JPEG IMAGE TAMPERING DETECTION BASED ON BLOCKING ARTIFACTS

ALI EBRAHIMI

A dissertation submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computing
Universiti Teknologi Malaysia

JUNE 2013

Dedicated to my beloved father and the memory of my loving mother…

ACKNOWLEDGEMENT

My appreciation first of all goes to my supervisor, Associate Professor Dr. Subariah Ibrahim for the detailed guidance, encouragement and advice she has provided throughout this thesis. I have been extremely lucky to have a supervisor who cared about my work, and who responded to my questions and queries promptly. Without her continued support and patience, this dissertation would not have been the same as presented here.

Thanks to my classmates, for their companionship and encouragement from beginning to end. Special thanks to my friends, I would not have done it without the help and motivation from all of you.

I must express my gratitude to my family for always being there despite of the distance. Last but not the least, I would like to thank God for His blessings.

ABSTRACT

In the modern world, digital images play very important role in areas like insurance processing, intelligence services, surveillance systems and forensic investigation. After the advent of the digital medium, image forgery has become a threat. In today’s digital age, because of the availability of many image editing and processing tools it is possible to change the information represented by a digital image very easily without leaving any obvious traces of tampering. Since tampering of digital images has become so easy, integrity or authenticity of digital images has become a question, resulting in a need for robust and reliable tamper detection methods. One of the methods that allowed copied areas actual detection on doctored JPEG images is blocking artifacts method. This study analyzes the blocking artifacts method and then proposed a new method to improve it. The improvement enables the blocking artifacts method to detect manipulations that uses painting technique. The proposed method called a Marker algorithm was added to the blocking artifacts method proposed by Tralic, et al. (2012). The addition of this algorithm facilitates the detection process of the blocking artifacts method by making the tampered area more visible. Finally, this study evaluated the proposed method in detecting a tampered area by using the percentage of effective detection as a measure. The analysis shows that the proposed method is capable of making the tampered area more visible, thus improving the blocking artifacts method.

ABSTRAK

Di zaman moden ini, imej digital memainkan peranan yang sangat penting terutamanya dalam bidang pemprosesan insuran, servis perisikan, sistem pengawasan dan penyiasatan forensik. Dengan kehadiran media digital, pemalsuan imej menjadi ancaman yang semakin berleluasa. Di zaman digital kini, oleh kerana terdapat banyak produk penyuntingan dan pemprosesan imej, maklumat yang diwakili dalam imej digital boleh dilakukan dengan mudah tanpa meninggalkan apa-apa kesan yang ketara. Disebabkan, pengubahsuaian imej digital yang semakin, integrity atau kesahihan imej digital dipersoalankan, dengan itu kaedah pengesanan pengubahsuaian yang kukuh dan boleh dipercayai diperlukan. Salah satu kaedah yang dapat mengesan kawasan yang disalin pada imej JPEG yang telah diubahsuai ialah melalui kaedah pemblokan artifak. Kajian ini menganalisis kaedah artifak pemblokan tersebut dan kemudiannya mencadangkan satu kaedah baru untuk memperbaikinya. Pembaikan ini membolehkan kaedah artifak pemblokan mengesan manipulasi yang digunakan dengan teknik mengechat. Kaedah yang dicadangkan dipanggil algoritma Penanda ditambah kepada kaedah pemblokan yang di cadangkan oleh Tralic, et al. (2012). Penambahan algoritma ini memudahkan proses pengesanan kaedah artifak pemblokan dengan membuat kawasan yang diubahsuai lebih jelas. Akhir sekali, kajian ini menilai kaedah yang dicadangkan untuk mengesan kawasan yang diubahsuai dengan peratusan untuk menilai keberkesanan pengesanan. Analisis menunjukkan kaedah yang dicadangkan mampu membuat kawasan yang diubahsuai lebih jelas, dengan itu memperbaiki kaedah artifak pemblokan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ACRONYM	**MEANING**
JPEG	Joint Photographic Experts Group
DCT	Discrete Cosine Transform
BAG	Blocking Artifact Grid
HVS	Human Visual System
CFM	Color Filter Mosaic
CFA	Color Filter Array
LE	Local Effect
QF	Quality Factor

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

A digital image defines as two dimensional representations among a person, thing, art, place or data which is similar to the real world at 0s and 1s. The usage of digital image is extensively in the print media and the electronic media. The digital images have also extensive applications such as medical diagnosis, journalism, forensics, entertainment, commercial photography, education etc. The numerous applications which utilize digital images can be categorized as sensitive applications; for instance the base of a medical diagnosis is an image. Likewise the base of a judgment in a courtroom is on an image which provides court evidence.

After the digital medium image arrived, forgery has developed a threat. Previously analog images are used, the interference of images was actually difficult to do. However, in current time of digital age, digital images can be changed very easily without leaving any obvious tampering traces because of the availability of numerous image editing and processing tools. Consequently digital image tampering has become very easy and integrity/authenticity of digital images has become a question, resulting aimed at a robust and reliable tamper detection method is essentially required (Elwin *et al.*, 2010).

Tamper detection methods can be classified into two subcategories namely; active methods and passive methods. Active methods are dependent on watermarking and digital signature for validating an image. Active methods are used when we have some prior information about the image. In the perspective of Elwin, et al. (2010), such a method is out of work once the handling images are from unidentified or unreliable sources. Also, the digital watermark effectiveness and robustness has not testified yet among the image tampering detection. The third-party is similarly desirable towards the license watermarks. Therefore, the characteristic of passive image tampering detection is related to be more practical and significant. As considered by Wang, Dong, & Tan (2009), passive methods can verify the authenticity of digital images without any prior information, similar to embedding watermarks in original images.

Several passive detection methods have been proposed from different aspects. Trails detection can be used to detect whether an image covers certain doctored trail. Consistency verification may be used to check if an image contains some special scripts that originated from claimed device. If an image is reasonable to nature phenomena, Rationality judgment is to verify it. According to W. Li, Yuan, & Yu (2009), every detection method affected on some kind of tampering attempts, while tampering an image has been still easier to do than detecting a tampered image.

Recently, the greatest phases of these methods need the doubtful uncompressed and high superiority images, although the JPEG standard is an image format that widely is used and utilizes a lossy compression. As considered by Tralic, Petrovic, & Grgic (2012), there are numerous different methods in JPEG image tampering detection like double quantization affect hidden amongst the discrete cosine transform (DCT) coefficients or checking the consistency of quantization remainders. Blocking artifacts method is one of those techniques that was implemented through extracting and analyzing blocking artifact grids (BAGs), introduced by block processing during JPEG compression. The analysis was based on the fact that BAGs typically mismatch after execution of copy-paste processes (Tralic *et al.*, 2012).

1.2 Background of the Problem

In the modern world, the role of digital images is significant in different areas such as insurance processing, intelligence services, forensic investigation, surveillance systems, journalism, and medical imaging; nevertheless the major obligation to accept that what we see refers to the authentic images. According to Kumar *et al.* (2011), by the technology advancement and the obtainability of the fast computing incomes, it is not so problematic to operate or forge the digital images. Some software tools availability makes the problematic phase more threatening; In spite of no technique available to detect all kinds of tampering accurately.

There are several types of available digital images tampering. Copy-paste tampering and painting tampering are two of the most common used methods. Active and passive methods are the techniques have been recommended to detect these two kinds of the forgery. Tralic, *et al.* (2012) considered that the key subject through the active approach is its application in modern devices that typically do not include any module related to digital watermarking or signatures. Additionally, the efficiency and robustness of the digital watermark for detecting image tampering are not certified till now. To license watermarks, the third-party is necessary too. On the other hand a passive method involves checking the integrity of an image. As opposite to digital watermarking, which requires a digital watermark to be embedded for later authentication, passive forensic analysis infers forensic information and implications from the contents without requiring extra information, such as digital watermark, to be embedded in advance (Li, 2009). One of the passive methods allowed copied areas actual detection on doctored JPEG images is JPEG image tampering detection through blocking artifacts proposed by Tralic *et al.* (2012). This method includes two steps: in the first step, a BAG extraction algorithm is proposed to create a BAG image and in the second step, an analysis process is suggested to detect a copy-pasted area via that BAG image. This analysis of BAG mismatching is performed base on judging with human eyes that could be subjective and different based on persons' understanding, background and ability to judge.

1.3 Problem Statement

Digital images are widely used in important areas like forensic investigation. On the other hand, there are numerous tampering methods to manipulate an image easily such as copy-paste tampering and painting tampering. The basic requirement to ensure that the content of an image is not manipulated is image authentication. The blocking artifacts method was proposed by Tralic *et al.* (2012) in order to authenticate a JPEG image. The proposed method can detect the copy-pasted areas in a JPEG image efficiently. However, it is being unable to detect painted areas in a tampered JPEG image. Moreover, the aforementioned method utilizes a BAG analysis process to detect tampered areas in a JPEG image which is performed base on judging with human eyes. Though, it is not easy to only judge with human eyes whether a JPEG image is tampered or not. In addition, a computer analysis can indicate the doctored areas much more accurate than analyzing with human eyes. These challenges threaten the authenticity of the blocking artifacts method.

1.4 Research Questions

The main questions this research motivates to answer are as follows:

i. What are the appropriate passive methods for detecting the tampered images?

ii. How to detect a painted JPEG image via the blocking artifacts method in order to improve the previous method?

iii. How much is the performance of the proposed method to detect a tampered JPEG image?

1.5 Project Aim

The project aim is to improve the blocking artifacts method proposed by Tralic *et al.* (2012) through detecting a painted area in JPEG images. To achieve this goal, a suitable BAG extraction algorithm will be used. Then, an efficient method will be proposed to detect a painted JPEG image. Finally, the proposed method will be evaluated to gauge its ability in detecting the painted JPEG images

1.6 Project Objectives

The objectives of this project are as follows:

i. To study the passive methods of image tampering detection especially Blocking Artifacts method

ii. To enhance checking the integrity of a JPEG image in the Blocking Artifacts method

iii. To analyze the performance of the proposed approach

1.7 Project Scope

The scope of the project includes the following areas:

i. The work is based on blocking artifacts method proposed by Tralic *et al.* (2012)

ii. Copy-paste and painting tampering detection

iii. Implementation with MATLAB

1.8 Organization of Thesis

This research consists of six chapters. The first chapter begins with an overview of the image tampering detection issues followed by the background of the problem. Some threats of the image forgery and the related detection methods in image forensics are mentioned. The problem statement is declared and the project aim is stated. Then the objectives and scope of the project are considered. In the next chapter, the literature review of the project is presented, which focuses on Passive detection methods that have been using for discovering tampered images. In Chapter 3, the research methodology and its three phases which been applied to achieve the objectives of the study are discussed. After that, Chapter 4 explains the design of proposed method in details. The proposed method includes two algorithms which are BAG extraction and Marker algorithm. In Chapter 5, the output results and the evaluation of the new method are discussed. Finally, the overall project is concluded in Chapter 6. The research achievements, contribution and some suggestions for future works are provided in the final chapter.

REFERENCES

Ahmed, N., Natarajan, T., and Rao, K. R. (1974). Discrete Cosine Transform. *IEEE Transactions on Computers, C-23*(1), 90-93.

De Queiroz, R. L. (1998). Processing JPEG-compressed images and documents. *IEEE Transactions on Image Processing, 7*(12), 1661-1672.

Dirik, A. E., and Memon, N. (2009). *Image tamper detection based on demosaicing artifacts.* Paper presented at the 2009 IEEE International Conference on Image Processing, ICIP 2009, November 7, 2009 - November 12, 2009, Cairo, Egypt, 1497-1500.

Elwin, G. R., Aditya, T. S., and Madhu Shankar, S. (2010). *Survey on passive methods of image tampering detection.* Paper presented at the 2010 International Conference on Communication and Computational Intelligence, INCOCCI-2010, December 27, 2010 - December 29, 2010, Perundurai, Erode, India, 431-436.

He, J., Lin, Z., Wang, L., and Tang, X. (2006). Detecting Doctored JPEG Images Via DCT Coefficient Analysis. *ECCV 2006, 3953*, 423-435.

ITU. (1992). T.81: INTERNATIONAL TELECOMMUNICATION UNION.

Kumar, S., Das, P. K., Shally, and Mukherjee, S. (2011). Copy-Move Forgery Detection in Digital Images: Progress and Challenges. *International Journal on Computer Science and Engineering 3*.

Li, C. T. (2009). Detection of Block Artifacts for Digital Forensic Analysis. *IEEE International Conference on Image Processing, 8*, 173-178.

Li, W., Yu, N., and Yuan, Y. (2008). *Doctored JPEG image detection.* Paper presented at the 2008 IEEE International Conference on Multimedia and Expo, ICME 2008, June 23, 2008 - June 26, 2008, Hannover, Germany, 253-256.

Li, W., Yuan, Y., and Yu, N. (2009). Passive detection of doctored JPEG image via block artifact grid extraction. *Signal Processing, Elsevier, 89*(9), 1821-1829.

Lin, S. D., and Wu, T. (2011). *An integrated technique for splicing and copy-move forgery image detection.* Paper presented at the 4th International Congress on Image and Signal Processing, CISP 2011, October 15, 2011 - October 17, 2011, Shanghai, China, 1086-1090.

Mahdian, B., and Saic, S. (2009a). A Cyclostationarity Analysis Applied to Scaled Images. *Lecture Notes in Computer Science, 5864/2009*, 683-690.

Mahdian, B., and Saic, S. (2009b). *Detection and description of geometrically transformed digital images.* Paper presented at the Media Forensics and Security, January 19, 2009 - January 21, 2009, San Jose, CA, United states, The Society for Imaging Science and Technology (IS and T); The International Society for Optical Engineering (SPIE).

Mahdian, B., and Saic, S. (2009c). Using noise inconsistencies for blind image forensics. *Image and Vision Computing, 27*(10), 1497-1503.

Plonka, G., and Tasche, M. (2005). Fast and numerically stable algorithms for discrete cosine transforms. *Linear Algebra and its Applications, 394*(0), 309-345.

Qu, Z., Qiu, G., and Huang, J. (2009). *Detect digital image splicing with visual cues.* Paper presented at the 11th International Workshop on Information Hiding, IH 2009, June 8, 2009 - June 10, 2009, Darmstadt, Germany, 247-261.

Tralic, D., Petrovic, J., and Grgic, S. (2012). *JPEG image tampering detection using blocking artifacts. 19th International Conference on Systems, Signals and Image Processing (IWSSIP)*, 5-8.

USC-SIPI Image Database. from http://sipi.usc.edu/database/

Wang, W., Dong, J., and Tan, T. (2009). *A survey of passive image tampering detection.* Paper presented at the 8th International Workshop on Digital Watermarking, IWDW 2009, August 24, 2009 - August 26, 2009, Guildford, United kingdom, 308-322.

Wu, M., and Liu, B. (1998). Watermarking for image authentication. *IEEE International Conference on Image Processing, 2*, 437-441.

Zhulong, L., Xianghua, L., and Yuqian, Z. (2011). *Passive detection of copy-paste tampering for digital image forensics.* Paper presented at the 2011 4th International Conference on Intelligent Computation Technology and Automation, ICICTA 2011, March 28, 2011 - March 29, 2011, Shenzhen, Guangdong, China, 649-652.