ENHANCED COPY-PASTE IMAGE FORGERY DETECTION BASED ON ARCHIMEDEAN SPIRAL AND COARSE-TO-FINE APPROACH

MOHAMMAD AKBARPOUR SEKEH

A thesis submitted in fulfilment of the
requirement for the award of the degree of
Doctor of Philosophy (Computer Science)

Faculty of Computing
Universiti Teknologi Malaysia

OCTOBER 2013

This thesis is dedicated to my wife, Malihe, to my daughter, Aida, and to my parents.

ACKNOWLEDGMENTS

First and foremost I would like to thank my supervisor, Professor Dr. Mohd. Aizaini Maarof, for his advice and guidance over the years, and for helping me understand the importance of hard work and dedication in doing a Ph.D. thesis. I express my gratitude towards my co-supervisor, Prof. Dr. Mohd. Zulkifli and Dr. Mohd. Foad Rohani for their attention to details and constructive comments. In particular, I would also like to thank: Dr. Babak Mahdian from department of image processing, institute of information theory and automation, Czech Republic and Dr. Seung-Jin Ryu, department of computer science, Korea advanced institute of science and technology. Moreover, I thank Malihe and Goli for proofreading the thesis and Mahdi as a Photoshop expert. I would also like to thank Universiti Teknologi Malaysia (UTM) for funding my PhD study using Fundamental Research Grant Scheme (FRGS). The most heartfelt gratitude should go my mother, my father, and my family members for their support of my study, encouragement, and companions. I am forever indebted to my wife Malihe for her love and support throughout my studies and to her I give especial thanks.

ABSTRACT

Duplicated region detection is one of the most common blind image forgery detection techniques to detect evidence of tampering and this is done by scrutinizing clues in a copy-paste image forgery. Two main issues for detecting copy-paste image forgery are robust feature extraction and computational complexity. The major and specific challenges are to improve robustness especially against rotation for small size duplicated regions and improve time complexity of block similarity detection due to blindly matching in current methods. In this study, a copy-paste image forgery detection model is enhanced by including two proposed algorithms. The algorithms are Spiral Unique Sequence feature (SUS) based on Archimedean spiral to address the robustness issue and Coarse-To-Fine (CTF) block-matching algorithm based on sequential straightforward block clustering technique to resolve the time complexity issue. For evaluating the performance of SUS and CTF, MICC-F220 dataset from University of Florence and FC2010 dataset from Universiti Teknologi Malaysia were used. To measure the robustness of SUS, two sizes of blocks including 16×16 pixels and 8×8 pixels were analysed and the results were compared with Zernike moment's robustness. For the first blocksize, the robustness improvement of SUS against noise and compression were 9.6% and 1.7% respectively but, was -2.9% against rotation. However, for the second blocksize, the robustness of SUS against noise, compression, and rotation were improved by 21.3%, 18.9%, 30.8% respectively. Next, the performance of CTF computational time was analysed in different cases of the number of clusters and compared with Lexicographical-sorting method. When the number of clusters exceeded a specific threshold, the computational time of CTF matching was significantly reduced. In conclusion, the experimental results and mathematical analysis demonstrated that SUS feature with coarse-to-fine block matching algorithm have made considerable improvements in terms of robustness and time complexity thus contributing to the area of duplicated region detection in forensic science.

ABSTRAK

Pengesanan rantau penduaan merupakan salah satu teknik pengesanan pemalsuan imej buta yang biasa digunakan untuk menemukan bukti gangguan melalui penelitian petunjuk pemalsuan dalam imej salin-tampal. Dua isu utama dalam bidang penyelidikan pengesanan pemalsuan salin-tampal ialah fungsi pengekstrakan ciri yang mantap dan pengiraan kerumitan. Cabaran paling utama adalah untuk meningkatkan keteguhan terhadap putaran kawasan penduaan bersaiz kecil dan menambah baik kerumitan masa dalam mengesan kesamaan blok disebabkan oleh pemadanan buta dalam kaedah semasa. Dalam kajian ini satu model pengesanan pemalsuan imej salin-tampal telah dipertingkatkan dengan memasukkan dua algoritma cadangan. Algoritma tersebut ialah *Spiral Unique Sequence (SUS)* berasaskan lingkaran *Archimedean* bagi menangani isu keteguhan dan algoritma blok padanan *Coarse-To-Fine (CTF)* berasaskan teknik urutan mudah blok kelompok bagi menyelesaikan isu kerumitan masa. Prestasi SUS dan CTF telah dinilai menggunakan set data MICC-F220 daripada University of Florence dan set data FC2010 daripada Universiti Teknologi Malaysia. Untuk mengukur keteguhan SUS dua saiz blok, iaitu 16×16 dan 8×8 telah dianalisis dan keputusannya telah dibandingkan dengan keteguhan *Zernike moments*. Bagi saiz blok 16×16 peningkatan keteguhan SUS terhadap kebisingan dan mampatan adalah 9.6%, dan 1.7% tetapi terhadap putaran adalah -2.9%. Walau bagaimanapun keteguhan SUS berbanding dengan kebisingan, mampatan dan putaran telah dipertingkatkan dengan lebih baik bagi saiz blok 8×8, iaitu 21.3%, 18.9% dan 30.8%. Seterusnya, penilaian prestasi kerumitan masa CTF telah dianalisis menggunakan kes-kes bilangan kelompok yang berbeza dan dibandingkan dengan teknik *Lexicographical-sorting*. Apabila bilangan kelompok melebihi nilai ambang tertentu kerumitan masa CTF padanan telah dikurangkan dengan ketara. Kesimpulannya, keputusan uji kaji dan analisis matematik menunjukkan bahawa ciri SUS dengan blok algoritma CTF sepadan telah menghasilkan peningkatan yang ketara dari segi keteguhan dan kerumitan masa kepada bidang pengesanan rantau penduaan dalam sains forensik.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

BST	-	Binary Search Tree
C_ROT_P	-	Copy-Rotate-Paste
CF	-	Column Frequency
Coef	-	Coefficient
CP	-	Copy-Paste
CP_JPEG	-	Copy-Paste Jpeg Compression
CP_NOISY	-	Copy-Paste Noisy
CPFD	-	Copy-paste Forgery detection
CRM	-	Copy-Rotate-Move
CTF	-	Coarse-To-Fine
DCT	-	Discrete Cosine Transform
DFT	-	Discrete Fourier Transform
DRD	-	Duplicated Region Detection
DWT	-	Discrete Wavelet Transform
ESS	-	Efficient Subwindow Search
FC2010	-	Dataset from Faculty of Computing
FMT	-	Fourier Mellin Transform
FPR	-	False Positive Rate
HAF	-	High Accurate Feature
GHz	-	Giga hertz
IF	-	Image Forgery
IFD	-	Image Forgery Detection
IFDS	-	Image Forgery Detection System
K-D Tree	-	K dimensional tree
Lex	-	Lexicographical

LAF	-	Low Accurate Feature
MICC-F220	-	Dataset from Media Integration and Communication Center
PCA	-	Principal Component Analysis
PCT	-	Principal Component Transform
Q-Factor	-	Quality Factor
RF	-	Row Frequency
RGB	-	Red Green Blue
RQ	-	Research Question
SF	-	Spatial Frequency
SIFT	-	Scale Invariant Feature Transform
SUS	-	Spiral Unique Sequence
SVD	-	Singular Value Decomposition
TPR	-	True Positive Rate

LIST OF SYMBOLS

α	-	Number of blocks in Image
ρ	-	Feature Vector Dimension
$O(\,)$	-	Order of Time Complexity
ψ	-	Number of Clusters
ρ_1	-	Dimension of Low accurate feature
ρ_2	-	Dimension of High accurate feature
β	-	Average Number of Blocks in each cluster
b	-	Blocksize
T(n)	-	Complexity Function
$\vec{L}$	-	Low accurate Feature Vector
$\vec{H}$	-	High Accurate Feature vector
C_i	-	Cluster i
M	-	Height of Image
N	-	Width of Image
$d(\vec{x},\vec{y})$	-	Distance of two vectors x,y
$\emptyset$	-	Empty
θ	-	Threshold
$\in$	-	Member of
p	-	Perimeter
π	-	3.14
r	-	Radius
$\hat{r}$	-	Distance of the center to the side
Tr_i	-	Triangle i
Fsb_n	-	Feature sub-block n
R 10°	-	Rotation 10 degree
τ_{ψ}	-	Minimum threshold of the number of clusters

τ_{ρ_1}	-	Maximum threshold of the low accurate feature vector dimension
τ_{ρ_2}	-	Minimum threshold of the high accurate feature vector dimension
τ_{b}	-	Maximum threshold of the block size

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Multimedia forensics has become important in the last few years in the forensic science. This area includes audio forensic, video forensic and digital image forensic. Digital image forensics is a form of image analysis, which deals with the problem of certifying the authenticity of a picture, or its origin. It can be roughly subdivided into two categories: *Image source identification*, which aims to identify which device was used to capture an image (different models of scanner, digital camera, etc.) and *Image tampering detection*, to discover if an image has been intentionally modified by human intervention (Ardizzone and Mazzola, 2009). Existing digital image technologies provide very easy-to-use software and tools for editing digital images. Unfortunately, by these tools, an expert forger can fake the image invisible to the naked eye without leaving any visual tampering clues. This can, and does, reduce the reliability of the digital image.

Digital forgeries affect the social and legal systems, forensic investigations, intelligence services as well as security and surveillance systems. Digital image forgery detection systems are designed to discover evidence of tampering by scrutinizing the forgery's clues on the image. There are several proposed methods to explore faked image (Mahdian, 2010; Li, 2012; Chen, Lu *et al.*, 2013). Generally, image forgery detection could be divided in two categories: active and passive (blind). The performance of active methods simply can be done by data hiding approach via watermarking and digital signature approach. Another approach is the passive, which analyses forged images, to detect the traces of tampering without any former information about the image. To detect the traces of tampering, blind methods use the image function. In fact, the forgeries can bring into the image specific detectable changes (e.g., statistical changes). The forgery can be detected by classifying the textures of images using statistical measures and find discrepancy in those statistics between different portions of the image. At this point, however, it appears that such approaches will produce a large number of missed detections as well as false positives.

In the past decade, for the passive (blind) approach, several image forgery detection techniques have been proposed. The publications on passive image forgery detection fall into following categories: Duplicated Region Detection (DRD) (Fridrich, 2003; Popescu and Farid, 2004; Mahdian and Saic, 2007; Ryu, Lee *et al.*, 2010; Cao, Gao *et al.*, 2012; Chen, Lu *et al.*, 2013), Traces of the re-sampling detection (Popescu and Farid, 2003), Color filter array processing (Popescu and Farid, 2005), DCT coefficient analysis (Lin, He *et al.*, 2009), Noise inconsistencies detection (Lukas, Fridrich *et al.*, 2006; Mahdian, 2009), and Light inconsistency (Johnson and Farid, 2007). Duplicated region detection is one of the most common blind image forgery detection techniques, which identify copy-paste forgery. The basic model of DRD system includes the following steps: Overlapping blocks, feature extraction, matching step and forgery decision (Fridrich, 2003).

Copy-paste forgery is one of the most popular ways to change the image information semantics by cloning a portion or portions of an image into another place within the same image. This leads to changes in the semantic of image in two cases: concealing an object within the image and duplicating specific objects. This type of forgery brings into the image several near-duplicated image regions. It is important to note that duplicated regions mostly are not exactly alike, because the forger usually modifies the copied regions by some operations such as JPEG compression, adding noise, and rotation.

Based on the basic model proposed by Fridrich (Fridrich, 2003), each overlapping block is a square with b×b pixels. The square slide along the image from the upper left corner to the lower right corner based on the value of sliding window. In the feature extraction step, feature vector of each block is extracted as a row of two-dimensional array $BlockArray$. If the image suppose to be $M \times N$ and the each block includes $b \times b$ pixels, the number of overlapping blocks is called with α and it is calculated by $\alpha = (M - b + 1) \times (N - b + 1)$. The next main component of this model in duplication region detection area is block-matching. In this step, the system should compare each of the blocks in the matrix $BlockArray$ with others. The goal of this step can be finding the same blocks (probability forgery blocks) in the image. After running the matching step, it can be seen that there are a lot of same blocks in the image. It can make difficult to determine which ones are the real duplicated regions. The number of same block depends on the rate of accuracy in the block feature extraction method. Low false positive match result in this step may be reachable with a high accurate feature. However, it is clear that high accurate features will have high feature vector dimension and will increase the computational time.

1.2 Background of the Problem

One of the significant branches in the image forensic science is image forgery detection. Scope of this study is limited to the duplicated region detection as one of the approaches in image forgery detection area. This method can explore the copy-paste image forgeries. In this section, the issues and the problems of DRD systems are briefly presented. For categorizing the issues in copy-paste image forgery detection area, a scenario framework leading to the problems are introduced. The issues in the duplicated region detection can be classified into two main branches namely robustness and computational time.

The first issue is difficulty in finding a robust block feature against under-modification operations. This difficulty is due to changing the texture of the image after rotation, noising, compression, scaling, and blurring. Another reason leading to the first problem is difficulty for detecting the small size forgery. In fact, for detecting the small size forgery, the block size should be small. There are two approaches for the feature extraction in copy-paste image forgery detection as described following.

The first approach is block-based methods in which the image is divided to several overlapping blocks. The feature extractions in this group fall into four categories. These categories and related publications are listed as follow: moment-based feature extraction (Mahdian and Saic, 2007; Ryu, Lee *et al.*, 2010), dimensionality reduction-based methods (Popescu and Farid, 2004; Kang and Wei, 2008; Bashar, Noda *et al.*, 2010), intensity-based feature extraction (Luo, 2006; Lin, Wang *et al.*, 2009; Wang, Liu *et al.*, 2009; Bravo-Solorio and Nandi, 2011), and frequency domain-based features (Fridrich, 2003; Bayram, 2009; Huang, Lu *et al.*, 2011; Cao, Gao *et al.*, 2012). The second approach is keypoint-based method in which the feature extraction step should compute the features only on image regions with high entropy, without any image subdivision (Ledwich and Williams, 2004; Huang, Guo *et al.*, 2008; Li, Zhang *et al.*, 2009; Amerini, Ballan *et al.*, 2010; Bo, Junwen *et al.*, 2010; Pan and Siwei, 2010; Amerini, Ballan *et al.*, 2011; Shivakumar and Baboo, 2011).

The metrics for the robustness evaluation of DRD system include robustness against noise, jpeg compression, blurring, rotation, and scaling. However, the important measure is the size of the block that affect on the robustness against these metrics. For example, blur moment proposed in (Mahdian and Saic, 2007) only work with the blocksize more than 24×24. Most of the above methods do not work accurately with blocksize 8×8. In the most of proposed feature extraction methods in DRD area including DCT (Fridrich, 2003; Huang, Lu *et al.*, 2011; Cao, Gao *et al.*, 2012), PCA (Popescu and Farid, 2004), FMT (Bayram, 2009), Blur moments (Mahdian and Saic, 2007), Zernike moment (Ryu, Lee *et al.*, 2010), SIFT (Huang, Guo *et al.*, 2008; Pan and Siwei, 2010)), when the block size became smaller than specific threshold, the rate of false positives is increased (Popescu and Farid, 2004; Mahdian and Saic, 2007; Pan and Siwei, 2010). False positive is the wrong positive decision and the false negative is the wrong negative decision.

The second concerning issue is how to improve the high computational time (Zhang, 2008; Mahdian, 2010; Christlein, Riess *et al.*, 2012) and finding an effective way to match all huge numbers of overlapping blocks with a reasonable time complexity. The important reasons leading to high computational time include the huge number of overlapping blocks, blindly block matching algorithm, and large feature vector dimension. Sometimes also matching the blocks (or other shapes) of pixels would become infeasible with increasing size of the image. For example in (Mahdian and Saic, 2007), the system needs at least 40 minutes to detect the forgeries on 640×480 pixels image. In fact, computational time in duplicated region detection depends on the following metrics: image size, block size, number of blocks, feature vector dimension, method of feature extraction, and method of block matching.

The proposed approaches to improve the time complexity are categorized into three categories namely decreasing number of instances (blocks) (Huang, Guo *et al.*, 2008; Pan and Siwei, 2010), reducing feature vector dimension (Popescu and Farid, 2004; Kang and Wei, 2008; Bashar, Noda *et al.*, 2010), and improving block matching algorithm (Fridrich, 2003; Mahdian and Saic, 2007; Bayram, 2009; Lin, Wang *et al.*, 2009; Zhang, Guo *et al.*, 2010). In duplicated region detection, the most time consuming step is to find similar blocks in the matching step. Most of the previous works (Fridrich, 2003; Popescu and Farid, 2004; Luo, 2006; Ju, Zhou *et al.*, 2007; Li, Wu *et al.*, 2007; Myrna, Venkateshmurthy *et al.*, 2007; Zhang, Feng *et al.*, 2008; Bashar, Noda *et al.*, 2010; Bravo-Solorio and Nandi, 2011; Huang, Lu *et al.*, 2011; Michael Zimba, 2011; Cao, Gao *et al.*, 2012) applied Lexicographical-based model with time complexity $T(\alpha, \rho) \epsilon O(\rho\alpha \log_2 \alpha)$. This complexity is a function of feature vector dimension ρ and the number of blocks α. This function shows that the Lexicographical sorting is high computational complex. This is due to the blind similarity searching. This non-intelligent method performs several extra block-matching operations. The proposed methods have attempted to improve the computational time. However, the method of block matching needs yet more intelligence to make more improvement on performance in term of time complexity.

It is clear that improving the robustness needs a high accurate feature. However, high accurate feature extraction leads to increase the computational time of the system. The main reasons to this increscent consist of two things. The first one is extracting the robust feature is high computational complex. The second reason is that the robust feature should have high feature vector dimension. However, a high feature vector dimension extremely increases the time required in the block-matching step. Therefore, based on these two issues in duplicated region detection namely robustness and time complexity, the research questions, purpose, objectives and scope of the study are stated in the following sections.

1.3 Statement of the Problem

As mentioned in the problem background section, there are two fundamental and concerning issues in image forgery detection area namely extracting a discriminate robust block feature and improving computational complexity. The major specific challenge in robustness issue is to improve the robustness against geometrical transformation for small size blocks (Ryu, Lee *et al.*, 2010). The main idea to solve the former problem is to apply an adapted Archimedean spiral sequence (Lockwood, 1967). In addition, another specific challenge in time complexity issue is to improve computational time of block matching step, because of blindly block matching in similarity detection of DRD. In this study, the main idea to solve the later problem is to grant some intelligence to the block-matching step. The suggested method is Coarse-To-Fine approach using sequential block clustering to reduce the number of match operations. This method localizes the search space in block similarity detection. Based on mentioned issues and two primary ideas to solve the problems, the main research question is stated as follow:

"*How to design a fast and accurate copy-paste image forgery detection model using Archimedean spiral and coarse-to-fine approach?*"

In order to answer the main question of the research, additional research questions are required to be answered as the following:

i. How to adapt Archimedean spiral to be used as a robust feature extraction method in duplicated region detection?
ii. How to adapt a CTF-based block-matching algorithm in duplicated region detection?
iii. How to determine the time complexity function of CTF-based duplicated region detection?
iv. How to design an enhanced model for copy-paste image forgery detection?
v. How to implement the proposed enhanced model?
vi. What are the metrics in duplicated region detection to evaluate the accuracy and computational time?

1.4 Purpose of the Study

The aim of this study is to propose an enhanced copy-paste image forgery detection model for improving accuracy and computational time.

1.5 Objectives of the Study

Based on the research questions, the following objectives are defined in this research:

i. To propose a block feature extraction method based on a spatial domain feature to improve accuracy of the forgery detection.
ii. To propose a block-matching algorithm based on coarse-to-fine approach to improve the computational time.

iii. To propose an enhanced image forgery detection model by integrating proposed block feature extraction method and block matching algorithm.

1.6 Scope of the Study

The scopes of this study can be enumerated as follow:

i. Type of the forgery: Copy-paste image forgery or duplicated regions in the image.
ii. Image format: The default image format is JPG (RGB color image and gray scale).
iii. Image datasets: Images from MICC-F220 dataset, created at Media Integration and Communication Center in University of Florence, and FC2010 datasets created at Faculty of Computing in Universiti Teknologi Malaysia.

1.7 Significance of the Study

As digital crimes are increasing, the need for digital forensics also is increased. Nowadays, there is a wide-spread availability of multi-media data in the digital form. Hence, multimedia information systems are increasingly used in some areas such as: forensic investigation, criminal investigation, insurance, surveillance systems, intelligence services, and journalism. Digital forensics is utilized to conduct investigations into digital crimes or incidents. An image as an important and common digital multimedia is not safe with current advance technology. Image can be easily changed (forged) with today's editing software without leaving any obvious clue or traces. As a result, the output of this study can be applied to improve robustness and complexity of detection in modern and intelligent image forensic tools.

1.8 Contributions

The main contribution of this study is to propose an enhanced duplicated region detection model. This contribution consists three main parts as follow:

i. Proposing a discriminative robust feature extraction method namely SUS (Spiral Unique Sequence). The deliverable for this contribution is a robust feature extraction method based on Archimedean spiral.
ii. Proposing a CTF-based image block-matching algorithm for duplicated region detection. The deliverable for this contribution is a time-efficient block-matching algorithm based on sequential straightforward block clustering.
iii. Proposing an enhanced duplicated region detection model for copy-paste image forgery detection. The deliverable for this contribution is an integration of CTF-based block matching and SUS feature extraction in form of a model.

1.9 Organization of the Thesis

This chapter has presented the motivation of the research by reviewing the background of the study, as well as an outline of the purpose and objectives of the research. In addition, the potential contribution of this research has also been highlighted. This thesis is organized into seven main chapters. In the second chapter, the literature survey as initial survey in image forgery detection area is presented. In the last sections of Chapter 2, the categorization of the existing researches in the area of duplicated region detection based on two challenges were presented. In the Chapter 3, the research framework of the study including three main phases namely SUS feature extraction, coarse-toe-fine block matching, enhance model was proposed. In the Chapter 4, the proposed block feature extraction namely spiral unique sequence (SUS) was presented. The Chapter 5 proposed a coarse-to-fine block-matching algorithm. Chapter 6 will presented integration of two proposed methods, which mentioned in Chapter 4 and Chapter 5, in form of a new duplicated region detection model. Chapter 7 concludes the findings of this research, contributions, and future works.

REFERENCES

Abramowitz and Stegun (1972). "*Handbook of Mathematical Functions*," McGraw-Hill.

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

Ardizzone, E. and G. Mazzola (2009). "*Detection of duplicated regions in tampered digital images by bit-plane analysis*." Image Analysis and Processing–ICIAP 2009, Springer**:** 893-901.

Baldi, P. and K. Hornik (1989). "*Neural networks and principal component analysis: Learning from examples without local minima.*" Neural networks 2(1): 53-58.

Bashar, M., K. Noda, N. Ohnishi and K. Mori (2010). "*Exploring duplicated regions in natural images.*" IEEE Trans. Image Process.

Bayram, S. (2009). "*An efficient and robust method for detecting copy-move forgery*." IEEE International Conference on Acoustics, Speech and Signal Processing. Washington, DC, USA**:** 1053 - 1056.

Bayram , S. and Sencar (2008). "*A Survey of Copy-Move Forgery Detection Techniques.*" IEEE Western New York Image Processing Workshop.

Blanco, J. L., J. Gonzalez and J. A. FernÂ´andez-Madrigal (2010). "*An Experimental Comparison of Image Feature Detectors and Descriptors applied to Grid Map Matching*," Technical Report in Department of System Engineering and Automation.

Bo, X., W. Junwen, L. Guangjie and D. Yuewei (2010). "*Image copy-move forgery detection based on SURF*." Multimedia Information Networking and Security (MINES), 2010 International Conference on, IEEE**:** 889-892.

Bravo-Solorio, S. and A. K. Nandi (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., T. Gao, L. Fan and Q. Yang (2012). "*A robust detection algorithm for copy-move forgery in digital images.*" Forensic Science International 214(1): 33-43.

Chen, W., Y. Q. Shi and W. Su (2007). "*Image splicing detection using 2-D phase congruency and statistical moments of characteristic function.*" New Jersey Institute of Technology, Newark, NJ 07102, USA.

Choras, R. S. (2007). "*Image Feature Extraction Techniques and Their Applications for CBIR and Biometrics Systems.*" International Journal of Biology and Biomedical Engineering 1: 6-16.

Christlein, V., C. Riess, J. Jordan and E. Angelopoulou (2012). "*An Evaluation of Popular Copy-Move Forgery Detection Approaches.*" Transactions on Information Forensics and Security VOL. 7(NO. 6): 1841-1854.

Delattre, B., R. M. Heidemann, L. A. Crowe, J.-P. Vallée and J.-N. Hyacinthe (2010). "*Spiral demystified.*" Magnetic resonance imaging 28(6): 862-881.

Dresser, A. (2007). "*Photoshop image retoucher.*" http://www.redferret.net/?p=9145.

Elena Deza, M. M. D. (2009). *Encyclopedia of Distances - Book*, Springer.

Farid, H. (2004). "*Creating and detecting doctored and virtual images: Implications to the child pornography prevention act.*" *Department of Computer Science, Dartmouth College, TR2004-518 13.*

ForensicScientist, R. (2012). "*Forensic Science News.*" http://www.forensicsguy.com/benchnotes/real-life-csi-success-story/.

Fridrich, J. (2003). "*Detection of copy-move forgery in digital images.*" Proceedings of Digital Forensic Research Workshop.

FunnyPictures (2013). "*Walk Into the Club.*" http://www.killthehydra.com/memes/walk-into-the-club/.

Gopi, E. S. (2007). "*Digital image forgery detection using artificial neural network and independent component analysis.*" Applied Mathematics and Computation 194(2): 540-543.

Hu, M.-K. (1962). "*Visual pattern recognition by moment invariants.*" Information Theory, IRE Transactions on 8(2): 179-187.

Huang, H., Weiqiang Guo and Y. Zhang (2008). "*Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm.*" IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application.

Huang, Y., W. Lu, W. Sun and D. Long (2011). "*Improved DCT-based detection of copy-move forgery in images.*" Forensic Science International 206: 178-184.

Jing, L. and C. Shao (2012). "*Image Copy-Move Forgery Detecting Based on Local Invariant Feature.*" Journal of Multimedia 7(1): 90-97.

Johnson, M. K. and H. Farid (2007). "*Exposing digital forgeries in complex lighting environments.*" Ieee Transactions on Information Forensics and Security 2(3): 450-461.

Jolliffe, I. (2005). "*Principal component analysis*," Wiley Online Library.

Ju, S., J. Zhou and K. He (2007). "*An authentication method for copy areas of images*." Image and Graphics, 2007. ICIG 2007. Fourth International Conference on, IEEE**:** 303-306.

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

Kang, X. and S. Wei (2008). "*Identifying tampered regions using singular value decomposition in digital image forensics*." Computer Science and Software Engineering, 2008 International Conference on, IEEE. 3**:** 926-930.

Kim, K. I., M. O. Franz and B. Scholkopf (2005). "*Iterative kernel principal component analysis for image modeling.*" Pattern Analysis and Machine Intelligence, IEEE Transactions on 27(9): 1351-1366.

Ledwich, L. and S. Williams (2004). "*Reduced SIFT features for image retrieval and indoor localisation*." Australian Conference on Robotics and Automation. 322.

Li, G., Q. Wu, D. Tu and S. Sun. (2007). "*A Sorted Neighborhood Approach For Detecting Duplicated Regions In Image Forgeries Based On DWT And SVD.*" *IEEE*.

Li, S. and Y. Wang (2005). "*Multifocus Image Fusion Using Spatial Features and Support Vector Machine.*" Lecture Notes in Computer Science - Advances in Neural Networks – ISNN 2005, Springer Berlin / Heidelberg. 3497**:** 753-758.

Li, S. H., A. X. Zhang, Y. S. Zheng, T. Zhu and B. Jin (2009). "*Detection of copy-move image forgeries based on SIFT.*" Jiefangjun Ligong Daxue Xuebao/Journal of PLA University of Science and Technology (Natural Science Edition) 10(4): 339-343.

Lian, S., Dimitris Kanellopoulos and G. Ruffo (2008). "*Recent Advances in Multimedia Information System Security.*" Informatica is an international journal with its base in Europe 33, Number 1.

Lin, H. J., C. W. Wang and Y. T. Kao (2009). "*Fast copy-move forgery detection.*" WSEAS Transactions on Signal Processing 5: 188-197.

Lin, Z., J. He, X. Tang and C. K. Tang (2009). "*Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis.*" Pattern Recognition 42(11): 2492-2501.

listverse (2007). "*Top 15 Photoshopped Photos That Fooled Us All.*" http://listverse.com/2007/2010/2019/top-2015-manipulated-photographs/.

Lockwood, E. H. (1967). "*A book of curves*," Cambridge University Press.

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

Lukas, Fridrich and Goljan (2006). "*Detecting digital image forgeries using sensor pattern noise*." Proceedings of SPIE - The International Society for Optical Engineering. San Jose, CA. 6072.

Luo, W. (2006). "*Robust Detection of Region-Duplication Forgery in Digital Image.*" IEEE Computer Society Washington, DC, USA.

Mahdian, B. (2009). "*Using noise inconsistencies for blind image forensics.*" Image and Vision Computing 27: 1497-1503.

Mahdian, B. (2010). "*A bibliography on blind methods for identifying image forgery.*" Signal Processing: Image Communication, Elsevier 25: 389-399.

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

MICC-F220 (2011). "*Dataset MICC-F220 : Media Integration and Communication Center.*" http://carson.micc.unifi.it/downloads/MICC-F220.zip.

Michael Zimba, S. X. (2011). "*DWT-PCA (EVD) Based Copy-move Image Forgery Detection.*" International Journal of Digital Content Technology and its Applications Volume 5: 251-258.

Myrna, A., M. Venkateshmurthy and C. Patil (2007). "*Detection of region duplication forgery in digital images using wavelets and log-polar mapping.*" Conference on Computational Intelligence and Multimedia Applications, 2007. International Conference on, IEEE.

Nixon, M. and A. S. Aguado (2008). "*Feature Extraction and Image Processing,*" 2nd Edition. London, Elsevier.

Pan, X. and L. Siwei (2010). "*Region Duplication Detection Using Image Feature Matching.*" Information Forensics and Security, IEEE Transactions 5: 857-867.

Pitas, I. (2000). "*Digital Image Processing Algorithms and Applications*," John Wiley \& Sons, Inc. New York, NY, USA ©2000.

Popescu and H. Farid (2004). "*Exposing Digital Forgeries by Detecting Duplicated Image Regions*," TR2004-515, Dartmouth College, Computer Science.

Popescu and H. Farid (2005). "*Exposing digital forgeries in color filter array interpolated images.*" IEEE Transactions on Signal Processing 53(10 II): 3948-3959.

Popescu, A. (2004). "*Statistical Tools for Digital Image Forensics*." DARTMOUTH COLLEGE, Hanover, New Hampshire.

Popescu, A. and H. Farid (2003). *Exposing digital forgeries by detecting traces of re-sampling*.

Richard Neapolitan, K. N. (2011). "*Foundations of Algorithms",* Fourth Edition. Ontario, Jones & Bartlett Publishers.

Ryu, S.-J., M.-J. Lee and H.-K. Lee (2010). "*Detection of copy-rotate-move forgery using Zernike moments*." Information Hiding, Springer**:** 51-65.

Ryu, S.-J., M.-J. Lee and H.-K. Lee (2010). Detection of copy-rotate-move forgery using Zernike moments. *Information Hiding*, Springer.

Senjian, A., P. Peursum, L. Wanquan and S. Venkatesh (2009). "*Efficient algorithms for subwindow search in object detection and localization*." Computer Vision and Pattern Recognition, 2009. CVPR 2009. IEEE Conference**:** 264-271.

Sergois, T. and Koutroumbas (2009). "*Pattern Recognition"* - book - Fourth Edition. San diego, Elsevier.

Shao, H., T. Yu, M. Xu and W. Cui (2012). "*Image region duplication detection based on circular window expansion and phase correlation.*" Forensic Science International.

Sheng, Y. and H. H. Arsenault (1986). "*Experiments on pattern recognition using invariant Fourier-Mellin descriptors.*" *JOSA A* 3(6): 771-776.

Shivakumar, B. and L. D. S. S. Baboo (2011). "*Detection of region duplication forgery in digital images using SURF.*" *IJCSI International Journal of Computer Science Issues 8(4): 199-205.*

Taneja, I. J. (2012). "*Inequalities having Seven Means and Proportionality Relations.*" The Smithsonian/NASA Astrophysics Data System.

Videoforensicsonline (2000). "*Video Forensics Online.*" http://www.digital-reproductions.co.uk/.

Wang, J., G. Liu, H. Li, Y. Dai and Z. Wang (2009). "*Detection of image region duplication forgery using model with circle block.*" Multimedia Information Networking and Security, 2009. MINES'09. International Conference on, IEEE.

Wiedermann, J. (1981). "*The complexity of lexicographic sorting and searching.*" Applications of Mathematics Vol. 26: 432-436.

William Ford, W. R. T. (2005). "*Data structures with Java*," Pearson Education Inc.

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

Wu, W. R. and S. C. Wei (1996). "*Rotation and gray-scale transform-invariant texture classification using spiral resampling, subband decomposition, and hidden Markov model.*" Image Processing, IEEE Transactions on 5(10): 1423-1434.

Xiaoyuan, X., H. Guoqiang and M. Huaqing (2004). "*A novel algorithm for associative classification of image blocks*." Computer and Information Technology, 2004. CIT '04. The Fourth International Conference: 46-51.

Yang, Q.-C. and C.-L. Huang (2009). "*Copy-Move Forgery Detection in Digital Image.*" *Springer-Verlag Berlin Heidelberg 2009* 5879: 816-825.

Zhang, C., X. Guo and X. Cao (2010). "*Duplication Localization and Segmentation.*" Lecture Notes - Advances in Multimedia Information Processing - PCM 2010 in Computer Science., Springer Berlin - Heidelberg. 6297: 578-589.

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

Zhang, Z. (2008). "*A Survey on Passive-Blind Image Forgery by Doctor Method Detection*." Proceedings of the Seventh International Conference on Machine Learning and Cybernetics. Kunming, IEEE**:** 3463 - 3467.

Zhang, Z., Y. Zhou, J. Kang and Y. Ren (2008). "*Study of Image Splicing Detection.*" Springer-Verlag Berlin Heidelberg 2008: ICIC 2008, LNCS 5226, pp. 1103–1110,.