IMAGE MANIPULATIONS ANALYSIS AND DETECTION METHODS FOR REFLECTION-BASED ATTACKS

NOR BAKIAH BINTI ABD. WARIF

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

2018

IMAGE MANIPULATIONS ANALYSIS AND DETECTION METHODS FOR REFLECTION-BASED ATTACKS

NOR BAKIAH BINTI ABD. WARIF

THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

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

2018

UNIVERSITY OF MALAYA

ORIGINAL LITERARY WORK DECLARATION

Name of Candidate: NOR BAKIAH BINTI ABD. WARIF

Matric No: WHA 140006

Name of Degree: DOCTOR OF PHILOSOPHY

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

Image Manipulations Analysis and Detection Methods for Reflection-Based Attacks

Field of Study: COMPUTER SCIENCE – DIGITAL FORENSIC

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 rights in the copyright to this Work to the University of Malaya ("UM"), who henceforth shall be 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

The extensive use of digital images at this age has led to the content manipulations that misrepresent the information with malicious intent. This issue demands the requirement of digital image investigation to verify the sources and validate trustworthiness. One of the image manipulation techniques is called copy-move forgery (CMF). It is a process of duplicating one or more regions in an image before being pasted to another location within the same image. The CMF is mainly comprised of translation attacks and commonly combined with other attacks, such as scaling, rotation, compression and Gaussian noise addition. In this thesis, the research is divided into two stages. The first stage looks into the performance analysis of the existing CMF detection methods, while the second stage focuses on proposing detection methods for reflection-based attacks in CMF. At present, CMF detection performance is evaluated, either through image-level evaluation, pixel-level evaluation, or both. Since there is no evaluation standard, the analysis also studies the effects of these evaluations towards the result interpretation. The study shows that both image and pixel-level evaluations are dependent, therefore, must be incorporated together to ensure fair evaluation. These evaluations are then applied to study the effects of reflection-based attacks in the second stage of research. Methods called SIFT-Symmetry and CMF-iteMS are proposed to alleviate the reflection-based problems in CMF. The SIFT-Symmetry incorporates symmetry matching in a keypoint-based CMF detection while the CMF-iteMS uses a block-based approach that includes iterative means of region size. To evaluate the performance of the two proposed methods, they are compared with state-of-the-arts methods, based on keypoint, block, and a combination of both approaches. The evaluations involve CombineTranslation, CPHALL, NB-Casia, and NBr-Casia datasets which include translation, scale, rotation, and reflection attacks. The results are measured using multiple F-score values which are for image, pixel, and both, image and pixel. The image score shows the ability of the detection methods in distinguishing the original image and CMF image, while the pixel score defines the reliability of determining the exact location of the CMF detection. Both scores are multiplied to get the overall percentages of the detection. The CMF-iteMS surpassed the minimum value of 96% for image score and 88% for both pixel score and percentages of detection for simple translation attacks, while having maintained the highest percentages for rotation, simple reflection, and a mix of attacks with the minimum value of 87%, 76%, and 62%, respectively. In terms of reflection-based CMF, the CMF-iteMS achieved the highest percentages in all reflection cases even if the reflection is combined with scale attacks. Alternatively, the SIFT-Symmetry obtained the highest image score with a value of 94% for simple reflection and 75% for reflection with scale attacks. Moreover, the results also proved that the combination of the existing CMF detection methods with the iterative means of region size increases the performance of the block-based approach. The combination with other approaches, on the other hand, is able to reduce the spurious matching even though the percentages of both image and pixel-levels are dropped.

ABSTRAK

Penggunaan imej digital yang meluas pada era ini telah membawa kepada aktiviti memanipulasi kandungan imej untuk memberi maklumat yang salah di samping tujuan yang tidak baik. Isu ini menjadikan penyiasatan imej digital amat diperlukan untuk mengesahkan kebolehpercayaan dan sumber imej tersebut. Salah satu teknik untuk memanipulasi imej dikenali sebagai *copy-move forgery* (CMF). CMF ialah satu proses menyalin satu atau lebih kawasan di dalam satu imej dan menampal kawasan tersebut di tempat yang berbeza di dalam imej yang sama. Teknik ini mengandungi sekurang-kurangnya operasi gerakan dan kebiasaannya digabungkan dengan operasi yang lain seperti pembesaran, pemusingan, pemampatan dan penambahan gangguan Gaussan. Di dalam tesis ini, kajian dibahagikan kepada dua peringkat. Peringkat pertama melibatkan analisis prestasi kaedah pengesanan CMF yang sedia ada. Manakala peringkat kedua memberi penumpuan kepada cadangan kaedah pengesanan CMF yang mengandungi operasi pemantulan. Pada ketika ini, prestasi kaedah pengesanan CMF dinilai melalui penilaian tahap imej, penilaian tahap piksel, atau keduanya. Oleh kerana tiada penyeragaman di dalam teknik penilaian tersebut, analisis dijalankan untuk menguji kesan teknik-teknik penilaian ini kepada tafsiran keputusan. Analisis menunjukkan bahawa penilaian tahap imej dan piksel memerlukan antara satu sama lain, dan perlu digabungkan bersama untuk memastikan penilaian yang adil. Kedua-dua tahap penilaian ini digunakan untuk mengkaji kesan operasi pemantulan di peringkat kedua kajian. Kaedah yang diberi nama SIFT-Symmetry dan CMF-iteMS dicadangkan untuk mengatasi masalah operasi pemantulan di dalam CMF. SIFT-Symmetry menggabungkan teknik padanan simetri di dalam kaedah pengesanan CMF berasaskan pendekatan *keypoints*. Manakala CMF-iteMS menggunakan kaedah berasaskan pendekatan blok yang mengandungi proses pengulangan purata saiz kawasan. Untuk menilai prestasi kedua-dua kaedah yang dicadangkan, kaedah-kaedah tersebut dibandingkan dengan kaedah pengesanan CMF yang sedia ada berasaskan *keypoints*, blok, dan gabungan keduanya. Penilaian ini juga melibatkan empat set data CMF iaitu CombineTranslation, CPHALL, NB-Casia, dan NBr-Casia yang mengandungi imej CMF dengan operasi gerakan, pembesaran, pemusingan dan pemantulan. Keputusan penilaian diukur menggunakan pelbagai nilai F-skor yang terdiri daripada skor imej, skor piksel, dan kedua-dua skor. Skor imej menunjukkan keupayaan kaedah pengesanan dalam membezakan imej asal dan imej CMF. Skor piksel pula memberi maksud kebolehpercayaan tentang ketepatan lokasi pengesanan kawasan CMF. Kedua-dua skor didarabkan untuk mendapat keseluruhan peratus pengesanan CMF. CMF-iteMS berjaya melepasi nilai minimum 96% untuk skor imej dan 88% untuk skor piksel dan kesuluruhan peratus bagi operasi gerakan mudah. Manakala bagi operasi pemusingan, pantulan mudah, dan campuran operasi, CMF-iteMS berjaya mengekalkan nilai peratus tertinggi dengan nilai minimum 87%, 76% dan 62% untuk setiap satu operasi. Untuk operasi pemantulan di dalam CMF pula, CMF-iteMS mendapat skor tertinggi di dalam semua operasi pemantulan walaupun pantulan tersebut digabungkan bersama operasi pembesaran. SIFT-Symmetry pula memperoleh skor imej tertinggi dengan nilai 94% untuk pantulan mudah, dan 75% untuk pantulan dengan operasi pembesaran. Tambahan lagi, keputusan juga membuktikan bahawa gabungan antara kaedah pengesanan CMF dengan proses pengulangan purata saiz kawasan meningkatkan prestasi kaedah pengesanan CMF berasaskan pendekatan blok. Bagi gabungan antara kaedah pengesanan berasaskan pendekatan lain pula, keputusan menunjukkan pengurangan kesalahan padanan walaupun prestasi kedua-dua skor imej dan piksel menurun.

ACKNOWLEDGEMENTS

First of all, I would like to extend my thanks and immense gratitude to Allah for spearing my life with good health to witness the successful completion of my PhD study.

It gives me great pleasure to express my gratitude, appreciation, and sincere thanks to my PhD supervisors. Thank you to Associate Prof. Dr. Ainuddin Wahid bin Abdul Wahab, Associate Prof. Dr. Mohd. Yamani Idna bin Idris and Associate Prof. Dr. Rosli bin Salleh for providing the inspiration for this research, and for their patience, guidance and support during this study.

Valuable comments received from the editorial board experts in peer-reviewed journals, especially *Journal of Network and Computer Applications* and *Journal of Visual Communication and Image Representation* have given me insight into the need for robustness in image forensics algorithms, through their valuable comments to achieve high quality research.

To all of my colleagues, both staff and students in the Department of Computer Systems and Technology at the University of Malaya, you have made my time in the department that much more enjoyable. I feel honored to have been a part of this department. Thank you also to the Bright Sparks Scholarship Program, for their financial support towards the success of this PhD study.

A special thanks to my mother, Missinga binti Kamni, for her emotional supports, prayers, and encouragements throughout this PhD and my entire education. Thank you also to my relatives and friends, who helped me to accept the sad things that happen in life, and who never stopped reminding me of the wonderful world outside of my computer.

Last, but not least, I dedicate this thesis to my late father, Abd. Warif bin Abdullah, who will always be in my heart.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS AND ABBREVIATIONS

CMF	Copy-Move Forgery
DCT	Discrete Cosine Transform
DS	Dense SIFT
DoG	Difference of Gaussian
DWT	Discrete Wavelet Transform
DyWT	Undecimated Dyadic Wavelet Transform
FMT	Fourier-Mellin Transform
HH	Hue Histogram
HOG	Histogram of Oriented Gabor Magnitude
JPEG	Joint Photographic Expert Group
LBP	Local Binary Pattern
MM	Mathematical Morphology
MROGH	Multi-support Region Order-based Gradient Histogram
PCA	Principal Component Analysis
PCET	Polar Complex Exponential Transform
PCT	Polar Cosine Transform
PHT	Polar Harmonic Transform
PNN	Probabilistic Neural Network
PST	Polar Sine Transform
SIFT	Scale Invariant Feature Transform
SURF	Speeded-Up Robust Features
StF	Steerable Filter
SVD	Singular Value Decomposition
ZM	Zernike Moments

LIST OF APPENDICES

CHAPTER 1: INTRODUCTION

In this chapter, an introduction is presented by discussing the development of image manipulations and the importance of image forensics in the community. Next, due to the simplicity and effectiveness of the copy-move forgery (CMF) image manipulation technique, this research is focused directly on the CMF and its detection methods. The current problems in the existing CMF detection methods are briefly explained while the research questions, objectives, and scope are defined. Furthermore, this chapter also describes the contribution and significance of this research, as well as the outline of this thesis.

1.1 Introduction

The advancements of photo editing software in the market today, such as Photoshop, Paint, Pixlr Editor and Photoscape have led to the development of image manipulations. Furthermore, with the rapid growth of digital imaging devices, the digital images captured are being duplicated and manipulated at ease without degrading the quality or leaving any visible clues. Thus, these manipulated images are easily and widely shared over the internet to misrepresent the information and altering the meaning with malicious intent.

CMF becomes a popular image manipulation technique because of its simplicity and highly visual effects representation. Also known as region duplication or cloning, CMF copies one or more regions in an image and paste the regions into other positions within the same image. The CMF manipulations typically occur by hiding an object in an image to conceal unwanted information or by emphasizing a large crowd to show the impression of great support.

In recent years, the detection of CMF has become one of the most active research topics in image forensics. To detect the CMF image, the CMF detection methods are primarily evaluated by looking at their sensitivity to various possible attacks. Al-Qershi & Khoo (2013) divided the attacks into two groups, namely intermediate and post-processing attacks. Intermediate attacks (also known as geometrical transformation) is a process of spatial manipulation changes created to the copied region, purposely meant to match its targeted neighborhood in the image. The basic transformation in the CMF is translation, however, translation can be combined with other attacks, including scale and rotation. Conversely, the post-processing attack is normally (but not necessarily) applied after the transformation process, to improve the blending of visual effects that can prevent the manipulations from being detected. These attacks are comprised of Joint Photographic Experts Group (JPEG) compression, noise, and blurring effects.

Based on the literature review, the earlier CMF detection methods started with the block-based approach, which aims to find the identical features among blocks in an image. In this research, the features in the approach are categorized into four extraction techniques, namely frequency, texture & intensity, moment invariants and log-polar transform. Fridrich et al. (2003) first applied frequency, specifically, Discrete Cosine Transform (DCT) features in their block-matching scheme to find the identical quantization values. They believed that the resaved and recompressed image changes the artifact values in the original image. Then, the approach evolved by proposing other features, such as intensity patterns (Langille & Gong, 2006) and blur-invariant moments (Mahdian & Saic, 2007) to also include the resistance ability against Gaussian noise, blurring and contrast changes. In the subsequent report, the block-based approach is enhanced by looking at the sensitivity of the methods against geometrical transformation attacks. For instance, Myna et al. (2008) implemented log-polar mapping to withstand the rotation attacks, however, the performances are restricted to a certain degree of rotation while being less effective against scale attacks.

Next, the keypoint-based approach sparked a turning point in CMF detection methods in 2008. Due to the reason that Scale Invariant Feature Transform (SIFT) is known to be robust against both scale and rotation, Huang et al. (2008) initiated an approach that is able to find the similarity through an exhaustive search of the SIFT features in an image. A few years later, the method proposed by Amerini et al. (2011) became the most popular CMF detection method, as their method is superior to other SIFT-based CMF detection methods, especially for scale and rotation attacks. Instead of improving the keypoint features detection, researchers started to combine the keypoint-based approach with block-based approach to improve the performance in the flat areas and highly uniform zones. The example of the method is proposed by Ardizzone et al. (2015) which employs several triangle segmentation techniques after the keypoint extraction, either SIFT, Speeded-Up Robust Features (SURF) or Harris points.

Despite the rapid development of the CMF detection method for years, two main problems are addressed in this research. The first problem will look into the requirement of image and pixel-level evaluations in measuring the performance of the existing CMF detection methods. The second problem, on the other hand, concentrates on the reflection attacks, which are not highlighted in the previous evaluation.

To analyze the problems, this research examined the effects of image and pixel-level evaluations to the performance of existing CMF detection methods against various CMF attacks. Based on the analysis, both image and pixel-level evaluations are relying on each other and should be combined together to obtain a fair evaluation. Therefore, a set of evaluation steps with the calculation to measure the percentages of both levels of performance is used in the overall CMF detection comparison.

To continue with the performance analysis against various attacks in CMF, three existing CMF detection methods are selected with each method representing each approach. In particular, the Amerini et al.'s method (2011) indicates the keypoint-based approach, the Cozzolino et al.'s method (2015) with two features (Zernike moments and Fourier-Mellin Transform (FMT)) signifies the block-based approach, and the Silva et al.'s method (2015) denotes the combination of both approaches. In the analysis, the selected methods are compared against various CMF attacks using four datasets. Two of those datasets are collected from the publicly available CMF datasets, which comprised of CombineTranslation (only translation attacks) and CPHALL (common attacks without reflection). Furthermore, the other two datasets are the newly created data, namely NB-Casia and NBr-Casia that are designed specifically to include reflection attacks in the CMF image. The NB-Casia considers common types of CMF attacks, including reflection. Meanwhile, the NBr-Casia contains a set of reflection data combined with other CMF attacks.

As the existing CMF detection methods show reduction of performance when dealing with reflection-based CMF images, two CMF detection methods are proposed using keypoint and block-based approaches, to cover the CMF with reflection attacks. The performances are measured using multiple F-score values which are meant for image, pixel and both levels of evaluations.

1.2 Problem Statement

Presently, the performances of the CMF detection methods are evaluated, either through image-level, pixel-level, or both levels. The image-level evaluation is performed to measure the ability of the detection methods in distinguishing an original and a CMF image. Since the CMF detection methods are primarily concerned with blind detection (which the original images are assumed to be unknown), the detection methods should be able to recognize any input image, either as original or forged. However, solely image-level evaluation does not guarantee the identified location is true, even if the methods are able to detect the CMF image. Thus, the pixel-level evaluation is required to confirm the trustworthiness of the detection of locations. Due to the reason that each level of evaluation has their own significance, this research examined the effects of both level of evaluations to the performance of the existing CMF detection methods. The purpose of the study is to get an insight of the trade-off between the individuality and relevance of each level of evaluation technique.

Apart from studying the influence of image and pixel-level evaluations, the second problem concentrates on the effect of reflection to the CMF detection. To date, very limited studies have considered the reflection-based attacks in CMF. The attack is believed to have similar destructive effects as other CMF attacks and therefore worth to be studied.

As mentioned before, there are three common approaches in detecting CMF, called keypoint-based, block-based and the combination of the two approaches. From the performance analysis, the combination of the two approaches (as in Silva et al. (2015)) does not show much improvement over the two aforementioned methods. Thus, this research only concentrates on proposing methods related to keypoint and block-based approaches.

Initial tests show that the current keypoint-based CMF detection methods are not robust to the reflection attacks. As reflection attacks change the features organization, the properties of the keypoint features between the original regions and the reflected regions are different. Thus, existing keypoint matching techniques could not find the similarity, resulting in lower performance against the attacks. Therefore, a method based on keypoint features, called SIFT-Symmetry is proposed by introducing a symmetry matching technique to withstand the reflection-based attack.

The research continues with the consideration of the block-based approach. Similar tests are conducted to evaluate the performance of the existing block-based CMF detection methods. The block-based methods show convincing results in detecting direct reflection attacks, but the performance degraded when the reflection is combined with scaling attacks. One of the reasons is due to the static threshold selection technique used in prior CMF detection methods. Therefore, a method called iterative means of region size for the CMF detection (CMF-iteMS) is proposed to reduce the effects of the static threshold selection technique.

1.3 Research Questions

This research is developed to answer the following questions for a CMF detection method:

i. Do the image-level and pixel-level evaluations effect the performance of CMF detection methods?

ii. Is the symmetry matching technique able to improve the performance of existing keypoint-based CMF detection methods against reflection attacks in CMF?

iii. Does an automatic threshold selection for final verification process will increase the performance of existing block-based CMF detection methods against various attacks?

iv. Can the proposed CMF detection methods improve the robustness of the existing CMF detection methods against various CMF attacks, for both image and pixel-level evaluations?

1.4 Research Aims and Objectives

The aim of this research is to develop a CMF detection method that is capable to detect CMF image with exact detection locations against various attacks, including translation, scale, rotation, reflection, and combinations of each attack.

In this research, three research objectives are addressed as follows:

I. To examine the effects of image and pixel-level evaluations to the performance of existing CMF detection methods against various CMF attacks, including reflection.

II. To propose CMF detection methods based on keypoint-based and block-based approaches that cover various attacks in CMF.

    To be specific, this objective is divided into two sub-objectives:

    a) To propose an improved CMF detection method based on keypoint approach using a symmetry matching technique that is not only robust against translation, scale and rotation, but also to the reflection.

    b) To propose an improved CMF detection method based on block approach by introducing iterative means of region size to replace the static threshold selection technique in the prior CMF detection method.

III. To evaluate the F-score performance of the proposed CMF detection methods for image, pixel, and both levels of evaluation.

1.5 Thesis Contribution

This research proposed two detection methods based on keypoint and block-based approach for CMF with reflection attacks. The methods are compared and analyzed with the existing CMF detection methods for both image and pixel-level evaluations against various possible attacks. The lists of the contributions to the image forensics field are stated below:

1. The literature discovers the limitations of the existing CMF detection methods.
2. The limitations of the existing CMF detection methods against various possible CMF attacks are proven by a set of performance analysis.
3. An improved method based on keypoint approach is implemented using a proposed symmetry matching technique for the detection of CMF image with reflection attacks.
4. Another improved method based on block approach is proposed by combining the most robust feature extraction and thresholding techniques with an iterative means of region size as a threshold selection technique to increase the detection performance of the CMF image with various attacks.
5. Finally, a method with the highest performance is selected as the most efficient detection method for CMF. The future research directions in the CMF detection field are also provided.

1.6 Significance of Research

This research provides two detection methods that are implemented to identify CMF images with various possible attacks (including reflection) while comparing the performance with the existing approaches for both image and pixel-level evaluations. The output of this research will assist the societies which conduct research in the field of image forensics, specifically in CMF detection. The current issues associated with CMF detection are discussed in detail in the literature review section. Moreover, this research may act as a forensic tool to help digital investigators to determine the authenticity of image evidence in legal action. Additionally, the tool may also be a new technique to validate any uploaded image over social media with an accurate detection result.

1.7 Thesis Organization

This research is divided into eight chapters. The research flow diagram is illustrated in the Figure 1.1 while the summary of each chapter is described as follows:

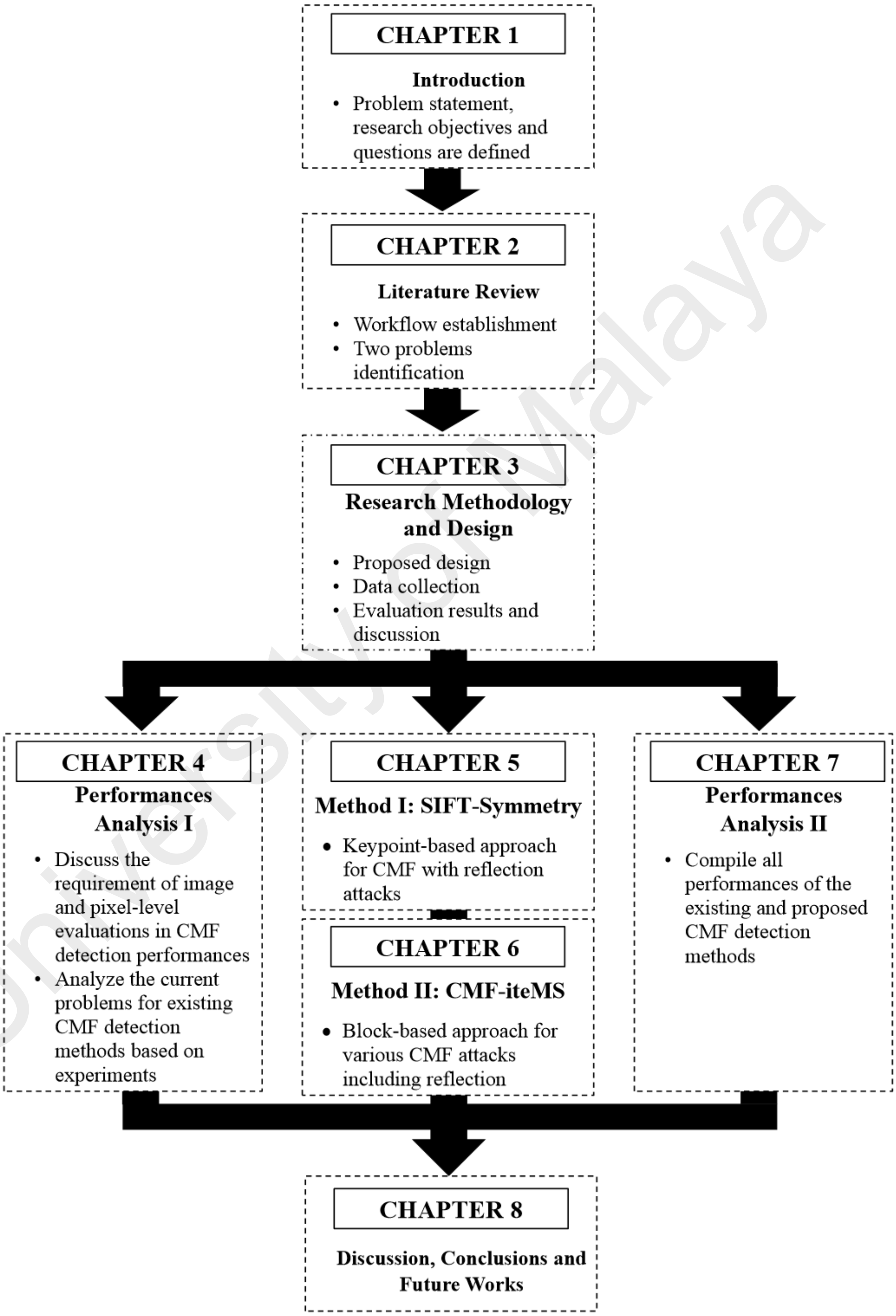

CHAPTER 1
Introduction
• Problem statement, research objectives and questions are defined
CHAPTER 2
Literature Review
• Workflow establishment
• Two problems identification
CHAPTER 3
Research Methodology and Design
• Proposed design
• Data collection
• Evaluation results and discussion
CHAPTER 4
Performances Analysis I
• Discuss the requirement of image and pixel-level evaluations in CMF detection performances
• Analyze the current problems for existing CMF detection methods based on experiments
CHAPTER 5
Method I: SIFT-Symmetry
• Keypoint-based approach for CMF with reflection attacks
CHAPTER 6
Method II: CMF-iteMS
• Block-based approach for various CMF attacks including reflection
CHAPTER 7
Performances Analysis II
• Compile all performances of the existing and proposed CMF detection methods
CHAPTER 8
Discussion, Conclusions and Future Works

Figure 1.1: Research flow diagram of this thesis

- **Chapter 1 (Introduction)**

Chapter one presents an introduction to the research field, issues, motivation, and their importance. Furthermore, the problem statement, the research questions, the research objectives, and the outline of the research is also stated.

- **Chapter 2 (Literature Reviews)**

Chapter two reviews and studies previous literatures relevant to the field of image forensics. The chapter gives an overview of the image forensics and their various components. Related works in CMF detection methods are discussed. The limitations of each method are put forward while two major problems are identified as an output of the review.

- **Chapter 3 (Research Methodology and Design)**

Chapter three provides a general discussion of the research methodology used, including research design, proposed methods, collection of data, and procedures employed in carrying out the research study.

- **Chapter 4 (Performance Analysis I)**

Chapter four studies the current performance evaluations of the existing CMF detection methods. A set of evaluation steps is used and explained. The performance of the three CMF detection methods (which represents keypoint-based, block-based and a combination of both approaches) are compared using the steps. The problems for each approach are analyzed.

- **Chapter 5 (Method I: SIFT-Symmetry)**

Chapter five describes and discusses the proposed keypoint-based approach that is able to detect the CMF image with reflection attacks and any combination of reflection. Several analysis are conducted to evaluate the robustness of the proposed solution against various possible attacks especially for reflection.

- **Chapter 6 (Method II: CMF-iteMS)**

Chapter six explains the proposed block-based CMF detection method. Four block-based feature extraction techniques are studied to see their effectiveness on various CMF attacks. Five thresholding techniques are explored to be combined with an iterative means of region size to automatically select a threshold value for the final verification of the CMF detection. Several experiments are carried out to evaluate the results of the feature extraction, conventional thresholding and automatic threshold selection techniques against various CMF attacks, including reflection. The combination of feature extraction, conventional thresholding and automatic threshold selection technique with the highest performance is considered in the proposed CMF-iteMS.

- **Chapter 7 (Performances Analysis II)**

Chapter seven compiles the performances of the existing and the proposed CMF detection methods. In this chapter, the most efficient CMF detection method is determined.

- **Chapter 8 (Discussion, Conclusion and Future Works)**

Chapter eight summarizes the whole thesis while discussing the implications of this research. This chapter also includes a suggestion for future works in CMF detection.

CHAPTER 2: LITERATURE REVIEW

In this chapter, the importance of image forensics field is discussed to present the significance value of this research. The background of image forensics is introduced, including its related components. Since Copy-Move Forgery (CMF) is the most popular of image manipulation techniques, this chapter primarily focused on the detection area. Firstly, a new workflow of the CMF detection methods is established. Then, the methods are reviewed based on its category in the pre-processing stage, which are block-based and keypoint-based approaches. The abilities and limitations of each method are identified and analyzed. Lastly, two major problems are discussed in detail. This chapter is based on the publication title "Copy-move forgery detection: Survey, challenges and future directions" (Warif et al., 2016) and has been reformatted to follow the university guidelines.

2.1 Introduction

Owing to the reason that imaging devices with high resolution are available inexpensively, there have been extensive use of digital images for various purposes. The purposes include fashion, publication, medicine, crime prevention and etc. In addition, people may also capture their moments at ease, anytime and anywhere. Furthermore, with the advanced photo editing and Internet of things, the image also can be altered, shared, and spread widely over the internet. These facilities have led to several disadvantages in some situations, although they offer many benefits to society. The example of the disadvantages is the digital image content is often manipulated to misrepresent the information with mischievous plans.

Surprisingly, academic papers were also exposed to such manipulation. Mike Rossner, the managing editor of the Journal of Cell Biology reported that as many as

20% of accepted manuscripts in his journal contain figures with inappropriate manipulations and at least 1% of each have fraudulent manipulations (Farid, 2006). Furthermore, based on the survey conducted by Tijdink et al. (2014), 15% of the Flemish biomedical scientists admitted that they have been involved in scientific misconduct such as fabricating, falsifying, plagiarizing, or manipulating data in the past three years. As a result, the credibility and value of images are often argued when used in academic papers and also in scientific fraud cases. Therefore, these issues have encouraged the development of research in image forensics to verify the authenticity in every single image.

2.2 Overview of Image Forensics

The issues highlighted in the previous section demand for methods that allow the investigation of a digital image to validate the truthfulness and verify the sources. Basically, there are two possible questions regarding the credibility of an image. Firstly, was the image truly produced by the claimed device? Secondly, is the scene in the image portrayed the real situation? To find the answers to these questions, researchers developed the interest by proposing several methods in image forensics.

Generally, image forensics is an area of studies that identifies the origin and the authenticity of an image. The study basically derives from multimedia security-related research, which require additional information from the image. To expand the research, image forensics aims to provide tools for blind investigation, specifically to expose evidence in a crime. As both acquisition and manipulation processes in an image are likely to leave subtle traces, existing knowledge of image processing and analysis tools are exploited to discover information about the image’s history. An overview of the components in image forensics is illustrated in Figure 2.1. The details are divided into two main components; active and passive approaches, while the discussion of each is presented in the following section.

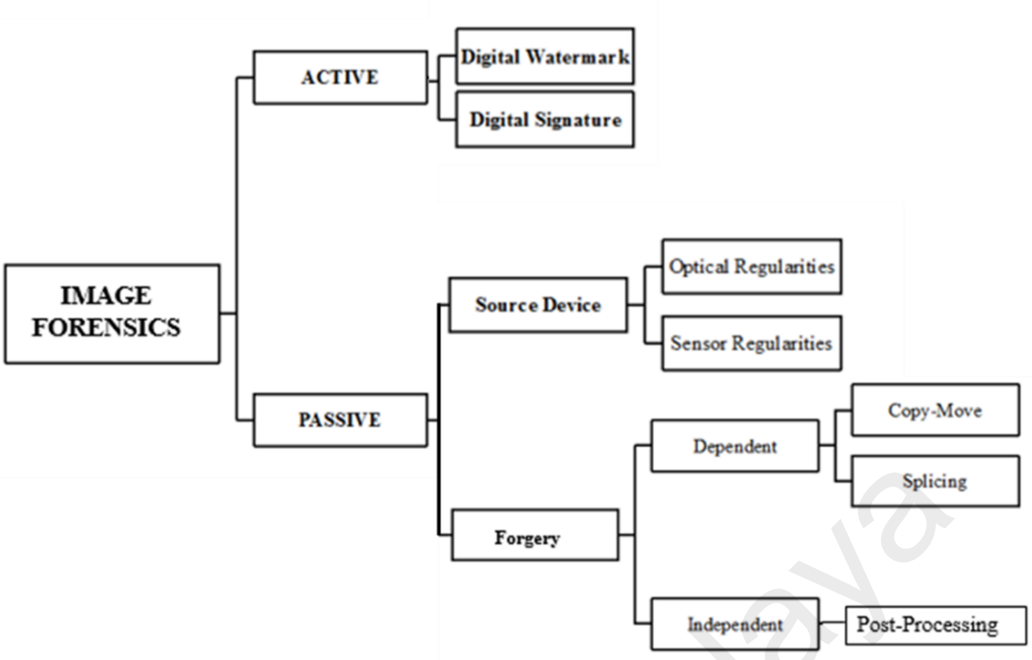


Figure 2.1: Overview of components in image forensics field

2.2.1 Active Approach

As the previous discussion mentioned that image forensics basically is a combination of multimedia security-related research with image processing tools, this category represents one of them. By applying the multimedia security principle, the active approach considered steganography and cryptography in their analysis tools. Steganography is an art of embedding information to an irrelevant image, while cryptography is an art of conveying secret writing as a code.

In image forensics, digital watermark theoretically applied the steganography art in the image content. Instead of hiding information to an image as a message, digital watermark hides the owner's information into the image to authenticate the owner and determine the originality, specifically for copyright protection (Piccinnano, 2014).

Most of the research in the digital watermarking mainly concerns two concepts, namely, perceptibility and robustness (Huynh-the, Banos, Lee, Yoon, & Le-tien, 2016). The perceptibility refers to the degree of watermarks being noticeable by a mind or sense after the process of embedding. Instead, the robustness denotes the ability of watermarks being changed for common image manipulation during the process of extraction. For that reason, Tsai et al.'s (2011) simulated several attacking procedures using some predefined attacks to evaluate the robustness of the watermarks.

Digital signature, on the other hand, takes the idea from cryptography by encrypting the unique secret code in an image to authenticate the sender and verify the trustworthiness. Furthermore, the digital signature in an image is commonly created by using a one-way hash function to make it difficult to be copied. Signature-based methods can work on both the integrity protection of the image and disclaimer prevention of the sender (Saad, 2009). In contrast to other approaches, digital signature assigns a private key in an image and requires a public key to verify the image. The procedures should be secure enough to prevent any attacked image from passing the authentication while being robust enough to accept some acceptable manipulations (e.g. compression) during the transmission (Sun & Chang, 2005).

In conclusion, the active approach is proposed in the past by computing either digital watermark or signature to the camera and is inserted later on the acquisition of an image. According to Lin (2000), digital watermark is more convenient as the information is always associated with the image, while digital signature requires an additional file which has to be requested from an authorized person to validate the image. Any modification of the image after the acquisition can be detected by comparing the value of the digital watermark or signature. Therefore, this approach requires additional information about the original image, however, if the information is unknown, the active approach seems impossible or ineffective.

Despite the difficulties, researchers started to propose blind watermarking techniques which do not require any original image information. By maintaining the quality in perceptibility and robustness, the Al-Nabhani et al.'s method (2015) is superior to existing methods when proposing a blind image watermarking based on Probabilistic Neural Network (PNN) in the wavelet domain. The authors proposed to embed a watermark in the middle-frequency coefficient decomposition before the PNN is applied to train the relation between the embedded watermarks, with the corresponding image.

2.2.2 Passive Approach

Turning to the passive approach, the main difference between the active and passive approaches is that the passive approach does not require the original image nor additional information about the image or the acquisition device which produces the image. Also called as blind analysis, the passive approach does not need any specific hardware to make the techniques practically feasible, however, it requires a study of statistical variations of the images.

Lin et al. (2013) classified blind detection techniques into two categories; visual and statistic. Visual category is based on visual clues like inconsistencies in images and light deformation of an object in the image. Aside from visual, the statistical category is considered to be robust and convincing as the pixel values of the image will be analyzed.

Instead of classifying the passive/blind approach into visual and statistic, this research categorized the approach into two main categories, namely source device authentication and forgery detection. The source device authentication is purposely used to identify the origin of an image based on detection of intrinsic image regularities. Conversely, forgery detection is more about revealing artifacts leftover due to specific manipulation operations in a forged image. The explanation of both categories is presented in the next subsections.

2.2.2.1 Source Device Authentication

For source device authentication, a forensic analyst may verify the authenticity of an original image by analyzing the regularities and anomaly of an image source. Furthermore, each source model is identified by its intrinsic and unique features to differentiate each device class (Kot & Cao, 2013). In a court of law, the origin of a particular image can be represented as a crucial evidence and the validity of this evidence might be compromised by a statistical analysis that confirmed the image has been captured from the claimed device.

The common features used in device classification are optical and sensor regularities. The optical regularities is often associated with some digital processing modules, including illumination, lens distortion, chromatic aberrations, and blurring, which are introduced in the optical domain. In contrast, the sensor regularities refer to sensor noise, dust characteristics and camera response function which are introduced when the light signals are converted to digital signals (Hong & Kot, 2009).

The research on source device authentication includes three aspects, which are imaging device identification (e.g. printer, digital camera, scanners, and mobile phone), imaging device brand identification (e.g. Nikon camera model), and imaging device individual identification (e.g. Nikon D70, and Nikon D70s). Most of the prior work focused on imaging device brand identification which classified the images based on the presence and inconsistencies of device attributes or data processing related characteristics. The examples of attributes are sensor pattern noise, camera response function, resampling artefacts, Color Filter Array interpolation artefacts, JPEG compression, lens aberration, etc. (Chang-Tsun Li, 2010)

In spite of that, since the current imaging device brands have numerous models itself (which have different attributes for each model), current research focus is emphasized on imaging device individual identification. Recently, Xu et al. (2015) and Qiao et al. (2017) proposed methods based on image texture features from selected color model and channel, and improved signal-dependent noise model, respectively.

2.2.2.2 Forgery Detection

Another main aspect of the operations performed in passive image forensics is forgery detection. In contrast to source device authentication (which identifies the origin of an image), forgery detection presents an attempt to discover evidence of tampering. Additionally, the attempt should able to locate the forged area in an image. There are two types of forgery which are classified by Redi et al. (2010), namely dependent, and independent of forgery. These types of forgery are categorized based on the manipulation techniques done by the counterfeiter. Next subsections describe both forgeries precisely.

(a) ***Dependent***

The first type of forgery is dependent in which the detection methods are designed to detect only certain types of forgeries which require a duplication process depending on the number of images involved. In view of the fact that the image manipulation technique is able to change the significant content of an original image, it will cause critical social impacts if these images are manipulated with malicious purpose. With the advanced image editing software, the forged images become common in our daily life that will lead to the untrustworthy record of an event. Therefore, the detection methods, specifically for the dependent-type has become a vital important technology for digital image authentication. There are two categories of forgery-dependent, namely, copy-move (single image), and splicing (multiple images).

i Copy-Move Forgery (CMF) Image

One of the simple yet effective image manipulation techniques in forgery is CMF image. In CMF, a region of an image is duplicated and pasted to another position within the same image to hide undesired objects or to replicate objects. This research focused on this category due to the reason that only one image is involved (which is practical), thus, gives important changes to a forged image. Hence, the primary mission of CMF detection is to detect the presence of two or more similar regions in a single image, and to locate them if there is any. The detailed explanations, discussions, limitations, and challenges in existing CMF detection methods are presented in Section 2.3.

ii Image Splicing

As an alternative to CMF, image splicing presents more complex image manipulation techniques. Also known as composite image, image splicing is a process of duplicating regions from different source images to an image. In other words, this kind of manipulation technique refers to one or more regions of an image from other images. Figure 2.2 shows an example of the image splicing where image of the person has been combined with image of the building. Despite the complexity of the process, this technique is widely seen in the community, since the massive amount information content might attract people’s interests. Therefore, the detection of image splicing aims at detecting the composite regions between cutting and joining two or more pictures.

There are two groups of techniques in image splicing detection, which the first group considers detection on specific operations in the boundary between spliced regions and original regions. For this group, researchers assumed that the spliced region will be blurred or resampled to match its targeted neighborhood in the original image. Meanwhile, the second group of technique searching for differentiation of certain intrinsic fingerprints in the original image. A typical example of this technique is the recognition of the inconsistencies in camera Photo Response Non-Uniformity.

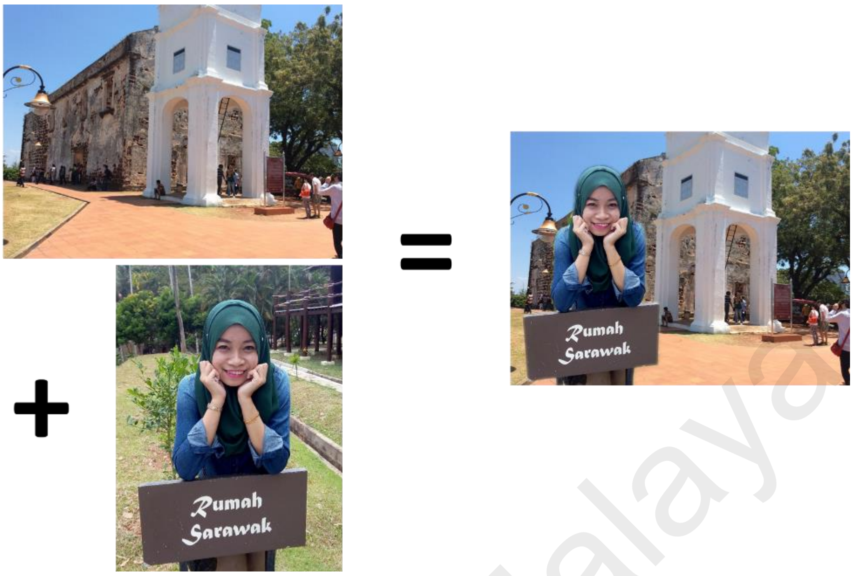


Figure 2.2: Example of image splicing where two images have been combines in another one image

Recently, there is one technique that can be classified into either group, namely noise-based localization. This technique derives from the assumptions that an image from a different origin usually has different noise levels. For instance, Zeng et al. (2016) proposed a method based on Principal Component Analysis (PCA) noise level estimation method. However, due to the noise level being always affected by brightness and textures, Pun et al. (2016) proposed a noise level function with multi-scale analysis to deal with noise fluctuations. In contrast to the noise-based groups, researchers improved the Markov model in DCT by avoiding color distortions and eliminating redundancy from the quantized transform coefficients using Contourlet transform domain (Q. Zhang, Lu, & Weng, 2016) and quaternion in a whole manner (C. Li, Ma, Xiao, Li, & Zhang, 2017).

(b) ***Independent***

As discussed in previous sections, forgery-dependent requires the knowledge of the kind of forgery that compromised the image. Conversely, forgery-independent type is a more universal approach which may act as stand-alone attacks without the process of duplication. Otherwise, as the primary purpose of the forgery-independent is to enhance the blending of visual effects and to smooth its manipulation content, this type of forgery will also be applied after the process of forgery-dependent. There are many open source software that provides independent types of forgery without the necessities of supplementary image editing-related skills.

In the event that forgery-independent takes place after the forgery-dependent manipulations, the forgery-dependent detection methods should consider to be robust to this type of forges. Or else, if the forgery-independent is working alone, then the detection is based on artifact traces left, either by resampling, compression or inconsistencies in the acquisition of fingerprints. The forgery is traced by analyzing proper artifacts introduced by JPEG recompression occurring when the forged image is created. This is showed by Bianchi and Piva (2012) which proposed a block-grained analysis of JPEG artifacts in the presence of double JPEG compression.

Instead of analyzing the JPEG traces, researchers attempt to analyze the inconsistencies in illumination color (Carvalho et al., 2013) or statistical properties of natural images (Lyu & Farid, 2005; P. Zhang & Kong, 2009). Recently, a blind de-convolution application has been extended to image resampling detection that also can be used for forgery-dependent manipulations (Su, Jin, Zhang, & Chen, 2017).

2.3 Copy-Move Forgery (CMF)

Copy-move forgery (CMF) is a forgery-dependent type in forgery detection, which belongs to the passive approach in image forensics area. Also known as region duplication or cloning, CMF involves only one image in which one or more regions have been copied and pasted to other locations within the same image. Due to the reason that both source and target regions are from the same image, the properties such as color temperature, illumination conditions and noise will generally be well-matched between the forged region and the image. As a result, this type of forgery is easy to perform and relatively effective with highly visual effects to be used for information exploitation.

Regardless of the characteristics, the CMF may be used to give a false impression to favor an individual’s personal agenda, including hiding an element in the image (e.g. steganography) or emphasizing a particular object (e.g. a crowd of demonstrators). Figure 2.3 shows an example of CMF image, where the grass has been copied and pasted to another location with the intention of hiding the house in the image.

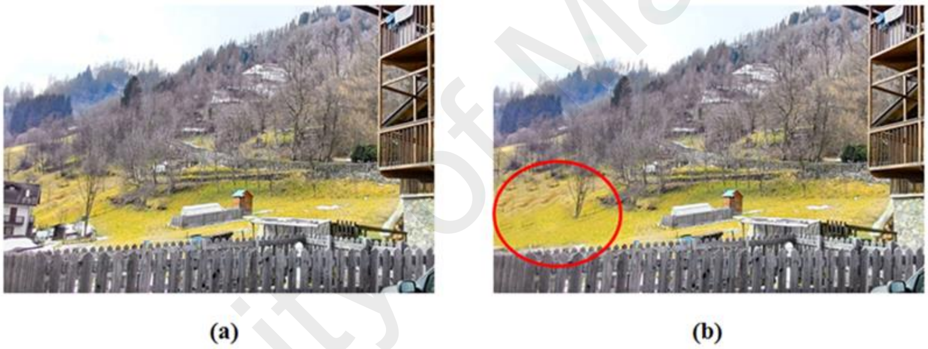


Figure 2.3: An example of CMF (a) original image (b) forged image

To reduce the chances of the forged regions from being discovered, the CMF manipulations are often combined with other image processing operations. In the CMF detection field, these operations are known as attacks, which are divided into two categories, namely post-processing and geometrical transformation as demonstrated in Figure 2.4.

Basically, the CMF detection methods are initiated by investigating the robustness against post-processing attacks (e.g. JPEG compression, noise, and blurring effects) that occur after the duplication process. Similar to forgery-independent types (explained in Section 2.2.2.2(b)), these attacks could reduce the visual manipulation footprints and blends the CMF effects. Geometrical transformation attacks, on the other hand, applied spatial manipulation changes on the region that match its targeted neighborhood in the image. The attacks are translation, rotation, scale, and reflection.

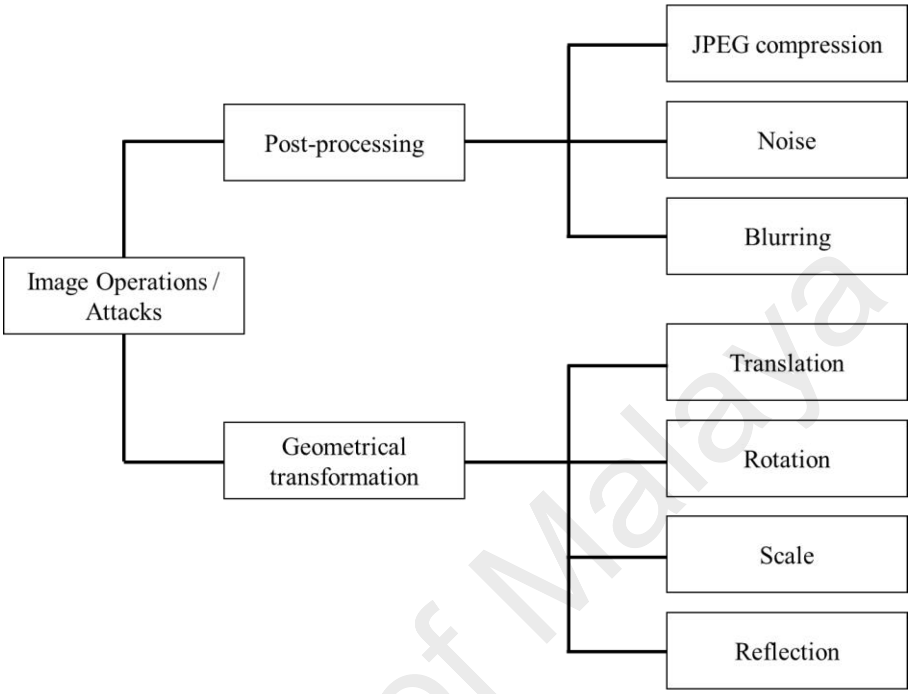


Figure 2.4: Categories of image operations/attacks in CMF

This research focused directly on CMF detection mainly because CMF has found significant interest from the scientific community in recent years. This is evident from the Figure 2.5 which located a total of 226 scientific papers related to CMF detection indexed by Web of Science over the last 10 years. 50% of the total papers consist of "Copy-Move Forgery Detection" as a title, while the remaining papers may use other terms, including region duplication or cloning. Otherwise, the topic of CMF may be discussed in the research paper for both dependent and independent-type of forgery detection.

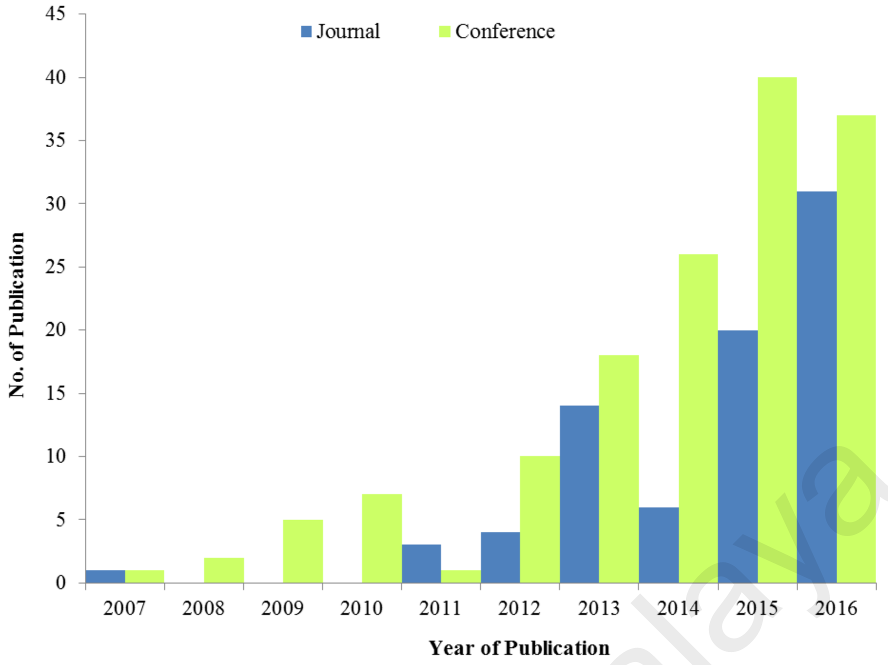


Figure 2.5: Scientific papers located by searching for "copy-move forgery detection" on Web of Science website

2.3.1 Common Workflow of CMF Detection Methods

In spite of the wide range of methods that have been proposed for CMF detection, most of the methods adhere to a common pipeline recognized by Christlein et al. (2012). Given an input image, the image will go through the pipeline, comprised of pre-processing, keypoint detection or block tiling, feature extraction, matching, filtering, and post-processing. Additionally, Al-Qershi et al. (2013) also developed the pipeline, however, replaced the filtering and post-processing steps with verification and detection map, respectively.

Owing to the reason that variations of pipeline are documented, this research generalized the pipelines into an established CMF detection workflow (presented in Figure 2.6). According to the workflow, the main stages are feature extraction and matching, which determine the efficiency of a CMF detection method. Nonetheless, pre-processing becomes optional as it is dependent on the techniques in the main stages, while visualization combines filtering, post-processing, verification, and detection map, compatibly. Each stage is discussed as follows.

(a) Pre-processing

The first stage in the CMF detection workflow is pre-processing. The aim of pre-processing is to enhance the image information content for further tasks. The typical enhancement of the image data includes suppressing of undesired distortions or increasing the image features (Miljkovi, 2009).

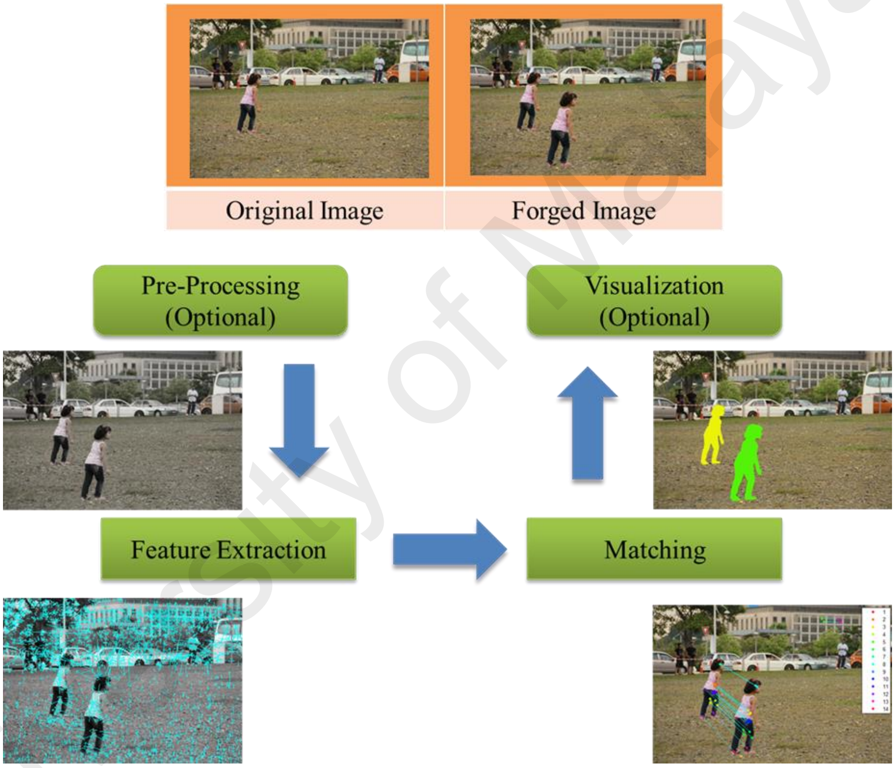


Figure 2.6: Common workflow of CMF detection methods

In CMF detection, researchers implemented the pre-processing technique depending on their feature extraction techniques. For example, if SIFT (Lowe, 1999) is employed as the feature extraction technique, the input image will first be converted into grayscale. In the conversion, the RGB channels are merged using $I = 0.228R + 0.587G + 0.114B$ to represent the grayscale component. The main reason of the conversion is that grayscale image simplifies the image features and reduces the computational costs, while color image will contain unnecessary information that could increase the complexity and affect the performance (Kanan & Cottrell, 2012). Furthermore, the grayscale conversion also appears to be the most frequently used pre-processing technique in CMF detection methods (e.g: (Amerini et al., 2011; E Ardizzone, Bruno, & Mazzola, 2010; Edoardo Ardizzone, Mazzola, Informatica, & Università, 2009; Cao, Gao, Fan, & Yang, 2012; H. Huang et al., 2008; Myna et al., 2008).

In view of the fact that the human visual system is more sensitive to luminance component, traces of forgery may be left in chrominance components. For that reason, the chrominance is suitable for extracting features that are sensitive to tampering traces (Hussain, Saleh, Aboalsamh, Muhammad, & Bebis, 2014). Alternatively, instead of grayscale conversion, several researchers attempt to convert the RGB image into YCbCr color system to operate on the luminance (Y), and chrominance components (Cb and Cr).

Apart from color conversion, there are several dimensional reduction techniques applied in the pre-processing stage, including Discrete Wavelet Transform (DWT) (Edwards, 1992) and PCA (Kroonenberg, 1983). These techniques are used to find the best low-dimensional representation of the original high-dimensional data based on image energy (Bhullar, Budhiraja, & Dhindsa, 2014) or least mean-square error (Gan & Cang, 2013) to select a few important variables, intentionally to reduce the dimensionality. Otherwise, these techniques can also be used in the feature extraction stage due to the reason that the techniques may be robust to certain operations in CMF.

In spite of the capability of color conversion and dimensional reduction, researchers started the pre-processing stage by dividing the input image into several blocks of squares or circles to increase the performance of matching techniques. The block division can reduce the computational time for matching process in order to find the similar feature vector in an image compared to an exhaustive search. Moreover, because of the compatibility with various feature extraction and matching techniques, block division approach becomes popular in CMF detection methods.

(b) ***Feature Extraction & Matching***

Next, the main stages for CMF detection workflow are feature extraction and matching techniques. Feature extraction is a technique of selecting relevant information that represent the characteristics of interest in the image (Chora, 2007). The features are represented in many forms, comprising frequency, color, texture, moments, and keypoint. Meanwhile, each feature has their own selection techniques that determine the number of characters selected. For instance, frequency have DCT (Narasimha & Peterson, 1978), DWT and Fourier Transform (Bochner & Chandrasekkharan, 1949) extraction techniques. Another example is keypoint, in which there are SIFT, Speeded-Up Robust Features (SURF) (Bay & Ess, 2008) and Harris points (Harris & Stephens, 1988) techniques in the literature.

In view of the fact that the CMF image will consist of at least two similar regions (from duplication process) in an image, each extracted feature is matched with other similar properties in the image to locate the forged areas. This is where the matching stage is required to seek out the similarities between two or more features in the image. Furthermore, the manipulations of CMF in the image are defined in this stage.

In order to determine the most identical properties of each feature, several similarity criteria (e.g. the Euclidian distance) are matched as pairs. However, the techniques might be different according to the pre-processing stage, either by block division or exhaustive search. As most of the feature extraction techniques preferred to divide the input image into block-based techniques, the blocks are matched by sorting the feature vectors, lexicographically or by calculating the nearest neighbor determination in a kd-tree. Alternatively, keypoint features are matched by calculating the distance of the nearest neighbor from all points in the feature space. This research further divided the CMF detection methods into block-based approach and keypoint-based approach in Section 2.3.2.1 and Section 2.3.2.2, accordingly.

(c) ***Visualization***

Finally, the process of CMF detection is visualized to display and locate the forged regions in the image. In this stage, the visualization techniques consist of filtering, post-processing, verification and detection map. Because the matching techniques are often included with spurious and irrelevant information (considered as noise), the results from the techniques should be verified and filtered before the forged areas are localized. Both block-based and keypoint-based approaches will go through this stage to validate their results.

For filtering and verification, researchers often predefined at least one threshold value to remove the outliers. There are four thresholds identified in the filtering process, specifically distance, cluster, size, and range. The match features with attributes above (or below) the threshold value are preserved, while the rest are removed. The block-based approach commonly allocated distance threshold value to find the most identical blocks (Mahdian & Saic, 2007). In the subsequent report, Huang et al. (2011) impose a minimum number of similar shift vectors between matched blocks in the CMF image.

On the other hand, keypoint-based approach generally assigned a threshold value for a number of point features between each cluster (Amerini et al., 2011; Yu, Han, & Niu, 2014). The image is verified as a CMF, if each cluster has achieved several number of matching points. Alternatively, researchers employed threshold for region size specifically for dense-based point features (Amerini et al., 2013; Cozzolino et al., 2015; J.-M. Guo, Liu, & Wu, 2013). In contrast, a range threshold is utilized by Jaberi et al.

(2013) who defined a range threshold between high and low threshold to detect strong edges and weak edges, respectively.

To finalize the detection map, the block-based approach may be presented by coloring or mapping the region of the matching blocks. The keypoint-based approach on the other hand, is commonly displayed by line transformation between each cluster point. However, both approaches can also be further refined by morphology operation using the shapes properties of the features such as contours, skeletons and convex hulls, to fill the holes on the marked regions and remove the isolated regions (Amerini et al., 2013; Cao et al., 2012; Jaberi et al., 2013; Pan & Lyu, 2010; Peng, Nie, & Long, 2011; Zhao & Guo, 2013).

2.3.2 CMF Detection Methods

As discussed in the previous sections, the main stages of CMF detection workflow are feature extraction and matching techniques. The stages are categorized depending on their pre-processing stage, either block division or exhaustive search techniques. If there is block-division process, the CMF detection methods are defined as block-based approach while keypoint-based features normally will go through exhaustive search. In the recent years, both approaches are combined together to improve each other while providing more robust detection. The overall overview of the category is drawn in the Figure 2.7 while the explanation is discussed in the following.

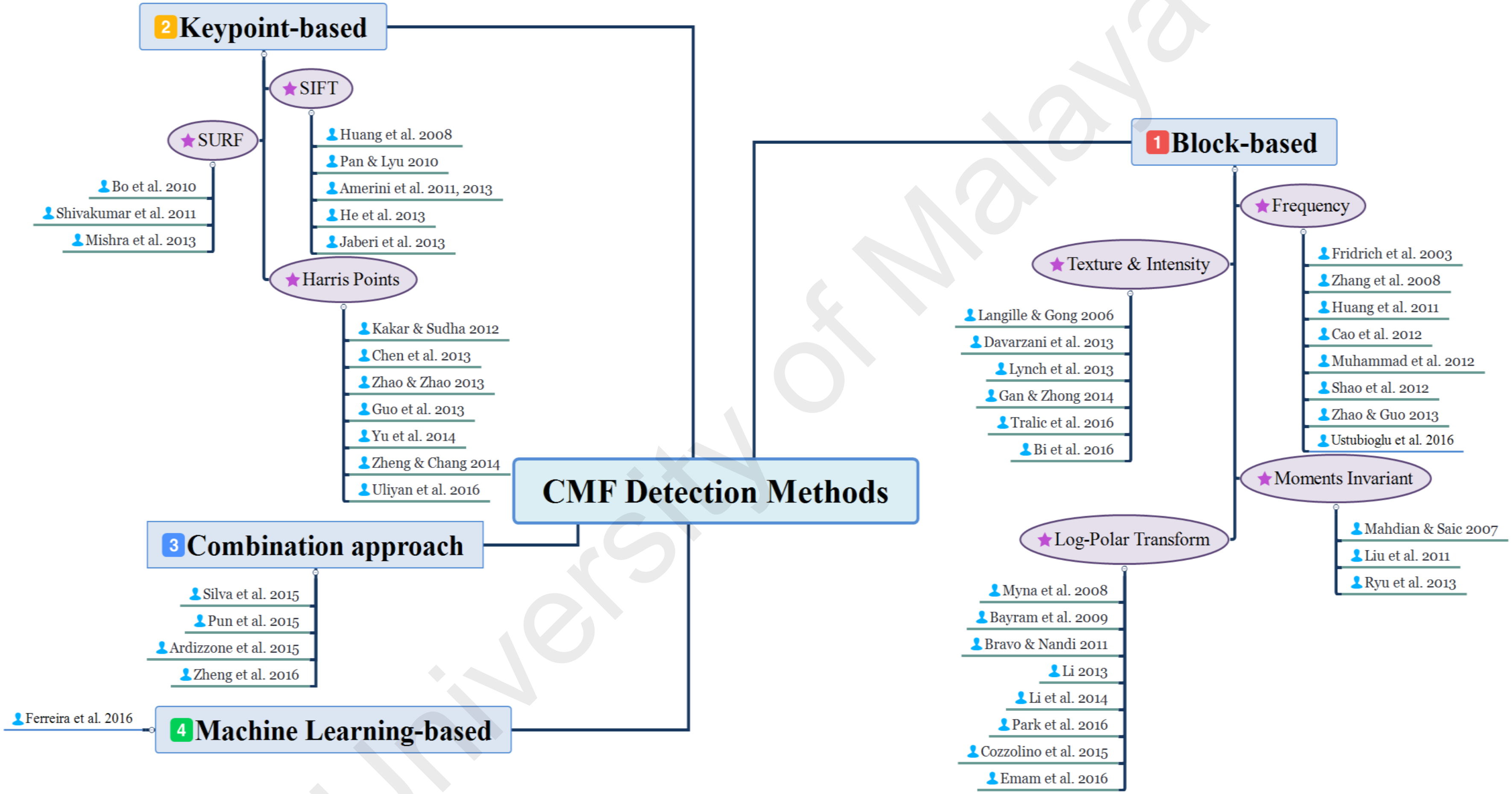
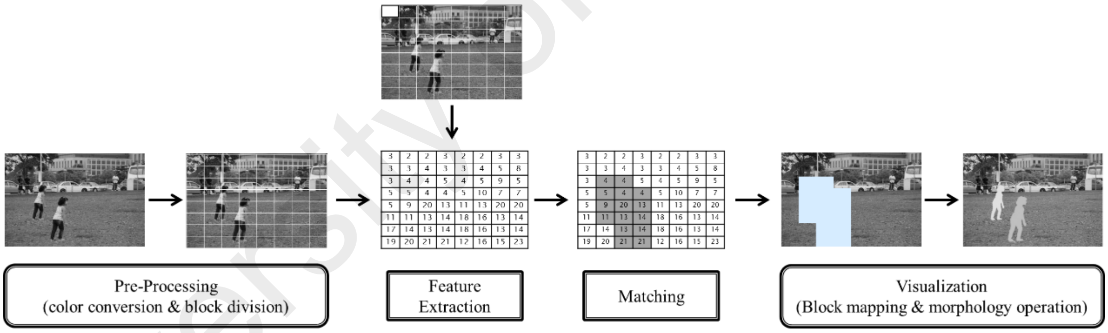


Figure 2.7: Overview of the categories in CMF detection methods

2.3.2.1 Block-based Approach

In block-based approach, the input image will be converted into either grayscale or YCbCr color to simplify the image information and reduce the computational cost. Then, the image is split into blocks either squares or circles by overlapping or non-overlapping depending on the proposed methods. For feature extraction stage, there are various features that can be extracted from each block. The features are grouped based on each form, comprising frequency, texture & intensity, moments invariant, and log-polar transform. To find the identical blocks, sorting techniques are employed and the distance is measured. Finally, the blocks with the highest similarity measurement will be mapped, and the holes are filled by morphology operations. Figure 2.8 illustrates the workflow of block-based approach and each group of features is explained in the following section.



3	2	2	3	2	2	3	3
3	3	4	3	3	4	5	8
3	4	4	5	4	5	9	5
5	5	4	4	5	10	7	7
5	9	20	13	11	13	20	20
11	11	13	14	18	16	13	14
17	14	13	14	18	16	13	14
19	20	21	21	12	16	15	23

3	2	2	3	2	2	3	3
3	3	4	3	3	4	5	8
3	4	4	5	4	5	9	5
5	5	4	4	5	10	7	7
5	9	20	13	11	13	20	20
11	11	13	14	18	16	13	14
17	14	13	14	18	16	13	14
19	20	21	21	12	16	15	23

Pre-Processing
(color conversion & block division)
Feature Extraction
Matching
Visualization
(Block mapping & morphology operation)

Figure 2.8: Workflow process for CMF detection in block-based approach

(a) ***Frequency***

Firstly, the CMF detection methods are started by detecting compression operations that normally (but not necessarily) occur after the CMF. The compression can smooth the tone and color variations of the forged images, so that the image will look natural. By assuming that the CMF images are usually resaved and recompressed as a new image, the CMF can be detected via the compression artifacts that change the artifact in the original image. Fridrich et al. (2003) initiated the methods by extracting DCT quantization value for each block. To improve the execution speed, Huang et al. (2011)

truncated the feature vector to the nearest integer, while Cao et al. (2012) applied circle block matching that can reduce the feature dimension. For the similar reason, Zhao and Guo (2013) represented each block by Singular Value Decomposition (SVD) after the DCT extraction. Despite the several numbers of improvement on DCT-based methods, the methods can only be robust to JPEG compression, Gaussian blurring and noise addition.

Instead of DCT, Zhang et al. (2008) attempted to employ DWT as their feature extraction technique. Though the method can reduce the computational cost, the speed depends on the location of CMF region. The detection process needs to be repeated into smaller blocks, if the region is located between two blocks. Furthermore, due to the reason that Undecimated Dyadic Wavelet Transform (DyWT) is shift invariant compared to DWT, the features is applied by Muhammad et al. (2012). Consequently, their method is not only robust to JPEG compression, but also invariant to (below) $20°$ of rotation. Turning to the rotation, Shao et al. (2012) proposed to calculate the Fourier transform of the polar expansion on overlapping blocks, which results on robustness to $-180°$ and $180°$ of rotation.

(b) ***Texture & Intensity***

In contrast to frequency group, the texture and intensity group attempts to cater the CMF region that exists in natural scenes or the background. The scenes are ideal for CMF regions because the areas will likely blend with the image and make it harder to detect (Fridrich et al., 2003). As the scenes may represent the texture contents, including grass, cloud, ground, and image properties such as smoothness, coarseness and regularity, texture and intensity can be utilized as features to locate the identical regions in the forged image. The early work in this group was performed by Langille and Gong (2006) who proposed to use intensity from patterns as their feature extraction.

Other pattern-based methods are implemented by Davarzani et al. (2013) and Tralic et al. (2016) who applied histogram of orientated Gabor magnitude (HOG) and multi-resolution Local Binary Pattern (LBP), and Cellular automata and LBP, respectively. However, these methods could only robust to a small degree of rotation (6°) and 5% of scaling (0.95–1.05).

Alternatively, researchers studied the color features in the forged images. Lynch et al. (2013) proved that the average value of gray from each block can robust to JPEG compression, Gaussian blurring and illumination variations. In the subsequent report, Gan & Zhong (2014) combined the average gray value with Tamura texture. These combinations are able to resist with fixed angle of rotation and 20% of scaling (0.8–1.2). Recently, although Bi et al. (2016) fused the color texture descriptor with moment descriptor (named as Multi-Level Dense Descriptor), the method could only resists to 10° degree of rotation, and 10% of scaling (0.9–1.1).

(c) ***Moments Invariant***

Image moment is a measurement of image intensity over the whole image. In view of the fact that moments have the ability to represent global features of the image, the moments can also classify shape and recognize object in binary images. In CMF detection, Mahdian and Saic (2007) initiated the utilization of moment features in their method. The authors proposed blur invariant functions in central moments, specifically to resist with blur degradation, additive noise and arbitrary contrast changes. In another report, Liu et al. (2011) extracted Hu moments from circle blocks particularly to overcome the effect of rotation in CMF. As a result, the method could only resist to certain angles of rotation.

To further analyze the moment features, Ryu et al. (2013) recommended Zernike moments feature to resilient rotation. The method achieved high robustness to rotation, Gaussian blurring and noise addition, for both textured and smooth CMF regions.

*(d) **Log-polar Transform***

Log-polar transform works by projection mapping from the points on the Cartesian plane (x, y), to points in the log-polar coordinate system. The coordinate system is a representation of two dimensions, which are the logarithm of the distance to a certain point, $log\ (x)$, and angle, θ. The authors who proposed this group of features believed that the CMF region would be rotated, scaled, or blurred before pasting it, to reduce the visual artifacts in the forged image. In CMF, this group is originated by Myna et al. (2008) which proposed to map the low frequency sub-band block (extracted from DWT) to log-polar coordinate. Then, Bravo and Nandi (2011) improved the method by producing one dimensional descriptor (1-D) invariant to reflection and rotation. Even though the results increased the robustness to various degrees of rotation, the detection is less effective to small CMF regions. While improving the small CMF region detection, the method proposed by Park et al. (2016) significantly reduced the performance for either high degree of rotation or large scale of factor.

On the other hand, Bayram et al. (2009) first introduced Fourier-Mellin Transform (FMT) (Sheng & Arsenault, 1986) in CMF detection. Owing to the reason that the detection is limited to $10°$ of rotation and 10% of scale factor (0.9–1.1), researchers adopt the orthogonal transform that belongs to the family of Polar Harmonic Transforms (PHT) (Yap, Jiang, & Kot, 2010). The PHT family is comprised of Polar Complex Exponential Transform (PCET), Polar Cosine Transform (PCT), and Polar Sine Transform (PST). As Emam et al. (2016) employed PCET, their performance decreased for $90°$ degree of rotation and above. However, the result is better than PCT that was implemented by Li (2013). Otherwise, Li et al. (2014) who utilized PST, show good results of simulation for CMF with rotation, reflection, and scale.

In the subsequent report, Cozzolino et al. (2015) explored the function of Circular Harmonic Transform (Hsu, Arsenault, & April, 1982) which consists of Zernike radial function, PCT and FMT. As the authors preferred to use Zernike Polar features, the method works well with all degrees of rotation, but is limited to 10% of scale factor of (0.9 to 1.1).

2.3.2.2 Keypoint-based Approach

Since the block-based approach solely relies on block comparison (which is variant to certain degrees of rotation and scale), keypoint-based approach started to be considered in CMF detection. In CMF detection, keypoint-based approach is defined as any keypoint feature extraction technique that matched each other without the block-division process. In view of the fact that keypoint features are seen to have outstanding computational cost and robustness, researchers have drawn much attention to these features.

In contrast to the block-based approach, the keypoint-based approach does not perform any block division technique. Figure 2.9 illustrates the workflow of keypoint-based approach in CMF detection. Firstly, the input image will be converted to grayscale to improve the distribution of salient point features. The salient points are extracted from the distinctive local features (e.g. corners, blobs and edges) and assigned with a set of descriptors which are generated within a region around the features. The purpose of the descriptor is to describe the points' neighborhood, subsequently, to increase the reliability against affine transformation. Both points and descriptors are matched by calculating the nearest neighbor of each point in the whole image. The identical points will be further analyzed to determine the forged area in the image. In this research, the keypoint features are grouped according to the point detector techniques, particularly SIFT, SURF and Harris points.

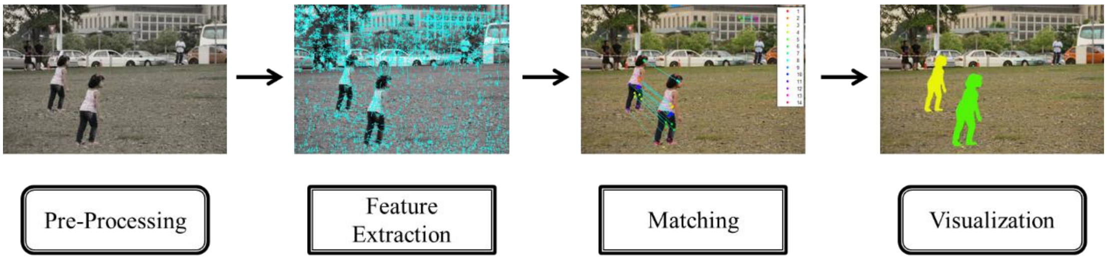


Figure 2.9: Workflow process for CMF detection in keypoint-based approach

(a) SIFT

Basically, the keypoint-based approach is motivated by the SIFT (Lowe, 1999) feature extraction technique. SIFT is the most popular keypoint feature extraction technique in object recognition area. SIFT detects salient points at different scales from Difference of Gaussian (DoG) pyramid in scale-space representation. The DoG is used to improve the computational speed during the extraction process in an image (Juan & Gwun, 2009). Subsequently, the SIFT descriptor is built from the gradient orientation histogram in each SIFT point to be rotation invariant. By providing a full set of features (point detector and descriptor), the technique also has its own matching technique which is 2-nearest-neighbors (also known to be 2NN). Since both point detector and descriptor are designed to be scale and rotation invariant, researchers attempt to explore such technique in CMF detection. Huang et al. (2008), the pioneer of SIFT-based CMF detection methods, proved that the SIFT technique could find identical regions in a CMF image. However, the technique is sensitive to small forged regions and computationally expensive.

With the aim to improve the limitations on the Huang et al.'s method, Pan & Lyu (2010) proposed a putative keypoint matching procedure and affine transformation parameter estimation. In the following year, Amerini et al. (2011) introduced the g2NN matching technique to increase the number of matching points in detecting multiple

CMF regions. Then, the method is upgraded by adopting J-Linkage clustering technique to provide more accurate forgery location (Amerini et al., 2013). In the similar year, He et al. (2013) reduced the false matching by applying the Least Median of Square estimation, while Jaberi et al. (2013) recommended to dense the feature pixels using hysteresis thresholding.

Despite the promising results (especially on scale and rotation), the SIFT-based methods do not perform well on flat surfaces and highly uniform features. As a result, the methods could not detect CMF if the forged regions are located at flat areas. Furthermore, the methods may also assume that uniform areas in the natural image as forged regions. Therefore, these limitations developed an open issue for further analysis.

(b) ***SURF***

Instead of SIFT features, the SURF technique is another version of keypoint-based features. Generally, SURF is originated by Bay et al. (2008) to provide faster keypoint features, while maintaining its robustness. In CMF detection, Bo et al. (2010) first introduced the SURF features and matched the features between two subsets. Otherwise, Shivakumar and Baboo (2011) improved the matching procedure with KD-tree technique, thus, the detection is vast to various sizes of forged regions. A more convincing method is shown by Mishra et al. (2013), who applied SURF features with 2NN matching and verified by Hierarchical Agglomerative Clustering technique. Though the method could reduce the false matching features, the recall rate is also reduced.

(c) ***Harris points***

Originally, the keypoint features were started by Harris and Stephens (1988), before SIFT feature extraction technique was invented in the field of computer vision. Also known as Harris Corner Detector, the keypoint features are represented as corners and edges, that are extracted from the regions based on local auto-correlation function. In CMF detection, Harris detector frequently combined with other compatible potential descriptor to resist affine transformation. Moreover, the distribution of points is enhanced to increase the reliability in detecting the forgery.

Chen et al. (2013) was able to improve the SIFT and SURF-based CMF detection methods, with the combination of Harris detector and step sector statistics descriptor. Meanwhile, Zheng and Chang (2014) reported that the combination of Harris detector with SURF descriptor has better accuracy than Chen's method.

Regardless of the issues with SIFT-based methods, the keypoint-based approach in CMF detection is further investigated. To improve the misdetection in highly uniform features, Kakar and Sudha (2012) adapted content-based image retrieval tools which applied Laplacian of Gaussian (with Harris filter) and circular region descriptor. Recently, Uliyan et al. (2016) enhanced the performance by using Harris detector and angular radial partitioning.

To increase the distribution of points on a flat surface, researchers implemented the dense-based point features. Among them are Guo et al. (2013) and Zhao and Zhao (2013) who employed Adaptive Non-Maximal Suppression with DAISY dense-descriptor and dense Harris point with LBP descriptor, correspondingly. However, the combination of Non-Maximal Suppression with Multi-support Region Order-based Gradient Histogram (MROGH) and Hue Histogram (HH) descriptor is able to cover both limitations on a highly uniform texture and flat surface (Yu et al., 2014).

2.3.2.3 Combination Approach

Based on the previous discussion, the dense-based point features are gaining more intention in CMF detection. Thus, researchers started to combine block-based approach with keypoint-based approach. This is evidenced by Silva et al. (2015) who preferred to use SURF features with multi-scale analysis through the block comparison scheme. Another example is presented by Pun et al. (2015), which introduced adaptive over-segmentation scheme using irregular shapes in pre-processing stage before SIFT feature extraction. Instead of using irregular shapes, Ardizzone et al. (2015) proposed triangle segmentation, however, the detections undergo missing regions due to the segmentation being triangle-based.

Though the previous three methods were able to increase the detection performance, the methods do not solve the distribution point problem in homogeneous regions. Therefore, Zheng et al. (2016) employed adaptive segmentation to segregate the smooth region and keypoint region. The smooth region will be analyzed using Zernike moment features while SIFT features is extracted for the keypoint region. Consequently, the method is performed well for both smooth and homogenous areas.

In contrast to all CMF detection methods, Ferreira et al. (2016) proposed a new scheme based on machine learning. Since machine learning algorithms work by learning and predicting data, the authors fused output of eight CMF detection methods as their learning data and predict the CMF image using multi-scale behavior knowledge analysis in the decision making process. Nonetheless, the CMF classification solely relies on the trained features which are built on the eight CMF detection methods that have limitations on certain operations. Instead of image classification, Bappy et al. (2017) proposed pixels classification by training the boundary discrepancy between manipulated and non-manipulated regions with the combination of Long-Short Term

Memory (LSTM) which is based on deep learning algorithms. The method able to localize the manipulated regions not only for CMF image, but also for image splicing.

2.3.3 Current Problems of the existing CMF Detection Methods

In spite of the growing number of improvements in CMF detection, there are several problems identified through these reviews. Firstly, this research realized that the CMF detection methods are evaluated either by three techniques. The techniques comprised of image-level, pixel-level, or both image and pixel-levels. Due to the various levels of evaluation techniques, the CMF detection methods face difficulties in establishing the comparisons.

The second problem, on the other hand, is that the reflection attacks are not highlighted in most of the methods’ evaluations. This is evidenced by the shortage amount of CMF datasets which include the attacks. Therefore, the proof or verifications for the reflection attacks are limited. In order to include the reflection attacks as one of the attacks’ evaluations, this research also considers two common drawbacks recognized by Al-Qershi et al. (2013). The first drawback concerns the ability of the CMF detection methods to deal with all possible types of attacks, particularly, JPEG compression, Gaussian noise, blurring, rotation, scale, and reflection that are used in CMF image. As the second drawback, the CMF detection methods are mainly determined by several thresholds, which the values require a lot of experiments and development.

This research incorporates the identified problems and the drawbacks to turns as several characteristics for evaluations of each method. In particular, the characteristics are evaluation techniques, robustness to all possible attacks, including reflection and amount of threshold selection for the final verification stage. For comparison purposes, several CMF detection methods along with their characteristics are listed in Table 2.1

(sorted by year). The discussion and explanation of each problem are provided as follows:

2.3.3.1 Evaluation Techniques

According to the comparison table, there are various evaluation techniques done by the existing CMF detection methods. 5/14 methods in the table prefer image-level evaluation, 4/14 methods employed pixel-level evaluation, while the remaining 5/14 of the methods consider both image and pixel-level evaluations. This situation has led to inconsistencies of detection performance. For example, although the methods achieve the highest score on image-level, the forgery detection might be included with falsely matching regions. In another case, the whole detection might show the wrong forgery location entirely based on the features' sensitivities. Pixel-level, on the other hand, might not identify the original image, even though the method has the highest score of exact forgery location. Figure 2.10 shows the example of the results from the image-level detection with falsely matching regions and the highest score of pixel-level performance.

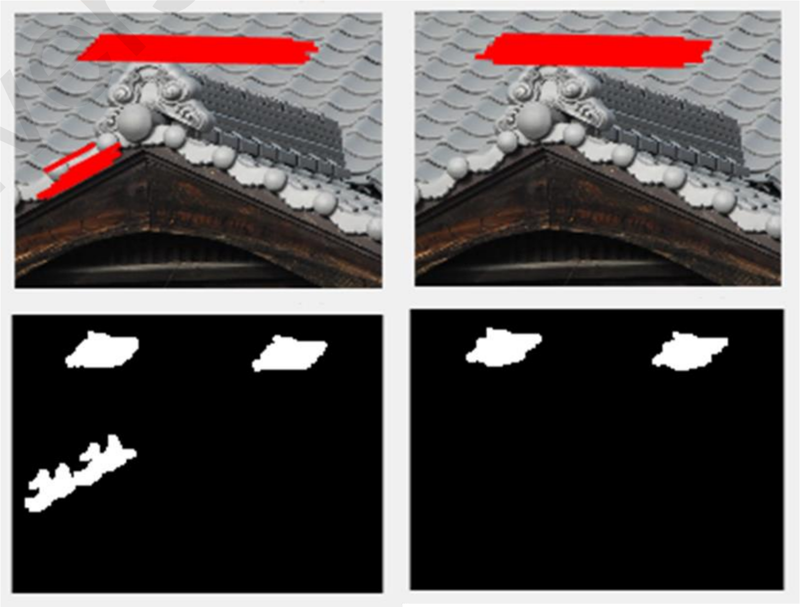


Figure 2.10: The example of detection results. From left: image-level detection includes the falsely matching regions, and the highest score pixel-level performance

Table 2.1: A comparison between selected CMF detection methods in term of their characteristics

Author(s)	Feature Extraction Technique	Evaluation	Robustness against CMF Attacks						Amount of Thresholds (Visualization stage)
		Image/Pixel	JPEG Compression	Gaussian Noise Addition	Variation of Illumination /blurring	Rotation	Scale	Reflection	
(Mahdian & Saic, 2007)	Central Moments	*Pixel*	✓	✓	✓	×	×	×	2
(Y. Huang et al., 2011)	DCT	*Image*	✓	✓	✓	×	×	×	2
(Bravo-Solorio & Nandi, 2011)	1-D descriptor Log Polar	*Image & Pixel*	✓	✓	✓	↓	↓	✓	2
(Amerini et al., 2011)	SIFT	*Image*	✓	✓	✓	✓	✓	×	2
(Muhammad et al., 2012)	DyWT	*Image*	✓	✓	✓	↓	×	×	1
(Lynch et al., 2013)	Average Gray Value	*Image*	✓	✓	✓	×	×	×	1
(Davarzani et al., 2013)	HOG + multi-resolution LBP	*Pixel*	✓	✓	✓	↓	✓	×	1
(Ryu et al., 2013)	Zernike Moments	*Image & Pixel*	✓	✓	✓	✓	↓	×	4
(Zhao & Guo, 2013)	SVD + DCT	*Image & Pixel*	✓	✓	✓	×	×	×	2
(Yu et al., 2014)	NMS + (MROGH + HH)	*Image*	✓	✓	✓	✓	↓	×	1
(Silva et al., 2015)	SURF + multi-scale & voting	*Pixel*	✓	✓	✓	↓	↓	×	1
(Cozzolino et al., 2015)	Zernike Polar	*Image & Pixel*	✓	✓	✓	✓	↓	✓	4
(Emam et al., 2016)	PCET	*Pixel*	✓	✓	✓	↓	↓	×	1
(Bi et al., 2016)	Texture + Moments Descriptor	*Image & Pixel*	✓	✓	✓	↓	↓	×	2
Legend : ✓ Robust × Not Robust ↓ Robust, but, limited to several parameters									

Furthermore, a standard dataset should consider both level of performances in order to execute the evaluations. For image-level evaluation, the total number of original and forged images must be balanced to avoid preference measurement. Evenly, the forged images, including various possible attacks in CMF should be delivered with its ground truth, specifically for pixel-level localization. This is to ensure that the detections are accurate with exact forgery position. Unfortunately, the current CMF datasets (which are publicly available) are inconsistent, due to the various evaluations applied by the methods. In image-level dataset, the forged images, together with its attacks are combined with the original images. Consequently, the total number of original and forged images is unbalanced, because one original image may have more than one attack in CMF image. For that reason, the researchers added a number of original images that might not relate to forged images. Moreover, the ground truth of each forged image is occasionally included. Conversely, in the pixel-level dataset, although the locations of forged regions are delivered, the original image is not examined. Thus, the objective to differentiate the original and forged images is not achievable. This has led to the development of new datasets that cover all requirements. Otherwise, the methods should be tested with a variety of datasets to achieve the desired results.

2.3.3.2 Robustness against CMF Attacks

As translation attack seems compulsory in CMF manipulations, the CMF detection methods are normally evaluated by looking at their sensitivity, specifically towards geometrical transformation attacks. Nonetheless, the methods are incapable of detecting all possible attacks that could be applied in a CMF image. According to the comparison table, each method has limitations on certain attacks. For instance, if the methods are robust to rotation, they are sometimes being sensitive to scale. Similarly, when the methods are robust to scale, they are variant to rotation. Or else, if the methods are resilient to both attacks, the robustness is limited to certain parameters. After all, there are a small number of studies on CMF detection methods who investigated the reflection attack.

Reflection Attack in CMF

Reflection is a process of transmitting each point to its mirror image in a plane (Birkhoff, 1933). Ideally, the transmitted point has the similar distance as well as size with the original region. Furthermore, there is a central line (which is known as axis) between the reflection and the original region. Similar to flipping, the region is reversed along the axis. In CMF, since the reflection attack able to change the form of specific regions, the attack is placed under geometrical transformation, similar to translation, rotation and scale, which is highlighted in Figure 2.11.

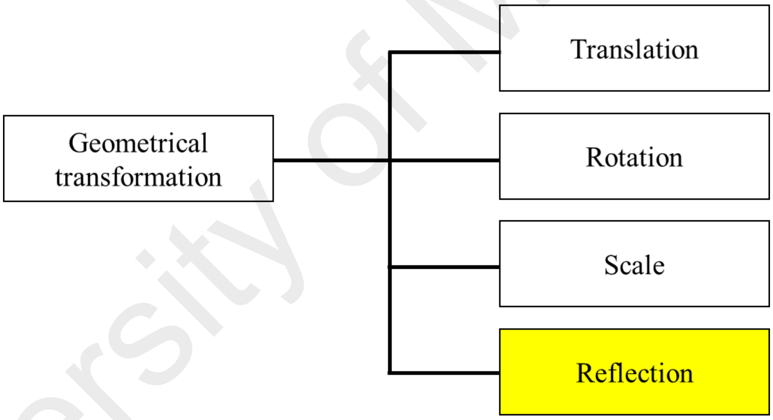


Figure 2.11: Reflection is placed under the geometrical attacks in CMF

Due to the reason that the threats of reflection attack are inevitable, there is an urgent need to provide a CMF detection method that is robust against this type of attack. According to the website (http://www.appbrain.com), there are around 300 free applications related to mirror photo that are available for Android smartphones. The example of the application is Mirror Image - Photo Editor (AppBrain, 2014), which has been downloaded more than 10 million times in three years. Such applications could be a solution to users in creating a CMF with reflection image, without the need to perform any manipulating activity. Figure 2.12 shows the example of the CMF with reflection attacks produced by the Android application.

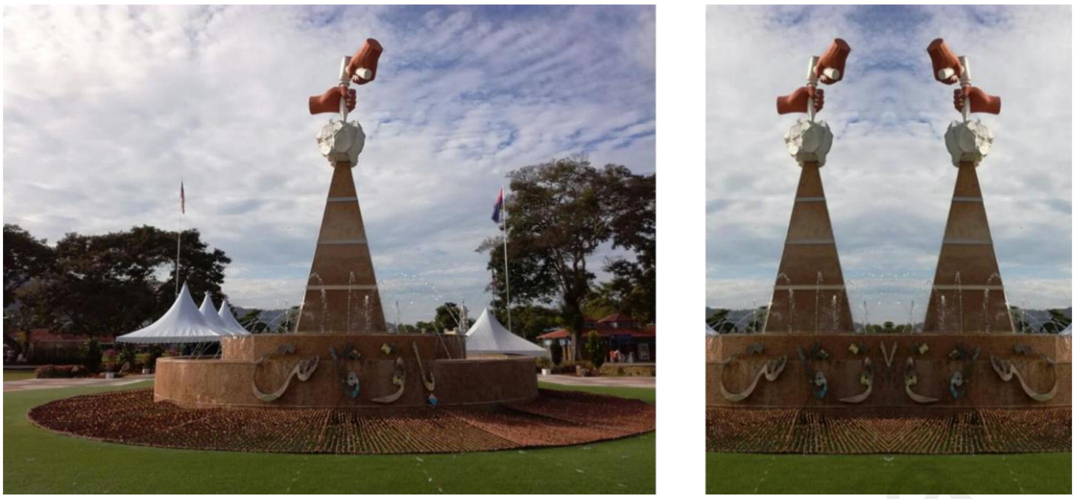


Figure 2.12: Example of original image (left) and CMF with reflection produced by the Mirror Image – Photo Editor application (right)

The Amerini et al.’s method (2011), for example, provides the most stable performance for all parameters of rotation and scale, however, the method is reflection variant. As Bravo and Nandi (2011) were the first to highlight the reflection attacks, the method could not detect small CMF regions and large scale factors. In addition, even though Cozzolino et al. (2015) is robust to reflection, the authors did not consider the attack in their evaluation.

Several Thresholds Selection

Turning to the Cozzolino et al.’s method, the method presents the highest threshold selection in the final verification stage of detection. The method assigned four thresholds, specifically the affine transformation estimation, thresholding, size and distance. Similarly, Ryu et al. (2013) also stated the identical number of thresholds, which include one value for minimum rotation angle estimation, and three values for affine transformation estimation.

As discussed in Section 2.3.1(c), the current practice of the existing CMF detection methods requires a filtering and verification of the preserved matching features. The purpose is to remove the spurious matching results and unwanted noise to get a more precise detection. The selection of an ideal filtering threshold value is important to determine the exact location of the region being forged, while increasing the robustness into various CMF attacks.

Due to the reason that the threshold is predefined to a static value, this will cause difficulties when various characteristics of CMF data that consist of diverse image qualities, sizes, and other elements are applied to the detection process. Generally, the existing CMF detection methods obtained the threshold value through trial & error and several experiments. However, the process becomes more challenging when the range value for each image in a dataset is large. For this reason, a dynamic threshold value is needed to suit the possibility of having diverse input characteristics. Nonetheless, there is a lack of studies on the selection of threshold value in the final stage of detection (visualization). Even though Ustubioglu et al. (2016) automatically defined their threshold value based on the compression history of each input image, their method is limited to post-processing attacks. This is because of the features applied in the whole process of CMF detection is based on DCT. Despite that, their method is the only method that proposed an automatic threshold in CMF detection.

2.4 Chapter Summary

In this chapter, a general overview of image forensics is discussed. Each component in the field is briefly explained. A general review of related literature for CMF detection methods was reported with a new workflow formation. According to the workflow, the methods are described based on the pre-processing stage, namely block-based and keypoint-based approaches. From the methods discussed, two major problems are identified and analyzed in terms of the detection ability and limitations.

CHAPTER 3: RESEARCH METHODOLOGY & DESIGN

This chapter describes the research methodology and design used to achieve the stipulated goals for this research. A structure of the research methodology is established, the data collected is briefly defined, two proposed methods that solve the research problems are introduced, and the evaluations for analysis are explained. Lastly, both methods are combined together with the existing CMF detection methods to discuss the final results. This chapter explained the linkage between Chapter 4, 5, and 6 which then will be further integrated in Chapter 7.

3.1 Introduction

Various CMF detection methods have been reviewed and explained together with their advantages and drawbacks in Chapter 2. However, it is noted from the outcome of the literature review that the current CMF detection methods still suffer from two major problems that need to be examined. The first problem looks at the necessity of both image and pixel-level evaluations in the performance measurement, while the second problem will look into reflection-based CMF attacks. The reflection-based CMF attacks have not been included in prior geometrical transformation analysis. With respect to the problems identification, three objectives have been specified accordingly, as a guide to the selection of methodology and design of this research.

After considering the research problems and questions, experimental-type research design is implemented to achieve the research objectives. The experimental design specifies the control environment and predicts what may occur (independent variable) that affects the result of an experiment (dependent variable) (Anastas, 1999). The control environments are stated while the results are discussed to make a conclusion. In this research, the control variables are the data for the image and pixel-level evaluations and reflection-based CMF attacks. Meanwhile, the performance of each method towards the variables are discussed and analyzed. Therefore, the methodology and design used in this research include the procedures used to collect the data, develop an algorithm, validate and analyze the results.

3.2 Research Methodology and Design

There are three objectives specified in this research. In order to achieve all the research objectives, this research follows a structure as illustrated in Figure 3.1. The figure also summarized all the processes involved in each phase for a general explanation. For detail clarification, this section is divided into five sections, comprising data collection, performance analysis for the existing CMF detection methods, proposing two CMF detection methods, compilation of performance for both existing & proposed CMF detection methods and system requirement. The first phase of the structure (which is Requirement Study) is excluded in this chapter, since the phase has been discussed in the previous chapter (Literature Review). The identified problems from the chapter are the main factors for each selection in the overall process of each phase.

3.2.1 Data Collection

Referring to the first research objective, this research aimed to examine the effects of the image and pixel-level evaluations of CMF detection methods against various possible attacks in the CMF image. Therefore, this research collects and analyzes all the available CMF data in the community. Some of the publicly available datasets are listed in Warif et al. (2016). From the data collections, two datasets are selected which are CombineTranslation and CPHALL that represent simple translation CMF and common CMF attacks, respectively.

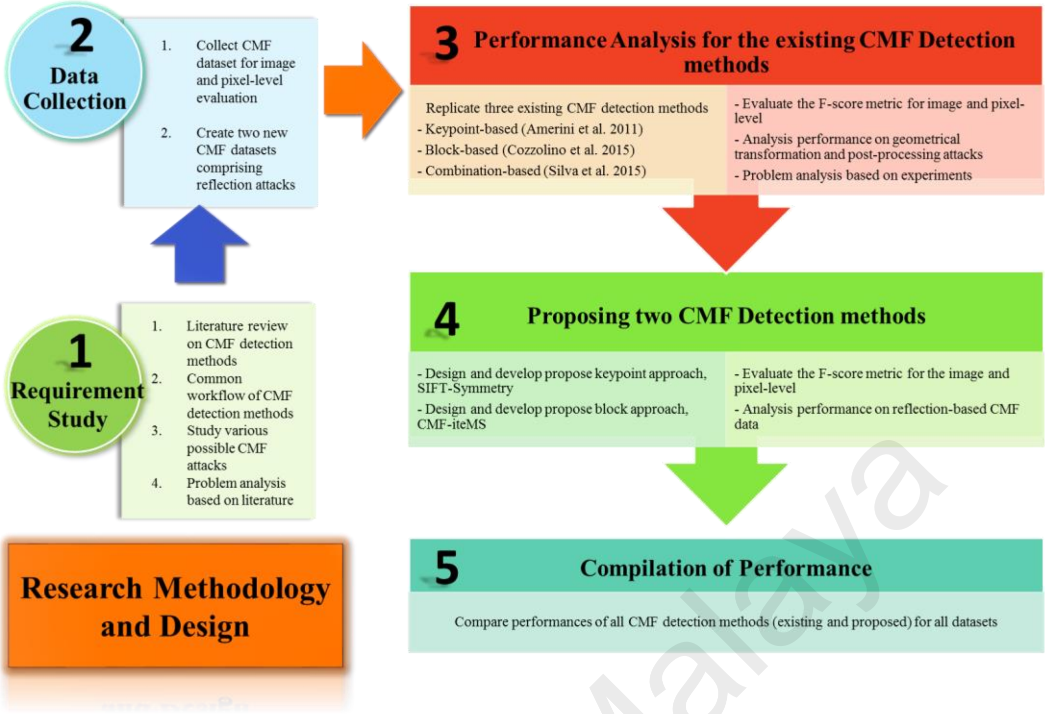

2
Data Collection
1. Collect CMF dataset for image and pixel-level evaluation
2. Create two new CMF datasets comprising reflection attacks
3 Performance Analysis for the existing CMF Detection methods
Replicate three existing CMF detection methods
- Keypoint-based (Amerini et al. 2011)
- Block-based (Cozzolino et al. 2015)
- Combination-based (Silva et al. 2015)
- Evaluate the F-score metric for image and pixel-level
- Analysis performance on geometrical transformation and post-processing attacks
- Problem analysis based on experiments
1
Requirement Study
1. Literature review on CMF detection methods
2. Common workflow of CMF detection methods
3. Study various possible CMF attacks
4. Problem analysis based on literature
4 Proposing two CMF Detection methods
- Design and develop propose keypoint approach, SIFT-Symmetry
- Design and develop propose block approach, CMF-iteMS
- Evaluate the F-score metric for the image and pixel-level
- Analysis performance on reflection-based CMF data
Research Methodology and Design
5 Compilation of Performance
Compare performances of all CMF detection methods (existing and proposed) for all datasets

Figure 3.1: Structure of the research methodology and design

The CombineTranslation dataset is a combination of three datasets comprising GRIP (Cozzolino et al., 2015), D0 (Edoardo Ardizzone et al., 2015), and NB-Casia (newly created). This dataset is named as CombineTranslation because all the forged images in the dataset consist of CMF image with translation attack only. The aim of the compilation is to acquire various types, qualities and sizes of the CMF images, especially for image-level evaluation. This is because the original images are related with the forged images as their ratio is 1 to 1 (1 original image produced 1 translation CMF image). Since the locations of the forged regions are also included, this dataset is also measured by the pixel-level evaluation. This research believes that the biasness on the CMF data could be avoided by combining the three datasets. Alternatively, this research also considers CPHALL (Silva et al., 2015) dataset that covers various common CMF attacks in the collection. However, owing to the reason that the original images are not provided, the performances are evaluated based on pixel-level only.

From the data analysis, the only dataset that considers the reflection-based CMF image in the collection is CASIA v2.0 (Jing & Wei, 2011). However, the dataset consists of 12614 images comprising original, CMF, and splicing images. The images are mixed together, hence, it is difficult to differentiate the types of image and attacks involved. Therefore, two datasets, namely NB-Casia, and NBr-Casia are created, specifically to include the reflection-based CMF attack. The NB-Casia is comprised of the CMF with common attacks, which are the combination of CMF translation with either rotation, scale, or reflection and mix of the attacks. The NBr-Casia, on the other hand, is allocated to specifically assess the results against the combination of CMF reflection with translation, rotation, scale, and mixture of the attacks. Furthermore, the datasets also include original images for image-level evaluation, and mask of the CMF region locations for the pixel-level evaluation.

3.2.2 Performance Analysis for the Existing CMF Detection Methods

This phase of performance analysis is discussed in Chapter 4, specifically for the first objective. The problems identified in the literature review are assessed and analyzed in detail. Several experiments have been carried out to investigate the effects of the image, pixel-level evaluation, and various possible attacks (including reflection), to the existing CMF detection methods. A set of evaluation steps which include both image and pixel-level performance is illustrated and used in the comparative studies. As the literature review divided the existing methods into three approaches, this research replicates the most established method to represent each approach. In particular, Amerini et al. (2011), Cozzolino et al. (2015) and Silva et al. (Silva et al., 2015) signifies the keypoint-based, block-based, and combination of both approaches, respectively. In the experiments, all four datasets are employed as the input image to ensure the reliability of the methods against various types of CMF image.

To validate the performance of each CMF detection method, a shared quantitative way is measured and evaluated. There are several evaluation parameters performed by the researchers in CMF Detection, which are F-score, precision, recall, TPR and FPR. Precision often paired with recall, meanwhile, TPR needs to be paired with FPR. Since precision represents a more perfect value (due to the falsely detected images/pixels are identified), recall rate is also preferred to ensure all CMF images/pixels are detected. Owing to the reason that this research considers various levels of evaluation, only F-score is chosen to get an average of both, precision and recall rates. F-score measure metric is applied to the whole experiments in this research. The F-score indicates an average between precision and recall rate, as defined in Equation (3.1).

$$\mathrm{F} = \frac{2\mathrm{TP}}{2\mathrm{TP} + \mathrm{FN} + \mathrm{FP}} \tag{3.1}$$

where true positive (TP), false negative (FN), and false positive (FP) count, respectively, the number of detected CMF images/pixels, undetected CMF images/pixels, and falsely detected original images/pixels. F-score is also preferred by recent researchers (Jin & Wan, 2017; F. Yang, Li, Lu, & Weng, 2017).

Since there are three evaluation techniques employed in the experiments (which are image-level, pixel-level, and both image and pixel-level), each technique will achieved different F-score results. Image-level evaluation (termed as image score) will employ the image definition, while pixel-level evaluation (termed as pixel score) will use the pixel definition. The image score shows the ability of the detection methods in distinguishing the original image and CMF image, while the pixel score defines the reliability of determining the exact location of the CMF detection. For a fair evaluation, the image score is multiplied by the pixel score, in order to obtain the percentage of detection. An efficient CMF detection method should be able to achieve the highest percentage of detection based on the two scores. This evaluation will determine the ability of the detected CMF image to localize at the exact CMF region. Such metric will be very helpful in comparing the different methods.

For comparison purpose, the three replicated CMF detection methods are tested with three datasets (CombineTranslation, NB-Casia, and NBr-Casia) for image and pixel-level performance, while the CPHALL dataset is limited to pixel-level evaluation only (due to the reason that the original images are not provided).

Instead of comparing the scores on the whole dataset, several analysis on the performance against various attacks are also performed. The analysis are divided into two sections, which are geometrical transformation and post-processing attacks. For geometrical transformation, this research grouped the attacks as simple translation, scale, rotation, simple reflection, reflection-based, and a mix of the attacks. The scores were calculated by averaging the results of each parameter in each group of attacks. Subsequently, for the post-processing attacks, the images in the datasets were applied with four quality factors for JPEG compression and four variances for Gaussian noise addition. The performance for each parameter are also discussed.

3.2.3 Proposing Two CMF Detection Methods

Based on the performance analysis, each approach shows significantly lower results for the newly created datasets (NB-Casia and NBr-Casia) that concern reflection attacks in CMF. Furthermore, the analysis also identifies the limitations of each approach, which the combination approach demonstrates the weakest performance among the tested methods.

Further investigation on reflection-based CMF attacks should be explored, especially for the keypoint and block-based approaches which have the potential to robust on such attacks. As the second objective, this research develops two improved methods (based on keypoint and block-based approaches) for the CMF detection, specifically to cover the reflection attacks. The proposed methods are explained in Chapters 5 and 6, individually. Additionally, each phase will undergo similar structure as illustrated in Figure 3.2 and the general overview of each approach is discussed in the following subsections. Since the purpose of the proposed methods is to cover the reflection-based CMF attacks, NB-Casia and NBr-Casia datasets were selected as the input image for both methods.

3.2.3.1 Method I - Keypoint-based Approach: SIFT-Symmetry

This section briefly describe the flow of the proposed keypoint-based approach (SIFT-Symmetry), from pre-processing until evaluation. The name of the SIFT-Symmetry is given because the SIFT features with symmetry matching technique is implemented in the method. The SIFT-Symmetry is inspired by the keypoint-based CMF detection method (Amerini et al., 2011), since the method provides stability and good performance in scale and rotation. The existing design of the method is modified by including the symmetry matching technique specifically to cater the reflection attacks.

Firstly, the input image will be converted to grayscale to increase the distinctive visual features of salient point. As reflection could change the feature properties of a region, the manipulated region represents as a new region instead. For that reason, the g2NN matching techniques from the prior methods couldn’t find the identical features between the original and the CMF regions. Therefore, the main contribution of the SIFT-Symmetry is the conversion of feature extraction and matching phase to deal with reflection-based attacks. The mirror-SIFT features (paired with symmetry matching technique) will only be commenced if the combination of SIFT features with g2NN matching technique is unable to detect at least five matching points in the image.

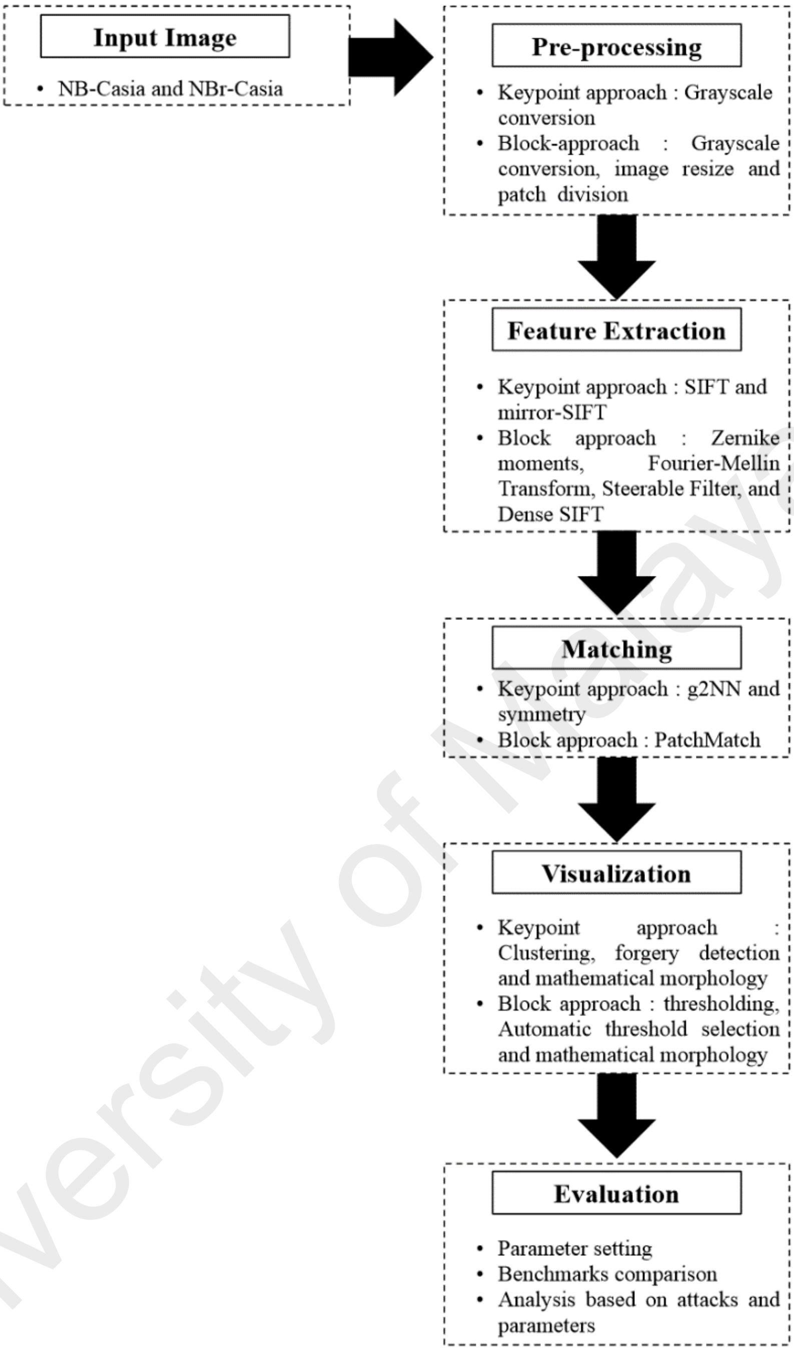

Input Image
• NB-Casia and NBr-Casia
Pre-processing
• Keypoint approach : Grayscale conversion
• Block-approach : Grayscale conversion, image resize and patch division
Feature Extraction
• Keypoint approach : SIFT and mirror-SIFT
• Block approach : Zernike moments, Fourier-Mellin Transform, Steerable Filter, and Dense SIFT
Matching
• Keypoint approach : g2NN and symmetry
• Block approach : PatchMatch
Visualization
• Keypoint approach : Clustering, forgery detection and mathematical morphology
• Block approach : thresholding, Automatic threshold selection and mathematical morphology
Evaluation
• Parameter setting
• Benchmarks comparison
• Analysis based on attacks and parameters

Figure 3.2: Structure of the proposed methods

Finally, the flow ends with the final verification of forgery localization by applying Hierarchical Agglomerative Clustering technique with six linkages. To improve the pixel-level detection, the SIFT-Symmetry is applied with mathematical morphology to form the CMF regions. The whole design of the SIFT-Symmetry is further described in Chapter 5.

For the evaluation, the six linkages of the clustering technique are trained and tested using the six-fold cross validation technique. The highest parameter and linkage are selected as the established parameter setting. The analysis based on each CMF attack and its parameters is also included.

3.2.3.2 Method II - Block-based Approach: CMF-iteMS

Other than proposing SIFT-Symmetry, this research also recommends a block-based approach in CMF detection method which is known as CMF-iteMS. The CMF-iteMS is primarily concerned with threshold value which is assigned at the final stage of CMF detection. Based on the literature, the filtering process in the existing CMF detection methods requires at least one threshold value to remove spurious matching and irrelevant data (considered as noise) before the morphological process. The threshold value should be properly determined to obtain the exact location of the forged region. Nonetheless, most of the threshold values are static, which is troublesome, especially when various characteristics of CMF data exist. Furthermore, the image data may consist of diverse image qualities, sizes, and other elements that can affect the detection process. For this reason, a dynamic threshold value is needed to suit the possibility of having diverse input characteristics.

This section briefly describes the flow of the CMF-iteMS, from pre-processing until evaluation. The name of the CMF-iteMS is given because the method proposed an iterative means of region size as a new automatic threshold selection, specifically to improve the CMF detection. Furthermore, the CMF-iteMS is inspired by the block-based CMF detection (Cozzolino et al., 2015) and the conventional thresholding techniques. The method is selected because of its stability and good performance in various possible attacks, particularly rotation, reflection and a mix of the attacks. Moreover, this research also investigates several feature extraction and conventional thresholding techniques to be combined with the proposed automatic threshold selection technique to enhance the robustness, especially to the reflection attacks.

In the design, four feature extraction techniques are adapted, including Zernike moments, FMT, Steerable Filter and Dense SIFT for the feature extraction phase. As the method is primarily aimed to improve the threshold selection of the block-based CMF detection method, the similar PatchMatch technique in the Cozzolino et al.'s method is applied in the matching phase. Lastly, to verify the CMF regions detection, a new automatic threshold selection technique is proposed based on the performance of four types of conventional thresholding techniques, such as iterative means (Ridler, T.W. Calvard, 1978), class variance (Otsu, 1979), and maximum entropy (Kapur, Sahoo, & Wong, 1980; Yen, Chang, & Chang, 1995). The details of the CMF-iteMS's design method are described in Chapter 6.

For the evaluation phase, several experiments were conducted to find the most robust feature extraction techniques against various CMF attacks. The best match between the feature extraction, conventional thresholding, and the new automatic threshold selection technique that could localize the best detection of the CMF regions is established as the final design of the CMF-iteMS method. Furthermore, the CMF-iteMS is also tested with the high resolution image dataset (namely FAU (Christlein et al., 2012)) to verify the effectiveness of the methods towards larger size of images. Similar to the SIFT-Symmetry, the analysis is based on each CMF attack and its parameters are also included.

3.2.4 Compilation of Performance

In the subsequent analysis, the two proposed methods are also evaluated with other datasets (CombineTranslation and CPHALL), while the results are compiled with the performance analysis in Chapter 4. The processing time for all methods are also discussed. As the additional evaluation, this research attempts to combine all individual methods (Amerini et al., Cozzolino et al., Silva et al., and SIFT-Symmetry) with the new iterative means of region size, (iteMS) procedures as an automatic threshold selection in the final verification stage. The results before and after the implementation are compared and discussed thoroughly with the proposed CMF-iteMS. The findings are discussed and concluded to get the most efficient CMF detection method that covers all attacks, including reflection, for image and pixel-level evaluations.

3.2.5 System Requirement

The CMF images were created using Adobe Photoshop and MATLAB R2014b. Besides that, all the proposed CMF detection methods were simulated using MATLAB R2014b. All experiments were performed on the following machine:

- Intel Core i5 processor (1.60 GHz) with 4 GB memory

3.3 Chapter Summary

In this chapter, the research methodology and design are presented which describe the whole implementation of the proposed methods for CMF detection. A more specific detail for each method and results are discussed in the next four chapters.

CHAPTER 4: PERFORMANCE ANALYSIS I

In this chapter, the problems identified in the literature review are verified and established. To verify the problems, the level of evaluations used in measuring the performance of the existing CMF detection methods are analyzed. Next, the performance of the existing CMF detection methods are measured and analyzed based on a set of evaluation steps that include both image and pixel-level of evaluations against various CMF attacks in four different datasets. Three state-of-the-art methods (Amerini et al. (2011), Cozzolino et al. (2015), and Silva et al. (2015)) were replicated to represent the three approaches that are available in the literature. The performances are further analyzed based on each group of attacks in each dataset.

This chapter is divided into six main parts: in the first section (Section 4.1), both levels of evaluations are discussed while the experimental setup is briefly introduced. Then, each level of evaluation is analyzed in the second section (Section 4.2). Based on the analysis, a set of evaluation steps (with a new calculation) is described in the third section (Section 4.3). By implementing the evaluation steps, the experimental results are discussed based on each group of CMF attacks in the fourth section (Section 4.4). Lastly, the fifth section (Section 4.5) concludes with a final discussion and summarized the whole chapter in the sixth section (Section 4.6).

4.1 Introduction

Based on the review in Chapter 2, the existing CMF detection methods are evaluated by two types of levels. The first level is image-level evaluation, while the second level is pixel-level evaluation. Although there are methods that consider both levels of evaluations, most of the methods only prefer one type of evaluation (e.g solely rely on either image or pixel-level evaluation).

This research analyzed each level of evaluation and a set of evaluation steps that include both levels is suggested to compare the performance of the existing CMF detection methods. In view of the fact that each level of evaluation has different meaning, a CMF detection method supposedly satisfies adequate performance for both image and pixel-level evaluations. Therefore, the percentage of detection that cover both levels of evaluations is also measured.

In this chapter, the performances of the existing CMF detection methods are assessed with various types of attacks which may be possible in CMF. Two CMF datasets, which are publicly available in the websites were selected to cover the various characteristics in CMF image, comprising CombineTranslation and CPHALL. Furthermore, as the reflection-based CMF data is limited in the community, this research designed two new datasets, namely NB-Casia and NBr-Casia to highlight the second problem of this research. The NB-Casia contains the common CMF attacks, including reflection while the NBr-Casia consists of reflection-based CMF attacks. Subsequently, the results of the image, pixel, and percentages of both levels against the attacks are examined.

4.2 Analysis of the Performance Evaluations

In the meantime, there are three evaluations of performance in the existing CMF detection, either through image-level, pixel-level and both image and pixel-levels. The image-level evaluation is performed to measure the ability of the CMF detection methods in differentiating an original image and a CMF image. Meanwhile, the pixel-level evaluation is implemented to verify the detection location of the CMF.

Generally, the selection of the level-evaluation will determine the data collections in the experiment. For image-level evaluation, the data involved original and CMF images while for pixel-level evaluation, the data should deliver the CMF images together with the exact location of the forged regions. Consequently, if the researchers chose image-level evaluation, the CMF data for pixel-level can't be appointed. Similar situations occurred if the researchers select pixel-level evaluation, where the CMF data for image-level evaluation is excluded. Furthermore, if the researchers want to consider both levels of evaluation, they need to select the CMF data that contains both original image and locations of the forgery. These conditions have encouraged other researchers to develop a new dataset since the available datasets are not suitable for their preferred level of evaluation. For that reason, numerous CMF detection methods and data later could be abandoned for comparisons, since the process of adjustment of the existing CMF detection methods required several efforts and becomes more challenging.

Regardless of the situations, it is important to establish the level of evaluations in measuring the performance of the CMF detection. Therefore, this section analyzed each level of evaluation, and illustrated a set of evaluation steps to be followed by future researchers. The ideas and limitations of each level of evaluation are described in the following subsections.

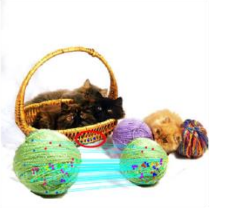
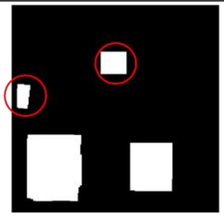
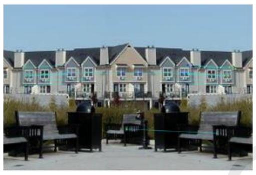
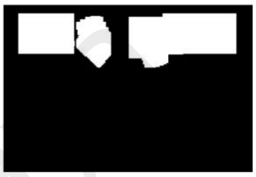
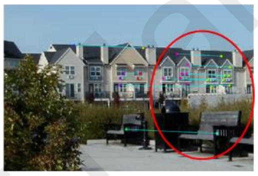
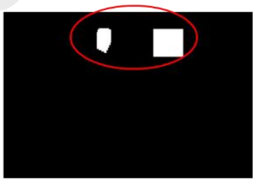
4.2.1 Image-level Analysis

Referring to the purpose of the image-level evaluation (which is to differentiate the original and forged images), the performance relies on the number of images in the dataset, which the higher number of images will produce more precise results. In addition, the current practice of the image-level evaluation requires the total number of CMF and original images to be balanced in a dataset. However, since the CMF images are often tested with several categories of attacks, the original images that are included in the dataset might not be related to the CMF images. The example is shown by the MICC-F220 dataset (Amerini et al., 2011). The dataset consists of 220 images, from which 110 are the original images and another 110 are the CMF images. In spite of the equal quantity of the two types of image, only 11 images have been selected (from the original images) to be applied with another 10 parameters of attacks; which 1/10 parameter is for simple translation, 4/10 parameters are for scale, 3/10 parameters are for rotation and the remaining 2/10 parameters are for mix of rotation and scale. This has led to the biased evaluation, since most of the examined original images are not originated from the forged images. As a suggestion, although the number of images is equal, the original images should be paired with its forged images (with any categories of attacks) to avoid any preference evaluation.

Another limitation on the image-level evaluation is the detection of the CMF does not guarantee the location of the forged regions is true. This is because researchers are focusing on the forged image identification, not the location of the forged region. Table 4.1 lists and presents three examples of false detection results by the methods from Amerini et al. (2011) and Silva et al. (2015). From the table, the first example shows that the CMF image is correctly detected as CMF, but the detection of locations include wrong forged pixels. This is due to the spurious matching arisen by both methods. The second example is the worst case scenarios, in which all the detected pixels are wrong, even the image is successfully identified as a CMF image. In the third example, a genuine unforged image is detected as original image. However, some false detection pixels still visible in both Amerini et al.'s and Silva et al.'s output.

Owing to the reason that the three examples (might be more than three) often happen in a detection, the methods that solely rely on image-level evaluation can be doubtful. That is the reason why pixel-level evaluation is required, which is discussed in the next section.

Table 4.1: Example of false detection results by Amerini et al.'s and Silva et al.'s methods

Example	Input Image	Output	
		Amerini et al.	Silva et al.
Input : CMF image Output : truly detected as CMF image Note : red regions represent the false detected regions			
Input : CMF image Output : truly detected as CMF image Note : red regions represent the forged regions (that are not detected)			
Input : Original image Output : truly detected as original image Note : red regions represent the original regions (that are wrongly detected)			

4.2.2 Pixel-Level Analysis

Since the image-level evaluation becomes unconvincing due to the false detection results that might be occurred, a number of researchers improved the evaluation by validating the detection by pixel-level evaluation. In this case, a set of ground truth images that contain the exact locations of the forged regions has to be created in the dataset. The current practice of the ground truth image creation is by providing a binary image with at least two regions (with a white area) as the copied and pasted areas. Therefore, in order to calculate the performance, the detected pixel should also be in binary form to be compared with the ground truth.

To measure the performance, the metrics are defined as true positive (TP) for the number of detected forged pixels, whereas false negative (FN) refers to undetected forged pixels, and false positive (FP) describes the falsely detected original pixels. The score is averaged to the whole CMF images in a dataset to obtain the whole performance for a full dataset. Figure 4.1 illustrates the measure metrics definition for one image.

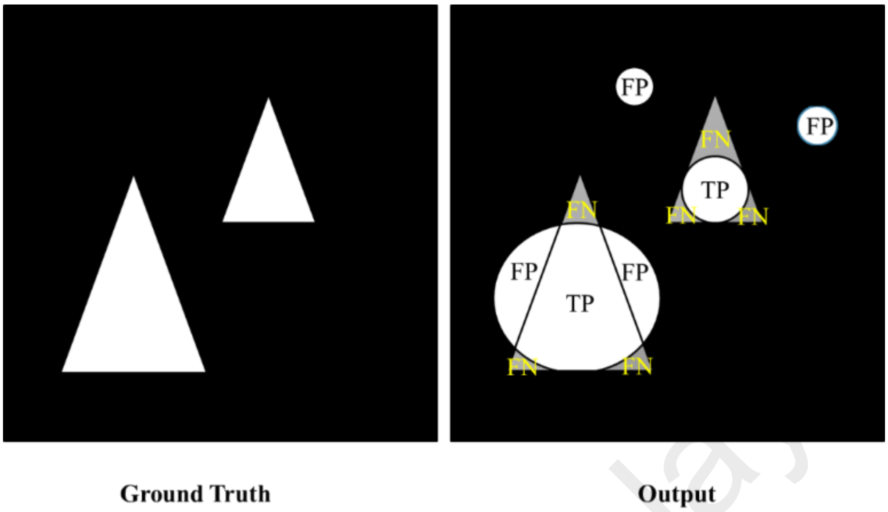


Figure 4.1: Example of ground truth (left) and the detection result with each measure metric

Even though the pixel-level evaluation gives positive effects on the forgery localization, this level of evaluation could not be applied to the keypoint features. This is because the keypoint features are detected by points (in which one point represents only one pixel), not the regions. Although the point detected was densed to certain pixels, the covered area could not include the whole detected region that will resulting on low recall rate. Therefore, a human interpretation might be needed in order to compare the results with the ground truth image. However, the human interpretation is not preferred due to the reason that the decision is affected by human desired results. Figure 4.2 shows the detection results by the Amerini et al.'s method that uses keypoint features for clustering-based, dense-based and human interpretation-based.

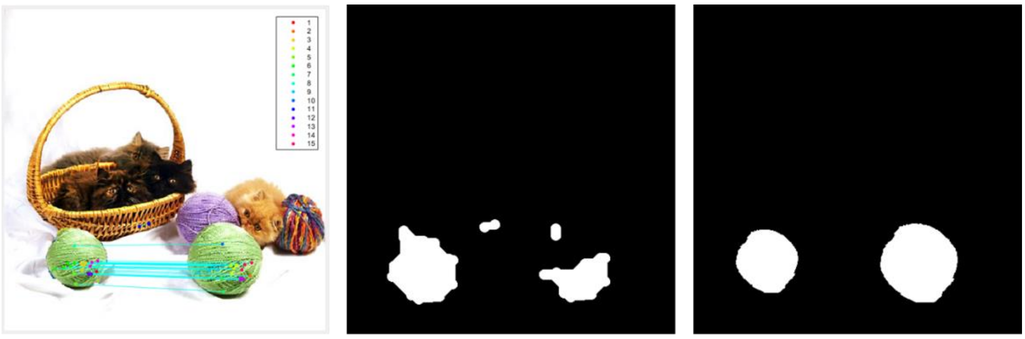


Figure 4.2: Example of detection results by Amerini et al. for (from left) clustering-based, dense-based, and human interpretation-based

4.3 A set of Evaluation Steps

Based on the analysis in the previous sections, both levels of evaluations are significant. Hence, this research believed that a CMF detection method should be measured for both image and pixel-level evaluations for a fair evaluation. Therefore, a set of evaluation steps that cover both levels is illustrated, which later, all new creation of the CMF data should satisfy the steps. Figure 4.3 presents the evaluation steps for a CMF detection method that describe the idea of each level. The explanation of each step is described in the next paragraphs.

Firstly, the methods should be able to detect any input image either as original or CMF. According to the figure, a CMF detection method will define the status of the input image. The number of CMF images, which truly detected as CMF images (TP), and undetected as CMF images (FN), together with the number of original images that are falsely detected as CMF images (FP) is recorded to measure the performance. Therefore, the performance solely relies on the number of original and CMF images in a dataset. The image-level dataset should have at least an equal number of both original and CMF images. If possible, the CMF image should be paired with its original image to avoid a biased evaluation.

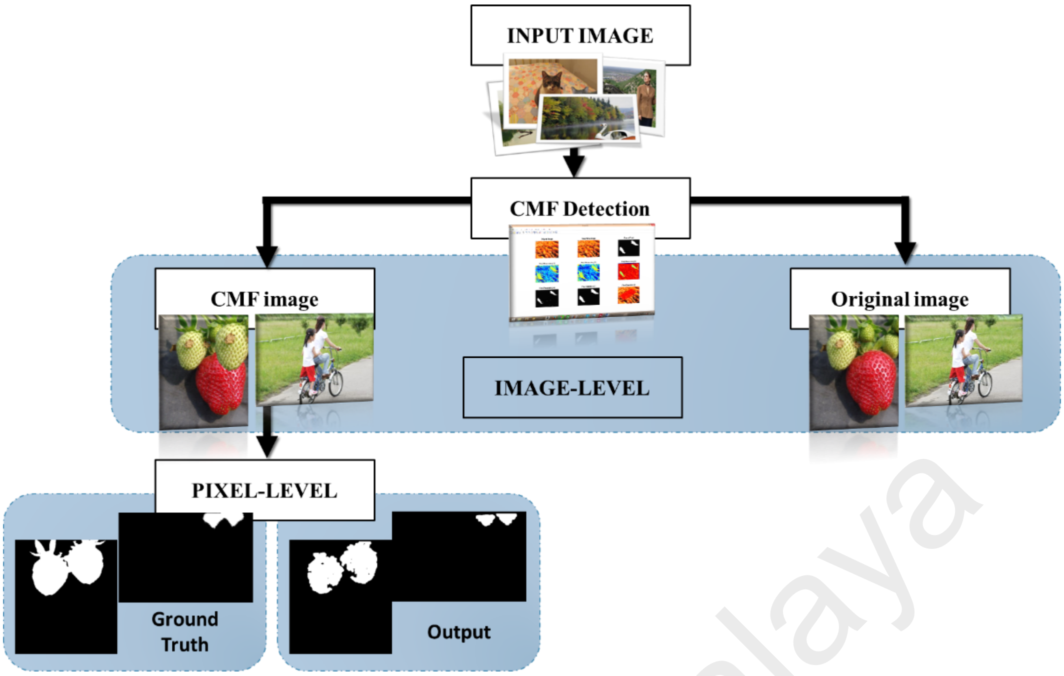


Figure 4.3: A set of evaluation steps for a CMF detection method

Then, once the image is considered as a CMF, pixel-level evaluation is required to ensure the detection location is true. The pixel-level evaluation compares the detection regions with the exact locations of the CMF regions. To obtain the score for the whole dataset, the average score for each image is summed and divided with the number of images in the dataset.

Both performances are multiplied to get the overall percentages of the detection. Table 4.2 lists the example results for the image score, pixel score and percentage of both scores. The summarized results are:

1. If image score is 90% and pixel score is 90%, the percentage of the detection is 81%
2. If image score is 90% and pixel score is 60%, the percentage of the detection is 54%
3. If image score is 60% and pixel score is 60%, the percentage of the detection is 36%
4. If image score is 90% and pixel score is 20%, the percentage of the detection is 18%
5. If image score is 20% and pixel score is 60%, the percentage of the detection is 12%

Table 4.2: List of example results for image score, pixel score and percentage of detection

Example	Image Score	Pixel Score	Percentage of Detection
1	0.900	0.900	0.810
2	0.900	0.600	0.540
3	0.600	0.600	0.360
4	0.900	0.200	0.180
5	0.200	0.600	0.120

The results show that the image-level is the highest importance, while the false detection in the CMF location is able to reduce the percentages. Furthermore, even if the location of detection is correct, the percentage will be dropped if the methods unable to detect an original image.

4.4 Experimental Results and Performance Analysis

To verify the analysis, the set of evaluation steps and the percentage of detection are implemented in this evaluation studies. The purpose of this evaluation studies is to measure the performance of the existing CMF detection methods against various possible attacks in CMF by using the evaluation steps. For the experimental setup, three existing CMF detection methods were replicated with each method representing the three approaches available in the literature. To be specific, the Amerini et al.'s (2011), Cozzolino et al.'s (2015) and Silva et al.'s (2015) method is selected to indicate the keypoint-based, block-based, a combination of both approaches, respectively.

This research compares two features, comprising Zernike moments and FMT particularly for the Cozzolino et al.'s method. It is also noted that based on the literature, the Amerini et al.'s method is designed specifically for image-level evaluation, while the Silva et al.'s method is measured in pixel-level performance. Therefore, the detected SIFT points which obtained from the Amerini et al.'s method are thickened (densed) for 10 pixels and applied with the mathematical morphology (dilation) to form a region. Meanwhile, for Silva et al.'s method, an input image is defined as a CMF image when there is at least one pixel detected as forged in the evaluation.

The overall performance were tested on four datasets, which two of those are the publicly available CMF datasets while the remaining two datasets are the newly created datasets. The results were also studied based on several groups of attacks in CMF. The details of the experimental results and analysis are discussed in the following subsections.

4.4.1 Datasets

To assign the input images for CMF detection, the CombineTranslation and the CPHALL datasets were selected from the available CMF datasets. The CombineTranslation was chosen specifically to obtain a fair evaluation for image-level, while the CPHALL was appointed to verify the performance against various CMF attacks in an available dataset. The details of the datasets are described as follows:

(a) ***CombineTranslation***

CombineTranslation is comprised of simple translation CMF images. In order to obtain various qualities and sizes, three datasets which are publicly available for CMF were combined. The datasets are GRIP (Cozzolino et al., 2015) (160 images), D0 (Edoardo Ardizzone et al., 2015) (100 images) and NB-Casia (30 images) which the resolutions are 768×1024, 700×1000, 240×160 and 900×600, respectively. A total of 290 images were collected, including 145 CMF-translation images and 145 original images. As the only attack involved is translation, the ratio of the original images and the CMF images is 1:1, therefore, could provide an equitable evaluation for image-level performance. Due to the availability of both original image and ground truth, the performance is measured by image and pixel-level.

(b) CPHALL

In contrast with CombineTranslation dataset, CPHALL is comprised of CMF images with its combination of geometrical transformation attacks. However, CPHALL is only limited to non-reflection CMF images, while the original images are not provided. Hence, the detection performance was measured by pixel-level, which matched with the ground truth images. The total images in the dataset are 108, comprising 23 images for simple translation, 26 images for scale, 25 images for rotation, and 34 images for mix of attacks. The resolutions of the images in the dataset vary from 845×634 to 1296×972.

4.4.1.2 Newly Creation Datasets

Instead of focusing on the image and pixel-level evaluations, this analysis includes the second problem stated in this research as one of the criteria in the CMF image. To recap, the second problem identified in the literature review is the CMF with reflection attack has not been focused and evaluated in the existing research. This is proven by the shortage amount of available datasets that provide the attacks in the collection.

Based on the previous chapter (Chapter 3), the only dataset that provides the CMF image with reflection attacks is Casia v2.0, however, the images are mixed with other types of image manipulation techniques. For that reason, this research creates two new datasets, namely NB-Casia and NBr-Casia which are comprised of common CMF attacks (translation, scale, rotation), including reflection and reflection-based attacks (simple reflection, reflection with scale, reflection with rotation and mixture of the reflection), respectively. Figure 4.4 shows two examples of original images, CMF with a simple transformation in NB-Casia and reflection-based attacks in NBr-Casia dataset. The setup of all datasets is described in the following:

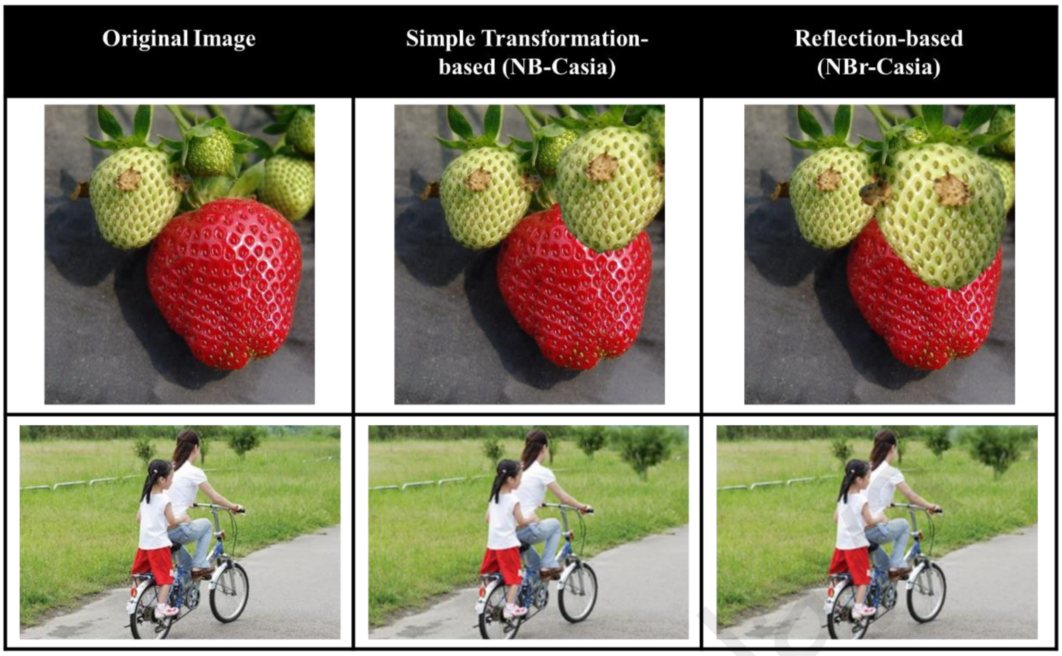

Original Image
Simple Transformation-based (NB-Casia)
Reflection-based (NBr-Casia)

Figure 4.4: From left: examples of original image, simple transformation CMF image and reflection-based CMF image

(a) NB-Casia

This dataset is composed of 510 images: 255 are original images and 255 are CMF images, which the original images were taken from the CASIA v2.0 (Jing & Wei, 2011) dataset. The resolution of the images may varies from 240×160 (the smallest) to 900×600 (the highest). 15 images from the original images were selected to create the 17 parameters of CMF images as listed in Table 4.3. A region on an image was copied and applied with the simple transformation attacks, comprising translation, scale, rotation, reflection and a mix of the attacks before being pasted on the image.

According to the table, the CMF images were divided into five groups of attacks, namely, simple translation, scale, rotation, simple reflection, and the mixture of simple translation, scale, and rotation. s_x and s_y refer to the scale factor when the copied region is scaled horizontally and vertically, respectively. On the other hand, $\theta°$ denotes the degree of rotation, while axis defines the flipped axis for the reflection attack. The dataset is freely available at the following website: https://github.com/nurbaqiyah/CMF-Dataset.

Table 4.3: Different combinations of geometrical transformation applied to the CMF image in the NB-CASIA dataset

Parameter / Group of Attack	s_x	s_y	$\theta°$	axis
Simple Translation	1	1	0	0
Scale	0.6	0.6	0	0
	0.8	0.8	0	0
	1.2	1.2	0	0
	1.4	1.4	0	0
	1.6	1.6	0	0
Rotation	1	1	20	0
	1	1	40	0
	1	1	60	0
	1	1	120	0
	1	1	240	0
Simple Reflection	1	1	0	y
Mix of attacks	1.2	0.8	0	0
	1.2	1.4	0	0
	1.2	0.8	20	0
	1.2	1.2	40	0
	1.6	0.8	330	0

(b) NBr-Casia

Instead of NB-Casia, this research also created a new dataset for reflection-based CMF images, called NBr-CASIA. This dataset consists of 480 images: 240 are original images and 240 are reflection-based CMF images. The overall setup of the dataset was similar to the NB-CASIA, except that all copied regions were horizontally flipped (summarized in Table 4.4). The CMF images were divided into four groups composed of simple reflection, reflection with scale, reflection with rotation, and the combination of reflection with scale and rotation manipulation.

Table 4.4: Different combinations of geometrical transformation applied to the reflection-based CMF image in NBr-CASIA dataset

Parameter / Group of Attack	s_x	s_y	$\theta°$	axis
Simple Reflection	1	1	0	y
Reflection with Scale	0.6	0.6	0	y
	0.8	0.8	0	y
	1.2	1.2	0	y
	1.4	1.4	0	y
	1.6	1.6	0	y
Reflection with Rotation	1	1	20	y
	1	1	40	y
	1	1	60	y
	1	1	120	y
	1	1	240	y
Combination of Reflection with other attacks	1.2	0.8	0	y
	1.2	1.4	0	y
	1.2	0.8	20	y
	1.2	1.2	40	y
	1.6	0.8	330	y

4.4.2 Performance Evaluation

In this section, the results of the existing CMF detection methods (Amerini et al., Cozzolino et al. (Zernike moments and FMT) and Silva et al.) were compared against four datasets (CombineTranslation, CPHALL, NB-Casia, and NBr-Casia). Table 4.5 lists the overall results for image-level, pixel-level, and percentages of both detections in all datasets, except CPHALL, which is only evaluated using pixel-level performance. According to the table, the Cozzolino et al.'s method with Zernike moments features achieved the highest score for CombineTranslation and NBr-Casia datasets for all, image-level, pixel-level, and percentage of both levels. For NB-Casia dataset, the Amerini et al.'s obtained the highest score, but is limited to image-level only, while the Cozzolino et al.'s with FMT features is much better for pixel-level and percentages of both levels. Furthermore, the FMT features also performed the best in CPHALL dataset. Among all tested CMF detection methods, the Silva et al.'s doesn't show much improvement compared to others, even with their dataset (which is CPHALL).

Table 4.5: Performance of the existing CMF detection methods in four datasets

All Datasets/Methods		Amerini et al. (2011)	Cozzolino et al. (2015) --ZM	Cozzolino et al. (2015) --FMT	Silva et al. (2015)
CombineTranslation	Image Score	0.724	**0.896**	0.880	0.737
	Pixel Score	0.574	**0.901**	0.884	0.740
	Percentage of Detection	0.416	**0.807**	0.778	0.545
NB-Casia	Image Score	**0.814**	0.654	0.745	0.667
	Pixel Score	0.549	0.557	**0.634**	0.548
	Percentage of Detection	0.447	0.364	**0.472**	0.365
NBr-Casia	Image Score	0.004	**0.593**	0.496	0.226
	Pixel Score	0.003	**0.491**	0.325	0.010
	Percentage of Detection	0.000	**0.291**	0.161	0.002
CPHALL	Pixel Score	0.551	0.825	**0.859**	0.647

Based on the performance results, the FMT features improved the Zernike moments features in terms of scale and variations of illuminations attacks only because the Zernike moments features is variant to scale and illumination changes (Kim & In-So, 2002). In spite of that, the SIFT features applied by the Amerini et al.'s show superior performance in term of image-level evaluation, however, due to the reason that the SIFT features are unable to form a region, the Amerini et al.'s scores were decreased for pixel-level evaluation and percentage of detection. For further analysis on each method against each dataset, the results listed in the table were further divided according to the five groups of geometrical transformation attacks. The detail analysis are discussed in the next subsections.

4.4.2.1 Analysis against Geometrical Transformation Attacks

In this section, this research analyzed the performance based on five groups of attacks, which are simple translation, scale, rotation, reflection, and mix of attacks. The performance for CombineTranslation, NB-Casia and NBr-Casia datasets are measured by image score, pixel score, and percentages of both scores, while the analysis are verified by the CPHALL dataset in pixel score. The analysis is divided into four subsections, specifically, simple translation attack, common CMF attacks (scale, rotation, simple reflection, and mix), reflection-based CMF attacks and common attacks in CPHALL.

For the NB-Casia dataset, the images were grouped based on the attacks. 1/17 of the images is simple translation, and another 1/17 is for simple reflection. Meanwhile, the remaining 15/17 of the images are divided into other groups, which 5/17 images are for scale, 5/17 images are for rotation, and another 5/17 are for mix groups. The image-level performance were calculated by averaging the results of 15 original images with its 15 CMF images for each parameter in each group of attacks. Furthermore, the CombineTranslation dataset was discussed in simple translation attack subsections, while the NBr-Casia dataset was explained under the reflection-based CMF attacks subsections. It is also noted that the original images in all datasets were excluded for the pixel-level evaluation.

(a) ***Simple Translation***

Basically, simple translation attack in CMF is the simplest operation in CMF manipulations. However, the detection performance are dependent on the types of images and CMF regions in a dataset. Before analyzing the simple translation attack, this research studies the images in both, CombineTranslation and NB-Casia datasets to come out with the analysis. CombineTranslation, which are the combination of three datasets (GRIP, D0, and NB-Casia) have diverse image resolutions. The majority of the images is belonging to GRIP dataset, which the CMF regions in the images often consists of flat, uniform and natural regions. Meanwhile, the CMF regions in D0 and NB-Casia datasets are more rigid and simple. Nonetheless, the images in NB-Casia dataset has small resolutions with various illuminations that are harder to be detected.

Figure 4.5 presents the results of image score, pixel score, and percentage of both scores for the existing CMF detection methods against simple translation attack in both, CombineTranslation and NB-Casia datasets. According to the figure, this research confirmed that all the existing CMF detection methods work well with simple translation CMF image, which were able to achieve a minimum image score of 72% and 80% for CombineTranslation and NB-Casia dataset, respectively. Nevertheless, due to the reason that the Amerini et al.'s method has low recall rate for the pixel-level evaluation, the minimum percentages of detections were dropped to 42% for the CombineTranslation dataset.

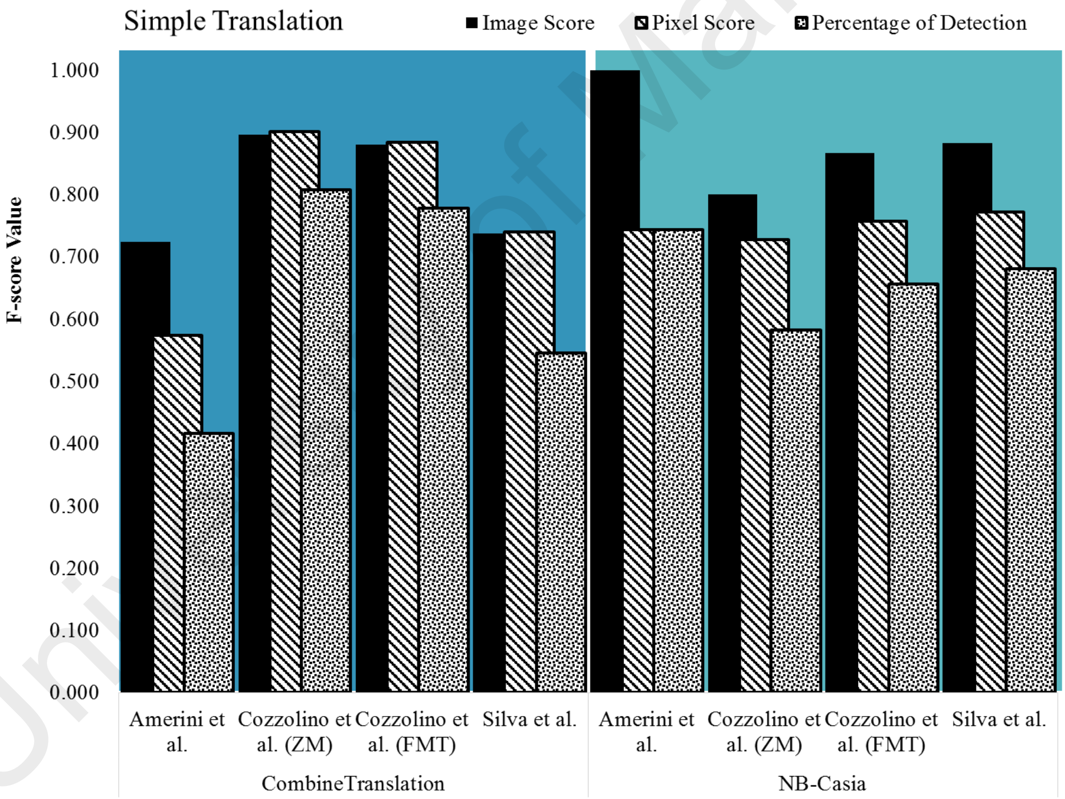


Figure 4.5: Comparative results (image score, pixel score, and percentages of both scores) for the existing CMF detection methods against simple translation attack in CombineTranslation and NB-Casia datasets

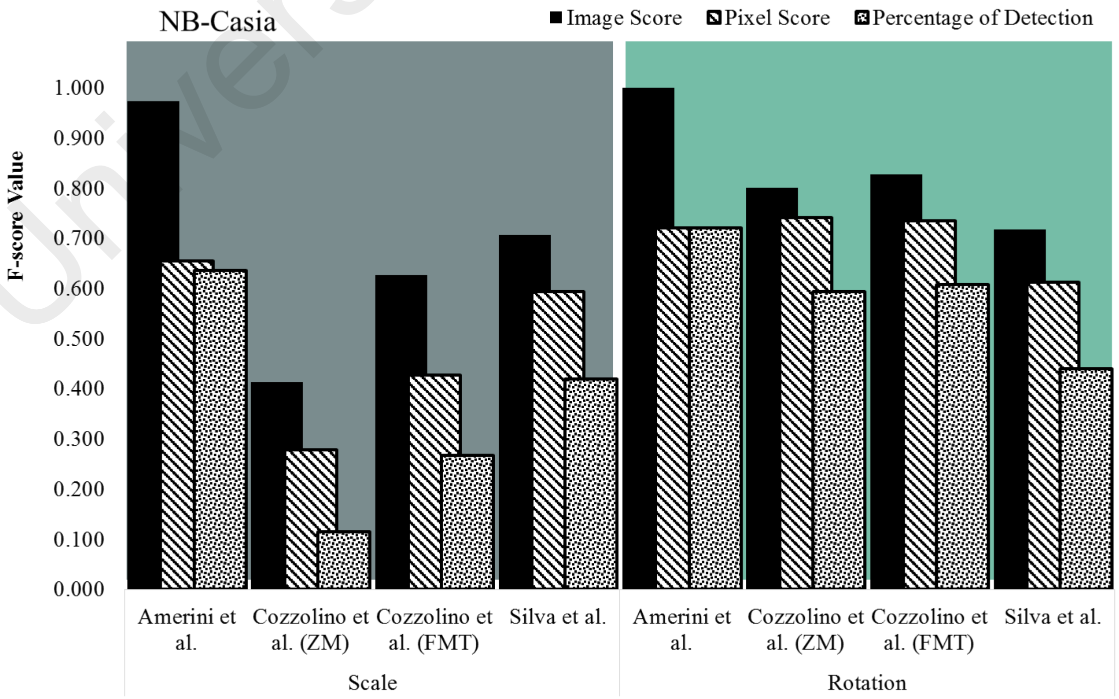
In particular, the Cozzolino et al.'s method with Zernike moments features achieved the highest score of all level evaluations for the CombineTranslation dataset, compared to other methods. The reason is the Zernike moments features has distinctive ability that may reduce the redundancy in features, while being able to describe the shape of objects very well (Q. Yang, 2014). In contrast, the SIFT point features in the Amerini et al.'s method is sensitive to flat and uniform regions (Amerini et al., 2011). Thus, the method couldn't detect any CMF with flat region, while regularly detecting the uniform regions as CMF. In addition, as Silva et al.'s improves the keypoint detection by block segmentation, they are able to improve the recall rate in the pixel-level compared to Amerini et al.'s method.

On the other hand, the performance of the Cozzolino et al.'s method with Zernike moments was dropped for the NB-Casia dataset. This is because the Zernike moments were unable to detect three images in the dataset, which have small and various illuminations. Since the Mellin transform has the advantages on scale and illumination invariant (Carkir & Cetin, 2010), the method with FMT features was able to improve the detection in the dataset. Furthermore, several predefined thresholds in the final verification steps of the Cozzolino et al.'s method has limit the performance of the method from being higher, especially when dealing with small resolution images. Hence, the results of both Amerini et al.'s and Silva et al.'s were higher than the Cozzolino et al.'s method due to the reason that keypoint features is robust to illumination changes (Mishra et al., 2013) while not being affected by the image size.

(b) ***Common CMF Attacks (Scale, Rotation, Simple Reflection and Mix Attacks)***

The performance of the existing CMF detection methods against NB-Casia dataset were continuously analyzed based on the common attacks in CMF. Figure 4.6 shows the results of image score, pixel score, and percentages of both scores for the existing CMF detection methods against common attacks, specifically scale, rotation, simple reflection and mix attacks in NB-Casia dataset.

Even though the Amerini et al.'s method achieved the highest performance against simple translation attack in NB-Casia dataset, the results were dropped when dealing with other attacks in CMF. They maintained the highest percentage of detection for scale and rotation attacks, but obtained the lowest percentage for simple reflection and mix of attacks. This is because the matching technique was not able to find any similar features for the reflection attacks and the performance will be dropped whenever large scale was combined with large rotation. The performance of Silva et al.'s method, on the other hand, was the lowest for rotation due to the reason that SURF features are sensitive to the large rotation degrees (Juan & Gwun, 2009). Furthermore, even though the Silva et al.'s method was able to obtain 29% of image score for simple reflection, they actually detects wrong CMF regions. Meanwhile, for the scale attacks, the detection often includes several false alarms, even they achieved the second highest performance. Figure 4.7 presents the examples of the false alarms in the detection of the Silva et al.'s method for simple reflection and scale attacks in NB-Casia dataset.



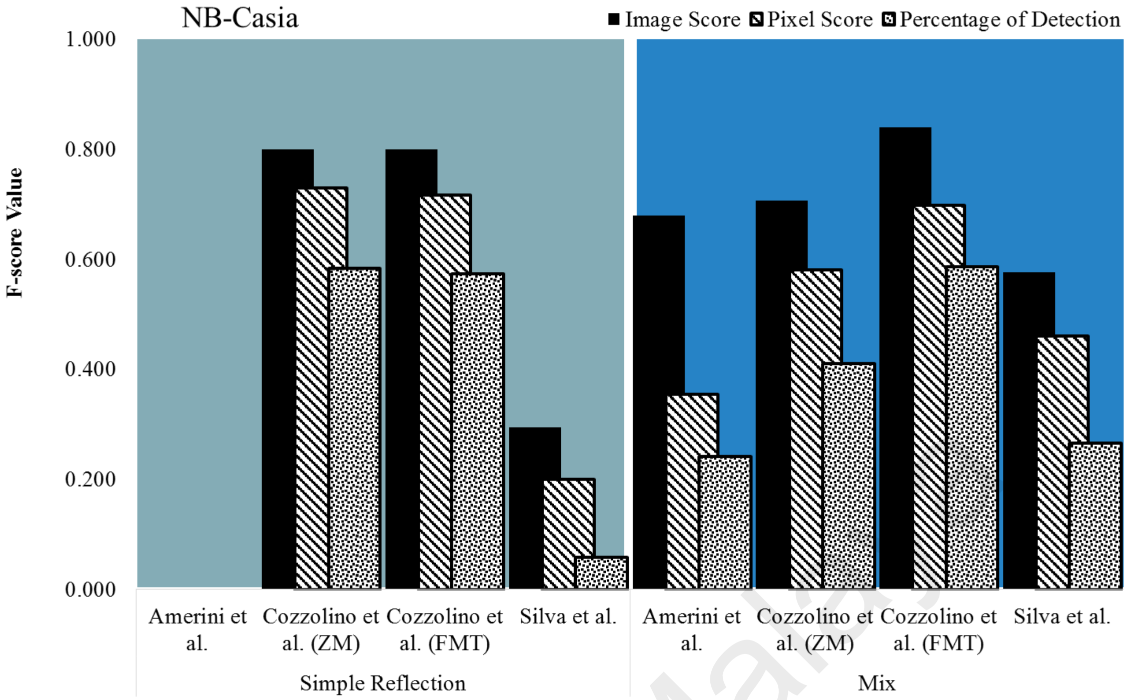


Figure 4.6: Comparative results (image score, pixel score, and percentages of both scores) for the existing CMF detection methods against scale, rotation, simple reflection and mix attacks in NB-Casia dataset

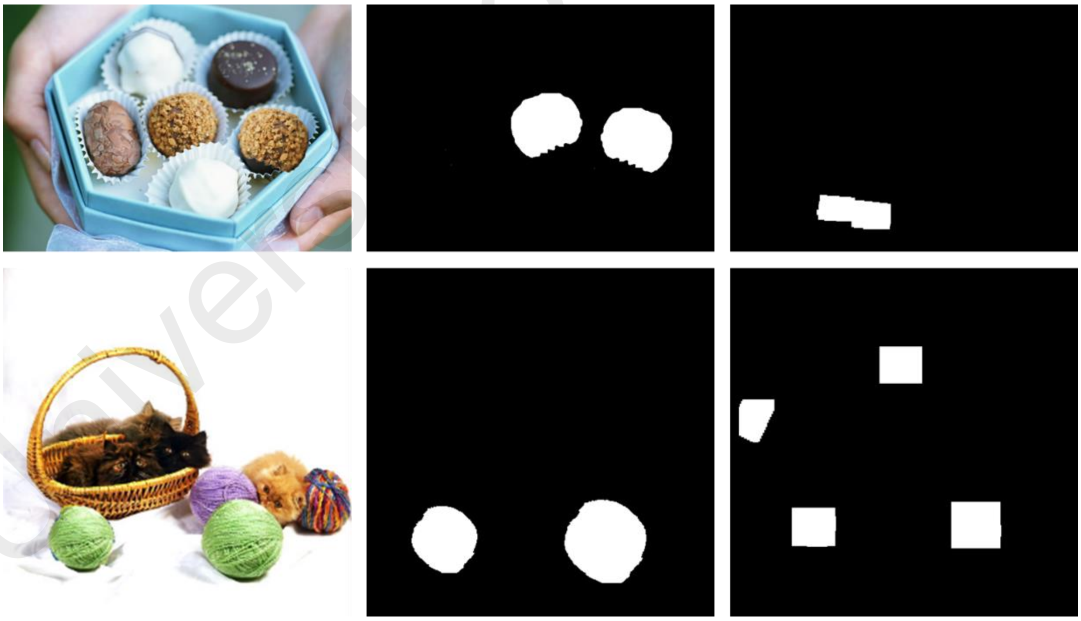


Figure 4.7: Examples of the (from left) CMF images, ground truth, and detection results by the Silva et al.'s method against reflection (top) and scale (bottom) in the NB-Casia dataset

On the contrary, although the performance of Cozzolino et al.'s method for both Zernike moments and FMT obtained the lowest performance for scale attacks, they were able to maintain at least 57% percentage of detection for rotation and simple reflection, while having achieved the highest performance for mix of attacks. However, since the FMT features is resistant to various illumination, the features demonstrate the higher performance than Zernike moments against all CMF attacks, except reflection.

*(c) **Reflection-based CMF Attacks***

Based on the previous analysis, the Zernike moments features in the Cozzolino et al.'s method shows the highest performance when dealing with simple reflection in CMF image. Therefore, this research continuously examined the method against reflection combination in CMF. Figure 4.8 displays the performance of the existing CMF detection methods against reflection with scale, reflection with rotation, and mixture of reflection. The figure proved that the performance of the Zernike moments is able to maintain the highest percentage of detection in all groups of reflection combination in CMF. Nevertheless, the performance on reflection with scale and mix of reflection were limited to 8% and 30% of detection because of the employed predefined thresholds. An ideal threshold may be able to improve the results. Meanwhile, the performance of the FMT features in Cozzolino et al.'s method was dropped whenever the reflection is involved.

The keypoint features, on the other hand, show the lowest performance for both Amerini et al.'s and Silva et al.'s method. These situations happened due to the reason that keypoint features, either SIFT or SURF, are not robust against reflection attacks. The feature coordinates between the original regions and the reflected regions are changed, hence, have led to the matching results failing.

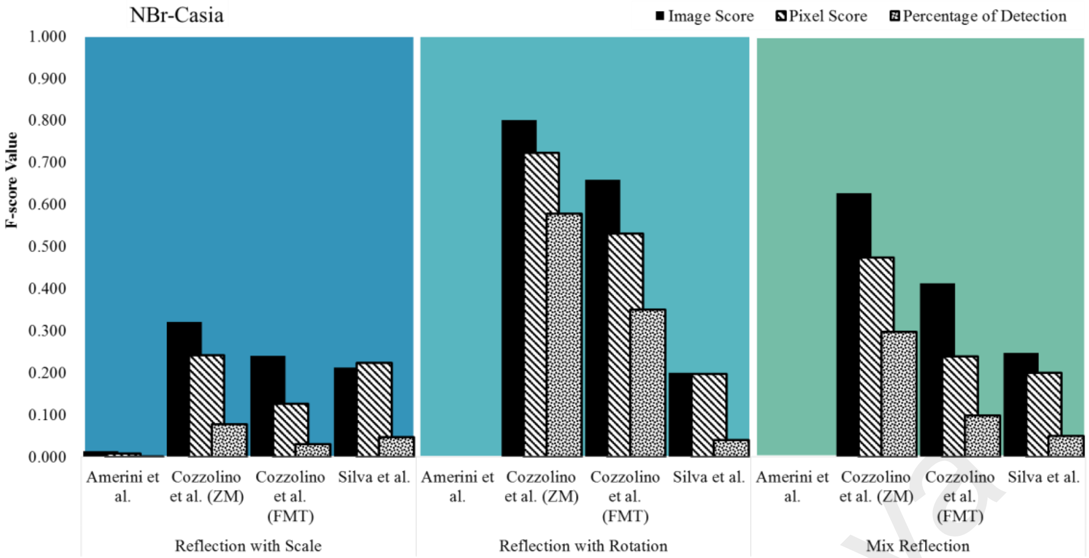


Figure 4.8: Comparative results (image score, pixel score, and percentages of both scores) for the existing CMF detection methods against reflection with scale, reflection with rotation, and mix of reflection attacks in NBr-Casia dataset

*(d) **Simple Translation, Scale, Rotation and Mix Attacks (CPHALL dataset)***

In view of the fact that the CPHALL dataset does not provide the original image in the collection, this research couldn't combine the performance with the NB-Casia dataset. Thus, this dataset was used to verify the previous analysis against the common attacks, except for reflection. Figure 4.9 presents the pixel score for the existing CMF detection methods for simple translation, scale, rotation, and mix of the attacks group in the dataset. The figure proved that the Amerini et al.'s method has the limitations when evaluated with pixel-level performance, while the performance of Silva et al.'s method was dropped with attacks other than simple translation. Hence, the Cozzolino et al.'s method shows the most efficient method among all the existing CMF detection methods. For features comparison, the FMT features show a higher performance compared to the Zernike moments in all attacks, mainly because the CMF regions in the dataset are too small to be detected by the Zernike moments.

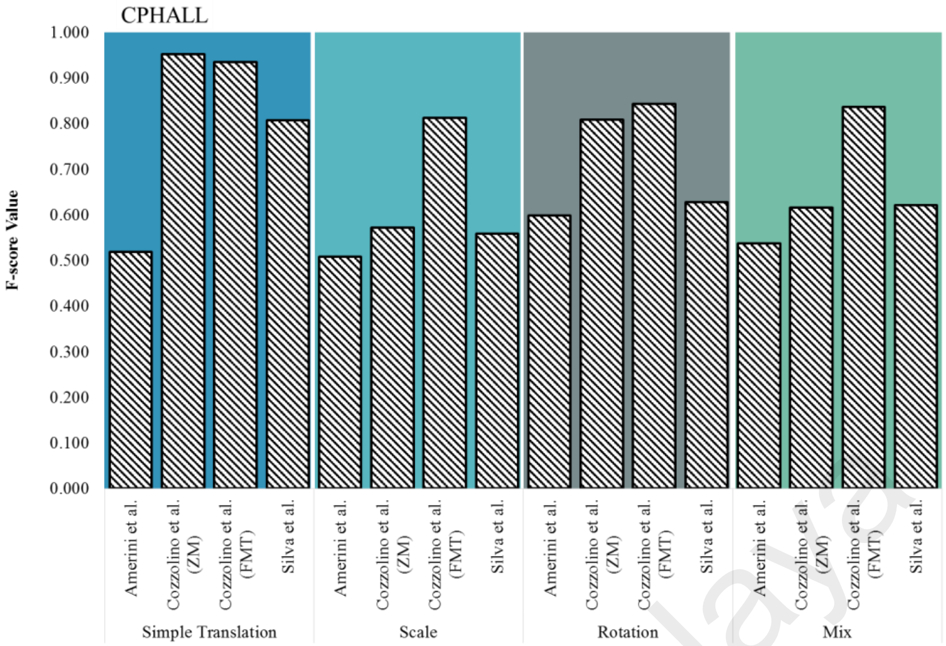


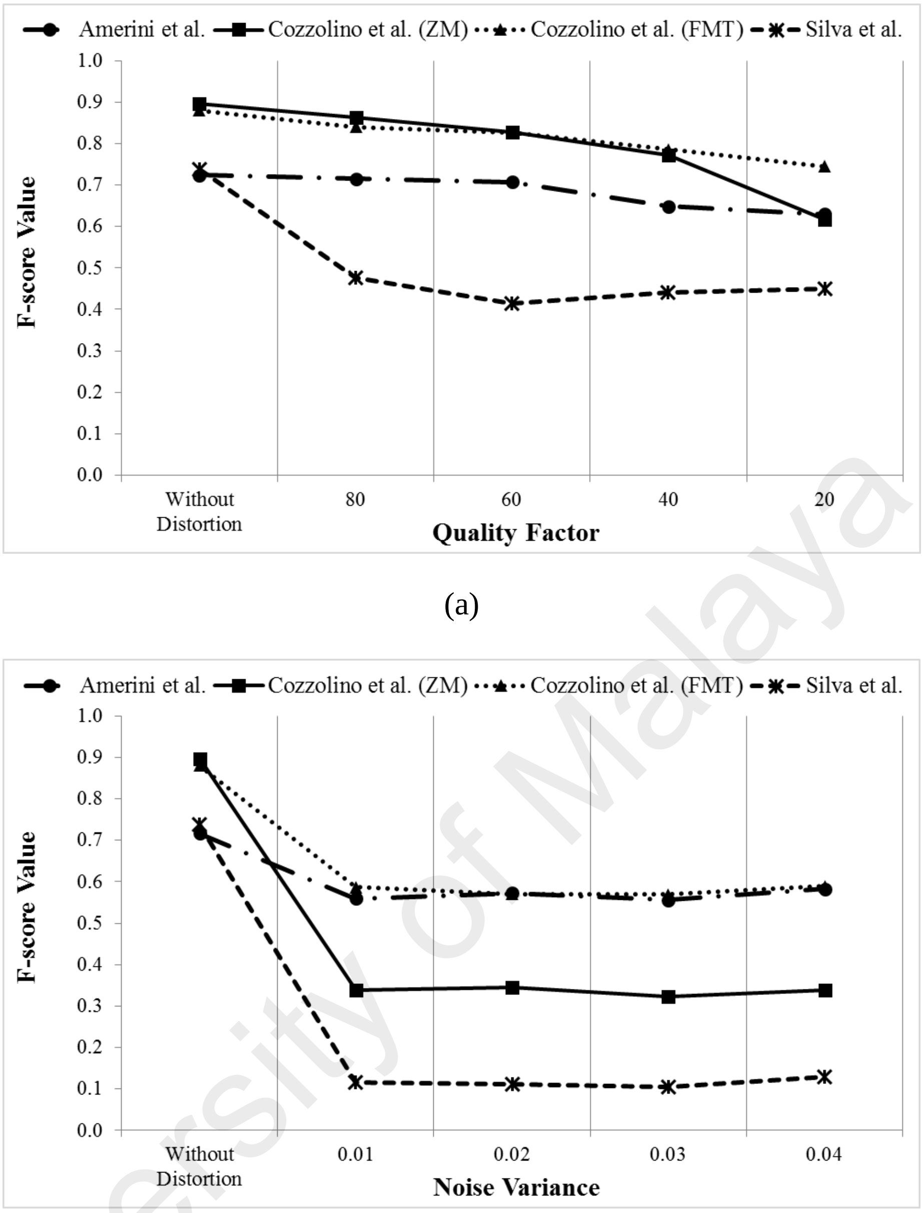
Figure 4.9: Pixel score for the existing CMF detection methods against simple translation, scale, rotation, and mix attacks in CPHALL dataset

4.4.2.2 Analysis against Post-Processing Attacks

Instead of analyzing the existing CMF detection methods against geometrical transformation, the performance against post-processing attacks was also measured. The performances were evaluated based on the image-level only, since the level is the highest importance and should be firstly measured compared to the pixel. Two sets of experiments were implemented to examine the robustness against JPEG compression and Gaussian noise addition. For the experiments, all images in CombineTranslation dataset were distorted by JPEG compression and Gaussian noise with four different parameters. In the first experiment, the images were compressed with various JPEG quality factors ranging between 80–20. Meanwhile, for the second experiment, four variances of Gaussian noise ranging between 0.01–0.04 were added to the images. The results are also compared with the results obtained without distortion in Section 4.4.2.1(a).

Figure 4.10 illustrates the image score values for the two experiments of post-processing attacks in image-level evaluation. Figure 4.10(a) shows the overall performance of the CMF detection methods against compression attack for each quality factor. Based on the figure, the Silva et al.'s shows the lowest performance for all quality factors. Even though the performance were increased, especially when dealing with the lowest quality factor, the method actually extracted more false matching features. The authors are aware of the drawback, as the results reported in their paper shows the lower performance compared to the Amerini et al.'s against the attacks. Furthermore, although the performance of the Amerini et al.'s method was higher than the Silva et al.'s method, the score was also decreased when compression was applied. Some artifacts, namely blockiness, may interrupt the amount of reliable keypoints in SIFT detection process each time compression were applied (Pan & Lyu, 2010).

Despite the challenges faced by other methods, only the Cozzolino et al.'s method could be maintained above 80% of image score, but only limited to 60 and 80 quality factors. Furthermore, the performance of the Zernike moments features was significantly dropped compared to the FMT for the lower quality factor. Similar results occurred with the method proposed by Ryu et al.'s (2010), which also applied Zernike moments features in their method. The authors notified that their method has low detectability for low quality of images. Subsequently, the performance of all methods continuously decreased for Gaussian noise addition. Figure 4.10(b) illustrates the image score values for all methods against Gaussian noise addition. In the figure, the results show that all scores tended to decrease when the variance of Gaussian noise was increased. However, the performance of the Amerini et al.'s method and FMT features achieve the highest score and demonstrate similar effects towards the attack.



(a)

(b)

Figure 4.10: Image score values of the existing CMF detection methods against (a) JPEG compression (b) Gaussian noise addition in CombineTranslation dataset

4.5 Discussion

There are two major problems recognized in the literature review, which are the requirement of both image and pixel-level evaluations in the CMF detection methods and the lack of evaluation on the reflection-based CMF attacks. Therefore, this chapter analyzed the problems through several experiments to prove the literature studies. For the first problem, a set of evaluation steps that include both levels is illustrated and used in the whole experiments. To deal with the second problem, two new datasets, NB-

Casia and NBr-Casia were created specifically to include reflection attacks in the evaluation.

Both evaluation steps and new datasets are the two important elements in this performance analysis. The elements are used to compare the performance of the existing CMF detection methods. The experiments proved the importance of both level evaluations, instead of solely relying on one level evaluation. For example, as the Amerini et al.'s method preferred only image-level evaluation, the pixel-level performance shows the reduction score even though they were the highest in the image-level. Contrarily, the Silva et al.'s method which considered only pixel-level performance, is not able to differentiate the original image and CMF image since the detected CMF images often localized the forged regions, incorrectly.

The performances of all CMF detection methods were analyzed based on geometrical transformation and post-processing attacks. For the geometrical transformation, the attacks were divided into five groups, comprised of simple translation, scale, rotation, simple reflection and mix of attacks. Based on the analysis, the Silva et al.'s method does not show much improvement in all attacks compared to the Amerini et al.'s and Cozzolino et al.'s method. Furthermore, the Amerini et al.'s method, performed the highest performance against scale and rotation groups, even though the method is not robust against reflection attacks. The Cozzolino et al.'s methods, on the other hand, is able to maintain the performance for simple translation, rotation, and reflection attack groups. However, several predefined thresholds in the final verification steps in their method has limit the performance from being higher, especially when dealing with small resolution of images. Finally, as the CMF image may be applied with the low quality of images, the Cozzolino et al.'s and the Amerini et al.’s method demonstrates the first and second best results for both JPEG compression and Gaussian noise.

Based on the performance analysis, both, keypoint (Amerini et al.’s) and block-based (Cozzolino et al.’s) approaches have their own merits and weaknesses against each CMF attack. Moreover, the performance towards the newly created datasets, NB-Casia and NBr-Casia show the lowest score due to the reason that reflection attacks are included. Hence, this research attempts to improve the score of the existing methods using both datasets. The following chapters will explain and describe the proposed methods, while the performance against both datasets are analyzed.

4.6 Chapter Summary

This chapter discusses the importance of both image and pixel-level evaluation techniques in CMF detection methods. A set of evaluation steps, which include both levels of evaluations is used to measure all methods’ performance. This chapter examined the effects of both image and pixel-level evaluations to the three existing CMF detection methods using four different datasets. The results are discussed based on geometrical transformation (including reflection-based CMF attacks) and post-processing attacks. Moreover, the advantages and the limitations of each method are also analyzed to come-out with improved solutions in the next chapters.

CHAPTER 5: METHOD I SIFT-SYMMETRY

This chapter presents the SIFT-Symmetry that is proposed to improve the robustness against CMF with various attacks including reflection. The experimental and comparison results are discussed and explained. The key contribution is the introduction of symmetry detection technique as a matching technique for the detection of CMF images with reflection attacks. Since the detection method proposed by Amerini et al. (2011) shows high performance for CMF with scale and rotation attacks, the method is combined with the symmetry matching to obtain better results in detecting reflection-based CMF images. The advantage of the symmetry matching is the technique could discover identical regions that involved almost all cases of reflection-based attacks in a CMF image.

This chapter is divided into five main parts: the first section (Section 5.1) briefly introduced the method, while the second section (Section 5.2) presents the proposed flowchart for the SIFT-Symmetry with explanation of each phase. The experimental results and analysis are presented in the third section (Section 5.3), whereas the fourth section (Section 5.4) concludes with the final discussion. The last section (Section 5.5) summarized the whole sections in the chapter. This chapter is based on the article’s title “SIFT-Symmetry: A Robust Detection Method for Copy-Move Forgery with Reflection Attack” (Warif, Wahab, Idris, Salleh, & Othman, 2017).

5.1 Introduction

Based on the performance analysis in the previous chapter, the score for the existing keypoints-based CMF detection method was significantly dropped when dealing with reflection-based CMF, although they achieved the highest score for both scale and rotation attacks. The results show that the Amerini et al.’s method was unable to detect any matching features whenever reflection is involved. Figure 5.1 displays the detection results produced by the method on simple translation with scale attacks compared with simple reflection attacks.

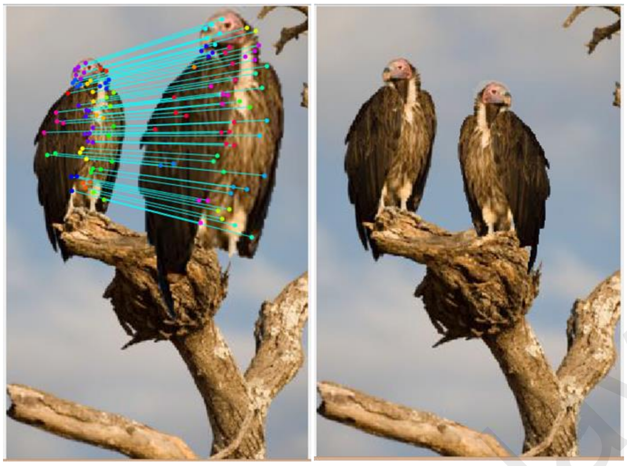


Figure 5.1: Detection results produced by the Amerini et al.'s method for CMF with simple translation and scale (left) and CMF with simple reflection (right)

Because of the stability, robustness and distinctiveness of the SIFT features, this research attempts to enrich the keypoint-based CMF detection method with reflection-based invariance while preserving existing merits. Basically, reflection is one type of symmetry, which could present itself in all forms and scales (Y. Liu, Hel-Or, Kaplan, & Gool, 2008). Furthermore, the symmetry is also invariant for various scales (Hauagge & Snavely, 2012) that has potential to maintain the performance on scale attacks. These properties have motivated this research to adopt the symmetry as a matching technique to discover the CMF with reflection attack. Therefore, a method, named as SIFT-Symmetry is proposed to incorporate the symmetry matching with the keypoint-based CMF detection method, specifically to solve the reflection-based problem in CMF. In the design, the SIFT feature extraction is changed to the mirror-SIFT features, while the g2NN matching technique is replaced with the symmetry matching technique.

To quantify the performance of the SIFT-Symmetry, the NB-Casia and NBr-Casia are selected as the input image. Then, the performances are compared with the existing

CMF detection methods based on each group of attacks. The advantages and limitations are discussed thoroughly.

5.2 SIFT-Symmetry

Owing to the reason that the keypoint-based CMF detection method (Amerini, Ballan, Caldelli, Bimbo, & Serra, 2011) shows good performance in detecting CMF translation with scale and rotation, the SIFT-Symmetry is aimed particularly to detect the combination of reflection with translation, scale, and rotation. In the design, the SIFT-Symmetry is innovatively combined and modified the keypoint-based CMF detection to be included with the symmetry matching technique. The flowchart of the whole design of the SIFT-Symmetry is illustrated in the Figure 5.2 where the blue color represents its unique characteristics. The processes are categorized into three phases, specifically (i) keypoint extraction, (ii) keypoint matching, and (iii) clustering and forgery detection. For the first and second phases (keypoint extraction and keypoint matching), each phase consists of two different techniques. Specifically, the SIFT feature extraction is paired with the g2NN matching technique to resist the non-reflection attacks, while the mirror-SIFT feature extraction are combined with the symmetry matching technique to discover the reflection-based attacks. The flow ends with the final verification of forgery localization in the third phase, and the explanation of the three phases is covered in the following section.

5.2.1 Keypoint Extraction

In the first phase, the keypoint extraction techniques are comprised of SIFT and mirror-SIFT feature extraction. The SIFT feature extraction technique, which is initially proposed by Lowe (1999) has been verified to be robust against CMF with scale and rotation attacks (Amerini et al., 2011). A set of SIFT point vectors representing the location, scale, and orientation is assigned to each feature point, $p_i = \{x_1, x_2, \dots, x_n\}$ in each image. The point detection is derived in scale space by looking at the maxima or minima of difference in Gaussian function to be robust to scale and Gaussian blurring. Moreover, each point generates a set of SIFT descriptors, $d_i = \{x_1, x_2, \dots, x_{128}\}$ from a normalized histogram of local gradients in a neighborhood of pixels for each point, p_i. d_i is formed from 4×4 array of histogram with eight orientation bins that resulted in 128 element vectors to increase the rotation invariant properties. This means that the vectors are used to describe the local image regions of the feature points.

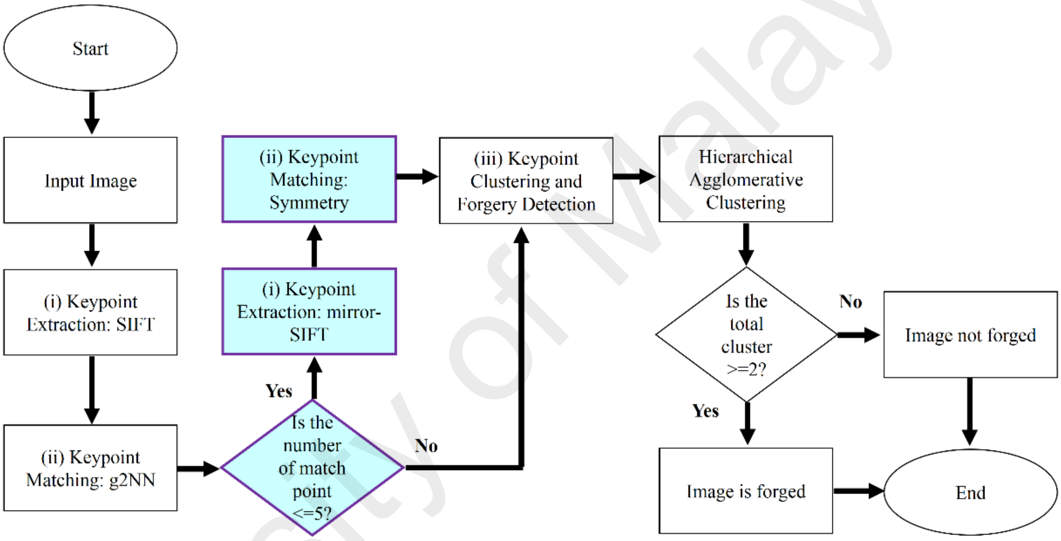

Start
Input Image
(i) Keypoint Extraction: SIFT
(ii) Keypoint Matching: g2NN
(i) Keypoint Extraction: mirror-SIFT
(ii) Keypoint Matching: Symmetry
Yes
Is the number of match point <=5?
No
(iii) Keypoint Clustering and Forgery Detection
Hierarchical Agglomerative Clustering
Is the total cluster >=2?
No
Yes
Image not forged
Image is forged
End

Figure 5.2: Flowchart of the SIFT-Symmetry method

To find the matching points, the SIFT descriptors are calculated and compared based on the distance of each features' neighborhood. However, since the SIFT technique is not robust against reflection attacks, the reflected SIFT descriptors are distinct from the original SIFT descriptors, which may lead to the matching result failing. Therefore, to cover the reflection-based attacks in CMF, the SIFT features is modified by reorganizing the descriptor, d_i, to form a new set of mirror-SIFT descriptors, d_j (X. Guo & Cao, 2012). By assuming that the given image was flipped at the axis that has been aligned with the dominant orientation of each feature point, p_i, the sequence of the elements in the SIFT descriptor, d_i, is reordered, and a new mirror SIFT descriptor, d_j, is formed. The example of the descriptor reorganization is presented in Figure 5.3. Furthermore, as the main factor of matching results failure is the descriptor, the mirror point, p_j, is expected to be similar to the location of SIFT point, p_i. The illustration of the whole process of mirror-SIFT is shown in Figure 5.4.

d_i =

1	**2**	**3**	**ABCDEFGH**	**5**	**6**	**.**	**.**	**.**	**15**	**16**

d_j =

13	**14**	**15**	**.**	**.**	**.**	**.**	**1**	**2**	**3**	**AHGFEDCB**

Figure 5.3: Example of reorganization between SIFT descriptor, d_i and mirror-SIFT descriptor, d_j

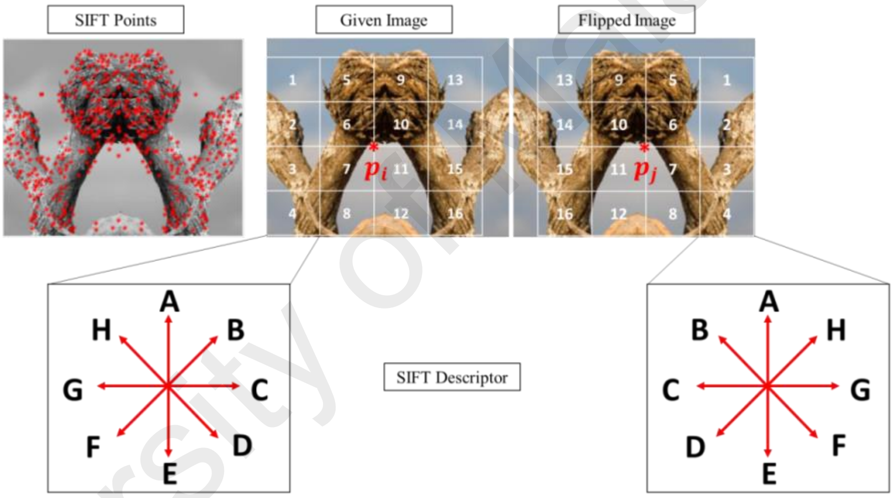


Figure 5.4: Illustration of the whole reorganization between SIFT point, p_j and mirror-SIFT point, p_j

5.2.2 Keypoint Matching

In the second phase, both points and descriptors from the feature extraction phase were calculated to remove their distinctive point. Meanwhile, identical points were classified and matched to each other to discover the duplicated regions in the CMF image. It is a very challenging task to match the points in one image since the features are compared to similar identity, thus, will lead to high computational complexity. Therefore, the standard matching technique for SIFT features is enhanced with two techniques, namely g2NN and symmetry matching. As previously mentioned, the SIFT features are paired with the g2NN matching for CMF with non-reflection attacks, while the mirror-SIFT is matched with the proposed symmetry matching technique to cover the CMF with reflection attack. For clarification, this phase is divided into two categories of matching which are g2NN and symmetry matching.

5.2.2.1 g2NN

The standard matching technique of SIFT (which is delivered by David Lowe (2004)) is 2NN, finds a ratio between the closest neighbor, ds_1 and the second-closest, ds_2, before comparing the ratio with a predefined threshold, ${}^{ds_1}/_{ds_2} < T$. Instead of comparing only two distances, g2NN, which is proposed by Amerini et al. (2011) iterated the procedure between ds_i/ds_{i+1} until the ratio is greater than the threshold, ${}^{ds_i}/_{ds_{i+1}} > T$ (note: the threshold value is set to 0.5). The points are considered as a match if the corresponding distance in $\{ds_i, \ldots., ds_x\}$ satisfies $1 \leq x < n$, where x is the value on which the procedure stops. This iteration is performed on all keypoints, p_i, which finally will produce a set of matched points. All matched points are retained for further evaluation, while the unwanted points are discarded. From the procedure, the number of matched points will lead to the better estimation of geometrical transformation and increases the ability to detect multiple similar features in a CMF image.

Furthermore, due to the dissimilarity of SIFT descriptor between the original and reflection regions, the g2NN matching technique is unable to find any identical points. To protect against reflection attacks, a new threshold is predefined to convert the matching techniques from g2NN to symmetry. Symmetry techniques are initiated only if the g2NN detects less than five matched points. The value is set to at least five pairs because the value is the least amount that g2NN could match for the common CMF attack. This is evidenced by the Figure 5.5 which shows the results of g2NN (non-reflection and reflection) and symmetry (reflection).

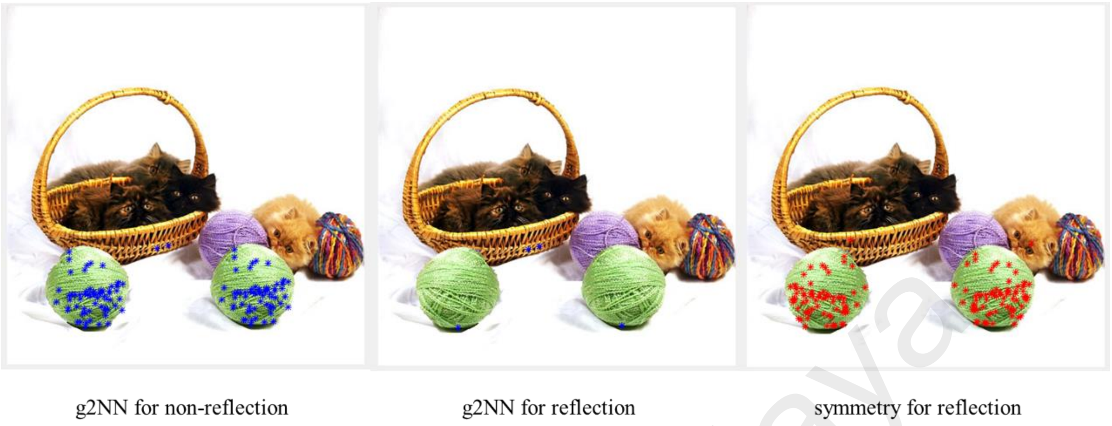


Figure 5.5: From left: examples of g2NN (non-reflection and reflection) and symmetry (reflection) results

5.2.2.2 Symmetry Matching

Symmetry is a consistent transformation which retained its component elements and remained unchanged as a whole (Hargittai & Hargittai, 2000). The transformation involved could be a translation, rotation, and reflection. As the CMF image should involve at least one transformation, this research made use of the symmetry properties to find the region's transition. Nonetheless, owing to the reason that this research is dedicated to the CMF with reflection attacks, only reflection transformation in symmetry (known as bilateral symmetry) is considered. This section describes the steps involved in symmetry matching technique after the flow changed from g2NN to symmetry matching.

Initially, the idea of the symmetry matching is started from Loy et al. (2006), which proposed a symmetry constellation features detection in an image. The authors grouped the feature points who underlie symmetry in an image. Instead of grouping the symmetry features, this research modified the technique to obtain symmetry points for clustering. The symmetry points are produced based on the dominant symmetry axis generated by the Hough transform from the matching feature vectors of SIFT points, p_i, with mirror points, p_j (consists of SIFT descriptor, d_i, and mirror SIFT descriptor, d_j). The steps are described comprehensively as the following and summarized in Algorithm 1.

Algorithm 1: Symmetry matching procedure

```
Input:
    $p$ (A set comprising all keypoint pairs. Each pair is composed by a source point, $p_i$ and a mirror point, $p_j$)
    $S_T$(percentage by which the scale can vary within a matched pair)
    $grouping\_threshold$ (angular and radial tolerances for symmetry particles associated with the same symmetry axis)
Output: $A$ (coordinate of the left and right associations with the symmetry axis)
 for each pair, $p$ do
    Calculate the correspondence scale weighting, $S_{ij}$ relative to $p$;
    if $S_{ij} < S_T$ then
    Create a new group of matching points, $M$ (a set of index values for $p$ that match with the scale)
    end if
    for each index, $M \in p$ do
        Calculate the phase weighting, $\rho_{ij}$ relative to $p$;
        if $\rho_{ij} > 0$ then
        Create a new group of matching points, $\rho$ (a set of pairs based on phase weighting)
        end if
        for each value, $\rho$ do
        Calculate the mean for each coordinate $x$ and $y$ relative to $p$;
          Create a new group of matching points, $H$ (a set of mean coordinates $p$ with angles, $\theta_{ij}$ and symmetry magnitudes, $M_{ij}$)
            for each value, $H$ do
              Cast a vote in Hough space, ($r_{ij}$,$\theta_{ij}$) weighted by $M_{ij}$ to determine the dominant symmetry axis
              Create a new group of dominant symmetry axis, $D$ (a set of maximum $r_{ij}$ and maximum $\theta_{ij}$)
                for each value, $D$ do
                    if $D < grouping\_threshold$ then
                    Create a new group of symmetry points, $A$ (a set of left and right associated with $D$)
                    end if
                end for
            end for
        end for
    end for
 end for
return $A$.
```

Firstly, the SIFT features, p_i are paired with the mirror-SIFT features, p_j. To measure a relative similarity in scale, the pairs are filtered per a scale weighting, S_{ij} as computed in Equation (5.1) where the parameter, S_T is a defined percentage to control the variety of scales. Next, phase weighting, ρ_{ij} from the Generalized Symmetry Transform (computed in Equation (5.2)) is adapted as an angular symmetry constraint. The value of the $\emptyset_i$, $\emptyset_j$, and θ_{ij}, is calculated based on the angles of SIFT point, $\emptyset_i$, mirror point, $\emptyset_j$, and the angles that determine the orientation of the line joining the pairs, θ_{ij}, presented in Figure 5.6.

$$S_{ij} = \exp\left(\frac{-\left|s_i - s_j\right|}{\sigma_s\left(s_i + s_j\right)}\right) < S_T \qquad (5.1)$$

Where $s_i = p_i, s_j = p_j, \sigma_s = 1$ and $S_T \in [0, 1]$

$$\rho_{ij} = 1 - \cos(\emptyset_i + \emptyset_j - 2\theta_{ij}) \qquad (5.2)$$

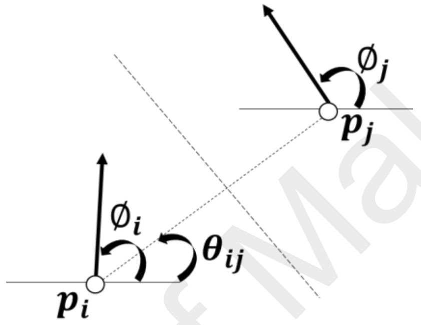


Figure 5.6: The angles used in Equation 5.2 between each pair

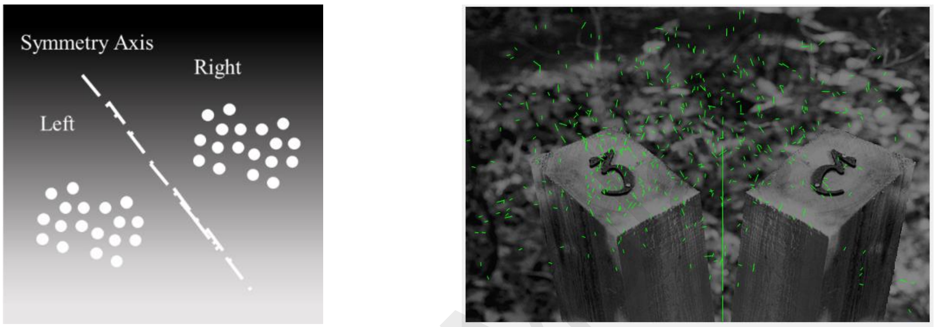
In order to extract the dominant symmetry axis between each pair, the symmetry magnitude, M_{ij} is calculated as in Equation (5.3). The magnitude is comprised of the combination of scale weighting, S_{ij} and phase weighting, ρ_{ij} as long as the phase weighting, ρ_{ij} is greater than 0.

$$M_{ij} = \begin{cases} S_{ij}\rho_{ij} \; if \; \rho_{ij} > 0 \\ 0 \quad Otherwise \end{cases} \qquad (5.3)$$

Each pair, (p_i, p_j), weighted by its symmetry magnitude, casts a vote (r_{ij},θ_{ij}) in Hough space. r_{ij} is computed as in Equation (5.4) where (x_c, y_c) is the center coordinates of midpoint between the line joining p_i and p_j, while θ_{ij} is the angle that this line subtends with the x-axis, similar to Figure 5.6.

$$r_{ij} = x_c \cos\theta_{ij} + y_c \sin\theta_{ij} \qquad (5.4)$$

The dominant symmetry axis is described by the maxima generated in the Hough space that is blurred with a Gaussian. Points located close to these maxima represent the symmetric pairs that are associated with this axis of symmetry. Meanwhile, the angular and radial tolerances are specified for points associated with the same symmetry axis to obtain the left and right identical points. The illustration of the symmetry matching is presented in Figure 5.7(a), while the real result is shown in Figure 5.7(b).



(a) (b)

Figure 5.7: (a) Illustration and (b) real result of dominant symmetry axis creation in Hough space

It should be noted that symmetry matching would face several challenges. Owing to the reason that nature environments often is recognized as symmetry, symmetry is sometimes defined as a kind of accident of geometry (Stewart & Golubitsky, 2010). From the definition, the authors are aware that there are several images in the nature that are occasionally symmetry by coincidence. This is evidenced by the butterfly behavior, in which the body is acting as the symmetry axis, while the patterns of the wing is sometimes reflected.

Logically, two different objects should have a unique feature in most of the natural behavior cases, as there is no transformation involved. For instance, although human face is expected to be symmetry, it is actually nearly symmetrical (Hoffman, 2003), in which the eyes, lips, and everything else are not reflective of each other. This is also agreed by Funk & Liu (2017) which mentioned that the growth of plants, insects and mammals with perfectly symmetrical objects and scenes are rare while approximate symmetries are readily observable in both natural and man-made worlds.

Another example is the effect of shadow in an object. The reflection object will show different features due to the combination of shadows' plane and object resulted with diverse features. Fortunately, this shadow effect should not be a problem since there are various algorithms related to shadow detection (Nguyen et al., 2017). These three examples have led to the failure of recognizing an original image, by means, if the image is symmetry in nature; the symmetry matching could wrongly detect the image as forged. Therefore, in view of the fact that there are several characters in symmetry, a behavior analysis should be conducted to produce basic principles of symmetry for each science area (e.g. animal, human, and physics behavior) (Jackson Marr, 2006). Figure 5.8 shows the example result of symmetry matching in a butterfly, and the asymmetry in a human face, and a shadow. Nonetheless, this is a very well-known open issue in symmetry-related scientific literature.

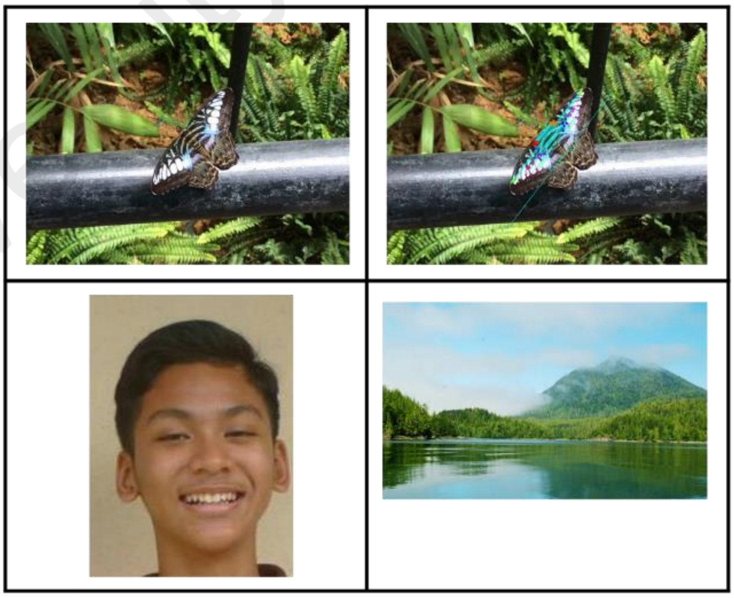
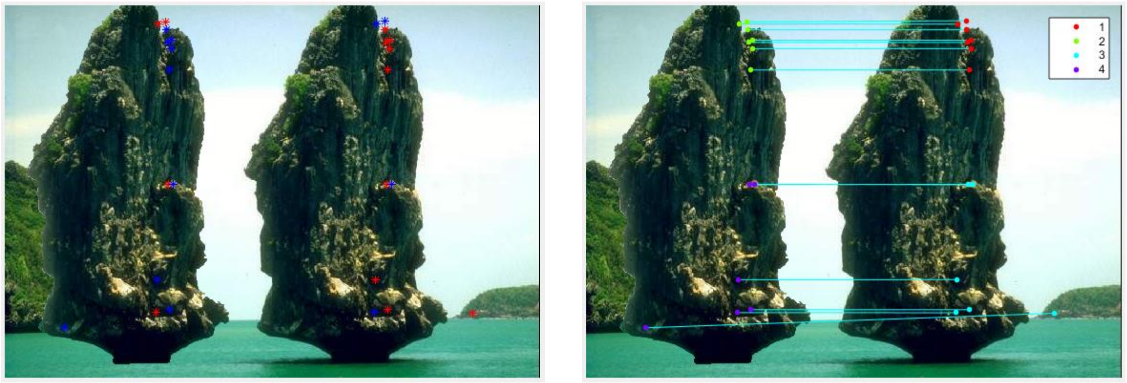


Figure 5.8: From top: example of symmetry in butterfly, and asymmetry in human face and shadow

5.2.3 Clustering and Forgery Detection

Finally, the results of the matching points, either by g2NN or symmetry matching are verified in this phase. Since the matching points generated may be scattered, thus, making it difficult to localize the CMF region, a Hierarchical Agglomerative Clustering (Hastie, 2009) technique is applied. This technique is performed on the spatial location, (x, y) of the associated points with several linkage parameters. Then, these processes iteratively find the closest pairs among the clusters and merge them into a single cluster, in which the parameters were tested and the results are presented in Section 5.3.1, to obtain the best threshold setting for forgery detection. The image will be considered as forged, if the condition of at least three pairs in one cluster is linked to another cluster.

In order to identify the linking cluster, RANSAC is performed to estimate the geometrical transformation between each cluster. A standard method of data normalization for homography estimation is used by randomly selecting a set of three pairs of points from each cluster. Figure 5.9(a) presents the scattered result produced by the symmetry matching, in which blue points represent the left association of the symmetry axis and red points indicate the right association. After all, the final CMF detection results after the RANSAC process is depicted in Figure 5.9(b). For image-level evaluation, the SIFT-Symmetry is verified with the clustered points. The pixel-level, on the other hand, thick (dense) the points in the cluster for 10 pixels, while a morphology (dilation) process is performed to segment the points' region.



(a) (b)

Figure 5.9: (a) An example of the points scattered due to maxima creation, and (b) the final points after clustering to verify the detection result

5.3 Experimental Results and Analysis

The performance of the SIFT-Symmetry was analyzed through a comprehensive set of experiments using two datasets, NB-Casia and NBr-Casia. Firstly, a six-fold cross validation technique was applied to identify the best parameter setting for clustering and forgery detection phase. Then, the parameter was established for all experiments in this research. To validate the results, a standard metric (F-score) was applied for image-level, pixel-level, and percentage of detection to compare with three existing CMF detection methods (Amerini et al. (2011), Cozzolino et al. for Zernike moments and FMT (2015), and Silva et al. (2015)). The overall performance were analyzed based on the CMF with geometrical transformation and post-processing attacks. The details of the experimental results and analysis are discussed in the following subsections.

5.3.1 Parameters Setting

As highlighted in Section 5.2.3, an image will be verified as forged, if the matching points satisfy the condition of at least three pairs in one cluster is linking to another cluster. For that reason, a suitable linkage and parameter setting should be performed to obtain the highest number of pairs among clusters. Six common linkages were tested, comprising centroid, average, ward, complete, median and weighted. To obtain the best combination of parameter and linkage, the six-fold cross validation technique was executed. The cross validation technique was used to specify the number of training and testing involved, in which the higher number of folds will produce more accurate results compared to a single fold validation. The validation was performed on NB-Casia dataset and the combination (parameter and linkage) with the highest score was established for all experiments and comparisons.

This section describes the procedures involved in the cross validation process. The validation process was performed on each parameter for each linkage. Firstly, 5/6 of the images in NB-Casia (510 images), which is a total of 425 images, were randomly selected and used as the training set. The best parameter for each linkage was used in the testing set with the remaining 1/6 of the images, which is a total of 85 images. Next, the experiment was repeated six times with different training and testing sets. Then, the training results were averaged and listed as in Table 5.1, while the average testing results were summarized in Table 5.2.

Both tables show that the SIFT-Symmetry was effective in detecting CMF images by exceeding 80% image score values for all parameters in each linkage. The **complete** linkage with parameter **2.2** was selected, since it produced the highest score in the validation process. The combination of parameter and linkage was used in all experiments and the results are reported in the next section.

Table 5.1: Average image score results of the training set for each linkage clustering method

Linkage/ Parameters	Centroid	Average	Ward	Complete	Median	Weighted
2.2	**0.829**	0.825	**0.829**	**0.835**	0.815	0.819
2.0	0.823	**0.829**	0.822	0.812	0.817	0.818
1.8	0.818	0.821	0.816	0.816	0.818	**0.821**
1.6	0.821	0.815	0.805	0.811	**0.827**	0.815
1.4	0.809	0.797	0.803	0.817	0.809	0.806

Table 5.2: Average image score results of the testing set for the best threshold parameter of each linkage clustering method

Linkage	Centroid	Average	Ward	Complete	Median	Weighted
Parameters	2.2	2.0	2.2	**2.2**	1.6	1.8
Image Score	0.830	0.829	0.830	**0.835**	0.827	0.821

5.3.2 Analysis of Robustness against Geometrical Transformation Attacks

In view of the fact that the existing CMF detection methods predominantly concern geometrical transformation attacks, an analysis and comparison should be performed to prove the results of the SIFT-Symmetry. This section presents the performance analysis of the SIFT-Symmetry in detecting CMF images with the combination of geometrical transformation attacks in the NB-Casia dataset. The **complete** linkage with parameter **2.2** was employed to both SIFT-Symmetry and the Amerini et al.'s method. The images that is detected as forged will be evaluated at pixel-level, before further calculated its percentage of detection.

Table 5.3 recorded the image score, pixel score, and percentage of both scores for each method in NB-Casia dataset. Remarkably, the SIFT-Symmetry achieved the highest image score and percentage of detection compared to other methods, however, the performances were dropped when measured by pixel. This situation is expected, as the previous analysis in the previous chapter has mentioned that the points' detection in the keypoint features are not able to recognize their exact region.

Since the SIFT-Symmetry has significant image score value, this research further analyzed the image-level performance for each method. Table 5.4 records the TP, FP, TN, and FN values that are used to calculate the image score for each method. The results from the table indicate that the SIFT-Symmetry was efficient in detecting CMF-translation with other transformation attacks, which are rotation, scale, and reflection, even when these attacks were applied together in the same image. Nevertheless, the FP value was slightly higher than others because the original images may contain highly uniform feature representations especially with a symmetry axis. Alternatively, the Amerini et al.'s method may be employed to the original image to improve the detection since their FP value is much lower than the SIFT-Symmetry.

Table 5.3: Image score, pixel score, and percentages of detection for each CMF detection method in NB-Casia Dataset

Dataset/Method	**NB-Casia**		
	Image Score	Pixel Score	Percentage of Detection
Amerini et al. (2011)	0.814	0.549	0.447
Cozzolino et al. (2015)---ZM	0.654	0.557	0.364
Cozzolino et al. (2015)---FMT	0.745	**0.634**	0.472
Silva et al. (2015)	0.667	0.548	0.365
SIFT-Symmetry	**0.835**	0.581	**0.485**

Among all state-of-the-art methods, the Silva et al.'s method shows the highest FP value, which means that the detections actually contain several false matching pixels, though their score is higher than the Cozzolino et al.'s method with Zernike moments features. In regards to the lowest FP value, the method of Cozzolino et al.'s is able to reduce the false matching regions, despite their difficulty in recognizing CMF with small regions.

Table 5.4: The comparison of image score with TP, FP, TN and FN values for each CMF detection method using the NB-Casia dataset

Method	**TP**	**FP**	**TN**	**FN**	**F-score**
Amerini et al. (2011)	215	9	246	40	0.814
Cozzolino et al. (2015)---ZM	168	2	253	87	0.654
Cozzolino et al. (2015)---FMT	195	7	248	60	0.745
Silva et al. (2015)	190	30	225	65	0.667
SIFT-Symmetry	**232**	**23**	**232**	**23**	**0.835**

The results are further divided according to the five groups of geometrical transformation attacks to see the effectiveness on such attacks. For image score, the performances were calculated by averaging the results of 15 original images with its 15

CMF images for each parameter in each group of attacks. Meanwhile, the detection locations in the CMF image are compared with the exact location to obtain the pixel score value. Both image and pixel scores are multiplied to obtain the percentages of detection.

Figure 5.10 presents the image score, pixel score, and percentage of detection for all CMF detection methods in each group of attacks. It is noted that because the SIFT-Symmetry is a modification of Amerini et al.'s method (which combined the mirror-SIFT and symmetry matching technique), the pixel performance of the SIFT-Symmetry was slightly similar to Amerini et al.'s in terms of non-reflection attacks. For image score, on the other hand, the performance of the SIFT-Symmetry was diminished since the method might also misinterpret an original image (which has a symmetry axis) as a CMF image. Despite that, although the score of the SIFT-Symmetry was lower than the Amerini et al.'s, the method outperformed other methods for all groups of attacks by exceeding the minimum value of 90% image score, except for a mix of attacks which obtained 70% of image score. This is because the performance of the SIFT-Symmetry dropped whenever a higher parameter of scale and rotation degree are involved. In spite of the limitation, the SIFT-Symmetry showed the highest performance for simple reflection with 94% of image score compared to all state-of-the-art methods.

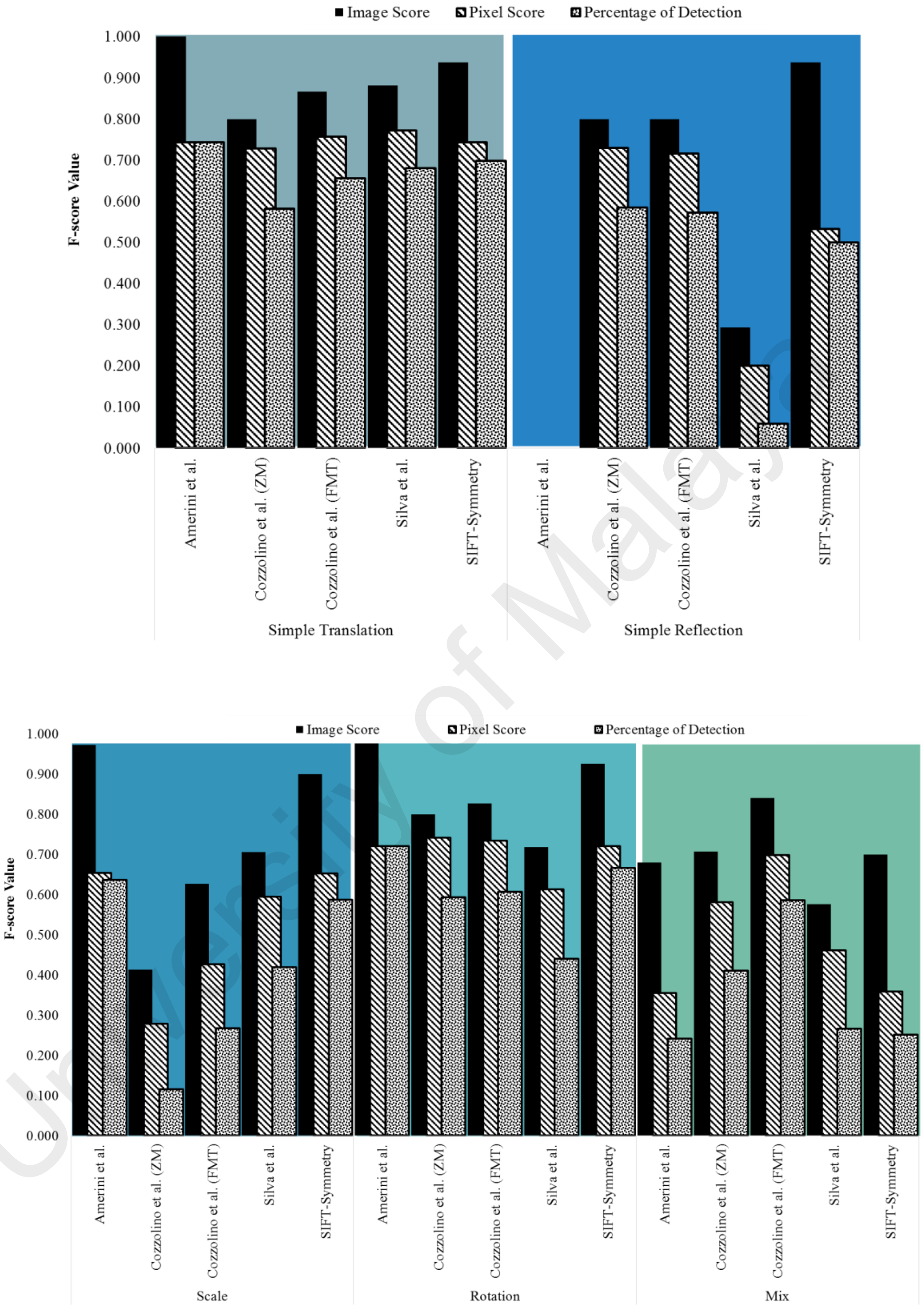


Figure 5.10: Comparative results between SIFT-Symmetry and the Existing CMF Detection methods for each group of geometrical transformation attacks

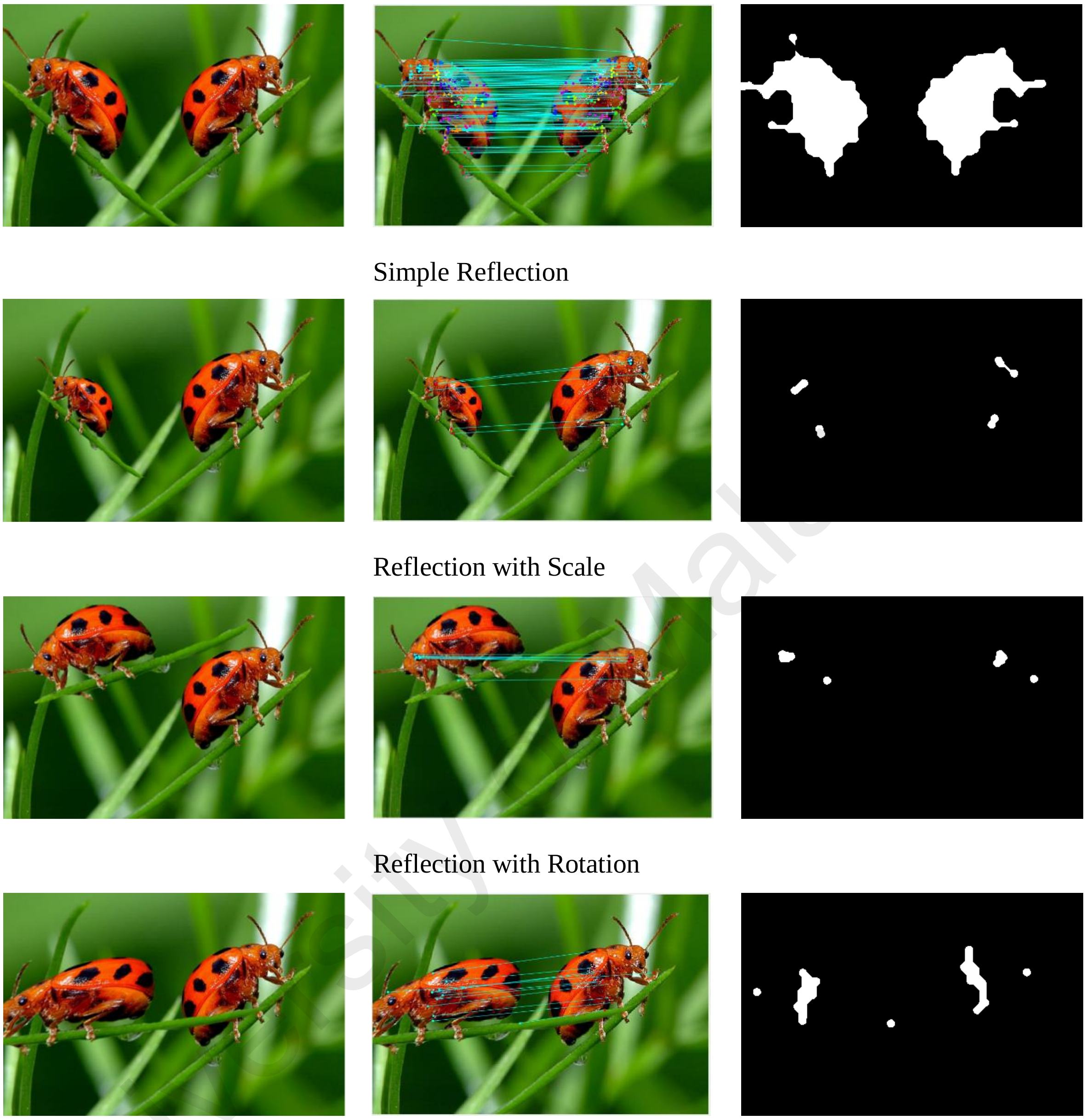
5.3.2.1 Analysis of Robustness against Reflection Attacks

Based on the analysis in the previous section, the SIFT-Symmetry showed the highest achievement (in image score) upon dealing with reflection attack in CMF compared to other methods. Therefore, the method was explored and examined on the reflection-based CMF image. Due to the shortage of reflection-based CMF image datasets, a new dataset, called NBr-Casia, particularly for reflection-based CMF images was created. Table 5.5 lists the image score, pixel score and percentage of detection for all state-of-the-art methods using NBr-Casia dataset. According to the table, the SIFT-Symmetry achieved the highest score for image-level. Due to the reason that only a few points were detected as symmetry, the pixel performance was dropped. This is shown in Figure 5.11, in which the few symmetry points were not able to detect the exact regions, resulting in a low recall rate. Regardless of the disadvantage on pixel-level performance, the clustering-based in image-level performance is enough to show the manipulated regions in the image.

Table 5.5: Image score, pixel score, and percentages of detection for each CMF detection method in NBr-Casia Dataset

Dataset/Method	NBr-Casia		
	Image Score	Pixel Score	Percentage of Detection
Amerini et al. (2011)	0.004	0.003	0.000
Cozzolino et al. (2015)---ZM	0.593	**0.491**	**0.291**
Cozzolino et al. (2015)---FMT	0.496	0.325	0.161
Silva et al. (2015)	0.226	0.010	0.002
SIFT-Symmetry	**0.698**	0.214	0.149

Table 5.6 shows the image score with TP, FP, TN, and FN values for each method using NBr-CASIA dataset. From the table, the SIFT-Symmetry outperformed other methods while the Amerini et al.’s method reported the lowest F-score value. The Amerini et al.’s, on the other hand, could detect only one image out of 240 reflection-based CMF images, due to the reason that the SIFT features are not reflection invariant.



Simple Reflection

Reflection with Scale

Reflection with Rotation

Combination of Reflection

Figure 5.11: Examples of CMF image (left), and the detection results of SIFT-Symmetry for image-level (middle) and pixel-level (right) in four groups in NBr-CASIA. From top: simple reflection, reflection with scale, reflection with rotation and combination of reflection

In addition, the g2NN matching technique was not established to protect against the attack. Similarly, the performance of the Silva et al.'s method also confirmed that they could not locate the exact position of the forged regions even when the images were detected as forged. Therefore, the Cozzolino et al.'s method presented the highest F-score value among all state-of-the-art methods tested, but it was lower than the performance of the SIFT-Symmetry in image level. Further performance analysis between the Cozzolino et al.'s and SIFT-Symmetry is discussed in the next section.

Table 5.6: The comparison of image score with TP, FP, TN and FN values for each CMF detection method using the NBr-Casia dataset

Method	TP	FP	TN	FN	F-score
Amerini et al. (2011)	1	7	233	239	0.004
Cozzolino et al. (2015)—ZM	143	1	239	97	0.593
Cozzolino et al. (2015)---FMT	120	2	238	120	0.496
Silva et al. (2015)	61	30	210	179	0.226
SIFT-Symmetry	**183**	**22**	**218**	**57**	**0.698**

The overall performance of all scores (in each group) for the reflection-based CMF dataset (NBr-Casia) are illustrated in Figure 5.12. The figure shows that the SIFT-Symmetry achieved the highest score for image-level in all groups of attacks, except for the reflection with rotation. The performance is able to maintain the results for reflection with scale and a combination of reflection with 78% and 75% of image score, respectively. Nevertheless, the score continuously decreased for reflection with rotation with a value of 58% image score. Meanwhile, the performance of the Cozzolino et al.'s methods were significantly reduced in detecting reflection with scale and combination of reflection, although they are able to maintain all scores for simple reflection and reflection with rotation. Further investigations were performed in the following paragraphs.

Next, the image score for each group of attacks are analyzed based on parameters. For the reflection with scale, the copy-reflected regions were scaled between 0.6–1.6 and applied in steps of 0.2 parameters. Figure 5.13(a) depicts the image score values for each parameter. The SIFT-Symmetry maintained a minimum score value of 81% for 0.8, 1.2, and 1.4 factors, but the values were reduced for large scales up (1.6) or down (0.6). Fortunately, the percentage of the scale weighting (as in Equation 1) can be changed to improve the scale performance.

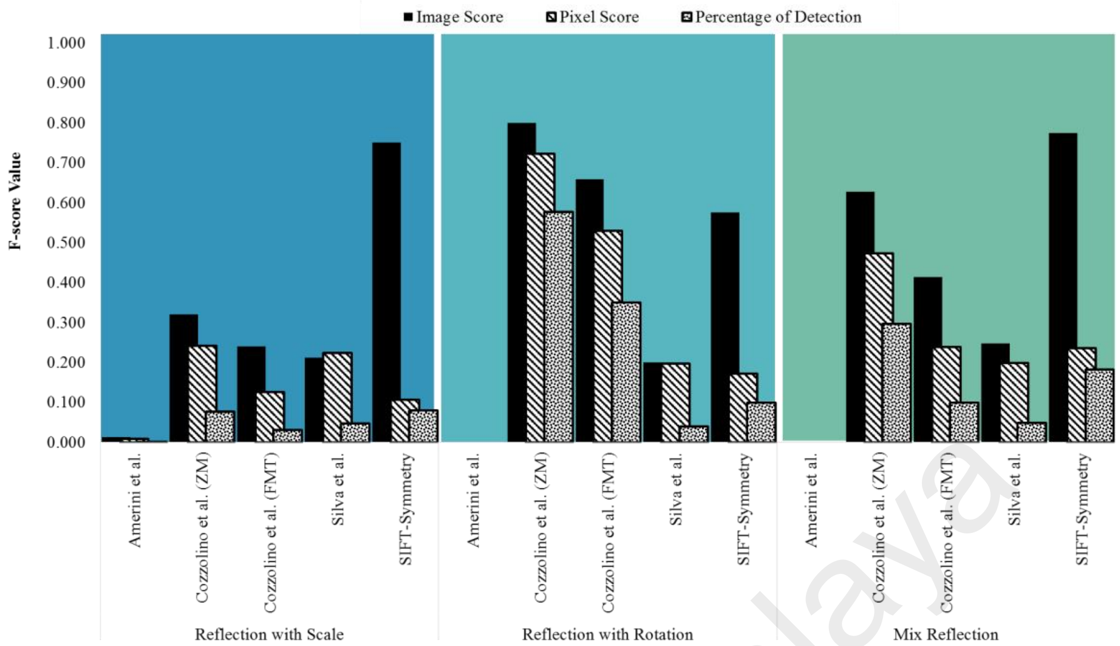
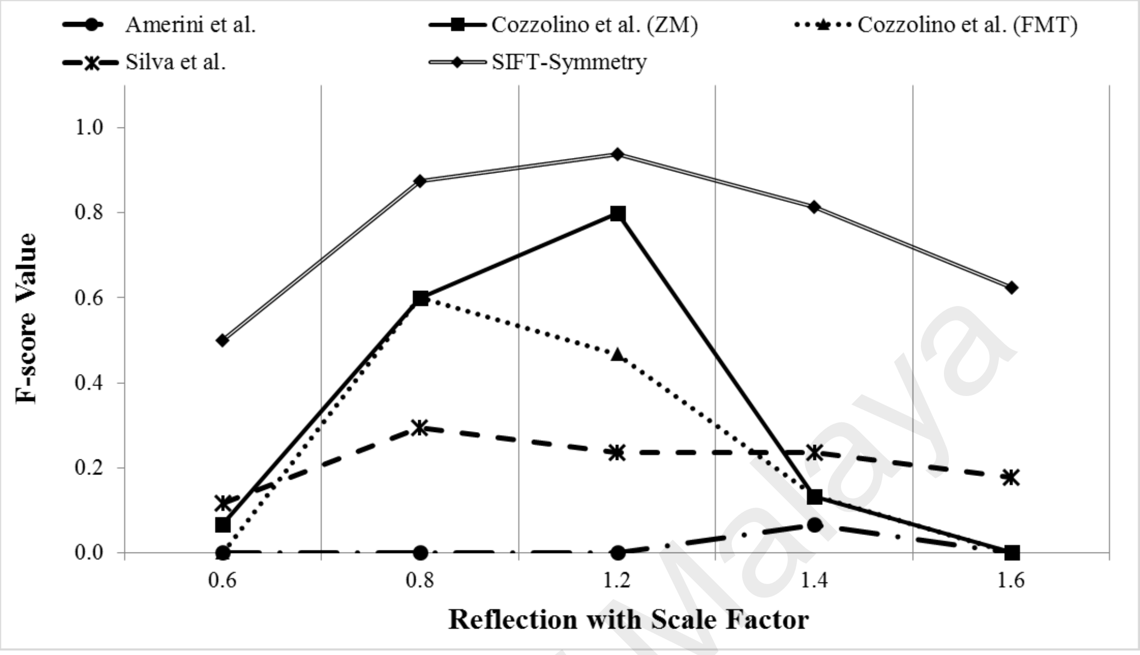


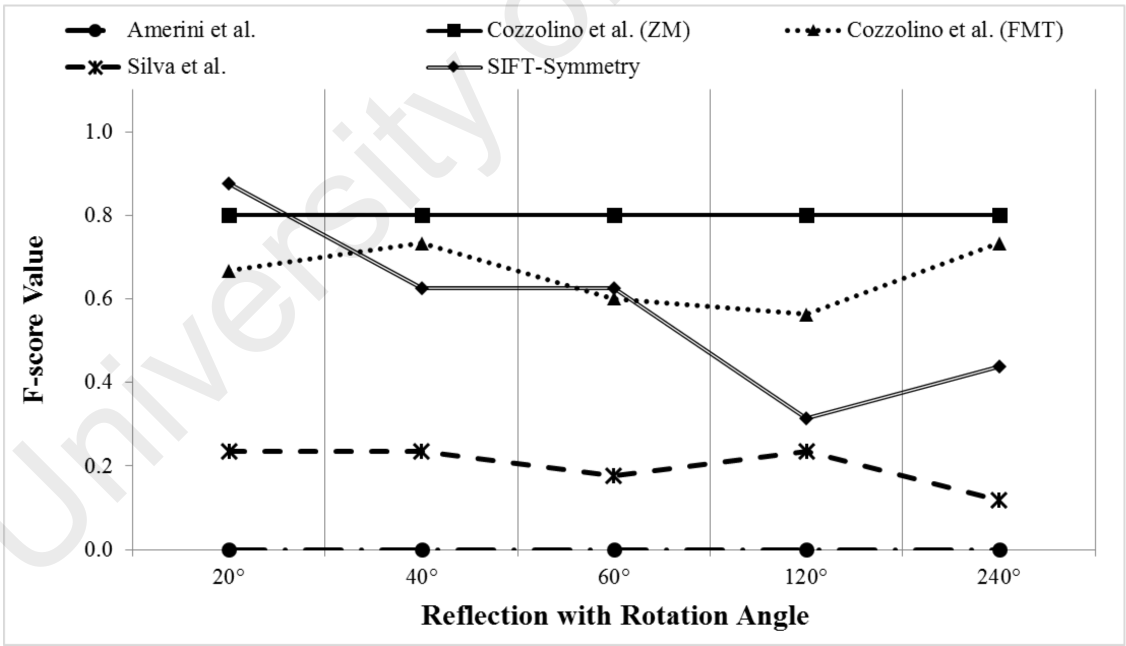
Figure 5.12: Overall performance of image score, pixel score, and percentages of detection results of each group for reflection-based CMF (NBr-CASIA) dataset

For the Cozzolino et al.'s method, the Zernike moments was higher than FMT in all reflection combinations since the Zernike moments is reflection invariant. Nevertheless, the results of the Cozzolino et al.'s method with Zernike moments features only had a steady performance for a scale-up (1.2), while the performance consistently reduces for the other scales. Despite a weak performance for the reflection with scale group, they showed specific achievement by maintaining an 80% score value for reflection with rotation, as shown in Figure 5.13(b). The results confirmed that their method worked well with all degrees of rotation while the SIFT-Symmetry was limited to only small degrees of rotation with reflection. The SIFT-Symmetry had difficulties to find the symmetry axis due to the large change in position in the event rotation occurred after reflection. This is the reason for the low performance in the combination of reflection with other attacks. The results were decreased if the combination of large scales and large degrees of rotation is applied, as depicted in Figure 5.13(c). However, the results may be improved if rotation symmetry implementation is developed. Overall, the SIFT-

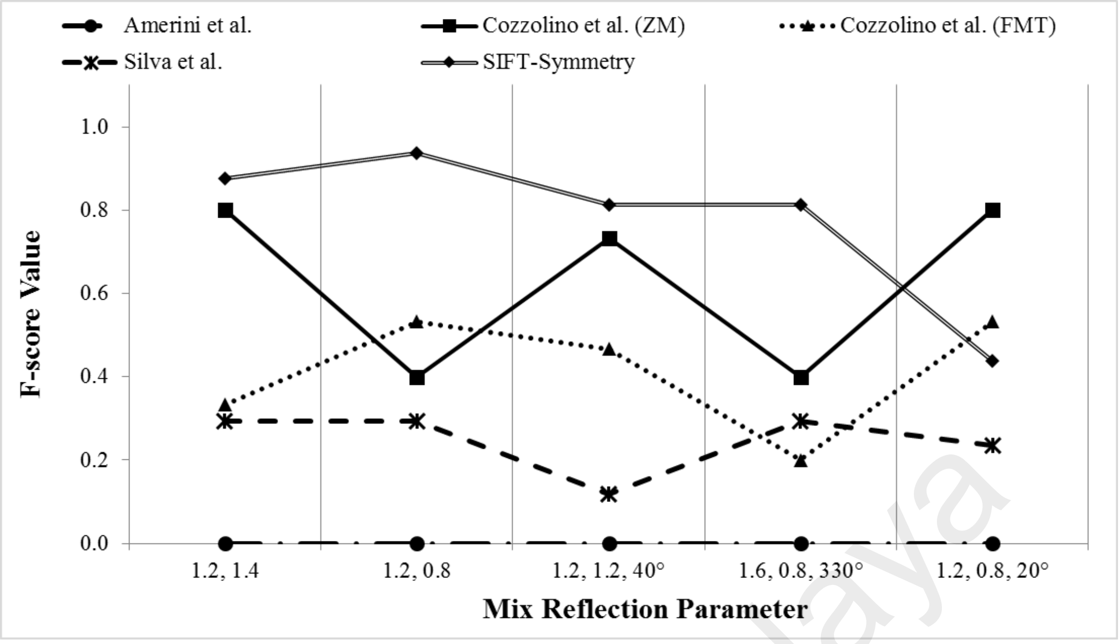
Symmetry provided almost perfect detection in all cases of reflection, except for high degrees of reflection with rotation.



(a)



(b)



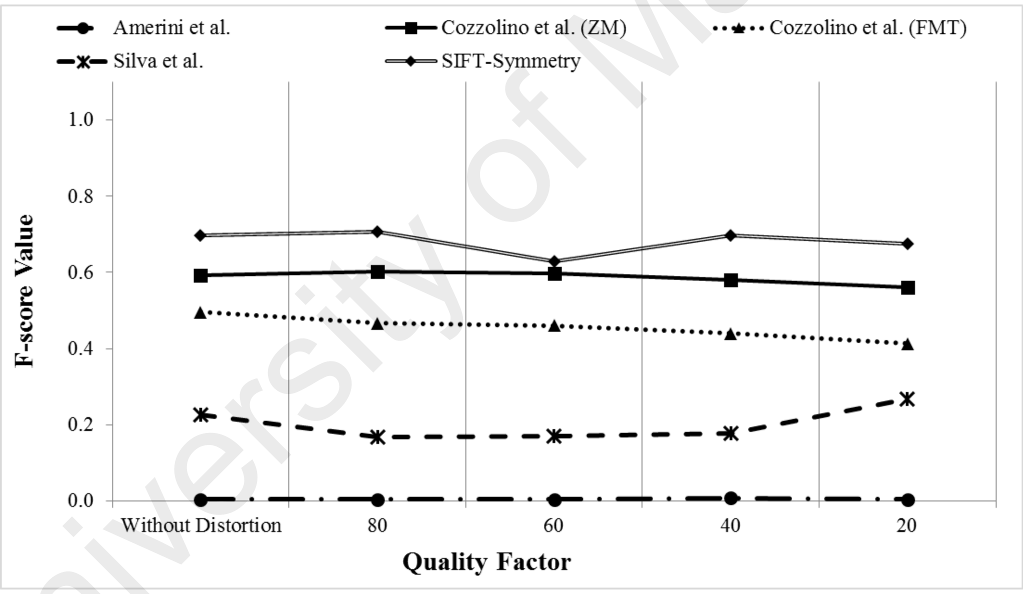
(c)

Figure 5.13: Image score values for the Amerini et al., Silva et al., Cozzolino et al., and SIFT-Symmetry for (a) reflection with scale, (b) reflection with rotation, and (c) combination of reflection

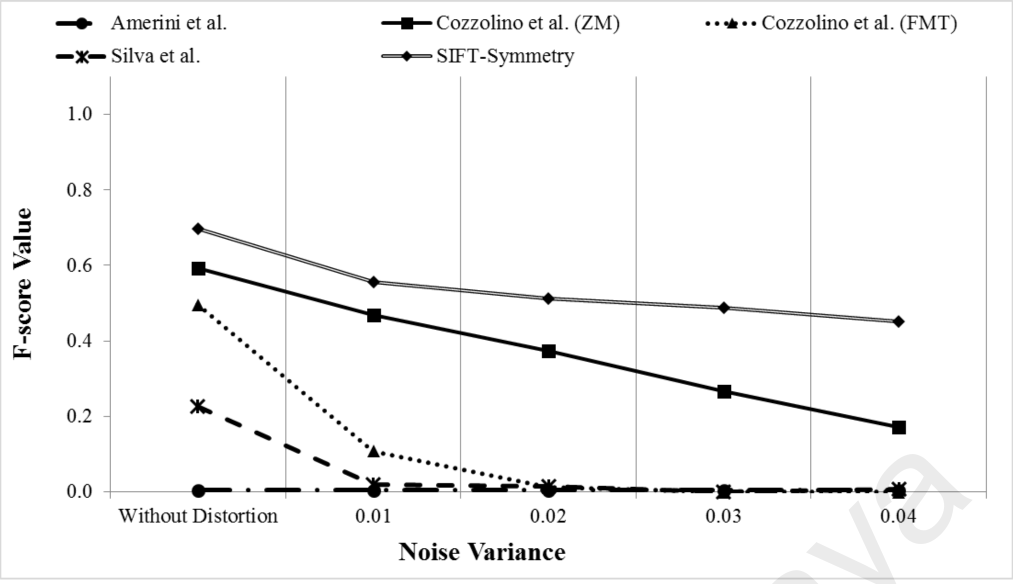
5.3.3 Analysis of Robustness against Post-Processing Attacks

As the post-processing attacks normally occurred after the geometrical transformation attacks, this research continuously analyzed the image-level performance against such attacks. Two sets of experiments were implemented to examine the robustness against JPEG compression and Gaussian noise addition, respectively. For the experiments, all images in NBr-CASIA dataset were distorted by JPEG compression and Gaussian noise with four different parameters. In the first experiment, the images were compressed with various JPEG quality factors ranging between 80–20. Meanwhile, for the second experiment, four variances of Gaussian noise ranging between 0.01–0.04 were added to the images. The results were not only compared with other state-of-the-art methods, but also with the results obtained without distortion in Section 5.3.2.1.

Figure 5.14 illustrates the image score values for the two experiments of post-processing attacks. For compression attack, Figure 5.14(a) shows the overall performance of the CMF detection methods for each factor. Although the performance of the SIFT-Symmetry was decreased especially for the low quality factor, the method was able to maintain the highest score with minimum value of 63% score for each factor. Subsequently, the performance of all state-of-the-art methods continuously decreased for Gaussian noise addition. Figure 5.14(b) illustrates the image score values for all state-of-the-art methods against Gaussian noise addition. In the figure, the results show that all scores tended to decrease when the variance of Gaussian noise was increased.



(a)



(b)

Figure 5.14: Image score values of the Amerini et al., Silva et al., Cozzolino et al., and SIFT-Symmetry against (a) JPEG compression (b) Gaussian noise addition in NBr-CASIA dataset

5.4 Discussion

Based on the performance analysis I in the previous chapter, the existing CMF detection methods have limitations when dealing with CMF with reflection attacks. In view of the fact that the keypoint-based CMF detection method has promising results against common geometrical transformation CMF attacks, which are translation, scale, and rotation, this research attempts to include symmetry matching technique to enhance the method for reflection-based CMF image. In particular, an improved CMF detection method, namely SIFT-Symmetry has been proposed in this research. Basically, it is a combination of keypoint-based CMF detection method with symmetry matching technique. The results showed that the SIFT-Symmetry obtained the highest image score, and percentage of detection in NB-Casia dataset. Even though the performance was diminished for non-reflection attacks compared to the Amerini et al.'s, the performance of the simple reflection attacks was able to outperform the Amerini et al.'s method. For the reflection-based CMF attacks in NBr-Casia dataset, the SIFT-Symmetry presents the highest image score compared to other state-of-the-art methods.

Furthermore, due to the reason that both SIFT-Symmetry and the Amerini et al.'s methods have low recall rate of pixel score, the performances were further analyzed based on image-level only.

Despite the good performance of both datasets, the SIFT-Symmetry has a limitation to differentiate the original image and CMF image because an original image sometimes has symmetry by chance. This was the reason for 22–23 value of the false-positive results acquired in the experiments, hence, further behavior analysis may be needed. In addition, the results of the Amerini et al.'s also confirmed that the SIFT technique also has misdetection rate which is caused by the similarity between two or more natural properties in the same image. An example of such detection is two original bottles with similar properties in an image that are detected as forged even when they are not tampered. Therefore, human interpretation may be required to differentiate a region as natural or forged.

Regardless of the disadvantages, the SIFT-Symmetry presents the most promising results in reflection-based CMF images, higher than the other three state-of-the-art methods. The results show that the method outperforms existing methods by exceeding a minimum value of 75% image score values for almost all cases of reflection-based CMF attacks, including simple reflection, reflection with scale, and mix of reflection. However, the performance for reflection with rotation dropped with an average score of 58%. The reason for the score reduction in reflection with rotation is because the method is unable to extract any symmetry axis when rotation was applied after reflection (large change in position). Remarkably, the results were still applicable for small degrees of rotation with reflection. Finally, as image manipulation may have occurred due to the low quality of images, the SIFT-Symmetry was able to detect CMF images with only 5% reduction in score from without distortion values, even with low quality compression.

5.5 Chapter Summary

This chapter discusses a contribution that presents a method in detecting CMF with reflection attacks by utilizing the symmetry detection as a matching technique. Experiments performed in this research have demonstrated that the existing CMF detection methods have limitations in detecting reflection-based CMF images; hence, the utilization of the symmetry matching technique has altogether enhanced the detection performance, especially for the image-level evaluation.

CHAPTER 6: METHOD II CMF-ITEMS

In this chapter, a method named with CMF-iteMS that proposed an iterative means of region size is presented. The experimental and comparison results are discussed and explained. The key contribution of this chapter is the introduction of the new automatic threshold selection based on iterative means of region size (called as iteMS), in the final verification of CMF detection. Since the detection method proposed by Cozzolino et al. (2015) provides the highest detection performance for CMF with various attacks, the predefined thresholds assigned at the final verification process is replaced by the iteMS procedure to obtain better results for both image and pixel-level evaluations.

This chapter is divided into five main parts: the introduction of the method is briefly described in the first section (Section 6.1). Then, the design of the CMF-iteMS (with its flowchart) is presented in the second section (Section 6.2). Each phase in the flowchart is explained in the section. In the third section (Section 6.3), the experimental results and analysis are discussed, whereas the final discussion is drawn in the fourth section (Section 6.4). Lastly, all sections are summarized in the Section 6.5 (chapter summary).

6.1 Introduction

The performance analysis in Chapter 4 verified that the existing block-based approach has limitation on the threshold selection. As a result, the Cozzolino et al.'s method was not able to detect any CMF regions with small resolution images, even though they performed well in various CMF attacks, including reflection. In the method, they assigned at least four thresholds in the final verification process, including median filtering, thresholding, size, and distance. For that reason, the predefined thresholds require several efforts and become challenging for various input images.

Threshold refers to the least value of a parameter or variable that will produce an identified effect (Threshold, 2009). It is a quantitative value that is used to set the limit of desired result. In CMF detection, threshold is used in various stages, either in feature extraction, matching, or visualization. Even though both stages, feature extraction and matching have their own threshold selection, the CMF detection demands another threshold, particularly to verify the matching results. To be specific, the threshold is assigned due to the reason that several noise and irrelevant information are normally preserved by the matching technique. Therefore, by setting the limit of the matching features, the detection performance produces an accurate result with the exact forged location. Moreover, the spurious matching features will also reduce, thus, this has led to better original image detection.

Unfortunately, due to the reason that many thresholds need to be defined, the values are often specific to a static value. The current practice of the threshold selection is by manually assigning a value which is obtained through several experiments and observations. This is a very challenging task, especially when various image types, qualities, sizes and related attacks are considered in the data collection. Figure 6.1 shows the example of detection results based on the static threshold value. From the figure, the top image should be assigned with threshold 100–400 pixels, while threshold 400–1200 is suitable with the bottom image. A wrong specified threshold value will lead to the reduction in the method's performance. Furthermore, as the CMF detection methods are aimed to blindly detect an image in forensics, a dynamic threshold value becomes a prerequisite to deal with homogeneous image data.

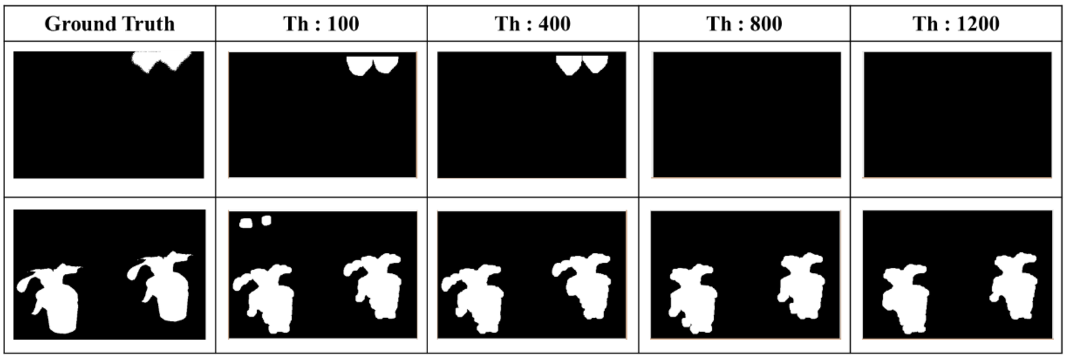


Figure 6.1: Detection results with various predefined thresholds for various types of CMF image

To automate the threshold selection for each input image, this research introduced an iterative means of region size (named as iteMS) procedure for the methods. The iteMS procedure works by iteratively calculating the means of the preserved regions (that is produced by the matching technique) into the smallest value. In addition, as the previous analysis has discussed the advantages of the Zernike moments and FMT features in the Cozzolino et al.'s method, this research continuously explores the features together with another two, including Steerable filter and Dense SIFT. Four conventional thresholding techniques based on iterative means, class variance, and maximum entropy are also studied to compare with the thresholding fitting error. Based on the investigation, the combination of the Zernike moments, thresholding fitting error, and iteMS procedure with limit value 325 pixels are selected as the final design of CMF-iteMS method. The method should be able to detect CMF with any combination of attacks without the need to predefine a threshold value for various inputs of CMF images. The results of the method are compared with the existing CMF detection methods while the performance are discussed thoroughly.

6.2 CMF-iteMS

Basically, the goal of the CMF-iteMS is to enhance the block-based CMF detection method by automatically selecting a threshold value for final verification process. The block-based CMF detection method (Cozzolino et al., 2015) is selected, since it provides stability and good performance in various possible attacks, particularly translation, scale, rotation, reflection and a mix of the attacks. In spite of its good performance, the method is sensitive to various illumination changes and scale attacks. Furthermore, the threshold value is fixedly defined, specifically for their dataset. Thus, the threshold is occasionally unsuitable to other datasets and in turn, leads to reduction in performance.

In the new design of CMF-iteMS, four feature extraction techniques are investigated, including Zernike moments (Teague, 1980), FMT (Sheng & Arsenault, 1986), Steerable filter (Freeman & Adelson, 1991), and Dense SIFT to obtain the most invariant features. Then, the existing PatchMatch CMF detection design is modified by exploring conventional thresholding techniques and introducing a new automatic threshold selection technique based on iterative means of regions size (iteMS). This is to replace the predefined threshold selection in most of the CMF detection methods. The flowchart of the whole design of the proposed method is illustrated in Figure 6.2 where the blue color represents its unique characteristics. The details are divided into five phases, specifically (i) feature extraction, (ii) PatchMatch, (iii) thresholding (iv) automatic threshold selection, and (v) mathematical morphology (MM).

The feature extraction techniques investigated are explained in the first phase. Then, the techniques are adapted and combined with PatchMatch CMF detection method (Cozzolino et al., 2015). Next, the results of the matching patch are applied with four conventional thresholding techniques, particularly iterative means, class-variance, maximum entropy I and II of intensity together with thresholding fitting error to study their efficiency. To remove the small unrelated features, the thresholding results are further refined and filtered by a new automatic threshold selection technique based on iteMS procedure, which is introduced in the fourth phase. The flow ends with the final verification of forgery localization in the fifth phase by segmenting the remaining regions using a MM operation. The explanations of the five phases are covered in the following subsections.

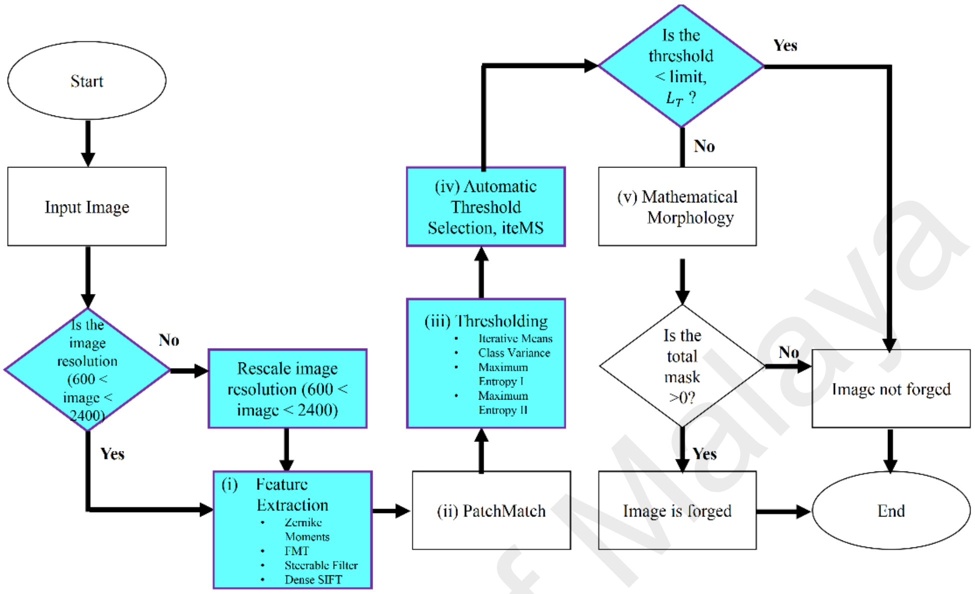


Figure 6.2: Flowchart of the CMF-iteMS method

6.2.1 Feature Extraction

In the first phase, the sensitivities of four feature extraction techniques towards various attacks in CMF are studied. The most invariant features are then included in the design of the CMF-iteMS. According to Chora (2007), feature extraction is a process to select relevant information that represents the characteristics of interest in the image. Each feature extraction technique has its own specifications to determine the interest in an image. These specifications describe the performance either as advantages or limitations when it deals with CMF and its combination attacks. In this section, Zernike moments is firstly discussed. Then, other three feature extraction techniques are included to observe the effects in detecting CMF images.

(a) Zernike Moments

Firstly, the input image, $(r \times c)$ is divided into a predefined patch size, SZ_z which is 16×16 as computed in Equation (6.1).

$$SZ_z\ (u,v)\ =\ (\frac{r}{16},\frac{c}{16}) \tag{6.1}$$

Then, each patch size, SZ_z is transformed to a polar coordinate, where $I\ (u,v)$ represents $I\ (\rho,\theta)$, which the $\rho\ \epsilon\ [0,\infty]$ while $\theta\ \epsilon\ [0,2\pi]$. A polar sampling procedure is employed by resampling the basic functions, $K_{n,m}(\rho,\theta)$ at the grid points (x,y) of the analysis patch, W. With the use of multiple sampling steps, $\Delta\theta$, the procedure provides a rotation invariants performance with a good estimation of it in all other cases. The basic function, $K_{n,m}(\rho,\theta)$, is the product of radial profile (which is Zernike) and a circular harmonic as in Equation (6.2).

$$K_{n,m}(\rho,\theta) =\ R_{n,m}(\rho) \tag{6.2}$$

Zernike radial function, $R_{n,m}(\rho)$ is computed based on polar sampling procedure with a finite number of (n,m) couples as computed in Equation (6.3) and (6.4), respectively.

$$R_{n,m}(\rho) = \sum_{h=0}^{\frac{n-|m|}{2}} C_{n,m,h}\rho^{n-2h} \tag{6.3}$$

$$\sum_{h=0}^{(n-|m|)/2} = 5 \tag{6.4}$$

where $\rho\ \in [0,1]$ and $C_{n,m,h}$ is the coefficients that ensure orthonormality of the basic functions. W represents the number of sampling along radius and angles in polar grid, $\rho \leq 8$, which the radius equal to 26 and the angles equal to 32.

Lastly, with the length of 12, Zernike polar function, $f(z)$ resulting the feature vector, $u \times v \times 12$ for the whole image, $(r \times c)$. To sum, $f(z)$ basically is the collection of magnitudes of each coefficient, $F_I'(n,m)$ in polar coordinates (referring to Equation (6.5).

$$F_I'(n,m) = \sum_{(x,y)\in W} I(x,y)K_{n,m}^{*}(\rho(x,y),\theta(x,y)) \qquad (6.5)$$

with $\rho(x,y)$ = $\sqrt{x^2 \ + y^2}$ and $\theta(x,y)$ = $\pm arctan(y/x)$

In view of the fact that common CMF image is comprised of simple translation with a combination of geometrical transformation and post-processing attacks, a feature extraction technique used in the design should be robust to the attacks. Turning to accuracy, the whole CMF-iteMS will be less effective if the feature extraction used is variant to various types of attacks. Since many image types are available, the suitable features may be needed to cater different images. For example, Zernike moments has limitations in detecting CMF with numerous luminance changes in an image. Hence, three different types of feature extraction are studied to be adapted with the PatchMatch method, namely FMT, Steerable Filter (StF) and Dense SIFT (DS). The parameters used in the features are listed in Table 6.1 and the usage is described in the next section.

Table 6.1: Parameter used for FMT, StF and DS features

Parameter	Value	Definition
$\boldsymbol{SZ_{FMT}}$	24×24	Patches of 24×24 are used with features of FMT, $\lvert f\rvert FMT$
$\boldsymbol{\lvert f\rvert FMT}$	25	Length of FMT features
$\boldsymbol{SZ_{StF}}$	12×12	Patches of 12×12 are used with features of Steerable filters, $\lvert f\rvert StF$
$\boldsymbol{\lvert f\rvert StF}$	19	Length of Steerable filters features
$\boldsymbol{SZ_{DS}}$	12×12	Patches of 12×12 are used with features of dense SIFT, $\lvert f\rvert DS$
$\boldsymbol{\lvert f\rvert DS}$	128	Length of dense SIFT features

(b) $\boldsymbol{FMT}$

Primarily, the development of the CMF-iteMS is focused on the limitations of the Zernike moments. Although Zernike moments is known to be rotation invariant, however, the feature is sensitive to scale and illumination changes (Kim & In-So, 2002). Since the Mellin transform has the advantages on rotation, scale and illumination invariant (Carkir & Cetin, 2010), FMT (Sheng & Arsenault, 1986) is considered. Similar procedure of Zernike moments is applied by considering the polar sampling procedure, $F_I'(n,m)$ to resample the basic functions of FMT, $f(f)$. The $K_{n,m}(\rho,\theta)$ represents the FMT radial function, while $R_v(\rho)$ is computed as in Equation (6.6) for each predefined patch, SZ_{FMT}. According to the equation, the values of (n,m) couples differ with Zernike moments, thus, resulting in the difference of length of FMT feature, $f(f)$. The length of the features and the patch size, SZ_{FMT} applied in the CMF-iteMS are listed in the Table 6.1.

$$R_v(\rho) = \frac{1}{\rho^2} e^{jv \log(\rho)}$$

$$v = \frac{2n\pi}{log \frac{\rho_{max}}{\rho_{min}}} \qquad (6.6)$$

$$n = 0, \pm 1, \pm 2$$

$$m = 0, 1, 2, 3, 4$$

(c) Steerable Filter (StF)

Instead of using CHT family, comprising Zernike moments and FMT, the methods of steerable filters (Freeman & Adelson, 1991) that is commonly described as texture features is also adopted. The input image, (r,c) is divided into a predefined patch size, SZ_{StF} which is 12×12. Each patch size is applied with the circularly symmetric Gaussian function, G which is written in Cartesian coordinates, x and y for 2-D distribution that only can be achieved by convolution. However, since an input image only has pixel values, the convolution process requires a discrete approximation to the Gaussian function. Therefore, a first derivative of Gaussian, $G_1^{0^\circ}$ and the rotated 90° version, $G_1^{90^\circ}$ is computed at an arbitrary orientation, θ which are synthesized by G_1^{θ}. (note that: θ is a directional derivatives evenly-spaced from 0 degrees to 360 degrees in $20°$ increments). Equation (6.7) summarized the basic calculation of the steerable filter with the length of 19 (also known as filter bank).

$$G(x,y) = e^{-(x^2+y^2)} \qquad (6.7)$$

$$G_1^{0^\circ} = \frac{\partial}{\partial x} e^{-(x^2+y^2)} = -2xe^{-(x^2+y^2)}$$

$$G_1^{90^\circ} = \frac{\partial}{\partial y} e^{-(x^2+y^2)} = -2ye^{-(x^2+y^2)}$$

$$G_1^{\theta} = \cos(\theta)\, G_1^{0^\circ} + \sin(\theta) G_1^{90^\circ}$$

(d) ***Dense SIFT (DS)***

In order to be adapted with the PatchMatch method, the filter bank procedure is continuously explored with different types of features. By seeing the potential of SIFT feature extraction (Lowe, 1999) towards scale, rotation and illumination changes, this research modified the features in a filter bank form. Similar to Steerable filter, the input image is divided into a predefined patch, SZ_{DS} which is 12×12. The feature detection phases are discarded, while 128 descriptors are extracted on each predefined patch, SZ_{DS}. For each pixel, SZ_{DS} the neighborhood is divided into 4×4 array of histogram with 8 orientation bins which resulted in 128 elements vector.

6.2.2 PatchMatch

To find a match for each patch, the PatchMatch method are implemented in the second phase. Both zero-order and first-order predictors are employed as computed in Equation (6.8) for a set of candidates, $\delta(s)$, in Equation (6.9). Zero-order is useful for rigid translations while First-order predictors could help in detecting CMF image with scale and rotation.

$$\begin{gathered} \tilde{}_{\delta}0x_{(s)} \;\; = \; \delta(s^x\ ) \\ \tilde{}_{\delta}1x_{(s)} = \; 2\delta(s^x) - \delta(s^{xx}) \\ x \;\in \{r, d, c, a\} \end{gathered} \tag{6.8}$$

where s^{xx} is the pixel for s^x along direction x in the scanning order, d and a, are the diagonal and antidiagonal directions, respectively. The whole set of predicted offsets is shown in Equation (6.10).

$$\delta(s) = \underset{\varphi \in \Delta^P(s)}{\arg\min}\ D\big(f(s), f(s + \varphi)\big) \tag{6.9}$$

where $\Delta^P(s) = \{\delta(s), \delta(s^r), \delta(s^c)\}$, and s^r and s^c are the pixels for s, in the scanning order, along rows and columns, respectively.

$$\Delta^P(s) = \{\delta(s), \tilde{\delta}0r_{(s)}, \tilde{\delta}0d_{(s)}, \tilde{\delta}0c_{(s)}, \tilde{\delta}0a_{(s)}, \tilde{\delta}1r_{(s)}, \tilde{\delta}1d_{(s)}, \tilde{\delta}1c_{(s)},\} \tag{6.10}$$

To sum, the PatchMatch will quickly propagate to the rest of the interested region whenever a correct offset field is found over a couple of neighboring pixels within two iterations.

6.2.3 Thresholding

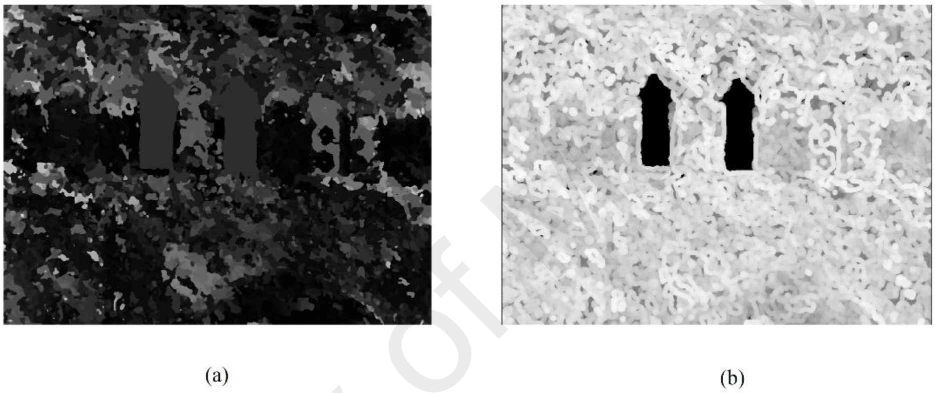
Subsequently, the offset field produced by the PatchMatch algorithm might be scattered and cluttered because of the presence of noise, compression, illumination changes and uniform regions. For that reason, an affine transformation is applied to remove the outliers and thresholding with a new automatic threshold selection to single-out the CMF regions. The affine transformations and thresholding techniques are explained in the next subsections, while the new automatic threshold selection are followed after this section.

6.2.3.1 Thresholding Fitting Error

Ideally, the existing CMF detection methods applied the RANSAC or SATS algorithm to estimate the affine transformation between the identical features. However, in view of the fact that the PatchMatch resulting adequate offset field, dense linear fitting is enough to fit in the offset. A suitable N-pixel neighborhood of the true offset field $\delta(s)$ is fitted through an affine transformation model, A similar to Equation (6.11), to minimize the sum of squared errors in Equation (6.12). Moreover, by assuming that the homography is symmetry and unchanged, the results of the homogenous coordinates in $\varepsilon^2(s\,)$ (when assigning the circular radius neighborhood, s as 6 pixels) is filtered for several times in quadratic form to obtain two offset components. In spite of the simplicity of the fitting error, the errors are sensitive to outliers. Hence, median filtering is firstly applied to the matching patch, specifically to remove the outliers and inconsistency of noise in the image before generate the fitting error. The final detection results for the median filtering and dense linear fitting are shown in Figure 6.3.

$$\delta'(s_i) = As_i \ , i = 1, \ldots, N \tag{6.11}$$

$$\varepsilon^2(s) = \sum_{i=1}^{N} ||\delta(s_i) - \delta'(s_i)||^2 \tag{6.12}$$


(a)

(b)

Figure 6.3: Detection results (a) median filtering (b) dense linear fitting

Based on the figure, the results of the dense linear fitting are able to generate two regions with several noise (denoted by black color). Thus, simple thresholding fitting error is performed by converting the pixels below 300 (RGB value with hue 60°) with black color, while the above pixels are changed to white color. Typically, thresholding techniques are designed to select a threshold value from the intensity of the pixels on the frontier between object and background. As a result, the output is a binary image where one part of the threshold will represent the foreground objects while the opposite part will relate to the background.

6.2.3.2 Conventional Thresholding Techniques

Instead of performing the simple thresholding fitting error, this research explores several conventional automatic gray-level thresholding techniques including iterative means (Ridler, T.W. Calvard, 1978), class variance (Otsu, 1979), and maximum entropy (Kapur et al., 1980; Yen et al., 1995). The techniques work by assuming that the object and the background of the image are in unimodal gray distribution, where the gray value between neighboring pixels within the object or background is highly relevant. The four techniques are originally taken from several information theories in statistics, comprising probability distribution, means, variances, and maximum entropy that are implemented to the intensity of an image. The example results for each thresholding techniques are shown in Figure 6.4.

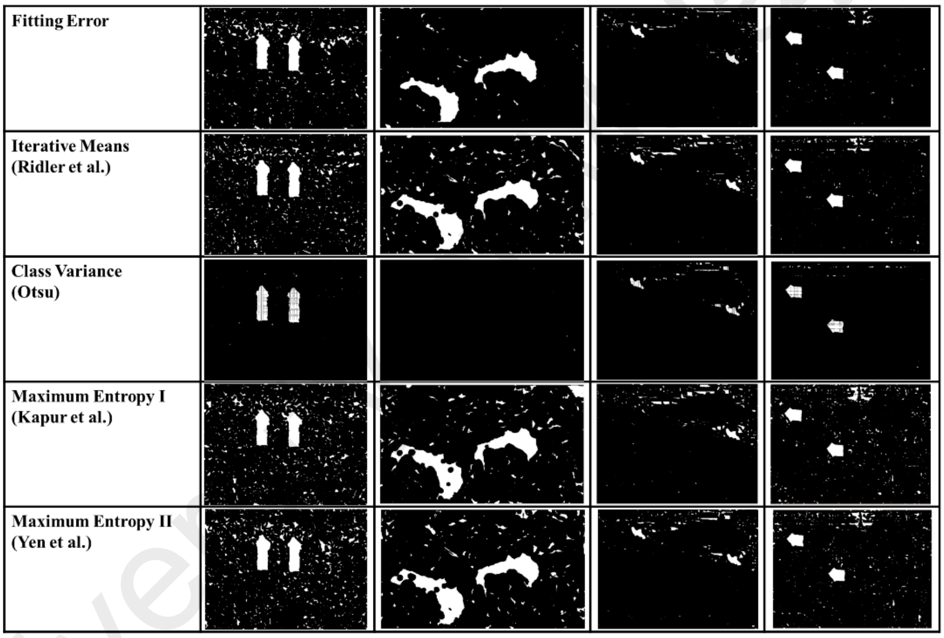

Fitting Error
Iterative Means (Ridler et al.)
Class Variance (Otsu)
Maximum Entropy I (Kapur et al.)
Maximum Entropy II (Yen et al.)

Figure 6.4: The example results of each thresholding technique against CMF image

Firstly, in order to generate the unimodal gray distribution between the object and the background, a histogram of the image is computed as two different probability distributions (pd) specifically for foreground, f and background, b. One pd is defined for discrete values, 1 to s and the other pd is for values from, $s+1$ to n. The two distributions are shown in Equation (6.13) and (6.14), respectively. These equations represent the basis function of P for the thresholding techniques based on iterative means, class variance and maximum entropy.

$$f = \frac{P_1}{P_s}, \frac{P_2}{P_s}, \dots \dots \dots \dots . \frac{P_s}{P_s} \tag{6.13}$$

$$P_f = \sum_{i=1}^{s} P_i$$

$$b = \frac{P_{s+1}}{1-P_s}, \frac{P_{s+2}}{1-P_s}, \dots \dots \dots \dots . \frac{P_n}{1-P_s} \tag{6.14}$$

$$P_b = \sum_{i=s+1}^{n} P_i$$

(a) ***Iterative means***

Referring to the pd, this research adopted the technique by Ridler et al. (1978) who firstly introduced an iterative scheme procedure. The mean, $m(s)$ for f and b, are calculated as in Equation (6.15).

$$m_f\ (s) = \sum_{i=1}^{s} iP_i \tag{6.15}$$

$$m_b\ (s) = \sum_{i=s+1}^{n} iP_i$$

Then, the means value is calculated iteratively, $Iter_m$ using Equation (6.16). The procedure will stop when the threshold value, $|s_m - s_{m+1}|$ become sufficiently small. The final s_m value is assigned as the threshold.

$$Iter_m = \lim_{m \to \infty} \left(\frac{m_f\ (s_m) - m_b\ (s_m)}{2} \right) \tag{6.16}$$

(b) ***Class variance***

The second thresholding technique investigated is class variance (Otsu, 1979). The author improved the iterative means by replacing the means value with the second-order statistics (variances) class. The inter-class variances, $\sigma_b^2(s)$ is maximizing as in Equation (6.17). The optimal threshold value, s is obtained by referring to ${}_{1 \le s < n}^{max} \sigma_m^2(s)$.

$$\sigma_b^2(s) = \left\{ \frac{P_s\ [1 - P_s\ ][m_f\ (s) - m_b\ (s)]^2}{P_s \sigma_f^2(s) + [1 - P_s] \sigma_b^2(s)} \right\} \tag{6.17}$$

(c) Maximum Entropy

Next, in view of the fact that the maximum entropy theory represents the most informative distribution that is acceptable by signal processing, this research explores the technique in thresholding. The maximum entropy technique based on probability distribution suggested by Kapur et al. (1980) is adapted to the dense linear fitting result. The sum of the two entropy probability distribution, $H(f)$ and $H(b)$ are calculated as φ_s represents in Equation (6.18).

$$\varphi_s = H(f) + H(b) \tag{6.18}$$

$$H(f) = \sum_{i=1}^{s} \frac{P_i}{P_s} \log \frac{P_i}{P_s}$$

$$H(b) = -\sum_{i=s+1}^{n} \frac{P_i}{1 - P_s} \log \frac{P_i}{1 - P_s}$$

On the other hand, a technique by Yen et al. (1995) which is based on maximum entropy correlation is also implemented as the threshold value in this research. The probability distribution suggested by Kapur et al. is changed to correlation, where sum of the two entropy correlation, $C(f)$ and $C(b)$ are computed as φ_s in Equation (6.19).

$$\varphi_s = C(f) + C(b) \tag{6.19}$$

$$C(f) = -\log \left\{ \sum_{i=1}^{s} \left[\frac{P_i}{P_s}\right]^2 \right\}$$

$$C(b) = -\log \left\{ \sum_{i=s+1}^{n} \left[\frac{P_i}{1 - P_s}\right]^2 \right\}$$

Both techniques of maximum entropy assigned the maximum information of φ_s as the threshold value.

6.2.4 Automatic Threshold Selection

Referring to the Figure 6.4, the figure shows that the single thresholding techniques may not able to separate the CMF region and original region. The single thresholding techniques would increase the misdetection and reduce the performance of CMF detection. Therefore, instead of determining single thresholding, an automatic threshold selection technique, which able to change the value based on the input images is proposed. Since most of the predefined threshold in CMF detection is typically based on the regions size, the conventional thresholding techniques based on iterative means is adopted by replacing the intensity value with the regions size. The regions size are obtained from the output of the thresholding techniques from previous subsection (Section 6.2.3). Due to the reason that each CMF image has different CMF regions, the proposed automatic threshold selection is able to automatically change the threshold value based on the input image. This section described the proposed automatic threshold selection technique based on iterative means of regions size (iteMS) procedure.

6.2.4.1 Iterative Means of Regions' Size. iteMS

Since the thresholding techniques only able to read the information of intensity histogram, which do not help to discover the exact CMF region, the final results of the CMF detection will include the false match that is considered as a foreground object. Eventually, it will reduce the CMF performance by increasing the false positive value. Hence, a new automatic threshold selection technique based on iterative means (Ridler, T.W. Calvard, 1978) is proposed. However, instead of the intensity histogram, the region size has been chosen, thus, called as iterative means of regions size, iteMS. In the iteMS procedure, a flood-fill algorithm is applied to the connected-component in the binary image of the thresholding result (where the target color is zero), particularly to obtain the size of each region, r_a. The mean of all regions size, m_s, is calculated iteratively to find the ultimate threshold value, s_m. Similar to Ridler's technique, the iteration will stop when the threshold value, $|s_m - s_{m+1}|$ is equal or more than 1. The calculation is summarized in Equation (6.20).

$$r_a = \{r_1, r_2, r_3, \dots \dots r_s\}$$

$$m_s\ (s) = \sum_{i=1}^{s} ir_i = s_m \tag{6.20}$$

$$Iter_m = \lim_{\mathrm{m}\to\infty} \left(\frac{r_{below}\ (s_m) + r_{above}\ (s_m)}{2} \right)$$

Although the iteMS procedure is feasible for all image resolutions, the detection is only effective for the CMF images (forged images), but not to the original images. In practice, the computed iterative means will calculate the average of all regions from the thresholding results in order to get some threshold value. Thus, it will only work if there is a major difference in size between the copied region and the background region. Contrarily, most of the original images will produce a small size of matched regions which is commonly caused by the uniform background in an image. The examples of the preserved size (after the iteMS procedure) between original and CMF images are shown in Figure 6.5.

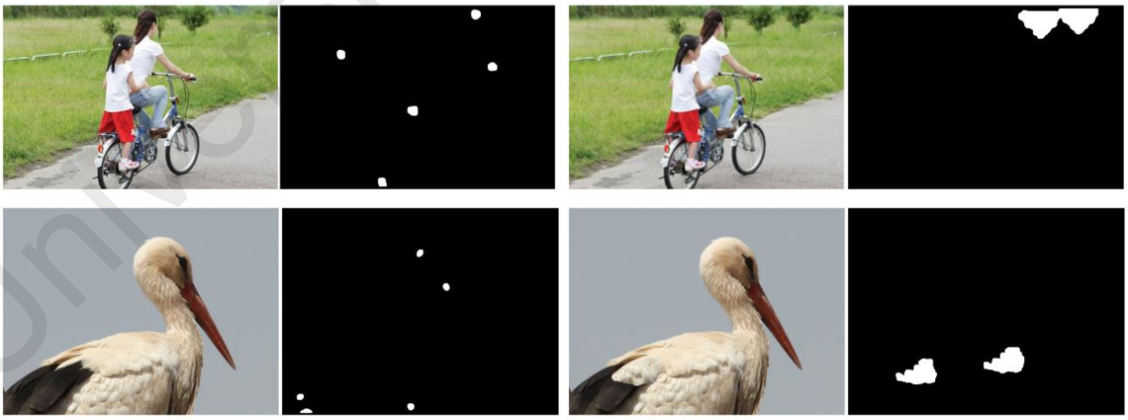


Figure 6.5: Two examples of the preserved region size (after iteMS is applied) for original images (left) and CMF images (right)

Therefore, the threshold value obtained from the iteMS procedure is proposed to limit the value for original image. Each combination of the thresholding techniques with the iteMS procedure will produce different limit threshold value, L_T. The procedure for the acquisition of L_T value is described in the next subsection.

6.2.4.2 Limit Threshold, L_T, for Original Image Detection

To identify the limit threshold value, L_T, for the original images, the iteMS values of the original images are accumulated. From the accumulated value, mean, μ, and standard deviation, s, are calculated as in Equation (6.21).

$$\mu = \frac{\sum T_o}{\sum o}$$

$$s = \sqrt{\frac{\sum (T_o - \mu)^2}{\sum o - 1}} \qquad (6.21)$$

where o is the original images in an image-level dataset, and T_o is the iteMS value of the original images. To fix the limit value, all images in the dataset are resized into two resolutions comprising 600 pixels and 2400 pixels. The mean and error, e, value for both resolutions are assigned as the potential iteMS limit, L_T, which computed in Equation (6.22).

$$e = \mu + 1s \qquad (6.22)$$

$$L_T = \{\mu_{2400}, \mu_{600}, median, e_{2400}, e_{600},\}$$

Then, the methods allocated the values in the L_T as the possible limit threshold value. If the iteMS value for the input image is less than the L_T value, the images will be considered as an original image. The L_T value with the highest F-score are used as the final iteMS limit value. Since the original images are supposed to be unknown, the limit value is obtained through GRIP dataset (Cozzolino et al., 2015). The dataset is selected because the images have a variety of types and features, which involves only simple translation attacks. Thus, the value will not be affected by other CMF attacks.

The whole process of the acquisition of limit threshold value, L_T, is illustrated in Figure 6.6.

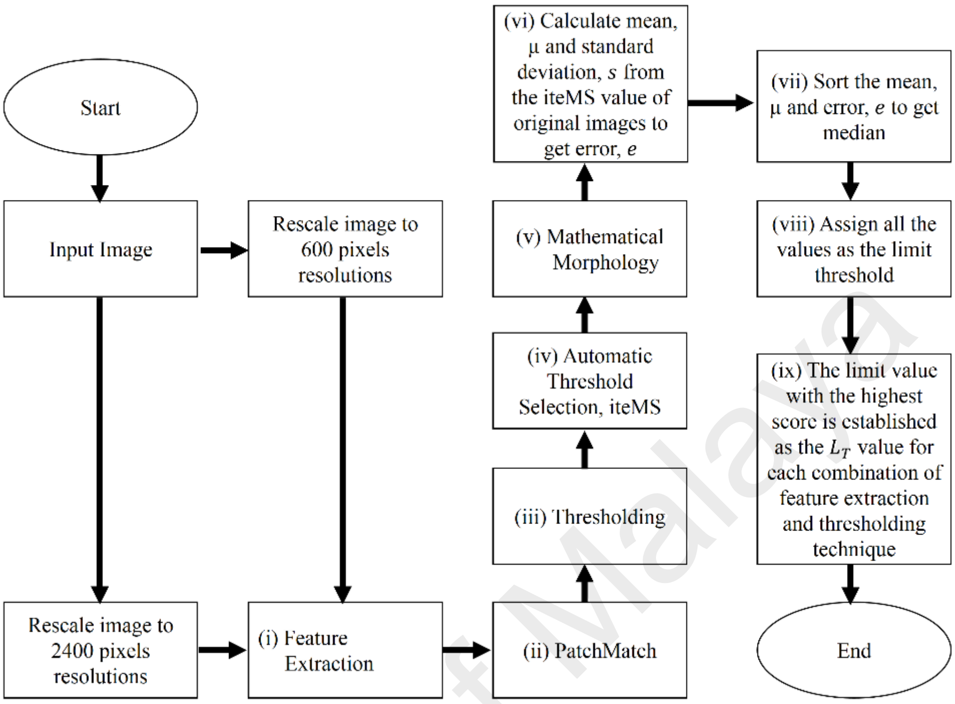

Start
Input Image
Rescale image to 600 pixels resolutions
Rescale image to 2400 pixels resolutions
(i) Feature Extraction
(ii) PatchMatch
(iii) Thresholding
(iv) Automatic Threshold Selection, iteMS
(v) Mathematical Morphology
(vi) Calculate mean, μ and standard deviation, s from the iteMS value of original images to get error, e
(vii) Sort the mean, μ and error, e to get median
(viii) Assign all the values as the limit threshold
(ix) The limit value with the highest score is established as the L_T value for each combination of feature extraction and thresholding technique
End

Figure 6.6: The whole process of the acquisition of limit threshold, L_T, value

6.2.5 Mathematical Morphology

In the final phase of detection, MM is applied to finalize the shape of CMF regions and localized the forged areas. MM is a set of mathematical theory (based upon logical which is related to pixels and geometric feature extraction) applied to a shape or structure in the image for analysis. After the filtering process by the automatic threshold selection technique, a morphological dilation is applied with a circular structuring element of radius (equal to ten pixels) to the identified copied regions. Finally, the forgery detection is identified, if the number of copied region equals to at least one pixel. Figure 6.7 shows the results before morphology has taken and after the morphology process.

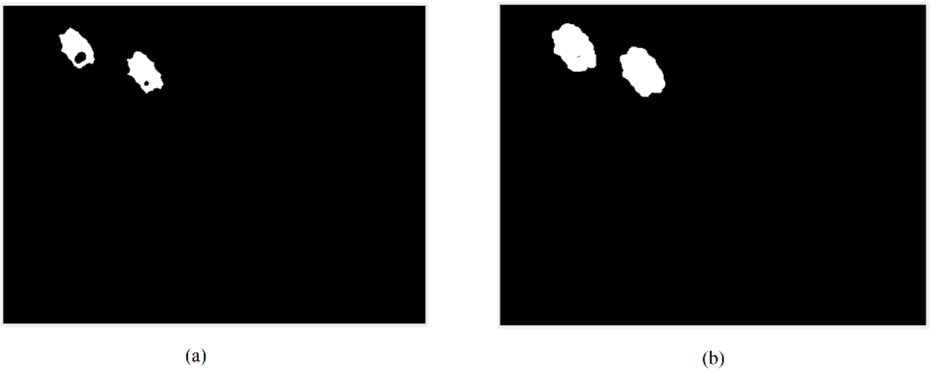


Figure 6.7: Detection results before (left) and after (right) the process of mathematical morphology

6.3 Experimental Results and Analysis

The performance of the CMF-iteMS was analyzed through several extensive sets of experiments using two datasets, NB-Casia and NBr-Casia. Firstly, several investigations on the four feature extraction and four conventional thresholding techniques were implemented to identify the best combination settings in the CMF-iteMS. Similar to the SIFT-Symmetry, the CMF-iteMS is compared with three related state-of-the-art methods (Amerini et al. (2011), Cozzolino et al. (2015) for Zernike moments and FMT, and Silva et al. (2015)) by using multiple F-score measure metrics (image, pixel and percentage of detection). Furthermore, the scores were also analyzed based on CMF with geometrical transformation and post-processing attacks. The details of the experimental results and analysis are discussed in the following subsections.

6.3.1 Initial Evaluations

In view of the fact that the existing block-based CMF detection method has limitations on feature extraction and threshold selection, this section aimed to verify the weaknesses and provide a solution to improve the methods. For that reason, the design of the CMF-iteMS involved three phases in this section. In the first phase, four feature extraction techniques were studied to analyze the most invariant technique, especially for reflection-based attacks. Then, the selected feature extraction technique was examined with five thresholding techniques that were combined with the proposed iteMS procedure in the second phase. In the phase, the performances of each technique were analyzed and discussed, which the best combination of feature extraction and thresholding technique with the iteMS procedure will be selected as the ultimate design of CMF-iteMS in the third phase. This design was established for all experiments and comparisons with the existing CMF detection methods.

6.3.1.1 Performance Evaluation Feature Extraction

In the first experiment, four feature extraction techniques comprising Zernike moments, FMT, Steerable filter and Dense SIFT were assigned with two predefined thresholds. Table 6.2 lists the image score, pixel score and percentage of detection values for each feature extraction technique with each threshold. According to the table, the performance of all feature extraction techniques for both NB-Casia and NBr-Casia were increased when the value of 400 is employed compared to 1200. This is happened because the threshold of 1200 is efficient for images with resolution of 1000 pixels and above. Since the NB-Casia and NBr-Casia datasets have resolutions of below 1000 pixels, a smaller threshold may be required for the datasets.

To observe the performance of each feature extraction technique against various attacks in CMF, the NB-Casia dataset was divided into five groups of attacks, specifically simple translation, scale, rotation, simple reflection and mix of attacks, while the NBr-Casia is grouped under reflection-based attacks. Figure 6.8 presents the comparison results of the feature extraction techniques based on the percentage of detection for each group of attacks with threshold value 400. As can be seen from the figure, all feature extraction techniques achieved a minimum 76% of detection for simple translation attacks. However, the performance were decreased depending on the attacks and the capability of feature extraction techniques.

Table 6.2: F-score values for each feature extraction technique for two predefined thresholds tested on the NB-Casia and NBr-Casia datasets

Predefined Threshold	Dataset		Zernike Moments	FMT	Steerable Filter	Dense SIFT
1200	NB-Casia	Image Score	0.654	**0.745**	0.113	0.395
		Pixel Score	0.561	**0.634**	0.072	0.304
		Percentage of Detection	0.367	**0.472**	0.008	0.120
	NBr-Casia	Image Score	**0.593**	0.496	0.000	0.004
		Pixel Score	**0.491**	0.325	0.000	0.004
		Percentage of Detection	**0.291**	0.161	0.000	0.000
400	NB-Casia	Image Score	0.804	**0.849**	0.242	0.467
		Pixel Score	0.666	**0.701**	0.110	0.349
		Percentage of Detection	0.535	**0.595**	0.027	0.163
	NBr-Casia	Image Score	**0.756**	0.614	0.050	0.027
		Pixel Score	**0.592**	0.402	0.000	0.005
		Percentage of Detection	**0.448**	0.247	0.000	0.000
Average		Image Score	**0.702**	0.676	0.101	0.223
		Pixel Score	**0.578**	0.516	0.046	0.166
		Percentage of Detection	**0.405**	0.348	0.005	0.037

Regardless of the decrement performance, the score of Steerable Filter was significantly dropped when dealing with other attacks, even though the features perform well in simple translation attacks. Meanwhile, although Dense SIFT works well with scale attacks, the performance was also diminished for rotation and reflection attacks. Thus, Zernike moments and FMT were competing with each other in each group of attacks. Under this circumstance, the FMT is good in scale and illumination changes, while the Zernike moments is good in rotation and reflection attacks. Furthermore, due to the reason that FMT is also good in rotation, the performance on the mix of attacks group was higher than Zernike moments features. Both, Zernike moments and FMT features are considered in the next evaluation, to find the most invariant features against all groups of attacks.

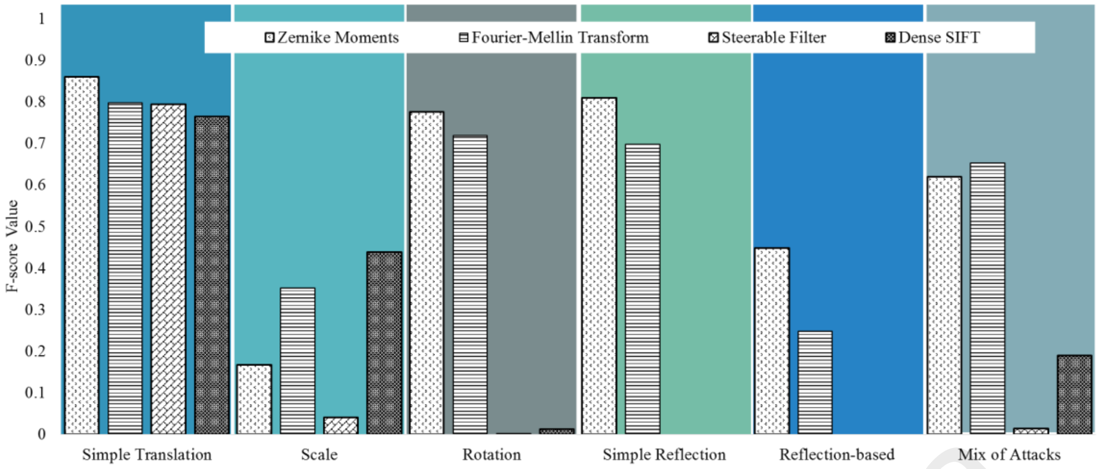


Figure 6.8: Overall performance of feature extraction techniques (with predefined threshold = 400) for each group of attacks in NB-Casia and NBr-Casia datasets

6.3.1.2 Performance Evaluation Thresholding and iteMS

Secondly, five thresholding techniques including the thresholding fitting error, iterative means (Ridler, T.W. Calvard, 1978), class variance (Otsu, 1979), and maximum entropy (Kapur et al., 1980; Yen et al., 1995) were combined with the iterative means of region size (iteMS) to evaluate the efficiency towards CMF image and to further obtain the most effective techniques. A total of 20 designs of method (four feature extractions combined with five conventional thresholding techniques) together with the iteMS procedure were tested on similar datasets (NB-Casia and NBr-Casia) that cover all possible attacks in CMF, including reflection. . The purpose of this experiment was to obtain the best combination of feature extraction and thresholding technique with the iteMS procedure.

Figure 6.9 presents the example of the detection results of each thresholding technique. From the figure, all the conventional thresholding techniques may retain several noise and false features in the CMF image. This is because the techniques only concern gray-level value between $0 - 255$, while the thresholding fitting error takes the hue degrees into considerations. Moreover, owing to the reason that the class variance technique proposed by Otsu (1979) often generates 0 (black value) as the threshold, the preserved regions show incorrect locations compared with other techniques. Thus, it verifies that the technique does not work for CMF. The predefined threshold presents in the figure also proved that the threshold may not suit certain images because of the availability of numerous feature sizes.

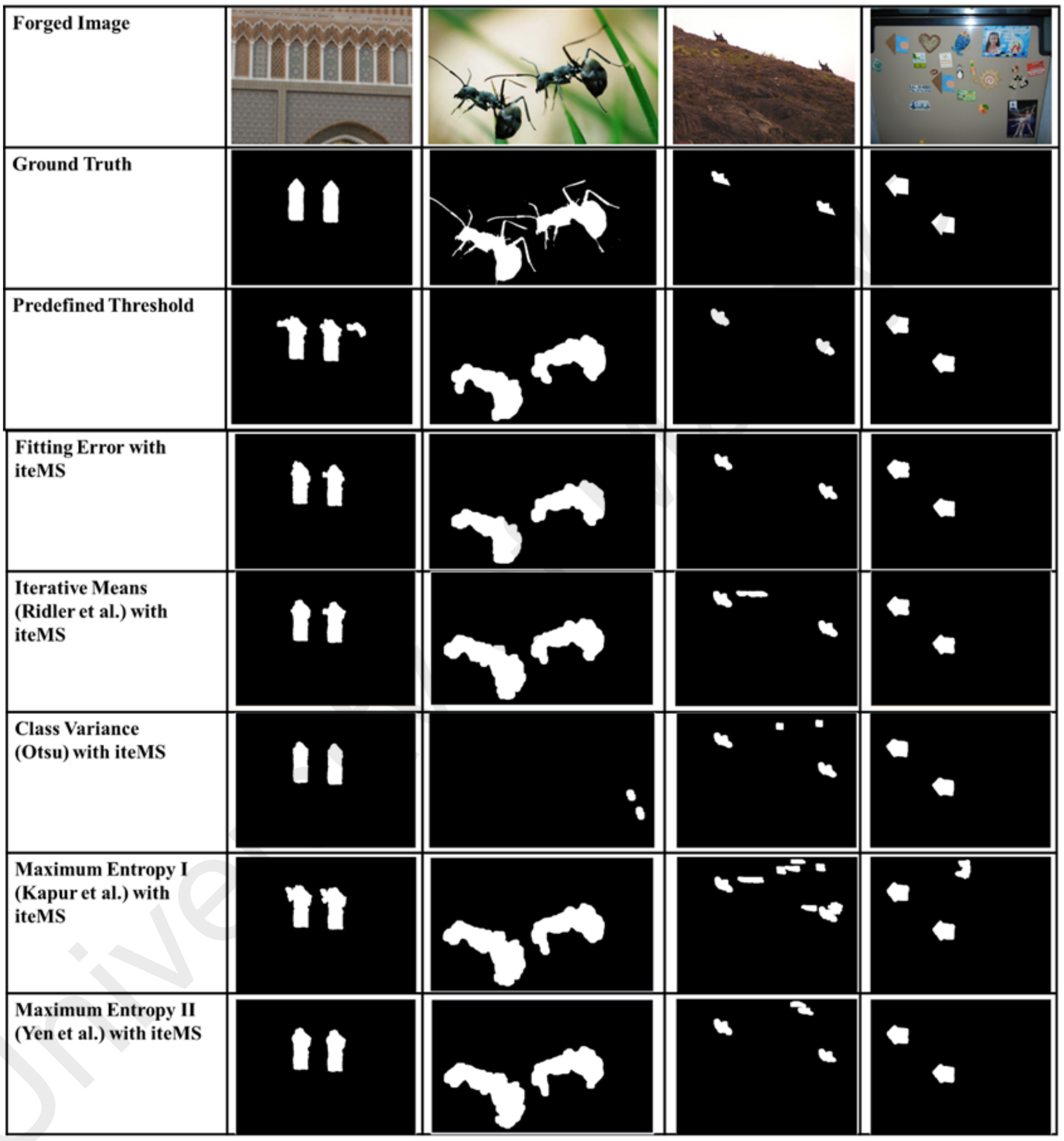

Forged Image
Ground Truth
Predefined Threshold
Fitting Error with iteMS
Iterative Means (Ridler et al.) with iteMS
Class Variance (Otsu) with iteMS
Maximum Entropy I (Kapur et al.) with iteMS
Maximum Entropy II (Yen et al.) with iteMS

Figure 6.9: Example results of each thresholding technique combined with iteMS procedure. From top: forged image, ground truth image, predefined threshold, fitting error, iterative means, class variance, Maximum Entropy

Instead of proving the detection on a single image, this research measures the pixel scores of each technique. The pixel scores of the 20 designs of feature extraction and thresholding techniques are reported in the table attached in Appendix A. Table 6.3 extracted the information of the Zernike moments and FMT features from the appendix.

Table 6.3: Pixel score of the combination of feature extraction, conventional thresholding techniques and iteMS procedure using NB-Casia and NBr-Casia datasets

Combination Feature Extraction+Conventional Thresholding+iteMS	NB-Casia	NBr-Casia	Average
ZMfittingItems	0.676	0.605	**0.641**
ZMIterativeMItems	0.669	0.589	0.629
ZMCVarianceItems	0.111	0.077	0.094
ZMMaxEntKItems	0.337	0.274	0.306
ZMMaxEntYItems	0.340	0.267	0.304
FMTfittingItems	0.734	0.411	0.573
FMTIterativeMItems	0.719	0.392	0.556
FMTCVarianceItems	0.067	0.019	0.043
FMTMaxEntKItems	0.376	0.192	0.284
FMTMaxEntYItems	0.371	0.189	0.280

According to the table, the combination of Zernike moments features with thresholding fitting error achieved the highest pixel score, while the combination of Zernike moments with iterative means thresholding technique shows the second highest score. The FMT features, on the other hand, is less robust against reflection attacks, although the performance on NB-Casia dataset was a success. Therefore, this research further investigates the Zernike moments with thresholding fitting error to assign the limit threshold, L_T, for image-level performance that is covered in the next subsection. This was the turning point of the final CMF-iteMS design, where the design with the highest scores was established for all experiments and comparisons.

(a) Limit Threshold, L_T, for the iteMS Procedure

Referring to the iteMS procedure in Section 6.2.4, the procedure has limitation on recognizing the original image. Therefore, a limit threshold value, L_T, is suggested to differentiate the original and CMF image. Based on the limit procedure in Section 6.2.4.2, each combination of thresholding techniques with the iteMS procedure will have their own limit value. Since the combination of the Zernike moments, thresholding fitting error with the iteMS procedure achieved the highest score in pixel-level performance for all conditions in CMF, the combination is further evaluated for the image-level performance. Table 6.4 lists the mean, μ, and the standard deviation, s, values of the original image in the GRIP dataset for 600 pixels and 2400 pixels resolution that is obtained from the combination. From the mean, μ, and the standard deviation, s, the values are sorted based on mean, μ, error, e, and median for the 600 and 2400 resolutions. Each value is assigned as the L_T values for the complete dataset (original and CMF images).

Table 6.4: Mean, μ and standard deviation, s, of iteMS value for original images with size (600 pixels and 2400 pixels)

Resolution	600	2400
Mean	122	88
SD	203	89

Table 6.5 records the image-level performance tested with GRIP dataset for both resolutions when applied with the L_T values, which is obtained from the Table 6.4. The value of 325 gives the highest average score, thus, the input image will be considered as original if the iteMS value is less than 325 pixels for the image resolution between 600 to 2400 pixels. If the resolution of the input image is less than the range, the input image will be rescaled to the size accordingly.

Table 6.5: F-score values for threshold 88, 122, 149.5, 177 and 325 for both original and CMF images with size 600 pixels and 2400 pixels

	min		**median**		**max**
Threshold/Resolution	**88**	**122**	**149.5**	**177**	**325**
2400	0.784	0.808	0.851	0.860	0.976
600	0.716	0.785	0.791	0.744	0.739
Average score	0.750	0.797	0.821	0.802	**0.857**

Table 6.6 lists the final results (image score, pixel score, and percentage of detection) for the proposed approach and their comparison to the existing Cozzolino et al.'s method (which employed Zernike moments as feature extraction techniques, thresholding fitting error and predefined 1200 as threshold) using the two datasets, NB-

Casia and NBr-Casia. Referring to the table, the iteMS procedure with the limit value able to improve the existing Cozzolino et al.'s method for both levels of evaluation. It is also noted that the pixel-level performances of the limit procedure decreased compared to the results in Table 6.3 due to the reason that the limit procedure requires the image to be resized to 600 (the smallest) or 2400 pixels (the largest). Despite that, the proposed iteMS procedure still performed the highest in both levels compared to the Cozzolino et al's method. The iteMS procedure able to automatically calculate the means of the regions size for each input image and defined the original images by the limit value. Therefore, the proposed design for the CMF-iteMS is Zernike moments combined with thresholding fitting error and iteMS, while 325 was selected as the limit of the iteMS procedure.

Table 6.6: Results for the iteMS limit for the Zernike moments with fitting error and previous Cozzolino et al. using NB-Casia and NBr-Casia

Dataset/ Method	NB-Casia			NBr-Casia			Average		
	Image Score	Pixel Score	Percentage of Detection	Image Score	Pixel Score	Percentage of Detection	Image Score	Pixel Score	Percentage of Detection
ZMfitting iteMS325	0.808	0.656	0.530	0.758	0.582	0.441	**0.783**	**0.619**	**0.485**
Cozzolino et al. (ZM)	0.654	0.557	0.364	0.593	0.491	0.291	0.624	0.524	0.328

6.3.1.3 The Design of the CMF-iteMS

Since the initial evaluations verified that the combination of Zernike moments, thresholding fitting error and iteMS procedure with 325 as the limit threshold value presented the most efficient combination for various characteristics in CMF, the method has been chosen in this research and named as the CMF-iteMS. CMF-iteMS offers the most robust CMF detection method against all attacks while being effective for any size of images. Figure 6.10 illustrates the final design of the CMF-iteMS where blue color represents the original contributions of the proposed method. Firstly, the size of the input image will be checked. The image will be resized with the resolutions between

600 to 2400 pixels. Next, Zernike moments features are extracted for each patch described in Section 6.2.1(a). After the patch are matched using PatchMatch algorithm, the matching patch will undergo the affine transformation estimation and thresholding fitting error. The remaining regions left by the process will then be calculated using the proposed iteMS procedure. 325 is assigned as the limit threshold value, L_T, to recognize the original images in the CMF datasets.

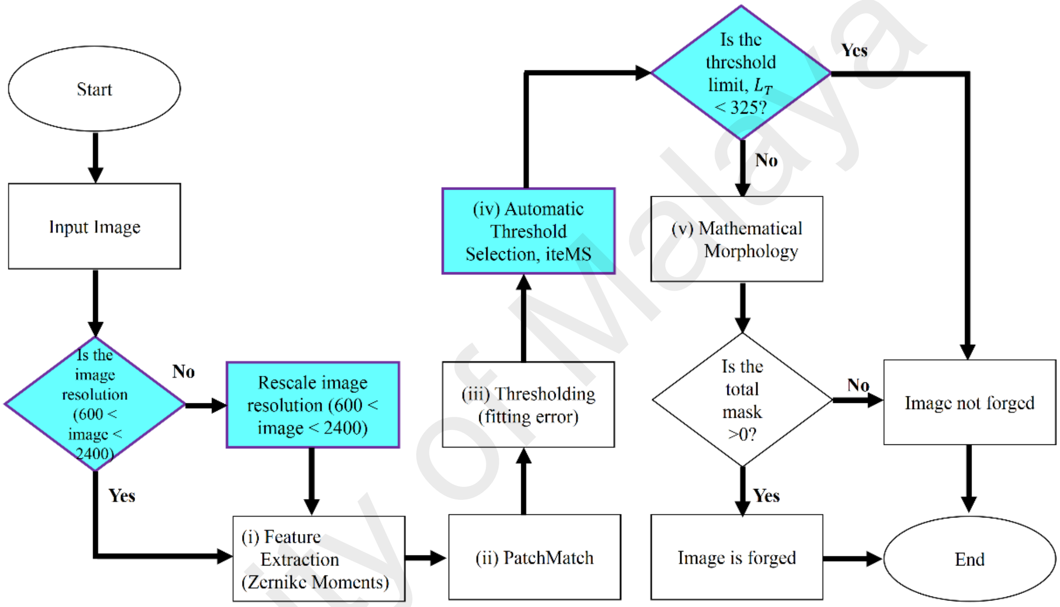

Start
Input Image
Is the image resolution (600 < image < 2400)
No
Yes
Rescale image resolution (600 < image < 2400)
(i) Feature Extraction (Zernike Moments)
(ii) PatchMatch
(iii) Thresholding (fitting error)
(iv) Automatic Threshold Selection, iteMS
Is the threshold limit, L_T < 325?
Yes
No
(v) Mathematical Morphology
Is the total mask >0?
No
Yes
Image not forged
Image is forged
End

Figure 6.10: The final design of the CMF-iteMS

(a) *Large Image Dataset Verification*

According to the previous subsection (Section 6.3.1.3), the image is considered as an original image if only the iteMS value is below 325 for image size 600–2400 pixels. To verify the limit procedure, this research examined the methods against another dataset (namely FAU) that consists of higher resolution images. FAU dataset (Christlein et al., 2012) is comprised of 48 original images and 48 simple translation-CMF images. The average sizes of the images in the dataset is 3000 × 2300 which is large enough compared with other datasets.

To evaluate the procedure in different sizes, the images in the dataset were resized into three factors which are 0.5, 0.25 and 0.17. Table 6.7 lists the results of the

Cozzolino et al.'s method (which employed Zernike moments as feature extraction techniques and predefined 1200 as threshold) and the CMF-iteMS against the FAU dataset with four image sizes (original size, resized to 0.5, 0.25 and 0.17). According to the table, the threshold value assigned by Cozzolino et al. was perfectly determined for the original size in the dataset. However, the performance will be decreased if the images were resized to the smaller size, hence, the threshold value should also be reassigned. Subsequently, the CMF-iteMS achieved adequate results for the original size while performed the highest scores than the Cozzolino et al. for all resized images in all scores (image, pixel and percentages of detection), except for image score with resized value of 0.5. Nevertheless, the pixel score and percentage of the detection is also led by the CMF-iteMS.

Table 6.7: Performance of the Cozzolino et al. and CMF-iteMS for FAU dataset in four sizes (original, resize 0.5, resize 0.25 and resize 0.17)

Method/Dataset		**Cozzolino et al. (ZM)**	**CMF-iteMS**
Original Size	Image Score	**0.940**	0.902
	Pixel Score	**0.940**	0.871
	Percentage of Detection	**0.884**	0.786
Resize = 0.5	Image Score	**0.863**	0.849
	Pixel Score	0.821	**0.853**
	Percentage of Detection	0.708	**0.724**
Resize = 0.25	Image Score	0.660	**0.745**
	Pixel Score	0.636	**0.711**
	Percentage of Detection	0.420	**0.530**
Resize = 0.17	Image Score	0.551	**0.686**
	Pixel Score	0.507	**0.709**
	Percentage of Detection	0.279	**0.486**

6.3.2 Analysis of Robustness against CMF Attacks

To validate the results of the CMF-iteMS with the existing CMF detection methods, this research analyzed the method through a comprehensive set of experiments and compared with three state-of-the-art methods: Amerini et al. (2011), Cozzolino et al.

(2015) for Zernike moments and FMT, and Silva et al. (2015). Table 6.8 summarizes the image score, pixel score and percentage of detection results for all CMF detection methods which are carried out using NB-Casia and NBr-Casia datasets.

Table 6.8: Image score, pixel score, and percentages of detection for each CMF detection method using NB-Casia and NBr-Casia Dataset

Dataset/ Method	**NB-Casia**			**NBr-Casia**			**average**		
	Image Score	Pixel Score	Percentage of Detection	Image Score	Pixel Score	Percentage of Detection	Image Score	Pixel Score	Percentage of Detection
Amerini et al. (2011)	**0.814**	0.549	0.447	0.004	0.003	0.000	0.409	0.276	0.113
Cozzolino et al. (2015)---ZM	0.654	0.557	0.364	0.593	0.491	0.291	0.624	0.524	0.327
Cozzolino et al. (2015)---FMT	0.745	0.634	0.472	0.496	0.325	0.161	0.621	0.480	0.298
Silva et al. (2015)	0.667	0.548	0.365	0.226	0.010	0.002	0.446	0.279	0.125
CMF-iteMS (ZM)	0.808	**0.656**	**0.530**	**0.758**	**0.582**	**0.441**	**0.783**	**0.619**	**0.485**

Referring to the table, the CMF-iteMS obtained the most valuable results in all datasets with an average of 49% of detection for both datasets. This value improved the prior Cozzolino et al.'s method which was only able to reach an average of 33% for Zernike moments and 30% for FMT features. These results proved that the Cozzolino et al.'s method has limitations on the features and threshold selection techniques. Meanwhile, the Amerini et al.'s and Silva et al.'s methods show the average of 11% and 13%, respectively. Although the image score of the Amerini et al.'s method shows the highest result for NB-Casia, the performance was dropped when a per-pixel basis was measured owing to the reason that their method is only working on image-level basis. This also indicates that the scores of the CMF-iteMS satisfy both image and pixel-level evaluation, resulting in the highest percentage of detection, even though the image score was lower than the Amerini et al.'s method. On the other hand, the Silva et al.'s method shows the moderate results in NB-Casia, but continuously decreased for NBr-Casia, similar to the Amerini et al.'s method. Each method was further analyzed according to each group of attacks, including geometrical transformations and post-processing attacks. The details are discussed in the following subsections.

6.3.2.1 Geometrical Transformation Attacks

The results for the NB-Casia dataset were further divided according to the five groups of geometrical transformation attacks to see the effectiveness on each attack. Figure 6.11 compares all scores of the CMF-iteMS with the state-of-the-art methods for each group of attacks in the dataset. Based on the figure, the CMF-iteMS was able to exceed the performance of the Cozzolino et al.'s methods in all groups of attacks by exceeding the minimum value of 62% of detection, except for the scale attacks. This is because the Zernike moments have limitations on scale and illumination changes, therefore, the CMF-iteMS results on the scale attack being improved if the features are replaced by the FMT. This also proved that the iteMS procedure provides a significant result compared to the predefined thresholds suggested by Cozzolino et al. Furthermore, although the Amerini et al.'s method achieved the highest scores for the scale attacks with 67% of detection, the method could not detect any CMF image with reflection attacks. It is contrasted to the CMF-iteMS that obtained 17% of detection for the scale attacks, while performed the highest scores (77% of detection) for the reflection attacks. Since the CMF-iteMS has the perfect scores for reflection attacks, the performance on the reflection-based CMF attacks were analyzed in the next subsections.

6.3.2.2 Reflection-based Attacks

Basically, the NBr-Casia dataset only consists of reflection-based CMF image. The image was grouped into four groups, which are simple reflection, reflection with scale, reflection with rotation, and mix of reflection. It is noted that the images under the simple reflection is similar to the group of simple reflection in the NB-Casia dataset. Hence, Figure 6.12 shows the image score, pixel score and percentage of detection for all CMF detection methods against each group of reflection-based attacks except simple reflection. The figure shows that the performance of the CMF-iteMS outperformed other methods for all groups of reflection, even when the reflection was combined with scale attacks. In particular, the CMF-iteMS achieved 11% of detection for reflection with scale, 80% of detection for reflection with rotation, and 47% of detection for mix of reflection. Furthermore, even though the FMT features are good for scale attacks, the performance was dropped when combined with reflection.

For further evaluation, this research investigates the performance of image score per parameter basis, particularly for reflection with scale, reflection with rotation, and mix reflection attacks. The image score was employed in this analysis because the performances were adequate enough to represent the performance of the CMF-iteMS. Figure 6.13(a) depicts the image score values for scale factors from 0.6 to 1.6. The CMF-iteMS could maintain an 80% (and above) of image score for 0.8 and 1.2. However, the performance continuously dropped by a huge scale either up or down. This limitation could be improved by using other feature extractions that are robust to reflection and scale attacks.

With respect to the weak performance for scale, the CMF-iteMS presented achievement by maintaining at least 88% of image score value for reflection with rotation as shown in Figure 6.13(b). This confirmed that the method worked well with all degrees of rotation and the rotation combination. Meanwhile, the performance maintained 94% of image score value for mix reflection, as long as the scale factor is in the range of 0.8 and 1.4, which displayed in Figure 6.13(c). Despite the limitations, the performances were higher than all CMF detection methods. In view of the fact that Zernike moments and predefined threshold have limitations on the scale and variation of illumination, the CMF-iteMS provided almost perfect detection in all cases of reflection-based attacks, except for high or low scale factor of attacks.

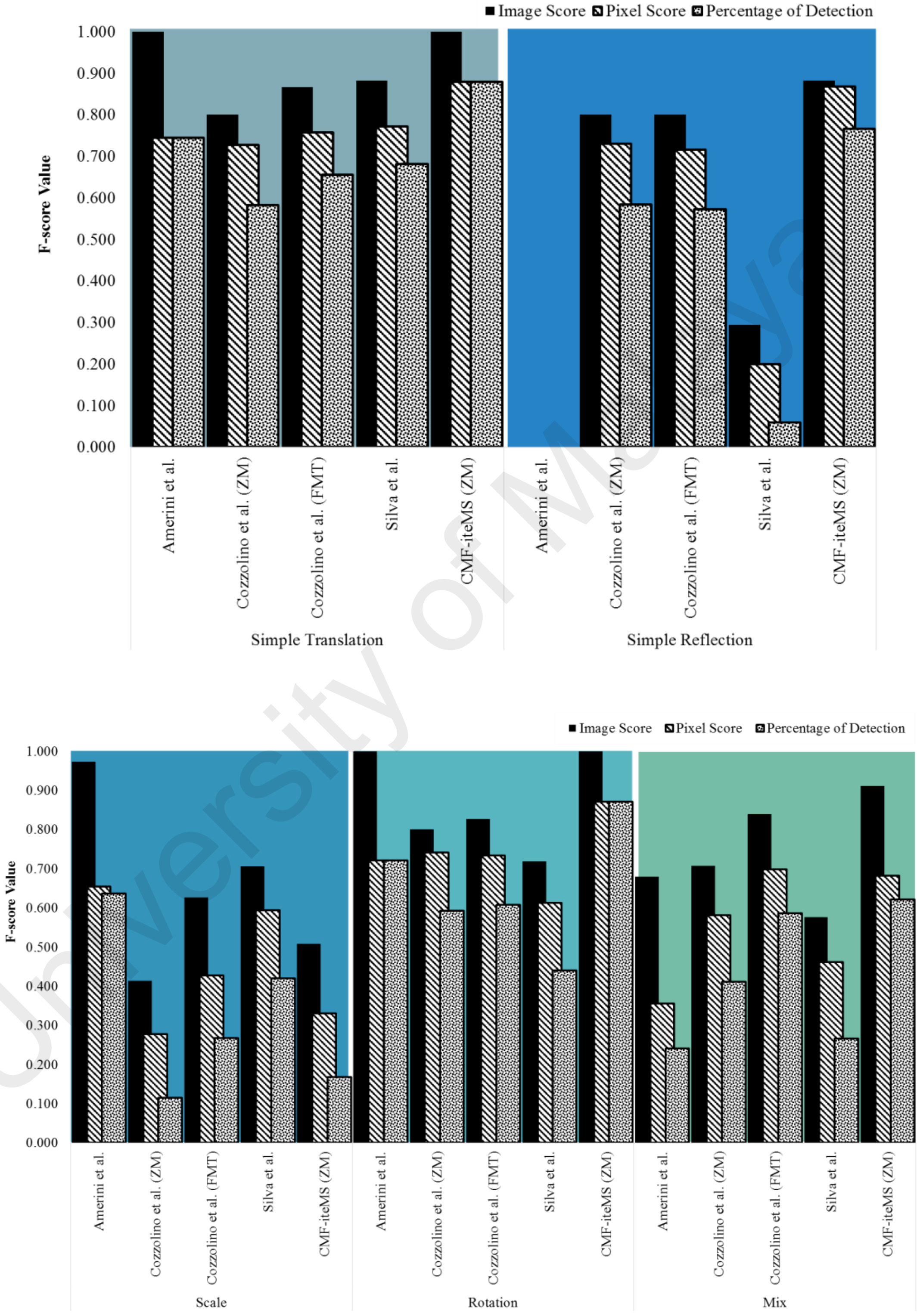


Figure 6.11: Comparative results between CMF-iteMS and the Existing CMF Detection methods for each group of geometrical transformation attacks

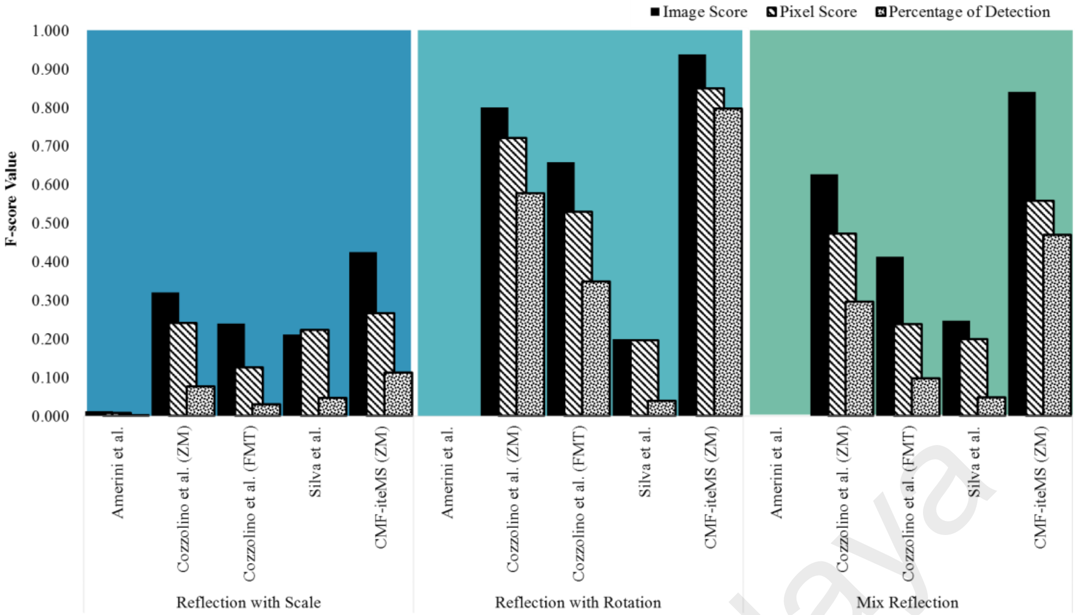
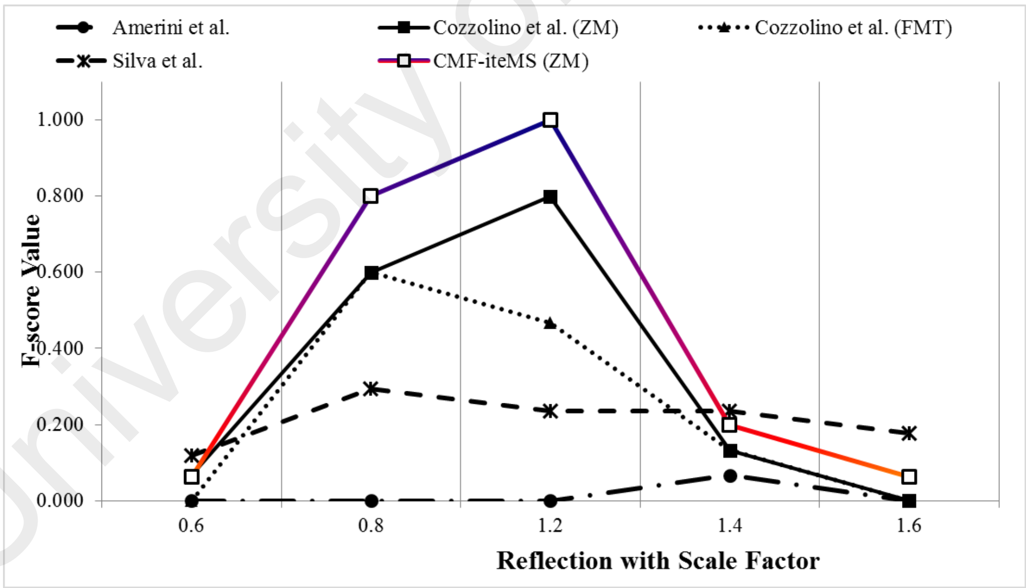
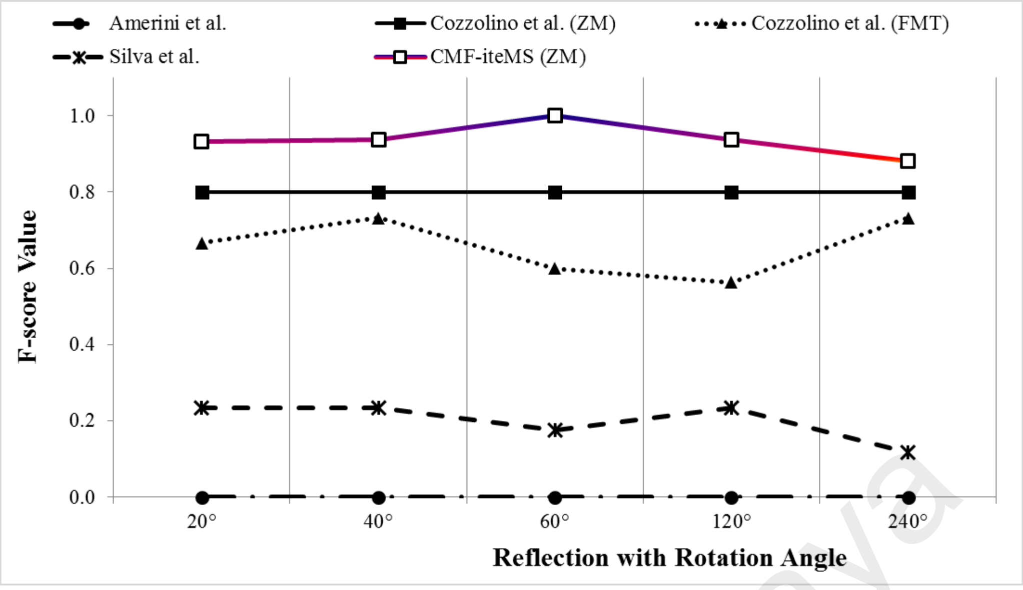


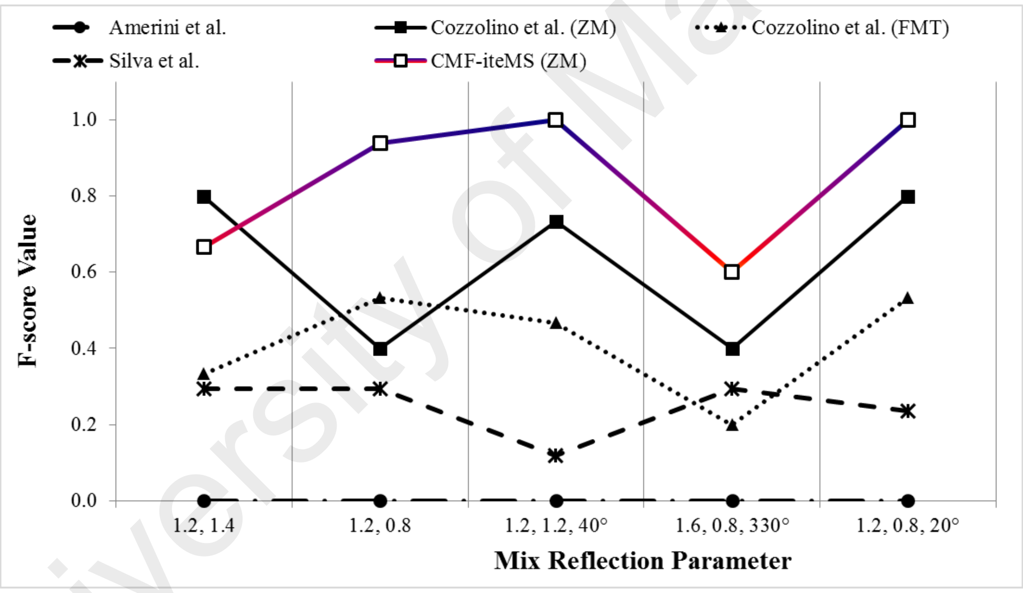
Figure 6.12: Comparative results between CMF-iteMS and the existing CMF detection methods for each group of reflection-based CMF attacks



(a)



(b)



(c)

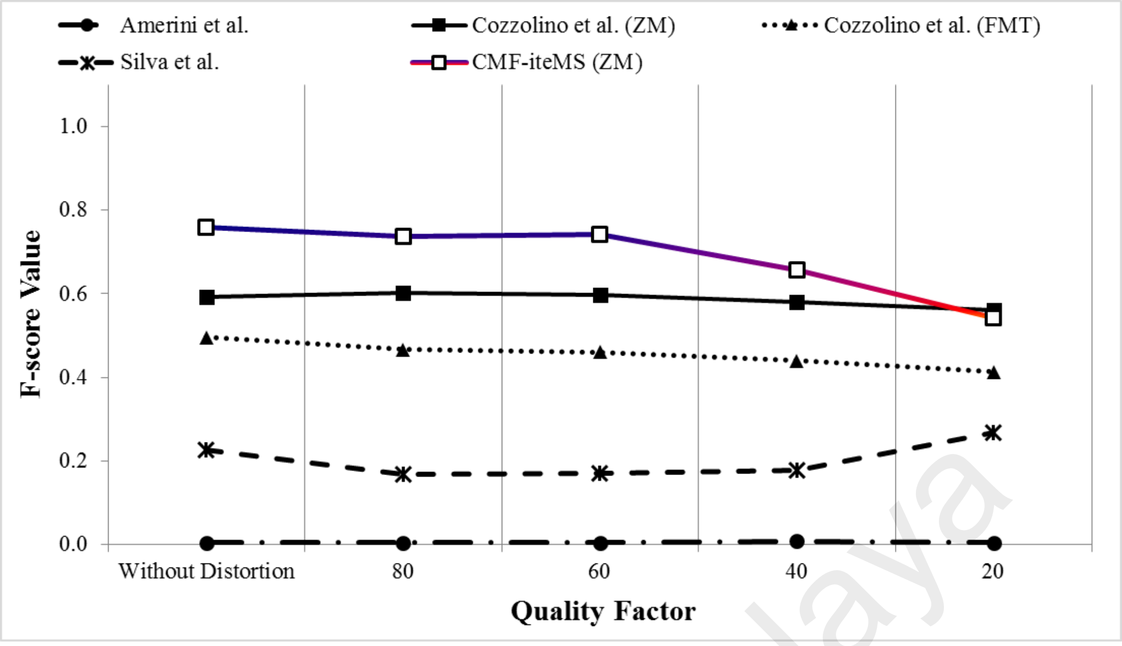
Figure 6.13: Image score values for the Amerini et al., Silva et al., Cozzolino et al., and CMF-iteMS for (a) reflection with scale, (b) reflection with rotation, and (c) combination of reflection

6.3.2.3 Post-Processing Attacks

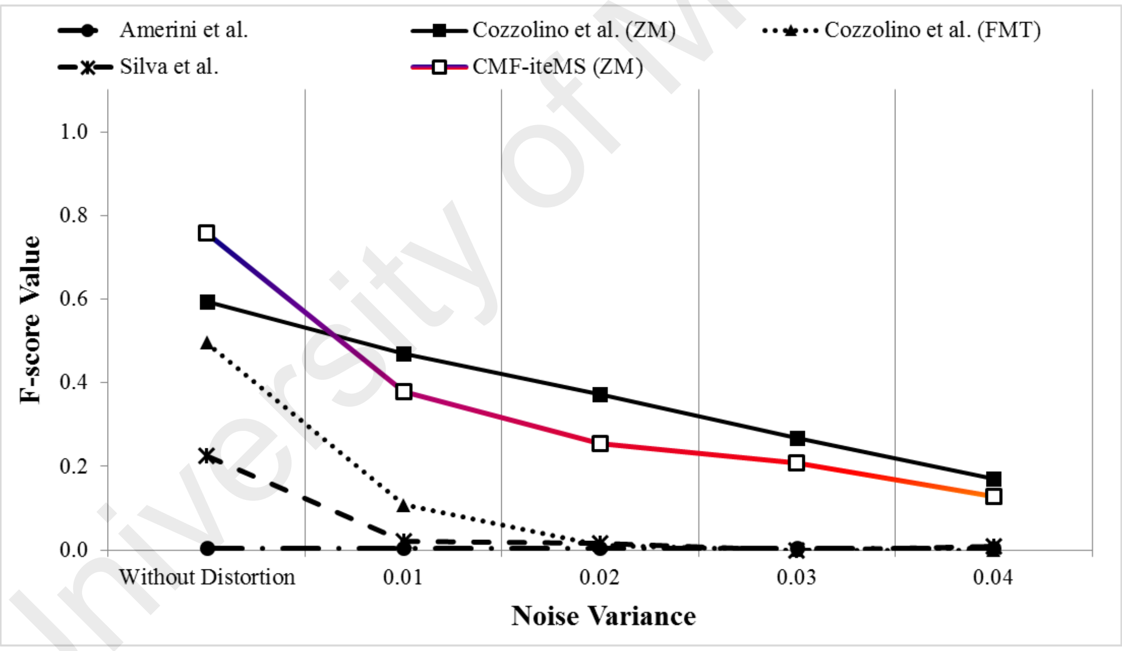
Instead of comparing the methods for geometrical transformation attacks, this research also includes the post-processing attacks in the evaluation. A new set of experiments was conducted to assess the performance of the CMF-iteMS with the three state-of-the-art methods against JPEG compression and Gaussian noise addition. All images in NBr-Casia dataset were distorted by JPEG compression and Gaussian noise with four different parameters. For the first experiment, various JPEG quality factors ranging from 20 to 80 were applied to the images. Meanwhile, for the second experiment, the images were added with four variances of Gaussian noise ranging from 0.01 to 0.04.

The results were not only compared with the state-of-the-art methods, but also with the results obtained without distortion in Section 6.3.2.2. Figure 6.14 shows the image score values for both experiments of post-processing attacks. As illustrated in Figure 6.14(a), the image score values for all methods were diminished when compression was applied. Despite that, the CMF-iteMS was still able to maintain at least 66% of image score for compression above 40 quality factor, resulting in the highest performance than other methods.

For the Gaussian noise attack, Figure 6.14(b) demonstrates the image score values for all methods. The methods tend to decrease when the variance of Gaussian noise was increased. However, the performance of the CMF-iteMS decreased and is lower than the Cozzolino et al. likely because the iteMS procedure is not able to preserve reflection regions when various noises were added. Despite that, the CMF-iteMS still outperformed the Amerini et al.'s and Silva et al.'s methods.



(a)



(b)

Figure 6.14: Image score values for Amerini et al., Silva et al., Cozzolino et al. and CMF-iteMS against (a) JPEG compression (b) Gaussian noise addition in NBr-Casia dataset

6.4 Discussion

Based on the performance analysis done in Chapter 4, the block-based CMF detection method (which is the Cozzolino et al.) shows promising results on various CMF attacks, including reflection. Nonetheless, the method requires several predefined thresholds to be set in the final verification process, which led to the reduction performance, if the value assigned is not suitable for certain image. Therefore, this research introduced an iterative means of region size to replace the static thresholds selection. This research also studies and investigates four feature extraction and conventional thresholding techniques for the formulation design of the CMF-iteMS.

As the Zernike moments features provide the most efficient feature extraction technique that can robust to various attacks, especially reflection, the CMF-iteMS considered the features in the designs. Furthermore, the thresholding fitting error suggested by the Cozzolino et al. obtained the highest performance compared to the conventional thresholding techniques due to the reason that the fitting error considers hue degree in the RGB value into consideration. In spite of the highest performance of the CMF-iteMS, the method only works for CMF image, not the original image. This is because the iteMS procedure often calculates the small matching regions left by the original image. Hence, this research provides a statistical analysis (means and standard deviation) to limit the iteMS value.

The purpose of this research is to achieve the best performance against CMF with any combination of possible attacks without a predefined threshold value for various inputs of CMF images. This research believes that the automatic improvement methods will be particularly valuable in big data applications of image forensics, where the huge heterogeneous data is a critical component in the recent years.

In comparison with the existing CMF detection methods, the CMF-iteMS presents the most promising results in almost all cases of attacks. The results proved that the method was able to outperform existing methods by exceeding the minimum score of 62% of detection, except for scale attacks. Despite the difficulty on the attack, the results are still applicable for scale within range 0.8 to 1.4 factor, resulting in 17% of detection from the whole images in the group. Furthermore, the CMF-iteMS shows the highest performance in all reflection-based CMF cases, which exceeds the minimum score of 11% of detection for reflection with scale, 80% of detection for reflection with rotation, and 47% of detection for mix of reflection. As image manipulation can be concealed by post-processing attacks, the CMF-iteMS was outperformed the other methods by exceeding 66% of image score with quality factor above 40 of compression.

6.5 Chapter Summary

This chapter presents CMF detection method with a new automatic threshold selection procedure called iterative means of region size, iteMS. The iteMS procedure is proposed to increase the detection of the existing CMF detection performance for both image and pixel-level evaluations. Experiments are conducted to investigate the performance of iteMS procedure when combined with four feature extraction (e.g. Zernike moments, FMT, Steerable Filter, and Dense SIFT) and five conventional thresholding (e.g. thresholding fitting error, iterative means, class variance and maximum entropy I and II) techniques. From the investigation, the combination of Zernike moments feature extraction, thresholding fitting error and iteMS procedure yields the highest results, therefore, are considered in the proposed CMF-iteMS. The experiments also confirmed that the existing CMF detection methods, which require at least one predefined threshold for final verification, have difficulties in detecting CMF image with various characteristics; hence, with the proposed automated procedure, have altogether enhanced the detection performance even against CMF with various attacks, including reflection.

CHAPTER 7: PERFORMANCE ANALYSIS II

This chapter discusses and compiles the performance of the existing CMF detection methods and the proposed methods. The time taken for each experiment is also recorded and analyzed in this chapter. Furthermore, the existing CMF detection methods are also applied with the iteMS procedure, while the results are also explored as an added value. There are four parts in this chapter, which the introduction of the analysis is briefly described in the first section (Section 7.1). Then, the performance of each method is presented in the second section (Section 7.2). In the section, the results are analyzed based on each category of attack. In the third section (Section 7.3), the performance of the existing CMF detection methods when combined with the iteMS procedure are examined. Lastly, the forth section (Section 7.4) summarized the chapter.

7.1 Introduction

Based on the performance analysis I, the Amerini et al.'s method (representing keypoint-based approach) is good in CMF detection for scale and rotation, however, the method is not robust against reflection attacks. On the other hand, the Cozzolino et al.'s method (representing block-based approach) is less effective to small resolution images although it is good in reflection. Furthermore, the Zernike moments features that is used in the method is less effective when dealing with scale and illumination changes, despite the fact that the features have distinctive properties and able to describe shape efficiently. These limitations can be improved by the FMT features that is good in rotation, scale and various illuminations. In contrast, the combination approach as in the Silva et al.'s method, does not present much improvement compared to both approaches. The method is sensitive to all types of attacks in CMF, except for simple translation.

Based on the analysis, this research proposed SIFT-Symmetry that improved the keypoint-based approach, and CMF-iteMS that enhanced the performance of the block-based approach, that were already discussed in Chapters 5 and 6, respectively. Therefore, this chapter compiled the performances of all methods, existing and proposed, against all four different datasets, to determine the most efficient CMF detection methods. Furthermore, the time performance for each method is also discussed. As an added value, this research attempts to combine the proposed iterative means of region size with the existing CMF detection methods. The results are discussed in the following sections.

7.2 Performance Evaluation

Table 7.1 lists the results of the existing CMF detection methods and the two proposed methods using all four datasets. The green color highlighted in the table presents the previous achievement, while the blue color emphasized the current accomplishments. According to the table, the CMF-iteMS achieved the highest performance for almost all datasets, except CPHALL. The lower performance in the CPHALL dataset mainly because the image are required to be resized to 600–2400 pixels to cope with the limit threshold. Despite that, the performance was still able to maintain 81% value of the pixel score.

The SIFT-Symmetry, on the other hand, reached the highest image score for NB-Casia dataset compared to other methods. However, since the keypoint features are unable to identify points' region, the pixel score of the SIFT-Symmetry was dropped, thus, resulting in low percentage of detection. Moreover, in spite of the good performance on reflection attacks, the symmetry matching technique has difficulty to differentiate the forged symmetry with original symmetry images. This is the reason for the low performance in other datasets. The following section will further discuss the processing time listed in the table.

Table 7.1: Comparative scores for image, pixel and percentages of detection with Average CPU-Time (in seconds) per image for the existing CMF Detection Methods and the proposed methods against Four Datasets

All Datasets/Methods		Amerini et al. (2011)	Cozzolino et al. (2015) -- ZM	Cozzolino et al. (2015) -- FMT	Silva et al. (2015)	SIFT-Symmetry	CMF-iteMS
Combine Translation	Image Score	0.724	**0.896**	0.880	0.737	0.689	**0.960**
	Pixel Score	0.574	**0.901**	0.884	0.740	0.577	**0.932**
	Percentage of Detection	0.416	**0.807**	0.778	0.545	0.398	**0.895**
	Time per image	11.418	16.441	30.441	12.993	57.714	16.245
NB-Casia	Image Score	**0.814**	0.654	0.745	0.667	**0.835**	0.808
	Pixel Score	0.549	0.557	**0.634**	0.548	0.581	**0.656**
	Percentage of Detection	0.447	0.364	**0.472**	0.365	0.485	**0.530**
	Time per image	2.729	4.455	6.961	2.283	7.173	11.494
NBr-Casia	Image Score	0.004	**0.593**	0.496	0.226	0.698	**0.758**
	Pixel Score	0.003	**0.491**	0.325	0.010	0.214	**0.582**
	Percentage of Detection	0.000	**0.291**	0.161	0.002	0.149	**0.441**
	Time per image	1.815	4.417	9.208	1.363	8.417	14.325
CPHALL	Pixel Score	0.551	0.825	**0.859**	0.647	0.551	0.814
	Time per image	17.750	15.750	34.194	21.259	60.843	25.843

7.2.1 Processing Time

One of the performance measurements in experimental-type research design is processing time. Thus, this research continuously analyzed the time taken for each CMF detection method when evaluated on all four datasets. According to the table, the processing time was strongly dependent on the complexity and size of the image.

Taking the two characteristics into the account, the CombineTranslation and CPHALL require extra time than other two datasets. This is because most of the images in both datasets are comprised of the high resolution images with maximum 1024 pixels and 1296 pixels, respectively. In contrast, the NB-Casia and NBr-Casia contain more small images with the minimum 160 pixels to the maximum of 900 pixels.

Instead of the two characteristics, the ability of the methods against dataset could also affect the processing time. For instance, if the method could not extract any features in the first phase, the process after the feature extraction phase was discarded. This is the reason why the Silva et al.'s method appears to be the smallest processing time in the NBr-Casia datasets among all CMF detection methods. Followed by the Amerini et al.'s method, both methods show the lowest performance results when tested with the reflection-based CMF datasets despite their achievement in the processing time. In contrast, due to the reason that the SIFT-Symmetry is the combination of the Amerini et al.'s method with the symmetry matching technique, the method requires the highest processing time among other CMF detection methods. In the method, the symmetry matching will initiate if only the Amerini et al. could detect less than five matching points. Therefore, the method requires the Amerini et al. to be run first, before the SIFT-Symmetry could handle the undetected CMF image.

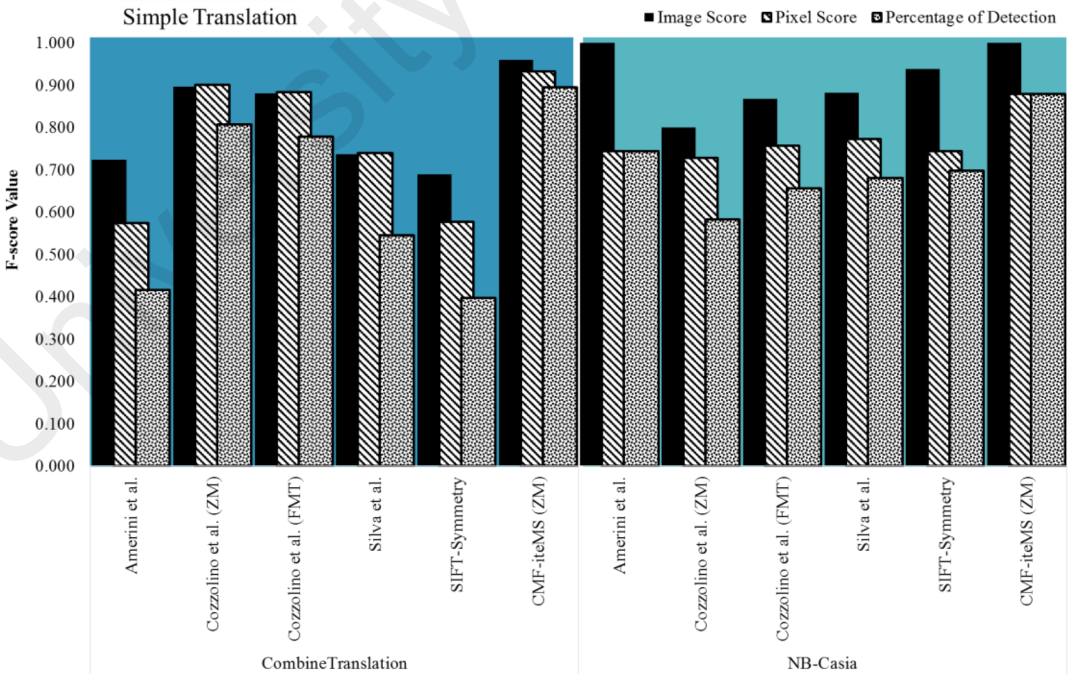
For the Cozzolino et al.'s method, since the FMT features require double patch size and feature length compared to Zernike moments, the FMT features shows an extra time than the Zernike moments features. (Noted that patch size and feature length for FMT are 24 and 25, respectively, while the patch size and feature length for Zernike moments are 16 and 12, accordingly). The time performance of the CMF-iteMS, on the other hand, may be increased if the input image needs to be resized. This is shown in the NB-Casia and NBr-Casia datasets, in which the method requires extra time compared to the

Cozzolino et al.'s method. Nevertheless, if the input image is within 600 to 2400 pixels, the processing time able to improve the Cozzolino et al.'s method.

After all, the processing time might differ according to the CPU capability. For example, the highest specification of CPU will generate the smallest processing time than the lowest specifications. Besides that, the processing time will also increase if the CPU performed several activities at one time. Therefore, parallelizable methods for increasing the computational efficiency appear to be promising.

7.2.2 Performance against Geometrical Transformation attacks

The performances of both proposed methods were further analyzed based on each group of geometrical transformation attacks. Figure 7.1 presents the performance of all CMF detection methods based on image score, pixel score and percentages of detection in all groups of CMF attacks.



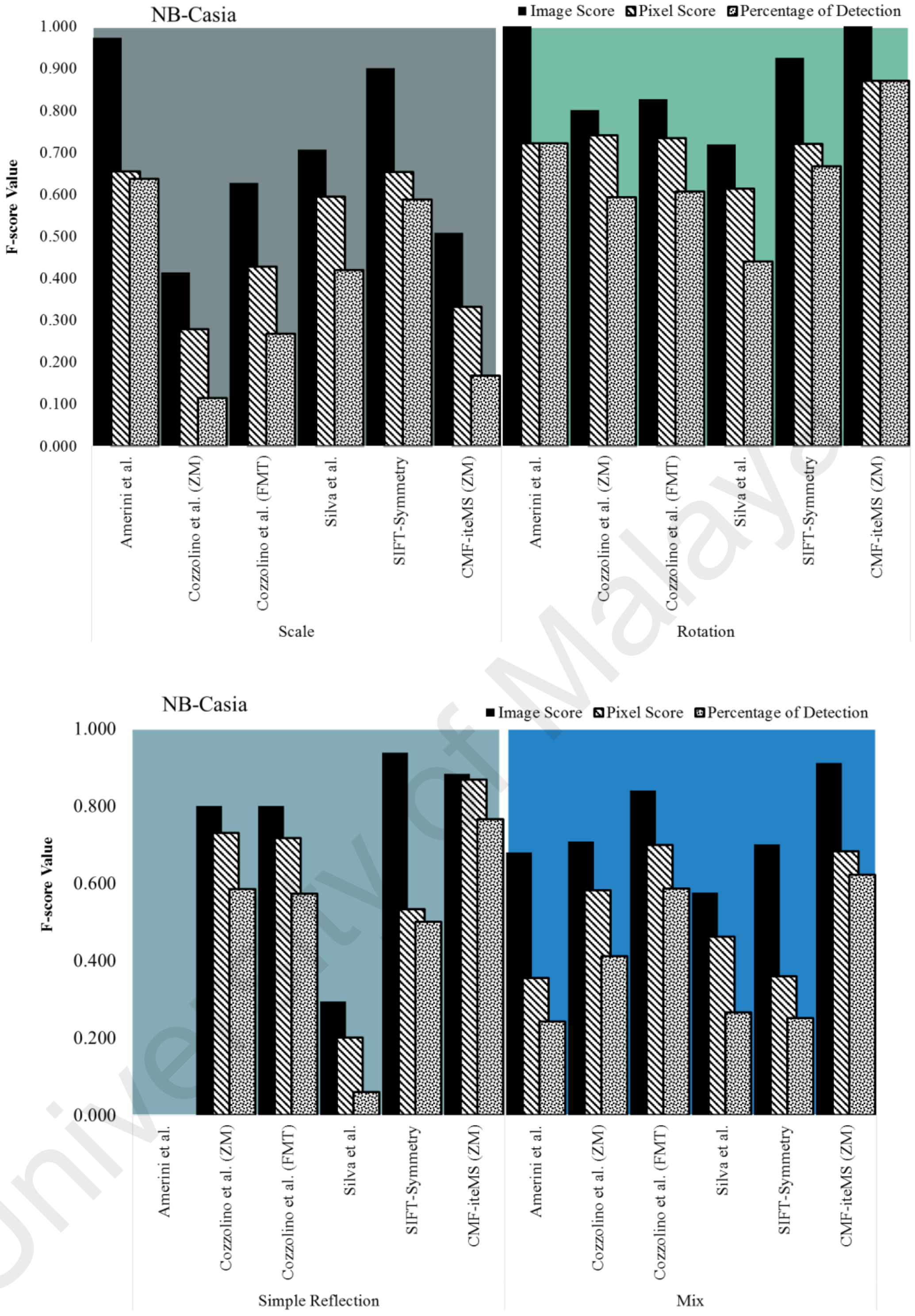


Figure 7.1: Comparative results (image score, pixel score, and percentages of both scores) for all CMF detection methods against scale, rotation, simple reflection and mix attacks in NB-Casia dataset

For simple translation attacks, the figure shows that the CMF-iteMS achieved the highest scores for all levels. The CMF-iteMS exceeded the minimum value of 96% image score and 88% for both pixel score and percentage of detection in both

CombineTranslation and NB-Casia datasets. Moreover, the CMF-iteMS was also able to maintain the highest percentage of detection for rotation, simple reflection, and mix of attacks with the minimum value of 87%, 76%, and 62% score, respectively. Alternatively, the SIFT-Symmetry obtained the highest image score with a value of 94% for simple reflection attacks, despite the weak performance on pixel-levels. In spite of the achievement of both proposed methods, the performance on the scale attacks are lower than Amerini et al.'s method. This is because the SIFT-Symmetry may detect natural symmetry image as CMF, while the CMF-iteMS employed Zernike moments features who is variant to scale attacks.

As this research focused on reflection-based CMF attacks, the performances were further analyzed based on reflection-based groups of attacks in NBr-Casia. Figure 7.2 presents the results of all CMF detection methods for group reflection with scale, reflection with rotation, and mix of reflection. Based on the figure, the CMF-iteMS was able to achieve the highest percentage of detection for all reflection combinations. To be specific, the scores are 11% for reflection with scale, 80% for reflection with rotation, and 47% for mix of reflection. Furthermore, the SIFT-Symmetry also performed well with the highest image score equal to 75% for reflection with scale attacks. In addition, since reflection is a process of points' transformation in a mirror plane, the detection methods should be able to identify all reflection in every direction, either it is horizontal, vertical, or tilt. Figure 7.3 shows the examples of detection by SIFT-Symmetry and CMF-iteMS for the three directions (horizontal, vertical, and tilt).

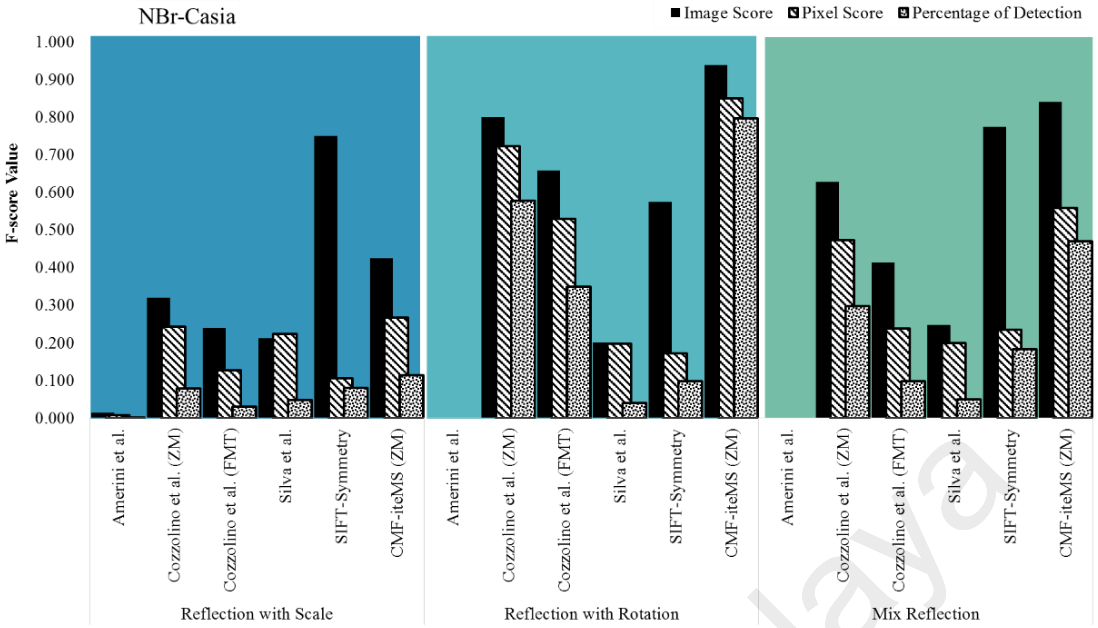


Figure 7.2: Comparative results (image score, pixel score, and percentages of both scores) for all CMF detection methods against reflection with scale, reflection with rotation, and mix of reflection attacks in NBr-Casia dataset

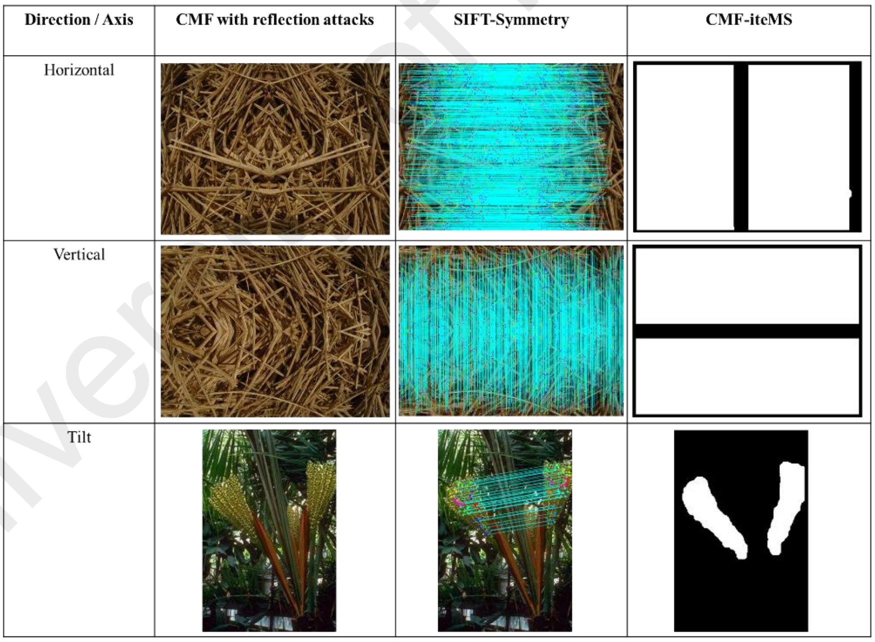


Figure 7.3: Examples of detection by SIFT-Symmetry and CMF-iteMS for CMF with reflection attacks in horizontal, vertical and tilt axis

The pixel score of all CMF detection methods for the CPHALL datasets are also presented in the Figure 7.4. The figure shows that the CMF-iteMS improved the performances of the Cozzolino et al. (Zernike moments) against all types of attacks, except the simple translation. The performance is decreased for the simple translation due to the reason that the images may be resized to the smaller resolutions. Nonetheless, the results were still able to achieve 93% of the pixel score. In spite of the achievement of the CMF-iteMS, the Cozzolino et al. (FMT) outperformed the other methods for the scale and mix of attacks. The results may be improved, if the CMF-iteMS applied the FMT features, instead of Zernike moments, specifically for the attacks.

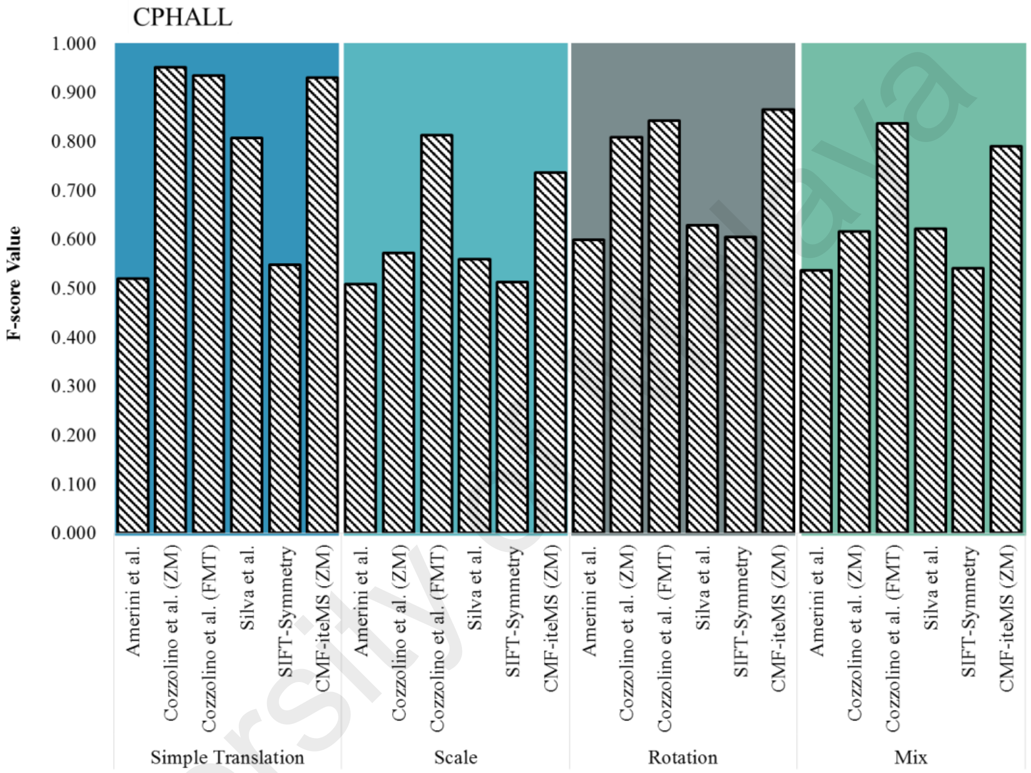
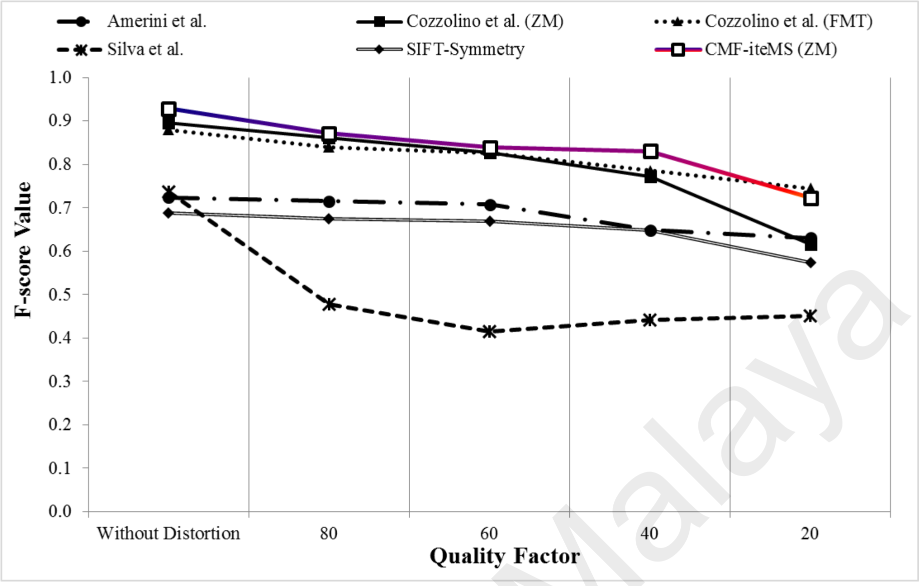


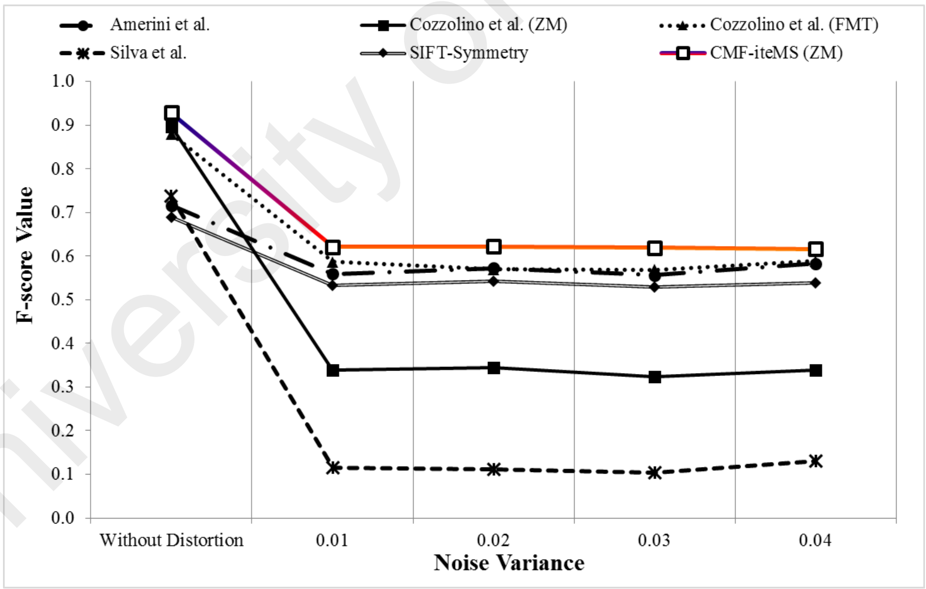
Figure 7.4: Pixel score for the existing CMF detection methods against simple translation, scale, rotation, and mix attacks in CPHALL dataset

7.2.3 Performance against Post-Processing attacks

Instead of analyzing the CMF detection methods against geometrical transformation, the performance against post-processing attacks are also measured. Figure 7.5 presents the image score for all methods for each parameter of JPEG compression and Gaussian noise addition using CombineTranslation dataset. The figure shows that although all performances were dropped compared to without distortion, the CMF-iteMS achieved the highest image score in all parameters, except for 20 quality factor of JPEG compression. This is because the Zernike moments is known to be more sensitive than FMT for the low compression.



(a)



(b)

Figure 7.5: Image score values of all CMF detection methods against (a) JPEG compression and (b) Gaussian noise addition in CombineTranslation dataset

7.3 Combination with iteMS procedure

In view of the fact that iteMS procedure is specifically designed to automatically remove spurious matching and noise based on the input image, this research believed that the procedure can be combined with the existing CMF detection methods. To prove the assumption, the iteMS was tested with the four CMF detection methods, including Amerini et al., Cozzolino et al. (Zernike moments and FMT), Silva et al., and SIFT-Symmetry. Table 7.2 demonstrates two examples of detection results before and after the iteMS procedure is combined with the methods. According to the table, the noise that is preserved by the Amerini et al., SIFT-Symmetry, and Silva et al. was discarded by the iteMS. The Cozzolino et al.'s method, on the other hand, was able to increase the possibility of forged detection since their method previously defined a wrong threshold value.

Table 7.2: Examples of detection results for the CMF detection methods before and after iteMS procedure is combined

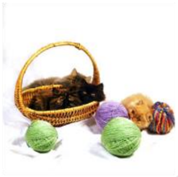
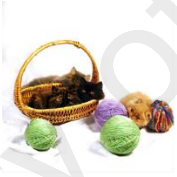
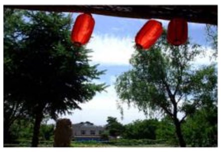
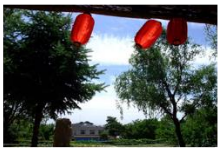
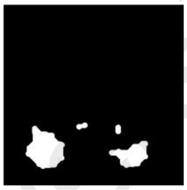
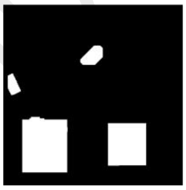
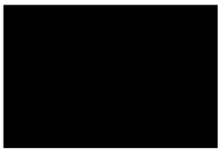
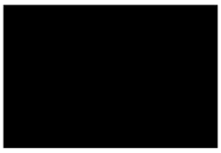
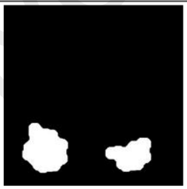
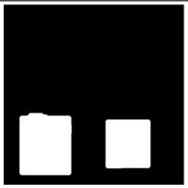
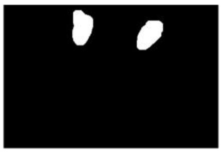
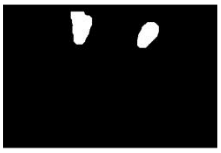
Method	Amerini et al. & SIFT-Symmetry	Silva et al.	Cozzolino et al. (Zernike moments)	Cozzolino et al. (FMT)
CMF image				
Before iteMS				
After iteMS				

Figure 7.6 shows the performance for image score, pixel score, and percentage of detection against CombineTranslation dataset for the CMF detection methods, before and after the iteMS procedure was combined. From the figure, all scores of the Cozzolino et al.'s method after the combination with iteMS procedure appears to be promising. This is because of the iteMS procedure could assign an ideal threshold value for each input image. Otherwise, the performance of the Amerini et al.'s, Silva et al.'s

and SIFT-Symmetry were decreased, especially for pixel score, due to the reason that the methods often include the spurious matching in their detection.

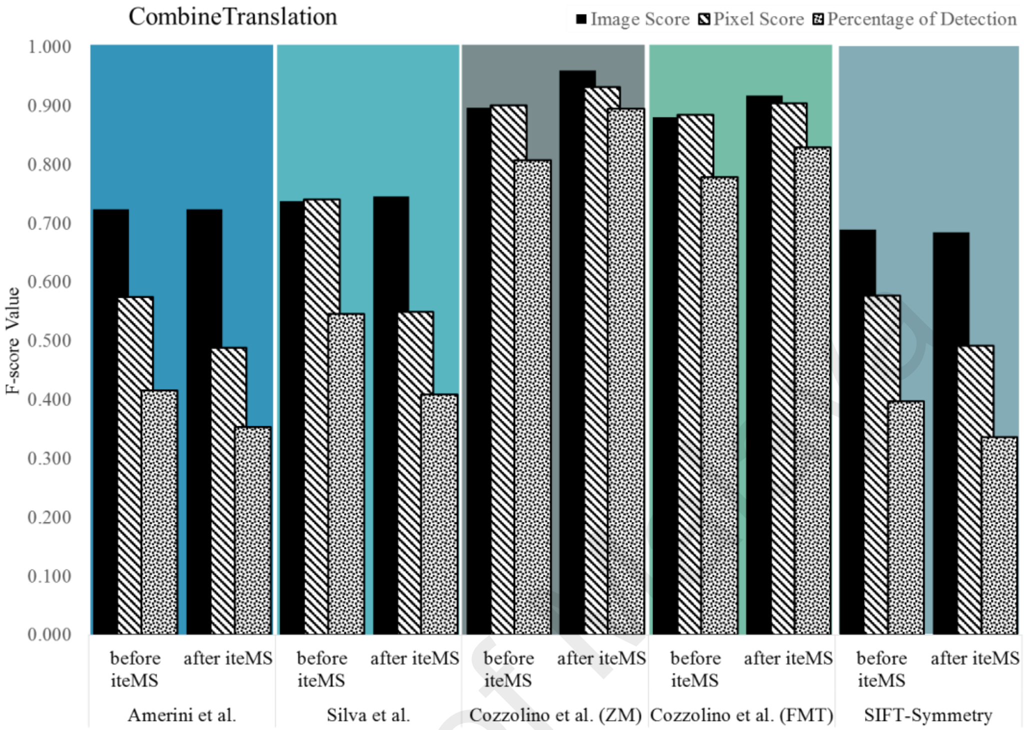


Figure 7.6: The results of the CMF detection methods before and after iteMS procedure is combined for CombineTranslation datasets

7.4 Chapter Summary

This chapter accumulates the results from the performance analysis I, the permance of SIFT-Symmetry, and the performance of the CMF-iteMS in one glance. The results are discussed based on overall performance in four datasets, processing time, geometrical transformation (including reflection-based CMF attacks) and post-processing attacks. Moreover, the iteMS procedure was also examined with the individual CMF detection methods to assess the efficiency of the automated threshold selection in the final verification CMF detection process. The CMF-iteMS shows the most efficient method among the established CMF detection methods.

CHAPTER 8: DISCUSSION AND CONCLUSIONS

This thesis is concluded by reappraising the research objectives and answering the research questions that have been set in Chapter 1. The goal of this chapter is to provide an important summary of the contribution of this research and also provide a direction of future research.

8.1 Reappraisal of the Research Objectives

The first objective of this research is **to examine the effects of image and pixel-level evaluations to the performance of existing CMF detection methods against various CMF attacks, including reflection**. This objective has been achieved by investigating the effects of each level of evaluation for the existing CMF detection methods. There are two-level evaluations commonly used by prior researchers to evaluate CMF detection performance. They are image-level evaluation and pixel-level evaluation. The image-level evaluation only evaluates whether an image has been forged or not. However, this evaluation does not evaluate the exact locations of the forged regions in an image. The exact locations of the forged regions can be evaluated through pixel-level evaluation. However, all images are treated as forged in the pixel-level evaluation.

Since many of the prior researchers conduct the two evaluations separately, exact performance of the methods may not be evaluated correctly. For this reason, three methods, comprise of Amerini et al., Cozzolino et al. (for Zernike moments and FMT), and Silva et al. that represent keypoint, block, and combination-based approaches, respectively are selected. The methods are tested on four different datasets, with each dataset containing different attacks, comprised of simple translation, scale, rotation, simple reflection, reflection-based and a mix of CMF attacks. From the experiments and observations, it can be seen that methods with high pixel-level performance may not have high image-level performance. To ensure acceptable performance, high accuracy of pixel evaluation should only follows after getting high accuracy of image-level evaluation. Therefore, a set of evaluation steps which include both levels is used in the whole experiment for this thesis. The results are measured using multiple F-score values which are for image, pixel and percentage of both detections.

The second objective is **to propose CMF detection methods based on the keypoint-based and block-based approaches that cover various attacks in CMF**. Based on the performance investigations of the existing CMF detection methods (which is prepared for the first objective), the keypoint-based approach shows good performance on CMF with various attacks, especially scale and rotation, but the method is not robust against reflection attacks. Meanwhile, the block-based approach suffers from threshold selection. Though the block-based approach is invariant to translation, rotation, and reflection attacks, the static threshold has limit the detection of CMF in various input images which have different resolutions, sizes and types. Therefore, this objective is divided into two sub-objectives:

a) **To propose an improved CMF detection method based on the keypoint-based approach using a symmetry matching technique that is not only robust against translation, scale and rotation, but also to the reflection**

The main contribution of this method is to increase the robustness of the keypoint-based approach against CMF with reflection attacks. A method called SIFT-Symmetry is proposed that combine the symmetry matching technique with the Amerini et al.'s method, specifically to cover the reflection attacks in the keypoint-based approach. In the method, mirror-SIFT features are paired with the symmetry matching technique and will commence if the Amerini et al.'s method only able to detect less than five matching points. The symmetry matching technique computes the symmetry magnitude in the image to generate the dominant symmetry axis. Then, the symmetry points which associate with the axis are clustered to verify the forged region. The results show that the SIFT-Symmetry is able to maintain at least 70% of the image score for all geometrical transformation cases, including simple reflection. Meanwhile, the CMF-iteMS is only able to achieve minimum value of 51% of image score among all geometrical transformation cases, while the performance of the Amerini et al.'s method is dropped to 0% for the simple reflection. Similar outcomes happened to the reflection-based CMF attacks, which the SIFT-Symmetry is able to outperform existing methods with 94% of image score for simple reflection, and 75% of image score for reflection with scale. However, the image scores for reflection with rotation and mix of reflection are less than the CMF-iteMS, which are 58% and 78%, respectively.

b) To propose an improved CMF detection method based on block approach by introducing iterative means of region size to replace the static threshold selection technique in prior CMF detection method

The main contribution of this method is to automate the static threshold value which often predefined in the existing CMF detection methods in the final verification process. The reason for the threshold selection is to remove the unrelated and wrong features which are extracted during the matching techniques. Instead of defining a static value, a method called CMF-iteMS is proposed by iteratively computes the means of the region size preserved by the matching techniques. Hence, an ideal threshold value could be assigned to each input image with various image resolutions, sizes and types. Several feature extraction and conventional thresholding techniques are also explored to be combined with the iteMS procedure to evaluate the effects towards a CMF image. From the studies, the combination of Zernike moments, thresholding fitting error and iteMS procedure achieved the highest result, therefore, are selected as the final design and has been named as CMF-iteMS. Furthermore, this research also implemented a statistical analysis (means and standard deviation) to limit the threshold value for the image-level evaluation. The results proved that the method is able to outperform existing methods by exceeding the minimum value of 88% of detection for simple translation, while maintaining the highest percentages for rotation, simple reflection, and mix of attacks with the value of 87%, 76%, and 62%, respectively. Previously, the Cozzolino et al.'s method with the static thresholds is only able to achieve the minimum value of 58% of detection for simple translation, 59% of detection for rotation, 58% of detection for simple reflection and 41% of detection for mix of attacks. Furthermore, the CMF-iteMS also shows the highest percentage of detection in all reflection-based CMF cases, which exceeds the minimum score of 11% detection for reflection with scale, 80% of detection for reflection with rotation, and 47% of detection for mix of reflection.

The third objective, which is the last objective of this research, is **to evaluate the F-score performance for the proposed CMF detection methods**. The score is not only calculated for image and pixel-level evaluations, but, also percentage of detection which is obtained by multiplying both scores.

As the main goal of this research is **to develop the efficient CMF detection method for both image and pixel-level evaluations against various attacks, including translation, scale, rotation, reflection, and combinations of each attack**, the CMF-iteMS shows the most efficient methods. They are able to achieve the highest percentage of detection for both non-reflection and reflection-based attacks, except for the scale attacks. This proved that both image and pixel scores of the method are satisfied, which is able to differentiate the original and CMF image with exact region locations.

8.2 Implications of Research

The implications of this research include having the set of evaluation steps likely applied to measure the performance of future CMF detection methods. Secondly, the two methods proposed for CMF detection would help in ensuring the authenticity of a digital image, particularly CMF-manipulation without the requirement of the original image (like the digital watermarking do). Furthermore, the methods proposed would also help in differentiating the original image and CMF image, while providing the exact location of the CMF region. In addition to this, new researchers in CMF detection can also make use of the result from the proposed methods as a benchmark for newer methods.

8.3 Originality and Contribution

The original contributions of this research are the performance analysis of the existing CMF detection methods; the employment of a symmetry matching technique to a CMF image with reflection attacks; and the implementation of a new automatic threshold selection using an iterative means of region size in the final verification of CMF detection. From the analysis, the research problems are verified, that has led to the development of both proposed methods in the CMF detection. As a final conclusion, the proposed methods are able to outperform the existing CMF detection methods against various CMF detection methods including reflection. In addition, the automated threshold selection technique is beneficial to this digital era, since the big data (which involve the heterogeneous data) is rapidly developing.

8.4 Future Research Directions

With regards to the first contribution to the CMF detection, this research employs a symmetry matching technique using a keypoint-based approach. However, issues may arise if the keypoint techniques used for the detection process have an original identical features, while the features are naturally symmetrical at the same time. To be specific, the SIFT features have limitations on differentiating the highly uniform features in the image, either as an original or forged image. This has led to the symmetry matching techniques being too sensitive in detecting natural symmetry image. Therefore, it could be useful if another distinctive feature can be used to enhance the reliability of the proposed method.

Concerning the second contribution for the CMF detection (which is to automate the threshold selection for final verification), future research can extend the proposed method for original image detection. The method proposed in this research can only detect the CMF image, hence, it will be of great benefit if the proposed method is extended to deal with the original image without the need to limit the value.

Despite of the achievements presented by both proposed methods towards geometrical transformation attacks, there is another area that may be looked into which is the effect of the post-processing attacks. The post-processing attacks, including JPEG compression and Gaussian noise addition will affect the visual detection and prevent the forged being detected. Although, the proposed method will also be useful in the case of the post-processing forged images, however the performance of the method would be reduced.

Finally, looking for both implementations, the consolidation of the two proposed methods for CMF detection, as an integrated module, will also be of great benefit. This will give profits by exploiting the advantages of various feature extraction and matching techniques, and further increase overall detection performance.

REFERENCES

Al-nabhani, Y., Jalab, H. A., Wahid, A., & Noor, R. (2015). Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network. *Journal of King Saud University - Computer and Information Sciences*, *27*(4), 393–401.

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*(1–3), 284–95.

Amerini, I., Ballan, L., Caldelli, R., Bimbo, A. Del, & Serra, G. (2011). A SIFT-Based Forensic Method for Copy – Move Attack Detection and Transformation Recovery. *IEEE Transactions on Information Forensics and Security*, *6*(3), 1099–1110.

Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., Del Tongo, L., & Serra, G. (2013). Copy-Move Forgery Detection And Localization by Means of Robust Clustering With J-Linkage. *Signal Processing: Image Communication*, *28*(6), 659–669.

Anastas, J. W. (1999). *Research Design for Social Work and the Human Services* (2nd ed.). Columbia University Press.

AppBrain. (2014). Mirror Image - Photo Editor. Retrieved March 30, 2017, from http://www.appbrain.com/app/mirror-image-photo-editor/com.lyrebirdstudio.mirror

Ardizzone, E., Bruno, A., & Mazzola, G. (2010). Detecting Multiple Copies in Tampered Images. In *17th International Conference on Image Processing* (pp. 2117–2120).

Ardizzone, E., Bruno, A., & Mazzola, G. (2015). Copy – Move Forgery Detection by Matching Triangles of Keypoints. *IEEE Transactions on Information Forensics and Security*, *10*(10), 2084–2094.

Ardizzone, E., Mazzola, G., Informatica, I., & Università, D. (2009). Detection of Duplicated Regions in Tampered Digital Images by Bit-Plane Analysis. In *15th International Conference Vietri sul Mare, Italy* (Vol. 5716, pp. 893–901).

Bappy, J. H., Roy-Chowdhury, A. K., Bunk, J., Nataraj, L., & Manjunath, B. S. (2017). Exploiting Spatial Structure for Localizing Manipulated Image Regions. In *Proceedings of the IEEE International Conference on Computer Vision* (Vol. 2017–Octob, pp. 4980–4989).

Bay, H., & Ess, A. (2008). Speeded-Up Robust Features (SURF). *Computer Vision and Image Understanding*, *110*, 346–359.

Bayram, S., Sencar, H. T., & Memon, N. (2009). An Efficient And Robust Method For Detecting Copy-Move Forgery. In *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (pp. 1053–1056).

Bhullar, L. K., Budhiraja, S., & Dhindsa, A. (2014). DWT and SIFT Based Passive Copy-Move Forgery Detection. *International Journal of Computer Applications*, *95*(23), 14–18.

Bi, X., Pun, C. M., & Yuan, X. C. (2016). Multi-Level Dense Descriptor and Hierarchical Feature Matching for Copy-Move Forgery Detection. *Information Sciences*, *345*, 226–242.

Bianchi, T., & Piva, A. (2012). Detection of nonaligned double JPEG compression based on integer periodicity maps. *IEEE Transactions on Information Forensics and Security*, *7*, 842–848.

Birkhoff, G. D. (1933). *Aesthetic Measure*. *Aesthetic Measure*.

Bo, X., Junwen, W., Guangjie, L., & Yuewei, D. (2010). Image Copy-Move Forgery Detection Based On SURF. In *International Conference on Multimedia Information Networking and Security* (pp. 889–892).

Bochner, S., & Chandrasekkharan, K. (1949). *Fourier Transforms*. Princeton University Press.

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*(1–3), 33–43.

Carkir, S., & Cetin, A. E. (2010). Two-Dimensional Mellin and Mel-Cepstrum for Image Feature Extraction. In *Proceedings of the 25th International Symposium on Computer and Information Sciences* (pp. 271–276).

Carvalho, T. J. De, Member, S., Riess, C., Member, A., Angelopoulou, E., Pedrini, H., & Rocha, A. D. R. (2013). Exposing Digital Image Forgeries by Illumination Color Classification. *IEEE Transactions on Information Forensics and Security*, *8*(7), 1182–1194.

Chang-Tsun Li. (2010). Source Camera Identification Using Enhanced Sensor Pattern Noise. *IEEE Transactions on Information Forensics and Security*, *5*(2), 280–287.

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.

Chora, R. S. (2007). Image Feature Extraction Techniques and Their Applications for CBIR and Biometrics Systems. *International Journal of Biology and Biomedical Engineering*, *1*(1).

Christlein, V., Riess, C., Jordan, J., Riess, C., & Angelopoulou, E. (2012). An Evaluation of Popular Copy-Move Forgery Detection Approaches. *IEEE Transactions on Information Forensics and Security*, *7*(6), 1841–1854.

Cozzolino, D., Poggi, G., & Verdoliva, L. (2015). Efficient Dense-Field Copy – Move Forgery Detection. *IEEE Transactions on Information Forensics and Security*, *10*(11), 2284–2297.

Davarzani, R., Yaghmaie, K., Mozaffari, S., & Tapak, M. (2013). Copy-move forgery detection using multiresolution local binary patterns. *Forensic Science International*, *231*(1–3), 61–72.

Edwards, T. (1992). Discrete Wavelet Transforms: Theory and Implementation. In *Draft #2*.

Emam, M., Han, Q., & Niu, X. (2016). PCET based copy-move forgery detection in images under geometric transforms. *Multimedia Tools and Applications*, *75*(18), 11513–11527.

Ferreira, A., Felipussi, S. C., Alfaro, C., Fonseca, P., Vargas-Munoz, J. E., dos Santos, J. A., & Rocha, A. (2016). Behavior Knowledge Space-Based Fusion for Copy-Move Forgery Detection. *IEEE Transactions on Image Processing*, *7149*(c), 1–1.

Freeman, W. T., & Adelson, E. H. (1991). The Design and Use of Steerable Filters. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *13*(9), 891–906.

Fridrich, J., Soukal, D., & Lukáš, J. (2003). Detection of Copy-Move Forgery in Digital Images. *International Journal of Computer Science Issues*, *3*, 652–663.

Funk, C., & Liu, Y. (2017). Beyond Planar Symmetry: Modeling Human Perception of Reflection and Rotation Symmetries in the Wild. In *Proceedings of the IEEE International Conference on Computer Vision* (Vol. 2017–Octob, pp. 793–803).

Gan, Y., & Cang, J. (2013). A detection algorithm for image copy-move forgery based on improved circular projection matching and PCA. *Sensors and Transducers*, *159*(11), 19–25.

Gan, Y., & Zhong, J. (2014). Image copy-move tamper blind detection algorithm based on integrated feature vectors. *Journal of Chemical and Pharmaceutical Research*, *6*(6), 1584–1590.

Guo, J.-M., Liu, Y.-F., & Wu, Z.-J. (2013). Duplication Forgery Detection Using Improved DAISY Descriptor. *Expert Systems with Applications*, *40*(2), 707–714.

Guo, X., & Cao, X. (2012). MIFT: A framework for feature descriptors to be mirror reflection invariant. *Image and Vision Computing*, *30*(8), 546–556.

Hargittai, I., & Hargittai, M. (2000). *In Our Own Image: Personal Symmetry in Discovery*. Springer US.

Harris, C., & Stephens, M. (1988). A Combined Corner and Edge Detector. In *Procedings of the Alvey Vision Conference 1988* (p. 23.1-23.6). Alvey Vision Club.

Hastie, T. (2009). *The Elements of Statistical Learning Data Mining, Inference, and Prediction* (2nd Editio). New York, USA: Springer US.

Hauagge, D. C., & Snavely, N. (2012). Image matching using local symmetry features. In *IEEE Conference on Computer Vision and Pattern Recognition* (pp. 206–213).

He, H., Huang, X., & Kuang, J. (2013). Exposing Copy Move Forgeries Based On A Dimension Reduced SIFT Method. *Information Technology Journal*, *12*(14), 2975–2979.

Hoffman, W. C. (2003). Symmetry in Psychology. *Visual Mathematics*, (20).

Hong, C., & Kot, A. C. (2009). Accurate Detection of Demosaicing Regularity from Output Images. In *IEEE International Symposium on Circuits and Systems 2009* (pp. 497–500).

Hsu, Y.-N., Arsenault, H. H., & April, G. (1982). Rotation-invariant digital pattern recognition using circular harmonic expansion. *Applied Optics*, *21*(22), 4012–4015.

Huang, H., Guo, W., & Zhang, Y. (2008). Detection Of Copy-Move Forgery in Digital Images Using SIFT Algorithm. In *IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application* (pp. 272–276). Ieee.

Huang, Y., Lu, W., Sun, W., & Long, D. (2011). Improved DCT-based Detection of Copy-Move Forgery in Images. *Forensic Science International*, *206*(1–3), 178–184.

Hussain, M., Saleh, S. Q., Aboalsamh, H., Muhammad, G., & Bebis, G. (2014). Comparison between WLD and LBP descriptors for non-intrusive image forgery detection. In *IEEE International Symposium on Innovations in Intelligent Systems and Applications (INISTA) Proceedings* (pp. 197–204). Ieee.

Huynh-the, T., Banos, O., Lee, S., Yoon, Y., & Le-tien, T. (2016). Improving digital image watermarking by means of optimal channel selection. *Expert Systems With Applications*, *62*, 177–189.

Jaberi, M., Bebis, G., Hussain, M., & Muhammad, G. (2013). Accurate And Robust Localization of Duplicated Region In Copy–Move Image Forgery. *Machine Vision and Applications*, *25*(2), 451–475.

Jackson Marr, M. (2006). Through the Looking Glass: Symmetry in Behavioral Principles? *The Behavior Analyst*, *29*(1), 125–128.

Jin, G., & Wan, X. (2017). An improved method for SIFT-based copy-move forgery detection using non-maximum value suppression and optimized J-Linkage. *Signal Processing: Image Communication*, *57*(January), 113–125.

Jing, D., & Wei, W. (2011). CASIA Tampered Image Detection Evaluation (TIDE) Database. Retrieved April 28, 2015, from http://forensics.idealtest.org/casiav2/

Juan, L., & Gwun, O. (2009). A Comparison of SIFT , PCA-SIFT and SURF. *International Journal of Image Processing*, *3*(4), 143–152.

Kakar, P., & Sudha, N. (2012). Exposing Postprocessed Copy-Paste Forgeries through

Transform-Invariant Features. *IEEE Transactions on Information Forensics and Security*, *7*(3), 1018–1028.

Kanan, C., & Cottrell, G. W. (2012). Color-to-Grayscale : Does the Method Matter in Image Recognition? *Plos One*, *7*(1), e29740.

Kapur, J. N., Sahoo, P. K., & Wong, A. K. C. (1980). A new method for grey-level picture thresholding using the entropy of the histogram. *Signal Processing*.

Kim, S., & In-So, K. (2002). Probabilistic Model-based Object Recognition using Local Zemike Moments. In *IAPR Workshop on Machine Vision Applications* (pp. 11–14).

Kot, A. C., & Cao, H. (2013). Image and Video Source Class Identification. In *Digital Image Forensics* (pp. 157–178).

Kroonenberg, P. M. (1983). *Three-mode Principal Component Analysis*.

Langille, A., & Gong, M. (2006). An Efficient Match-based Duplication Detection Algorithm. In *3rd Canadian Conference on Computer and Robot Vision (CRV'06)* (pp. 64–64). Ieee.

Li, C., Ma, Q., Xiao, L., Li, M., & Zhang, A. (2017). Image splicing detection based on markov features in QDCT domain. *Neurocomputing*, *228*, 29–36.

Li, L., Li, S., Zhu, H., & Wu, X. (2014). Detecting copy-move forgery under affine transforms for image forensics. *Computers and Electrical Engineering*, *40*(6), 1951–1962.

Li, Y. (2013). Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching. *Forensic Science International*, *224*(1–3), 59–67.

Lin, C. (2000). *Watermarking and Digital Signature Techniques for Multimedia Authentication and Copyright Protection*.

Lin, W., Khan, S. U., Yow, K. C., Qazi, T., Madani, S. a., Xu, C.-Z., … Hayat, K. (2013). Survey on Blind Image Forgery Detection. *IET Image Processing*, *7*(7), 660–670.

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.

Liu, Y., Hel-Or, H., Kaplan, C. S., & Gool, L. Van. (2008). Computational Symmetry in Computer Vision and Computer Graphics. *Foundations and Trends® in Computer Graphics and Vision*, *5*(1–2), 1–195.

Lowe, D. G. (1999). Object Recognition from Local Scale-Invariant Features. In *The Proceedings of the Seventh IEEE International Conference on Computer Vision, 1999.*

Lowe, D. G. (2004). Distinctive Image Features from Scale-Invariant Keypoints. *International Journal of Computer Vision*, *60*(2), 91–110.

Loy, G., & Eklundh, J. O. (2006). Detecting symmetry and symmetric constellations of features. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 3952 LNCS, pp. 508–521).

Lynch, G., Shih, F. Y., & Liao, H.-Y. M. (2013). An efficient expanding block algorithm for image copy-move forgery detection. *Information Sciences*, *239*, 253–265.

Lyu, S., & Farid, H. (2005). How realistic is photorealistic? *IEEE Transactions on Signal Processing*, *53*(2), 845–850.

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

Miljkovi, O. (2009). Image Pre-Processing Tool. *Kragujevac J. Math.*, *32*, 97–107.

Mishra, P., Mishra, N., Sharma, S., & Patel, R. (2013). Region Duplication Forgery Detection Technique Based On SURF And HAC. *The Scientific World Journal*, *2013*(July 2008).

Muhammad, G., Hussain, M., & Bebis, G. (2012). Passive Copy Move Image Forgery Detection Using Undecimated Dyadic Wavelet Transform. *Digital Investigation*, *9*(1), 49–57.

Myna, A. N., Venkateshmurthy, M. G., & Patil, C. G. (2008). Detection of region duplication forgery in digital images using wavelets and log-polar mapping. In *Proceedings - International Conference on Computational Intelligence and Multimedia Applications, ICCIMA 2007* (Vol. 3, pp. 371–377).

Narasimha, M., & Peterson, A. (1978). On the Computation of the Discrete Cosine Transform. *IEEE Transactions on Communications*, *26*(6), 934–936.

Nguyen, V., Vicente, T. F. Y., Zhao, M., Hoai, M., Samaras, D., & Brook, S. (2017). Shadow Detection with Conditional Generative Adversarial Networks. In *Proceedings of the IEEE International Conference on Computer Vision* (pp. 4510–4518).

Otsu, N. (1979). A threshold selection method from gray-level histograms. *IEEE Transactions on Systems, Man, and Cybernetics*, *9*(1), 62–66.

Pan, X., & Lyu, S. (2010). Region Duplication Detection Using Image Feature Matching. *IEEE Transactions on Information Forensics and Security*, *5*(4), 857–867.

Park, C. S., Kim, C., Lee, J., & Kwon, G. R. (2016). Rotation and scale invariant upsampled log-polar fourier descriptor for copy-move forgery detection. *Multimedia Tools and Applications*, *75*(23), 16577–16595.

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*(1–3), e21–e25.

Piccinnano, A. C. (2014). *Techniques for Digital Image Forensics and Counter-Forensics (Doctoral Dissertation)*. University of Siena, Italy.

Pun, C. M., Liu, B., & Yuan, X. C. (2016). Multi-scale noise estimation for image splicing forgery detection. *Journal of Visual Communication and Image Representation*, *38*, 195–206.

Pun, C., Member, S., Yuan, X., & Bi, X. (2015). Oversegmentation and Feature Point Matching. *IEEE Transactions on Information Forensics and Security*, *10*(8), 1705–1716.

Qiao, T., Retraint, F., Cogranne, R., & Thai, T. H. (2017). Individual camera device identification from JPEG images. *Signal Processing: Image Communication*, *52*(January), 74–86.

Redi, J. a., Taktak, W., & Dugelay, J.-L. (2010). Digital image forensics: a booklet for beginners. *Multimedia Tools and Applications*, *51*(1), 133–162.

Ridler, T.W. Calvard, S. (1978). Picture Thresholding Using an Iterative Slection Method. *IEEE Transactions on Systems, Man and Cybernetics*, *8*(8), 630–632.

Ryu, S. J., Kirchner, M., Lee, M. J., & Lee, H. K. (2013). Rotation invariant localization of duplicated image regions based on zernike moments. *IEEE Transactions on Information Forensics and Security*, *8*(8), 1355–1370.

Ryu, S. J., Lee, M. J., & Lee, H. K. (2010). Detection of copy-rotate-move forgery using zernike moments. In *12th International Conference* (Vol. 6387, pp. 51–65).

Saad, S. M. (2009). Design of a robust and secure digital signature scheme for image authentication over wireless channels. *IET Information Security, 3*(September 2007), 1–8.

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*(1–3), 71–82.

Sheng, Y., & Arsenault, H. H. (1986). Experiments on pattern recognition using invariant Fourier-Mellin descriptors. *Journal of the Optical Society of America A*, *3*(6), 771.

Shivakumar, B. L., & Baboo, S. S. (2011). Detection Of Region Duplication Forgery in Digital Images Using SURF. *International Journal of Computer Science Issues*, *8*(4), 199–205.

Silva, E., Carvalho, T., Ferreira, A., & Rocha, A. (2015). Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes. *Journal of Visual Communication and Image Representation*, *29*, 16–32.

Stewart, I., & Golubitsky, M. (2010). *Fearful Symmetry: Is God a Geometer?* Courier Corporation.

Su, Y., Jin, X., Zhang, C., & Chen, Y. (2017). Hierarchical Image Resampling Detection Based on Blind Deconvolution. *Journal of Visual Communication and Image Representation*.

Sun, Q., & Chang, S. (2005). A Secure and Robust Digital Signature Scheme for JPEG2000 Image Authentication. *IEEE Transactions on Multimedia*, *7*(3), 480–494.

Teague, M. R. (1980). Image analysis via the general theory of moments. *Journal of the Optical Society of America*, *70*(8), 920–930.

Threshold. (2009). *In A Dictionary of Physics* (6th ed.). Oxford University Press.

Tijdink, J. K., Verbeke, R., & Smulders, Y. M. (2014). Publication Pressure and Scientific Misconduct in Medical Scientists. *Journal of Empirical Research on*, *9*(5), 64–71.

Tralic, D., Grgic, S., Sun, X., & Rosin, P. L. (2016). Combining cellular automata and local binary patterns for copy-move forgery detection. *Multimedia Tools and Applications*, *75*(24), 16881–16903.

Tsai, J., Huang, W., & Kuo, Y. (2011). On the Selection of Optimal Feature Region Set for Robust Digital Image Watermarking. *IEEE Transactions on Image Processing*, *20*(3), 735–743.

Uliyan, D., Jalab, H., Abdul Wahab, A., & Sadeghi, S. (2016). Image Region Duplication Forgery Detection Based on Angular Radial Partitioning and Harris Key-Points. *Symmetry*, *8*(7), 62.

Ustubioglu, B., Ulutas, G., Ulutas, M., & Nabiyev, V. V. (2016). A new copy move forgery detection technique with automatic threshold determination. *AEU - International Journal of Electronics and Communications*, *70*(8), 1076–1087.

Warif, N. B. A., Wahab, A. W. A., Idris, M. Y. I., Ramli, R., Salleh, R., Shamshirband, S., & Choo, K.-K. R. (2016). Copy-move forgery detection : Survey, challenges and future directions. *Journal of Network and Computer Applications*, *75*, 259–278.

Warif, N. B. A., Wahab, A. W. A., Idris, M. Y. I., Salleh, R., & Othman, F. (2017). SIFT-Symmetry: A Robust Detection Method for Copy-Move Forgery with Reflection Attack. *Journal of Visual Communication and Image Representation*, *46*, 219–232.

Xu, B., Wang, X., Zhou, X., Xi, J., & Wang, S. (2015). Source camera identification from image texture features. *Neurocomputing*, *207*, 131–140.

Yang, F., Li, J., Lu, W., & Weng, J. (2017). Copy-move forgery detection based on hybrid features. *Engineering Applications of Artificial Intelligence*, *59*(May 2016), 73–83.

Yang, Q. (2014). Zernike Moments Descriptor Matching based Symmetric Optical Flow for Motion Estimation and Image Registration, (61273261), 350–357.

Yap, P.-T., Jiang, X., & Kot, A. C. (2010). Two-Dimensional Polar Harmonic Transforms for Invariant Image Representation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *32*(7), 1259–1270.

Yen, J. C., Chang, F. J., & Chang, S. (1995). A New Criterion for Automatic Multilevel Thresholding. *IEEE Transactions on Image Processing*, *4*(3), 370–378.

Yu, L., Han, Q., & Niu, X. (2014). Feature point-based copy-move forgery detection : covering the non-textured areas. *Multimedia Tools and Applications*.

Zeng, H., Zhan, Y., Kang, X., & Lin, X. (2016). Image splicing localization using PCA-based noise level estimation. *Multimedia Tools and Applications*, 1–17.

Zhang, J., Feng, Z., & Su, Y. (2008). A new approach for detecting copy-move forgery in digital images. In *11th IEEE Singapore International Conference on Communication Systems, ICCS 2008* (pp. 362–366).

Zhang, P., & Kong, X. (2009). Detecting image tampering using feature fusion. In *IEEE Conference Availability, Reliability, and Security* (pp. 335–340).

Zhang, Q., Lu, W., & Weng, J. (2016). Joint image splicing detection in DCT and Contourlet transform domain. *Journal of Visual Communication and Image Representation*, *40*, 449–458.

Zhao, J., & Guo, J. (2013). Passive Forensics for Copy-Move Image Forgery Using A Method based on DCT and SVD. *Forensic Science International*, *233*(1–3), 158–66.

Zhao, J., & Zhao, W. (2013). Passive forensics for region duplication image forgery based on harris feature points and local binary patterns. *Mathematical Problems in Engineering*, *2013*.

Zheng, J., & Chang, L. (2014). Detection Technology of Tampering Image Based on Harris Corner Points ⋆ . *Journal of Computational Information Systems*, *10*(4), 1481–1488.

Zheng, J., Liu, Y., Ren, J., Zhu, T., Yan, Y., & Yang, H. (2016). Fusion of block and keypoints based approaches for effective copy-move image forgery detection. *Multidimensional Systems and Signal Processing*, *27*(4), 989–1005.

LIST OF PUBLICATIONS AND PAPER PRESENTED

Articles on Research Topic

1. Warif, N. B. A., Wahab, A. W. A., Idris, M. Y. I., Salleh, R., & Othman, F. SIFT-Symmetry: A Robust Detection Method for Copy-Move Forgery with Reflection Attack, Journal of Visual Communication and Image Representation, Volume 46, July 2017, Pages 219-232. (*ISI-Indexed*)
2. Warif, N. B. A., Wahab, A. W. A., Idris, M. Y. I., Ramli, R., Salleh, R., Shamshirband, S., & Choo, K. K. R. (2016). Copy-move forgery detection: Survey, challenges and future directions. Journal of Network and Computer Applications, 75, 259-278. (*ISI-Indexed*)
3. Warif, N. B. A., Idris, M. Y. I., Wahab, A. W. A., & Salleh, R. CMF-iteMS: An Automatic Threshold Selection for Copy-Move Forgery Detection, Forensic Science International. (*Under Review*).

Conference Proceedings on Research Topic

1. Nor Bakiah Abd Warif, Mohd. Yamani Idna Idris, Ainuddin Wahid Abdul Wahab, Rosli Salleh. An Evaluation of Error Level Analysis in Image Forensics. 2015 IEEE International Conference on System Engineering and Technology (ICSET 2015). (*Non-ISI/Non-SCOPUS*)

Collaboration Article

1. Mohd. Yamani Idna Idris, Nor Bakiah Abd. Warif, Hamzah Arof, Noorzaily Mohamed Noor, Ainuddin Wahid Abdul Wahab, Zaidi Razak**.** Accelerating FPGA-SURF Feature Detection Module by Memory Access Reduction. Malaysian Journal of Computer Science. (*Accepted*).

Seminars/Conference Presentation

1. Postgraduate Research Excellence Symposium (PGRes), Faculty of Computer Science and Information Technology, Universiti Malaya. Malaysia. Held in Pullman Hotel, Kuala Lumpur. June, 2015.
2. 2015 IEEE International Conference System, Engineering and Technology, held in Universiti Teknologi Mara, Shah Alam, Selangor, Malaysia. 10 August 2015.
3. Postgraduate Research Excellence Symposium (PGRes), Faculty of Computer Science and Information Technology, Universiti Malaya. Malaysia. Held in Eastin Hotel, Kuala Lumpur. June, 2016.

Awards

1. **Best Paper Presentation Awards.** SIFT-Symmetry: A Robust Detection Method for Copy-Move Forgery with Reflection Attacks. Postgraduate Research Excellence Symposium (PGRes), Faculty of Computer Science and Information Technology, Universiti Malaya. Malaysia. Held in Eastin Hotel, Kuala Lumpur. June, 2016.
2. **1st Place UM 3 Minutes Thesis – Faculty Level**. Held in Faculty of Computer Science and Information Technology, University Malaya, 28 March 2018.