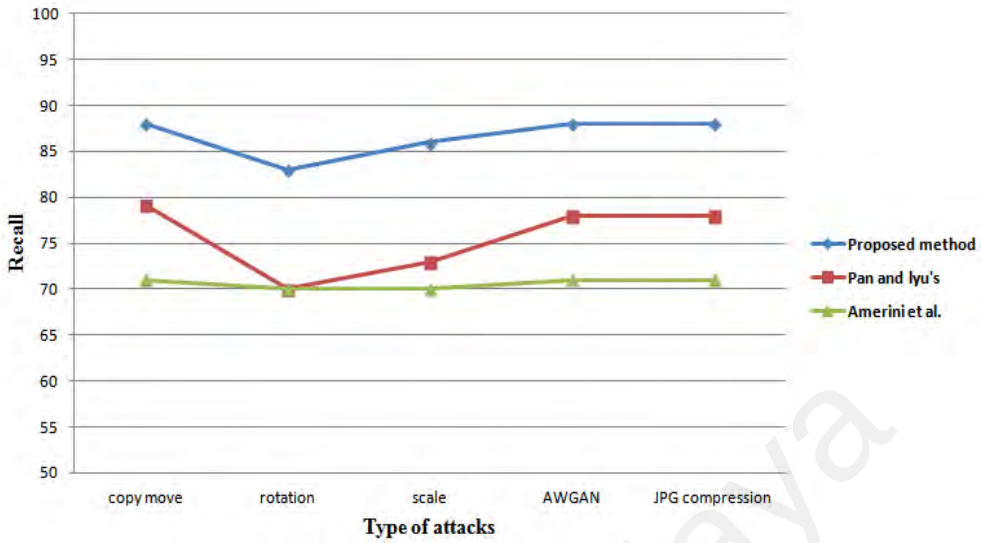


Figure 6.13: Comparison of detection performance in Precision and Recall of the proposed rotation invariant CMFD method, (Pan & Lyu, 2010) method and (Amerini et al., 2011) method .

The Precision and Recall performance of the proposed method were compared to two standard methods Pan and Lyu's (Pan & Lyu, 2010) and Amerini et al (Amerini et al., 2011) as illustrated in Fig. 6.13. The graph indicates that our method has a best performance with precision of more than 90% under most conditions: normal copy move, scale, AWGAN and JPEG compression. Furthermore, for different amount of rotations, our method performs better than Pan and Lyu's method. In the recall rate, our method solved the problem of detecting region duplication forgery with acceptable recall rate of 85% or higher. Among these, the proposed method provides a good balance between precision and recall followed by Amerini et al method.

- **Approach 2: Copy move forgery detection method under blurring**

  The most important issue of practical CMFD application is the capability to recognize both forged and original images. Thus, we adopt the evaluation metric defined in (Christlein et al., 2012) to assess the performance of our proposed

methodology at the image level. The experimental results are listed in Table 6.7. T_{PR} reflects the performance of the detection algorithm in terms of accurately locating the blurred forged region, whereas F_{PR} is the fraction of original images that is erroneously detected. A high T_{PR} (toward 1) and a low F_{PR} (toward 0) indicate good detection performance. According to the results for the two image data sets MICC-F220 and image data manipulation, our method can accurately detect copy–move forgery with blur manipulation.

Table 6.7: Detection results of proposed method for blurred copy–move forgery

Image database	Number of images	Average Detection rate	
		TPR	FPR
MICC-F220 (Amerini et al., 2011).	110	0.963	0.063
Image data manipulation (Christlein et al., 2012).	48	0.958	0.062

The performance of our method is compared with other methods (Amerini et al., 2011; Kakar & Sudha, 2012; Mishra et al., 2013) . Two key approaches are utilized as baselines, namely, block-based method (Kakar & Sudha, 2012) and key point based methods (Amerini et al., 2011; Mishra et al., 2013). Furthermore, the performance of detection methods is measured in terms of TPR and FPR, which are in turn evaluated on the basis of forged and authentic images from MICC-F220 (Amerini et al., 2011). As indicated in Table 6.8, our method reduces FPR which is approximately 6% less than the FPR of Amerini's method (Amerini et al., 2011). We achieve a good detection rate, and TPR value is approximately 96%. This value is reasonably higher than those obtained by Kakar el al. (Kakar & Sudha, 2012), Mishra et al. (Mishra et al., 2013).

Table 6.8: Average TPR and FPR values for each method evaluated on the basis of the MICC-F220 database.

Methods	TPR	FPR
Kakar et al. (Kakar & Sudha, 2012)	90	3
Mishra et al.(Mishra et al., 2013)	73.64	3.64
Amerini et al. (Amerini et al., 2011)	100	8
The proposed blur invariant CMFD method.	96	6

- **Approach 3: Illumination invariant CMFD method**

  Our third proposed method was evaluated with two other methods: one that uses SIFT keypoints (Pan & Lyu, 2010) and one that uses SURF with hierarchical agglomerative clustering (Mishra et al., 2013) . The performance of detection methods is measured in terms of true positive rate (TPR) and false positive rate (FPR). As shown in Table 6.9, our method achieved high TPR value (92%) than those obtained by (Pan & Lyu, 2010), and (Mishra et al., 2013).

Table 6.9: Comparison of the experimental results of Average Detection rate with other standard methods.

Methods	T_{PR}%	F_{PR}%
Pan and Lyu's method (Pan & Lyu, 2010)	89.96	8.8
P. Mishra et.al (Mishra et al., 2013)	73.6	3.64
The proposed illumination invariant CMFD method	92	8

6.6 Summary

Throughout this chapter, the proposed copy-move forgery detection has been examined against several tampering attacks. As the experimental results in this chapter illustrated, the proposed schemes in each algorithm are very effective at detecting and localizing different types of general tampering, such as rotation, scale, blur, illumination changes and JPEG compression attacks. However, the experimental results show that the proposed algorithms improved the false

positive rate and can locate forgery more accurately. The analysis of the proposed algorithm in terms of the false positive rate (FPR) and true positive rate (TPR) clearly verified the efficiency of the tamper localization algorithm. Moreover, the performance analysis and experimental results clearly demonstrated that the proposed schemes outperform other algorithms in terms of detection rate and robustness.

CHAPTER SEVEN

CONCLUSION

7.1 Research findings

With a rapid growth of digital image technology and ease of use in digital image editing tools such as Photoshop, no effort is needed to alter images without leaving any visual traces. Unfortunately, digital images are vulnerable to malicious attacks such as copy move forgery with widespread transmission via Internet. This situation may cause trouble in many occasions; where a large number of forged images distributed in Digital newspapers and TVs. As a result, the public has lost its trust in digital images. Furthermore, we cannot examine the trustworthiness of forged images visually. To tackle this crisis of trust, we proposed a forensic method to detect such forgeries in digital images such as region duplication forgery.

When considering the importance of image authentication and digital image forgeries, effective authentication and detection of duplicated regions in images is both important and essential. Various aspects, such as the size of the image, forgery attacks (rotation, scale, blur, illumination changes, addition of Gaussian noise and JPEG compression) and image types can affect the way image authentication and forgery systems work. Therefore, forgery detection algorithms should be robust against forgery attacks, should work on different images of various types and size, and should be able to detect region duplication forgery in reasonable time.

The main goal of this research is to develop a copy-move forgery detection algorithm to authenticate and accurately detect duplicated regions of a digital image. In this research, we designed, developed, and implemented a robust detection method for copy move forgery

with a high detection rate. The general architecture of the system encompasses different methodologies to cope with the various challenges.

The following discussions demonstrate how these objectives are achieved.

i. To investigate different copy-move forgery detection methods to improve tamper detection rate: This objective has been achieved by investigating several existing copy-move forgery detection methods. Various copy-move detection methods, along with their feature extraction and tamper localization procedures, were analyzed to identify the best method for improving detection rate. The structure of each method is summarized and discussed in chapter 2.

ii. To propose an efficient copy-move forgery detection method that is robust to noise, rotation, scale and JPEG compression: The second objective of this research focuses on presenting an efficient copy-move forgery detection method and providing a step-by-step procedure of the proposed method. The main contribution of this approach is to develop a technique which is able to detect small duplicated regions under copy-move forgery in the presence of malicious and innocent attacks such as addition of noise, rotation, scale and JPEG compression.We detected Harris features inside segmented regions in the image, and feature matching is done by clustering the extracted features using Tamura texture and searching for matched clusters (see Section 4.2).

iii. To propose a new copy-move forgery detection method that is able to detect multiple forgeries: Due to the difficulty in detecting copy-move forgery in case of multiple forgeries, developing a method with the capability of detecting multiple forgeries was the third objective of this thesis. In some cases, one part of the image is copied and pasted in multiple places, making forgery detection more difficult. It is one of the challenges for

copy-move forgery detection algorithms to be able to detect multiple forgeries with different regions size of the digital image.

iv. To test and evaluate the proposed algorithm by measuring detection rate: The last objective is met by carrying out various types of experiments for testing and evaluating the proposed method under different conditions. The experimental results were conducted on two well-known standard datasets (MICC-F220, Image manipulation Dataset) which are used for evaluation of copy-move forgery detection in most research. The performance evaluation of the method is presented in Chapter 6.

The significance of digital image authentication has lately gained much attention due to the everyday use of digital multimedia in different security applications and organizations. Moreover, one of the most important factors of digital image authentication is the accuracy rate of its forgery detection technique. The proposed algorithm in this research presents an image authentication and copy-move forgery detection method with a high detection rate. The proposed algorithm can be used in many commercial and law enforcement applications, especially security organizations which work frequently with digital images, such as immigration departments. In addition, the real-time usage of the proposed algorithm can be expanded for forensics purposes. For example, forensic lawyers and law enforcement officials are required to validate whether digital images submitted as evidence are original or fake. The result of the authentication method proposed by this study is suitable to be used in online applications or highly sensitive applications such as an e-passport, which needs a 95% assurance to validate the integrity of the images stored on passport chips or in smart cards. It is a convenient and quick way to authenticate and locate copy-move areas in images such as exchange contracts, photographs, or identity verification documents (e.g. birth certificate, utility bill, etc.).

7.2 Conclusions

Forged images created with duplicated and distorted regions are visually difficult to detect. An effective and robust forensic method using Harris interest points and Hölder estimation regularity based descriptor (HGP-2) is proposed in this research. We demonstrated the effectiveness and robustness of the proposed method with a series of experiments on realistic forged images with high resolution from two image databases: MICC-F220 and Image data manipulation. The experiment results showed that the first proposed method can detect the small duplicated and multiple regions effectively, and with high accuracy, in the presence of several geometric transformation operations, including (rotation and scaling), image degradations including JPEG compression and additive white Gaussian Noise. The proposed technique can detect rotated regions in multiple of 30 degrees and different rotation angles up to 360 with estimation of rotation angle between duplicated regions. A current limitation of the proposed technique is that it cannot detect the duplicate regions when distorted with blurring and illumination changes. So, involving a blur invariant features and multiresolution local binary pattern descriptor is part of the second research work are explored to improve the technique.

Image forgeries with blurred and duplicated regions are visually difficult to detect. In the second proposed method, we therefore propose a blur forensic scheme to identify forged duplicated regions. Our scheme includes image segmentation based on SRM, blur metric estimation, and feature similarity based on PCy and gradient magnitudes. BME is also applied to locate blurred regions. We analyze image regions using PCy to derive highly informative features, such as edges. Given the inherently blur-invariant feature of the PCy method, blurred copy–move forgeries can be successfully detected at different blur radius parameters. A current limitation of the proposed method is that it must improve its

capability to distinguish regions that are intentionally blurred by Gaussian filtering from regions that are artificially blurred by camera processing and reduce errors in detection rate.

Finally, a passive copy-move image forgery detection using Hessian features and CSLBP is proposed in our research. The combined Hessian points and CSLBP make the features invariant to translation, scale, and illumination. The best TPR and FPR are observed in our proposed method at 92% and 8% respectively.

7.3 Implication of Future Direction

Based on some of the contributions mentioned in the previous sub-chapter, a few guidelines are provided in this section for researchers who are working on copy-move forgery detection. The recommendations are summarized as follows:

• Improving the overall performance of the CMFD method by enhancing detection rate in terms of true positives and false positives of the CMFD method.

• Although the proposed method is able to locate tampered areas accurately, in some cases when there are no keypoints extracted from specific areas, it will not be possible to locate tampered regions. It is desirable for future work to reduce false positive rate and flase negative rate of the proposed method in case the program cannot extract such keypoints.

• Developing methods for detecting other types of forgeries, such as image retouching.

• Enhancing the efficiency of the system in case of very high signal-to noise ratios (SNRs) of white Gaussian noises.

REFERENCES

Abdul Jauwad, S., & Ullah, R. (2011). On Robustness of Multi Fractal Spectrum to Geometric Transformations and Illumination. In A. Abd Manaf, A. Zeki, M. Zamani, S. Chuprat & E. El-Qawasmeh (Eds.), *Informatics Engineering and Information Science* (Vol. 252, pp. 76-95): Springer Berlin Heidelberg.

Akbarpour Sekeh, M., Maarof, M. A., Rohani, M. F., & Mahdian, B. (2013). Efficient image duplicated region detection model using sequential block clustering. *digital investigation, 10*(1), 73-84. doi: 10.1016/j.diin.2013.02.007

Al-Qershi, O. M., & Khoo, B. E. (2013). Passive detection of copy-move forgery in digital images: State-of-the-art. *Forensic science international, 231*(1), 284-295. doi: 10.1016/j.forsciint.2013.05.027

Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., & Serra, G. (2011). A sift-based forensic method for copy–move attack detection and transformation recovery. *Information Forensics and Security, IEEE Transactions on, 6*(3), 1099-1110. doi: 10.1109/TIFS.2011.2129512

Ardizzone, E., Bruno, A., & Mazzola, G. (2010). *Copy-move forgery detection via texture description.* Paper presented at the Proceedings of the 2nd ACM workshop on Multimedia in forensics, security and intelligence, pp. 59-64.

Avidan, S., & Shamir, A. (2007). *Seam carving for content-aware image resizing.* Paper presented at the ACM Transactions on graphics (TOG), pp. 10.

Bao, R., Zhang, T., Tan, F., & Wang, Y. E. (2011). *Semi-fragile watermarking algorithm of color image based on slant transform and channel coding.* Paper presented at the Image and Signal Processing (CISP), 2011 4th International Congress on, pp. 1039-1043.

Battiato, S., Farinella, G. M., Messina, E., & Puglisi, G. (2012). Robust image alignment for tampering detection. *Information Forensics and Security, IEEE Transactions on, 7*(4), 1105-1117. doi: 10.1109/TIFS.2012.2194285

Bay, H., Tuytelaars, T., & Van Gool, L. (2006). Surf: Speeded up robust features *Computer vision–ECCV 2006* (pp. 404-417): Springer.

Bayram, S., Sencar, H. T., & Memon, N. (2008a). Classification of digital camera-models based on demosaicing artifacts. *digital investigation, 5*(1), 49-59.

Bayram, S., Sencar, H. T., & Memon, N. (2008b). *A survey of copy-move forgery detection techniques.* Paper presented at the IEEE Western New York Image Processing Workshop, pp. 538-542.

Bayram, S., Sencar, H. T., & Memon, N. (2009). *An efficient and robust method for detecting copy-move forgery.* Paper presented at the Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on, pp. 1053-1056.

Beaudet, P. R. (1978). *Rotationally invariant image operators.* Paper presented at the International Joint Conference on Pattern Recognition, pp. 583.

Birajdar, G. K., & Mankar, V. H. (2013). Digital image forgery detection using passive techniques: A survey. *digital investigation, 10*(3), 226-245. doi: 10.1016/j.diin.2013.04.007

Bo, X., Junwen, W., Guangjie, L., & Yuewei, D. (2010). *Image copy-move forgery detection based on SURF.* Paper presented at the Multimedia Information Networking and Security (MINES), 2010 International Conference on, pp. 889-892.

Bravo-Solorio, S., & Nandi, A. K. (2009). *Passive forensic method for detecting duplicated regions affected by reflection, rotation and scaling.* Paper presented at the European Signal Processing Conference 17th, pp. 824-828.

Bravo-Solorio, S., & Nandi, A. K. (2011). Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics. *Signal Processing, 91*(8), 1759-1770.

Cao, Y., Gao, T., Fan, L., & Yang, Q. (2012). A robust detection algorithm for copy-move forgery in digital images. *Forensic science international, 214*(1), 33-43. doi: 10.1016/j.forsciint.2011.07.015

Chalechale, A., Mertins, A., & Naghdy, G. (2004). Edge image description using angular radial partitioning. *IEE Proceedings-Vision, Image and Signal Processing, 151*(2), 93-101. doi: 10.1049/ip-vis:20040332

Chang, C.-C., Lin, P.-Y., & Chuang, J.-C. (2007). Fragile watermarking scheme for digital image authentication using pixel difference. *The Imaging Science Journal, 55*(3), 140-147. doi: 10.1179/174313107X165227

Chang, I.-C., & Hsieh, C.-J. (2011). Image Forgery Using An Enhanced Bayesian Matting Algorithm. *Intelligent Automation & Soft Computing, 17*(2), 269-281. doi: 10.1080/10798587.2011.10643148

Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing, 90*(3), 727-752. doi: doi>10.1016/j.sigpro.2009.08.010

Chen, L., Lu, W., Ni, J., Sun, W., & Huang, J. (2013). Region duplication detection based on Harris corner points and step sector statistics. *Journal of Visual Communication and Image Representation, 24*(3), 244-254. doi: 10.1016/j.jvcir.2013.01.008

Chen, M., Fridrich, J., Goljan, M., & Lukáš, J. (2008). Determining image origin and integrity using sensor noise. *Information Forensics and Security, IEEE Transactions on, 3*(1), 74-90.

Chen, Y.-L., & Hsu, C.-T. (2011). Detecting recompression of JPEG images via periodicity analysis of compression artifacts for tampering detection. *Information Forensics and Security, IEEE Transactions on, 6*(2), 396-406. doi: 10.1109/TIFS.2011.2106121

Christlein, V., Riess, C., & Angelopoulou, E. (2010). *On rotation invariance in copy-move forgery detection.* Paper presented at the Information Forensics and Security (WIFS), 2010 IEEE International Workshop on, pp. 1-6.

Christlein, V., Riess, C., Jordan, J., & Angelopoulou, E. (2012). An evaluation of popular copy-move forgery detection approaches. *7*(6), 1841 - 1854 doi: DOI: 10.1109/TIFS.2012.2218597

Crete, F., Dolmiere, T., Ladret, P., & Nicolas, M. (2007). *The blur effect: perception and estimation with a new no-reference perceptual blur metric.* Paper presented at the Electronic Imaging 2007, pp. 64920I-64920I-64911.

Davarzani, R., Yaghmaie, K., Mozaffari, S., & Tapak, M. (2013). Copy-move forgery detection using multiresolution local binary patterns. *Forensic science international, 231*(1), 61-72.

de Carvalho, T. J., Riess, C., Angelopoulou, E., Pedrini, H., & de Rezende Rocha, A. (2013). Exposing digital image forgeries by illumination color classification. *Information Forensics and Security, IEEE Transactions on, 8*(7), 1182-1194.

Devi Mahalakshmi, S., Vijayalakshmi, K., & Priyadharsini, S. (2012). Digital image forgery detection and estimation by exploring basic image manipulations. *digital investigation, 8*(3), 215-225. doi: 10.1016/j.diin.2011.06.004

Fan, B., Wu, F., & Hu, Z. (2012). Rotationally invariant descriptors using intensity order pooling. *Pattern Analysis and Machine Intelligence, IEEE Transactions on, 34*(10), 2031-2045.

Farid, H. (2009). Image forgery detection. *Signal Processing Magazine, IEEE, 26*(2), 16-25. doi: 10.1109/MSP.2008.931079

Franzen, R. (1999). Kodak lossless true color image suite [Online]. Available :http://r0k.us/graphics/kodak/.

Fridrich, A. J., Soukal, B. D., & Lukáš, A. J. (2003). *Detection of copy-move forgery in digital images.* Paper presented at the in Proceedings of Digital Forensic Research Workshop, pp.

Gallagher, A. C. (2005). *Detection of linear and cubic interpolation in JPEG compressed images.* Paper presented at the Computer and Robot Vision, 2005. Proceedings. The 2nd Canadian Conference on, pp. 65-72.

Gharibi, F., RavanJamjah, J., Akhlaghian, F., Azami, B. Z., & Alirezaie, J. (2011). *Robust detection of copy-move forgery using texture features.* Paper presented at the Electrical Engineering (ICEE), 2011 19th Iranian Conference on, pp. 1-4.

Gloe, T., Kirchner, M., Winkler, A., & Böhme, R. (2007). *Can we trust digital image forensics?* Paper presented at the Proceedings of the 15th international conference on Multimedia, pp. 78-86.

Gonzalez, R. C., Woods, R. E., & Masters, B. R. (2009). Digital Image Processing. *Journal of Biomedical Optics, 14*(2), 9901.

Granty, R., Aditya, T., & Madhu, S. (2010). *Survey on passive methods of image tampering detection.* Paper presented at the Communication and Computational Intelligence (INCOCCI), 2010 International Conference on, pp. 431-436.

Guo, X., & Cao, X. (2010). *FIND: A neat flip invariant descriptor.* Paper presented at the Pattern Recognition (ICPR), 2010 20th International Conference on, pp. 515-518.

Guojuan, Z., & Dianji, L. (2011). *An overview of digital watermarking in image forensics.* Paper presented at the Computational Sciences and Optimization (CSO), 2011 Fourth International Joint Conference on, pp. 332-335.

Harris, C., & Stephens, M. (1988). *A combined corner and edge detector.* Paper presented at the Alvey vision conference, pp. 50.

Hsiao, D.-Y., & Pei, S.-C. (2005). *Detecting digital tampering by blur estimation.* Paper presented at the Systematic Approaches to Digital Forensic Engineering, 2005. First International Workshop on, pp. 264-278.

Hsieh, C.-T., & Wu, Y.-K. (2006). *Geometric invariant semi-fragile image watermarking using real symmetric matrix*. Paper presented at the Proceedings of the 5th WSEAS international conference on Signal processing, Istanbul, Turkey. pp. 70-75

Hsieh, C.-T., Wu, Y.-K., & Hung, K.-M. (2006). Geometric invariant semi-fragile image watermarking using real symmetric matrix. *WSEAS Transaction on Signal Processing, 2*(5), 612-618.

Hsu, H.-C., & Wang, M.-S. (2012). *Detection of copy-move forgery image using Gabor descriptor.* Paper presented at the Anti-Counterfeiting, Security and Identification (ASID), 2012 International Conference on, pp. 1-4.

Huang, D.-Y., Lin, T.-W., Hu, W.-C., & Chou, C.-H. (2014). Boosting Scheme for Detecting Region Duplication Forgery in Digital Images *Genetic and Evolutionary Computing* (pp. 125-133): Springer.

Huang, H., Guo, W., & Zhang, Y. (2008). *Detection of copy-move forgery in digital images using SIFT algorithm.* Paper presented at the Computational Intelligence and Industrial Application, 2008. PACIIA'08. Pacific-Asia Workshop on, pp. 272-276.

Huo, Y., He, H., & Chen, F. (2013). A semi-fragile image watermarking algorithm with two-stage detection. *Multimedia Tools and Applications*, 1-27. doi: 10.1007/s11042-012-1317-4

Hussain, M., Muhammad, G., Saleh, S. Q., Mirza, A. M., & Bebis, G. (2012, 25-29 Nov. 2012). *Copy-Move Image Forgery Detection Using Multi-Resolution Weber Descriptors.* Paper presented at the Signal Image Technology and Internet Based Systems (SITIS), 2012 Eighth International Conference on, pp. 395-401.

Jian, L., Xiaolong, L., Bin, Y., & Xingming, S. (2015). Segmentation-Based Image Copy-Move Forgery Detection Scheme. *Information Forensics and Security, IEEE Transactions on, 10*(3), 507-518. doi: 10.1109/TIFS.2014.2381872

Johnson, M. K., & Farid, H. (2005). *Exposing digital forgeries by detecting inconsistencies in lighting.* Paper presented at the Proceedings of the 7th workshop on Multimedia and security, pp. 1-10.

Johnson, M. K., & Farid, H. (2008). Detecting photographic composites of people *Digital Watermarking* (pp. 19-33): Springer.

Kakar, P., & Sudha, N. (2012). Exposing Postprocessed Copy–Paste Forgeries Through Transform-Invariant Features. *Information Forensics and Security, IEEE Transactions on, 7*(3), 1018-1028. doi: 10.1109/TIFS.2012.2188390

Kang, X., & Wei, S. (2008). *Identifying tampered regions using singular value decomposition in digital image forensics.* Paper presented at the Computer Science and Software Engineering, 2008 International Conference on, pp. 926-930.

Koenderink, J. J. (1984). The structure of images. *Biological cybernetics, 50*(5), 363-370.

Kovesi, P. (2003). *Phase congruency detects corners and edges.* Paper presented at the The australian pattern recognition society conference: DICTA 2003, pp.

Leutenegger, S., Chli, M., & Siegwart, R. Y. (2011). *BRISK: Binary robust invariant scalable keypoints.* Paper presented at the Computer Vision (ICCV), 2011 IEEE International Conference on, pp. 2548-2555.

Leys, C., Ley, C., Klein, O., Bernard, P., & Licata, L. (2013). Detecting outliers: Do not use standard deviation around the mean, use absolute deviation around the median. *Journal of Experimental Social Psychology, 49*(4), 764-766. doi: DOI: 10.1016/j.jesp.2013.03.013

Li, B., He, J., Huang, J., & Shi, Y. Q. (2011). A survey on image steganography and steganalysis. *Journal of Information Hiding and Multimedia Signal Processing, 2*(2), 142-172.

Li, C.-T. (2010). Source camera identification using enhanced sensor pattern noise. *Information Forensics and Security, IEEE Transactions on, 5*(2), 280-287. doi: DOI:10.1109/TIFS.2010.2046268

Li, G., Wu, Q., Tu, D., & Sun, S. (2007). *A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD.* Paper presented at the Multimedia and Expo, 2007 IEEE International Conference on, pp. 1750-1753.

Li, J., & Allinson, N. M. (2008). A comprehensive review of current local features for computer vision. *Neurocomputing, 71*(10), 1771-1787.

Li, L., Li, S., Zhu, H., & Wu, X. (2013). Detecting copy-move forgery under affine transforms for image forensics. *Computers & Electrical Engineering, 40*(6), 1951–1962. doi: 10.1016/j.compeleceng.2013.11.034

Li, Y. (2012). Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching. *Forensic science international, 224*(1-3), 59–67. doi: 10.1016/j.forsciint.2012.10.031

Lin, H.-J., Wang, C.-W., & Kao, Y.-T. (2009). Fast copy-move forgery detection. *WSEAS Trans. Sig. Proc., 5*(5), 188-197.

Lin, S. D., & Wu, T. (2011). *An integrated technique for splicing and copy-move forgery image detection.* Paper presented at the Image and Signal Processing (CISP), 2011 4th International Congress on, pp. 1086-1090.

Lindeberg, T. (1994). Scale-space theory: A basic tool for analyzing structures at different scales. *Journal of applied statistics, 21*(1-2), 225-270.

Ling, H., Wang, L., Zou, F., & Yan, W. (2011). Fine-search for image copy detection based on local affine-invariant descriptor and spatial dependent matching. *Multimedia Tools and Applications, 52*(2-3), 551-568.

Liu, G., Wang, J., Lian, S., & Dai, Y. (2013). Detect image splicing with artificial blurred boundary. *Mathematical and Computer Modelling, 57*(11), 2647-2659.

Liu, G., Wang, J., Lian, S., & Wang, Z. (2011). A passive image authentication scheme for detecting region-duplication forgery with rotation. *Journal of Network and Computer Applications, 34*(5), 1557-1565. doi: 10.1016/j.jnca.2010.09.001

Lowe, D. G. (1999). *Object recognition from local scale-invariant features.* Paper presented at the Computer vision, 1999. The proceedings of the seventh IEEE international conference on, pp. 1150-1157.

Lowe, D. G. (2004). Distinctive image features from scale-invariant keypoints. *International journal of computer vision, 60*(2), 91-110.

Luo, W., Huang, J., & Qiu, G. (2006). *Robust detection of region-duplication forgery in digital image.* Paper presented at the Pattern Recognition, 2006. ICPR 2006. 18th International Conference on, pp. 746-749.

Luo, W., Qu, Z., Huang, J., & Qiu, G. (2007). *A novel method for detecting cropped and recompressed image block.* Paper presented at the Acoustics, Speech and Signal Processing, 2007. ICASSP 2007. IEEE International Conference on, pp. II-217-II-220.

Luo, W., Qu, Z., Pan, F., & Huang, J. (2007). A survey of passive technology for digital image forensics. *Frontiers of Computer Science in China, 1*(2), 166-179.

Luo, X.-Y., Wang, D.-S., Wang, P., & Liu, F.-L. (2008). A review on blind detection for image steganography. *Signal Processing, 88*(9), 2138-2157.

Mahdian, B., & Saic, S. (2007). Detection of copy–move forgery using a method based on blur moment invariants. *Forensic science international, 171*(2), 180-189.

Mahdian, B., & Saic, S. (2008). Blind authentication using periodic properties of interpolation. *Information Forensics and Security, IEEE Transactions on, 3*(3), 529-538. doi: DOI: 10.1109/TIFS.2004.924603

Mahdian, B., & Saic, S. (2009). Using noise inconsistencies for blind image forensics. *Image and Vision Computing, 27*(10), 1497-1503. doi: doi:10.1016/j.imavis.2009.02.001

Mahdian, B., & Saic, S. (2010). A bibliography on blind methods for identifying image forgery. *Signal Processing: Image Communication, 25*(6), 389-399. doi: doi>10.1016/j.image.2010.05.003

Mikolajczyk, K., & Schmid, C. (2004). Scale & affine invariant interest point detectors. *International journal of computer vision, 60*(1), 63-86.

Mikolajczyk, K., & Schmid, C. (2005). A performance evaluation of local descriptors. *Pattern Analysis and Machine Intelligence, IEEE Transactions on, 27*(10), 1615-1630.

Mikolajczyk, K., Tuytelaars, T., Schmid, C., Zisserman, A., Matas, J., Schaffalitzky, F., Kadir, T., et al. (2005). A comparison of affine region detectors. *International journal of computer vision, 65*(1-2), 43-72. doi: DOI: 10.1007/s11263-005-3848-x

Mishra, P., Mishra, N., Sharma, S., & Patel, R. (2013). Region Duplication Forgery Detection Technique Based on SURF and HAC. *The Scientific World Journal, 2013*. doi: http://dx.doi.org/10.1155/2013/267691

Mokhtarian, F., & Suomela, R. (1998). Robust image corner detection through curvature scale space. *Pattern Analysis and Machine Intelligence, IEEE Transactions on, 20*(12), 1376-1381. doi: DOI:10.1109/34.735812

Muhammad, G., Hussain, M., & Bebis, G. (2012). Passive copy move image forgery detection using undecimated dyadic wavelet transform. *digital investigation, 9*(1), 49-57. doi: doi:10.1016/j.diin.2012.04.004

Muhammad, N., Hussain, M., Muhamad, G., & Bebis, G. (2011). A non-intrusive method for copy-move forgery detection *Advances in Visual Computing* (pp. 516-525): Springer.

Nathalie Diane, W. N., Xingming, S., & Moise, F. K. (2014). A Survey of Partition-Based Techniques for Copy-Move Forgery Detection. *The Scientific World Journal, 2014*.

Ng, T.-T., Chang, S.-F., Hsu, J., & Pepeljugoski, M. (2005). Columbia photographic images and photorealistic computer graphics dataset.

Nguyen, H. C., & Katzenbeisser, S. (2011). *Security of copy-move forgery detection techniques.* Paper presented at the Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on, pp. 1864-1867.

Nielsen, F., & Nock, R. (2003). *On region merging: The statistical soundness of fast sorting, with applications.* Paper presented at the Computer Vision and Pattern Recognition, 2003. Proceedings. 2003 IEEE Computer Society Conference on, pp. II-19-26 vol. 12.

Nock, R., & Nielsen, F. (2004). Statistical region merging. *Pattern Analysis and Machine Intelligence, IEEE Transactions on, 26*(11), 1452-1458. doi: DOI:10.1109/TPAMI.2004.110

Pan, X., & Lyu, S. (2010). Region duplication detection using image feature matching. *Information Forensics and Security, IEEE Transactions on, 5*(4), 857-867. doi: 10.1109/TIFS.2010.2078506

Pandey, R., Agrawal, R., Singh, S., & Shukla, K. K. (2015). Passive Copy Move Forgery Detection Using SURF, HOG and SIFT Features. In S. C. Satapathy, B. N. Biswal, S. K. Udgata & J. K. Mandal (Eds.), *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014* (Vol. 327, pp. 659-666): Springer International Publishing.

Peng, F., Nie, Y.-y., & Long, M. (2011). A complete passive blind image copy-move forensics scheme based on compound statistics features. *Forensic science international, 212*(1), e21-e25.

Piva, A. (2013). An Overview on Image Forensics. *ISRN Signal Processing, 2013*. doi: DOI: http://dx.doi.org/10.1155/2013/496701

Poisel, R., & Tjoa, S. (2011). *Forensics investigations of multimedia data: A review of the state-of-the-art.* Paper presented at the IT Security Incident Management and IT Forensics (IMF), 2011 Sixth International Conference on, pp. 48-61.

Popescu, A. C., & Farid, H. (2004). Exposing digital forgeries by detecting duplicated image regions. *Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515*. doi: doi=10.1.1.136.2374

Popescu, A. C., & Farid, H. (2005). Exposing digital forgeries in color filter array interpolated images. *Signal Processing, IEEE Transactions on, 53*(10), 3948-3959.

Quan, X., & Zhang, H. (2012). *Copy-move forgery detection in digital images based on local dimension estimation.* Paper presented at the Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on, pp. 180-185.

Rawat, S., & Raman, B. (2011). A chaotic system based fragile watermarking scheme for image tamper detection. *AEU-International Journal of Electronics and Communications, 65*(10), 840-847. doi: DOI: 10.1016/j.aeue.2011.01.016

Redi, J. A., Taktak, W., & Dugelay, J.-L. (2011). Digital image forensics: a booklet for beginners. *Multimedia Tools and Applications, 51*(1), 133-162. doi: 10.1007/s11042-010-0620-1

Rokach, L., & Maimon, O. (2005). Clustering methods *Data mining and knowledge discovery handbook* (pp. 321-352): Springer.

Ryu, S.-J., Kirchner, M., Lee, M.-J., & Lee, H.-K. (2013). Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments. *Information Forensics and Security, IEEE Transactions on, 8*(8), 1355-1370. doi: 10.1109/TIFS.2013.2272377

Ryu, S.-J., Lee, M.-J., & Lee, H.-K. (2010). *Detection of copy-rotate-move forgery using Zernike moments.* Paper presented at the Information Hiding, pp. 51-65.

Sencar, H. T., & Memon, N. D. (2013). *Digital Image Forensics: There is More to a Picture Than Meets the Eye*: Springer.

Shan, Q., Jia, J., & Agarwala, A. (2008). *High-quality motion deblurring from a single image.* Paper presented at the ACM Transactions on Graphics (TOG), pp. 73.

Shao, H., Yu, T., Xu, M., & Cui, W. (2012). Image region duplication detection based on circular window expansion and phase correlation. *Forensic science international, 222*(1), 71-82. doi: 10.1016/j.forsciint.2012.05.002

Sheng, G., Gao, T., Cao, Y., Gao, L., & Fan, L. (2012). Robust algorithm for detection of copy-move forgery in digital images based on ridgelet transform *Artificial Intelligence and Computational Intelligence* (pp. 317-323): Springer.

Sheng, Y., Wang, H., & Zhang, G. (2013). Comparison and Analysis of Copy-Move Forgery Detection Algorithms for Electronic Image Processing *Advances in Mechanical and Electronic Engineering* (Vol. 178, pp. 343-348): Springer.

Shi, J., & Malik, J. (2000). Normalized cuts and image segmentation. *Pattern Analysis and Machine Intelligence, IEEE Transactions on, 22*(8), 888-905.

Shivakumar, B., & Santhosh Baboo, L. D. S. (2010). Detecting copy-move forgery in digital images: a survey and analysis of current methods. *Global Journal of Computer Science and Technology, 10*(7).

Singh, C., & Ranade, S. K. (2013). Geometrically invariant and high capacity image watermarking scheme using accurate radial transform. *Optics & Laser Technology, 54*, 176-184. doi: DOI: 10.1016/j.optlastec.2013.05.016

Solomon, C., & Breckon, T. (2011). *Fundamentals of Digital Image Processing: A practical approach with examples in Matlab*: John Wiley & Sons.

Su, B., Lu, S., & Tan, C. L. (2011). *Blurred image region detection and classification.* Paper presented at the Proceedings of the 19th ACM international conference on Multimedia, pp. 1397-1400.

Sutthiwan, P., & Shi, Y. Q. (2012). Anti-Forensics of double JPEG compression detection *Digital Forensics and Watermarking* (pp. 411-424): Springer.

Szeliski, R. (2011). *Computer vision: algorithms and applications*: Springer.

Tamura, H., Mori, S., & Yamawaki, T. (1978). Textural features corresponding to visual perception. *Systems, Man and Cybernetics, IEEE Transactions on, 8*(6), 460-473. doi: DOI:10.1109/TSMC.1978.4309999

Trujillo, L., Legrand, P., Olague, G., & Lévy-Véhel, J. (2012). Evolving estimators of the pointwise Hölder exponent with Genetic Programming. *Information Sciences, 209*, 61-79. doi: doi>10.1016/j.ins.2012.04.043

Van Lanh, T., Chong, K.-S., Emmanuel, S., & Kankanhalli, M. S. (2007). *A survey on digital camera image forensic methods.* Paper presented at the Multimedia and Expo, 2007 IEEE International Conference on, pp. 16-19.

Wang, J., Liu, G., Li, H., Dai, Y., & Wang, Z. (2009). *Detection of image region duplication forgery using model with circle block.* Paper presented at the Multimedia Information Networking and Security, 2009. MINES'09. International Conference on, pp. 25-29.

Wang, J., Liu, G., Xu, B., Li, H., Dai, Y., & Wang, Z. (2010). *Image Forgery Forensics Based on Manual Blurred Edge Detection.* Paper presented at the Multimedia Information Networking and Security (MINES), 2010 International Conference on, pp. 907-911.

Wang, T., Tang, J., & Luo, B. (2013). *Blind Detection of Region Duplication Forgery by Merging Blur and Affine Moment Invariants.* Paper presented at the Image and Graphics (ICIG), 2013 Seventh International Conference on, pp. 258-264.

Wang, W., Dong, J., & Tan, T. (2009). A survey of passive image tampering detection *Digital Watermarking* (pp. 308-322): Springer.

Wang, Z., Fan, B., & Wu, F. (2011). *Local intensity order pattern for feature description.* Paper presented at the Computer Vision (ICCV), 2011 IEEE International Conference on, pp. 603-610.

Wu, Q., Wang, S., & Zhang, X. (2011). Log-Polar Based Scheme for Revealing Duplicated Regions in Digital Images. *Signal Processing Letters, IEEE, 18*(10), 559-562.

Xiao, R., Yang, G., Yin, Y., & Yang, L. (2013). Modified Binary Pattern for Finger Vein Recognition *Biometric Recognition* (pp. 258-265): Springer.

Yang, Z.-C., & Li, Z.-H. (2012). *An Anti-JPEG Compression Digital Watermarking Technology with an Ability in Detecting Forgery Region for Color Images.* Paper presented at the Computer Distributed Control and Intelligent Environmental Monitoring (CDCIEM), 2012 International Conference on, pp. 93-97.

Ye, S., Sun, Q., & Chang, E.-C. (2007). *Detecting digital image forgeries by measuring inconsistencies of blocking artifact.* Paper presented at the Multimedia and Expo, 2007 IEEE International Conference on, pp. 12-15.

Yerushalmy, I., & Hel-Or, H. (2011). Digital image forgery detection based on lens and sensor aberration. *International journal of computer vision, 92*(1), 71-91.

Zhang, L., Zhang, D., & Mou, X. (2011). FSIM: a feature similarity index for image quality assessment. *Image Processing, IEEE Transactions on, 20*(8), 2378-2386.

Zhang, L., & Zhou, P.-P. (2010). Localized affine transform resistant watermarking in region-of-interest. *Telecommunication Systems, 44*(3-4), 205-220. doi: DOI: 10.1007/s11235-009-9260-z

Zheng, J., & Liu, M. (2009). A digital forgery image detection algorithm based on wavelet homomorphic filtering *Digital Watermarking* (pp. 152-160): Springer.

Zheng, L., Lei, Y., Qiu, G., & Huang, J. (2012). Near-duplicate image detection in a visually salient riemannian space. *Information Forensics and Security, IEEE Transactions on, 7*(5), 1578-1593.

Zhou, L., Wang, D., Guo, Y., & Zhang, J. (2007). Blur detection of digital forgery using mathematical morphology *Agent and Multi-Agent Systems: Technologies and Applications* (pp. 990-998): Springer.

Zimba, M., & Xingming, S. (2011). DWT-PCA(EVD) Based Copy-move Image Forgery Detection. *International Journal of Digital Content Technology and its Applications, 5*(1). doi: doi:10.4156/jdcta.vol5.issue1.27