



FORENSIC ANALYSIS OF DIGITAL IMAGE TAMPERING

A thesis submitted in partial fulfilment of the requirements for the
degree of Master of Science in Information Security

Submitted to:

Department of Information Security, College of Computer and
Information Security Naif Arab University for Security Sciences

By:

Abdullatif Al-zahrani

Under Supervision of:

Dr. Fahad Al-harby

May 2019

Table of Contents

ABSTRACT	II
ACKNOWLEDGMENT	III
LIST OF FIGURES	VII
LIST OF TABLES	VIII
LIST OF ABBREVIATIONS	IX
INTRODUCTION	1
1.1 Background	1
1.2 Problem statement	3
1.3 Research Aims.....	4
1.4 Scope of the Study	5
1.5 Objectives	5
1.6 Thesis Contribution	5
1.7 Organization of Thesis	6
BACKGROUND AND LITERATURE REVIEW	7
2.1 Digital Image Forensics.....	7
2.1 Image Source Identification	7
2.2 Detection of Computer Generated Images	8
2.3 Forgery Detection for Digital Images.....	9
2.4 Mechanisms for Image Forgery Detection	10
2.4.1 Active Methods	11
2.4.1.1 Digital Watermarking.....	11
2.4.1.2 Digital Signature	11
2.4.2 Passive Methods	12
2.5 Types of Digital Image Forgery	12
2.5.1 Image Morphing	13
2.5.2 Image Splicing.....	13
2.5.3 Image Retouching.....	14
2.5.4 Image Enhancing.....	15
2.5.5 Copy-Move Image Forgery	15
2.6 Copy-Move Forgery Detection Classification.....	18
2.6.1 Block-Based Algorithms	30
2.6.2 Keypoint-Based Algorithms.....	32
PROPOSED METHODOLOGY	36
3.1 Copy-Move Forgery Detection Techniques Overview	36
3.1.1 Evaluation Of The Bravo Algorithm	36
3.1.1.1 Advantages And Disadvantages Of Bravo Algorithm	37
3.1.2 Evaluation Of The Luo Algorithm	37
3.1.2.1 Advantages And Disadvantages Of Luo Algorithm	39
3.1.3 Evaluation Of Pca Algorithm	39
3.1.3.1 Advantages And Disadvantages Of Pca Algorithm	41
3.1.4 Evaluation Of The Local Binary Pattern (Lbp) Algorithm	41
3.1.4.1 Advantages And Disadvantages Of Lbp Algorithm	43
3.2 Proposed Algorithm	43

3.2.1	Methodology.....	43
3.2.2	The Proposed Framework	44
3.2.2.1	Parameterization	55
3.2.3	Advantage of the Proposed Algorithm	56
3.3	Summary.....	57
EXPERIMENTAL RESULTS AND DISCUSSION.....		58
4.1	Data collection.....	58
4.1.1	MICC-F2000 Dataset	58
4.2	Evaluation Criteria	60
4.3	Possible Attacks and Challenges	62
4.3.1	JPEG Compression.....	62
4.3.2	Gaussian Noise.....	63
4.4	Experimental Setup	63
4.5	Experimental Results.....	64
4.5.1	Visual Results.....	64
4.5.2	Results for the Forged Images without Attacks.....	65
4.5.3	Results Using Gaussian Noise and JPEG Compression Attacks.....	66
4.5.4	Results for Images with Uniform Background Challenge Using Gaussian Noise and JPEG Compression Attacks	67
4.6	Summary	69
CONCLUSION AND FUTURE WORK		70
5.1	Conclusions.....	70
5.2	Future Work:	71
REFERENCES.....		70

List of Figures

Figure 2.1: Create a human face in Unity editor	8
Figure 2.2: Create a human face in Belender editor	9
Figure 2.3: Examples of computer generated images.....	9
Figure 2.4: Image forgery classification.....	10
Figure 2.5: Image morphing example.....	13
Figure 2.6: Example of image splicing.....	14
Figure 2.7: Example of image retouching	14
Figure 2.8: Image enhancement example	15
Figure 2.9: The Iranian missiles forged image case	16
Figure 2.10: The US president speech forged image case.....	17
Figure 2.11: The North Korean military training forged image case	17
Figure 2.12: The general framework of CMFD algorithms.	19
Figure 2.13: Tree diagram of CMFD algorithms.....	22
Figure 2.14: Apply Largest Singular Value (LSV) on each DCT block to extracting features in Zaho algorithm	24
Figure 2.15: Grayscale image regions used in the Luo algorithm	25
Figure 2.16: Extend LBP to circular neighborhoods	26
Figure 2.17: Example of image forgery detection by using DyWT method	28
Figure 2.18: Plain CMFD algorithm scheme.....	32
Figure 2.19: Example of applying Gabor filter on a forged image.....	33
Figure 3.1: The four directions of Luo algorithm.....	38
Figure 3.2: Different LBP patterns	41
Figure 3.3: Framework of proposed method	45
Figure 3.4: Calculation of histogram of the 3 channels of an image	48
Figure 3.5: Histogram of greyscale image.....	48
Figure 3.6: The shift vectors of two copied areas.....	50
Figure 3.7: False positive with same shift vectors.....	52
Figure 3.8: Visual results.....	53
Figure 3.9: Flow chart of the framework for the proposed method.....	54
Figure 4.1: Examples of further forged images from MICC-F2000 Datasets.....	59
Figure 4.2: Different level of jpeg compression.....	62
Figure 4.3: Uniform background example	63
Figure 4.4: Examples of visual results (a) the original image, (b) the forged image, (c) algorithm results	64
Figure 4.5: Comparison of PCA, Luo, Bravo, LBP and our proposed method.....	65
Figure 4.6: Comparison CMFD method with Gaussian noise and JPEG compression attacks	67
Figure 4.7: Comparison CMFD method with uniform background and Gaussian noise and JPEG compression attacks.....	68

List of Tables

Table 4.1: Various evaluation metrics.....	61
Table 4.2: Detection results of CMFD methods	65
Table 4.3: Detection results of CMFD methods with Gaussian Noise and JPEG Compression Attacks.....	66
Table 4.4: Detection results of CMFD methods with uniform background and Gaussian noise and JPEG compression attacks.....	68