COARSE-TO-FINE COPY-MOVE IMAGE FORGERY DETECTION METHOD BASED ON DISCRETE COSINE TRANSFORM

MAS ELYNA BINTI MOHD AZOL

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

Faculty of Computing
Universiti Teknologi Malaysia

AUGUST 2016

To my dear beloved husband
for his endless love and support

ACKNOWLEDGEMENT

I would first like to thank my dissertation advisor Prof. Dr. Ghazali Sulong, for consistently allowed this to be my own work, but steered me in the right the direction whenever he thought I needed it. I really appreciate his willingness to give a helpful hand whenever it is required.

Besides my advisor, I would like to acknowledge the members of the Faculty of Computing, Universiti Teknologi Malaysia especially my study program coordinator, Dr. Mohamad Shukor Talib for his helpful advice towards completing this research. I would also like to acknowledge Dr. Farhan Mohamed as the second reader of this thesis, and I am gratefully indebted to him for his very precious comments on this thesis.

My sincere thanks also go to my dear best friend, Noor Baidura Ismail as well as my sister, Mas Elyza Mohd Azol for providing me with valuable help whenever needed during the period of my study.

Finally, I must express my very profound gratitude to my parents and to my husband, Dr. Mior Azrizal M. Ibrahim for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

ABSTRACT

Digital image forgery has become a serious problem in the present society. As the world is advancing in the information and communication technology, it has become more crucial for researchers to take part in overcoming the wide-spreading digital image forgery to prove an image authenticity especially when the legislative field is involved. Copy-move forgery is a type of image forgery where one part of an image is copied and pasted in other regions of the same image, and it is one of the most common image forgeries to conceal some information in the original image. There are numerous techniques available to detect copy-move forgeries which each of them have their own advantages and drawbacks. Discrete Cosine Transform (DCT) is a powerful algorithm developed as a method to detect copy-move forgery which is well known for its detection efficiency. However, the detection rate relies intensely on the size of block used. Small block size is known for its ability to detect fine cloned objects, but the drawback is it produces too many false positive and requires high execution time. In this research, a method to overcome the weaknesses of using small block size by applying the coarse-to-fine approach with the two-tier process is proposed. The proposed method is evaluated on fifteen forged images on the CoMoFoD dataset. The results demonstrated that the proposed method is able to achieve high precision and recall rate of over 90% as well as improves the computation time by reducing the overall duration of forgery detection up to 73% compared to the traditional DCT method using small block size. Therefore, these findings validate that the proposed method offers a trade-off between accuracy and runtime.

ABSTRAK

Pemalsuan imej digital sudah menjadi masalah yang semakin parah dalam masyarakat masa kini. Seiring dengan kemajuan teknologi informasi dan komunikasi, ia telah menjadi sesuatu yang sangat mustahak pagi para penyelidik untuk mengambil bahagian dalam mengatasi pemalsuan imej digital yang semakin berleluasa bagi memastikan keaslian sesuatu imej terutamanya apabila melibatkan bidang perundangan. Pemalsuan salin-pindah adalah sejenis pemalsuan imej yang mana satu bahagian dalam imej disalin dan ditampal pada bahagian lain dalam imej yang sama, dan ia adalah salah satu daripada pemalsuan imej yang paling biasa bagi menyembunyikan sebahagian maklumat dalam imej digital. Terdapat pelbagai teknik yang didapati berupaya mengesan pemalsuan salin-pindah yang mana setiap satunya mempunyai kelebihan dan kekurangan masing-masing. Pengubahan Kosinus Diskret (DCT) adalah algoritma berkuasa yang dibangunkan sebagai satu kaedah bagi mengesan pemalsuan salin-pindah yang telah dikenali atas kemampuan keberkesanan pengesanannya. Walaubagaimanapun, kadar pengesanan adalah sangat bergantung kepada saiz blok yang digunakan. Blok bersaiz kecil telah dikenali atas kemampuan untuk mengesan objek klon yang lebih halus, namun kelemahannya ialah ia menghasilkan terlalu banyak positif palsu dan memerlukan waktu perlaksanaan yang tinggi. Dalam kajian ini, satu kaedah untuk mengatasi kelemahan menggunakan blok kecil dengan mengaplikasikan kaedah kasar-ke-halus dengan pemprosesan dwi-peringkat telah diusulkan. Kaedah yang diusulkan telah dinilai ke atas lima belas imej yang telah dipalsukan dari set data CoMoFod. Keputusan menunjukkan bahawa kaedah yang diusulkan mampu untuk mencapai kadar ketepatan dan pemanggilan semula yang tinggi melebihi 90% di samping menambah baik waktu perlaksanaan dengan mengurangkan jangkamasa keseluruhan bagi mengesan pemalsuan sehingga 73% berbanding kaedah DCT biasa menggunakan blok bersaiz kecil, yang mana mengesahkan bahawa kaedah yang diusulkan menawarkan imbalan antara ketepatan dan waktu larian.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

BLUR	Blur Moment Invariants
CMFD	Copy-Move Forgery Detection
CoMoFoD	Copy-Move Forgery Detection Database
DCT	Discrete Cosine Transform
DWT	Discrete Wavelet Transform
FMT	Fourier Mellin Transform
HU	Hu Moment
LBP	Local Binary Pattern
PCA	Principal Component Analysis
PNG	Portable Network Graphics
RGB	Red, Green, Blue Image Components
SIFT	Scale Invariant Feature Transform
SURF	Speed Up Robust Features
SVD	Singular Value Decomposition
ZERNIKE	Zernike Moment

LIST OF SYMBOLS

A	DCT Matrix Table
B	Block Size
C	Shift Vector Counter
F_k	DCT Coefficient of 1D DCT Matrix
F_N	False Negative
F_P	True Negative
$F_{u,v}$	DCT Coefficient of 2D DCT Matrix
G	Copy-move Quantity Threshold
I	Grayscale Image
i,j	Matching Blocks Positions
M	Length of Picture
N	Width of Picture
N_b	Number of Blocks
p	Precision
Q	Quantization Matrix
Q'_8	8×8 Enlarged Quantization Matrix
r	Recall
R,G,B	Red, Green, Blue Color Channel
s	Shift Vector
T	Detected Pixels Threshold
T_P	True Positive

CHAPTER 1

INTRODUCTION

1.1 Overview

In this current era of science and technology, it can be clearly observed that the digital images are very widely used and distributed, thanks to the emerging usage of smart phones equipped with digital camera and the increasing popularity of the social media which make it possible for an image to distribute worldwide within seconds. This situation however, promotes the questioning integrity of the digital imagery which is undoubtedly vulnerable to the act of forgery. This act of forgery or tempering is also a threat to society as it may be part of the cause to the act of defamation. Therefore, it is essential for the contribution of research in the area of image forgery as well as the promising area of digital forensics.

The fundamental concept of image forgery is the digital manipulation of pictures with the aim of distorting some information in them. There are several types of image forgeries which include copy-move (or cloning), splicing (or cut-and-paste) technique, and image resampling. Generally, the digital image forgery detection techniques can be categorized into two types; namely active and passive (or blind) techniques. In active method, the digital watermark is embedded into the image in order for it to be available for tracing of authentication, if later questioned. However, the glaring flaw of this technique is the watermark needs to be inserted at the time of recording, which limits the approach to specially equipped digital cameras (H. Farid, 2009). On the other hand, the passive method does not require any prior information about the source image. These approaches manipulates the statistical changes in the forged digital image assuming that there are some marks left by the camera during creation, and these marks can be used to trace any forgery attack.

1.2 Problem Background

The growth of the refined techniques for digital image forgery as well as the diminishing cost to obtain a high quality digital image has made it easy for anyone to manipulate a digital image easily without leaving any visible clues. One way to ensure that the image is not tempered is by authentication. Various techniques has been proposed to overcome the issues of image forgery, by which most methods are extending and improving the algorithm of the previous by mainly focusing on enhancing the accuracy, efficiency and reliability.

Image forgery detection can be categorized into two main clusters, namely active and passive (or blind) methods. Active methods are basically done by placing the watermarks or digital signatures in order for it to be feasible of authentication. The glaring flaw of this technique is the need of pre-processing of the raw data which therefore are often considered as an impractical practice. As an alternative, the passive method is more likely regard as a better forgery detection system as it requires no pre-processing in order to identify tempering. This type of method which is also known as non-intrusive technique, utilizes the intrinsic characteristic traces of image to detect the suspicious forged regions (S. D. Lin and Tszan, 2011).

There are a number of types of tempering that can be detected which come in interest of image forensics, which are splicing, retouching, resampling, and copy-move forgery. Copy-move forgery can be further categorized into two types, block-based and keypoint based methods (Thajeel and Sulong, 2013). In block-based method, the image is divided into several overlapping or non-overlapping blocks which later compared to each other to detect the matching blocks. Several researches have been utilizing this type of method which approached can be identified as moment-based, dimensionally reduction based, and frequency-based methods. On the other hand, the keypoint based method is trying to detect the copy-move forgery from the entire image by extracting the point of interest as features for detection.

1.3 Problem Statement

The used of quantized Discrete Cosine Transform (DCT) for the detection of copy-move forgery was introduced by Fridrich *et al.* (2003). In their approach, the image was divided into several overlapping blocks of the same size to extract the DCT coefficients as features. Then, lexicographical sorting was used to reduce the computational complexity to detect the duplicated regions and shift vectors are used to find the matching of copied blocks.

This method is widely used in detecting image forgery with various enhancement of the algorithm by many researchers. Nevertheless, there are still rooms for improvement as the accuracy and performance are taken into considerations. The advantage of using DCT as a feature descriptor is the simplicity and the relative reduction in the feature vector size (Al-Qershi and Khoo, 2013). It has proven to be robust to post processing operations, such as additive noise, retouching, and JPEG compression.

As other common techniques of detecting copy-move forgery, the robustness and computational complexity involved in the detection usually depends on the parameters used in the implementation of the detection algorithm. In DCT copy-move image forgery detection (CMFD) algorithm, a few parameters are used to determine the sensitivity of the detection program such as the overlapping block size, matching pixel occurrence threshold, and the quantization matrix. The overlapping block size is one of the most crucial parameter in determining the quality of detection. Large block size usage will result in visually adequate detection given that the size of copy-move is larger than the block itself, but it is insufficient to be used when detail of the object is needed or when the object is significantly tiny. In contrast, applying small overlapping block size can result in a more detail detection. However, it will also result in too many false positive result and slow matching rate. According to Gupta *et al.* (2013) the computation time raised when the size of block used is reduced, while the efficiency of correct forgery detection decreased and they recommended keeping the block size small for detection robustness.

Giving the advantage of using the small block size, this research aims to overcome the drawbacks, in terms of increasing the accuracy of the copy-move forgery detection with reduced false-matching rate, and also intends to enhance the performance of the copy-move detection which is to reduce the computational cost of matching, compared to the traditional DCT copy-move forgery detection algorithm. In this study, we proposed the utilization of coarse-to-fine approach which consists of two tier feature extractions and refinement of the detection areas.

1.4 Research Aim

The project aim is to propose a new copy-move forgery detection using a coarse-to-fine approach based on Discrete Cosine Transform descriptor to enhance the accuracy rate and execution time.

1.5 Research Objectives

The project objectives are as follows:

i. To propose a two-tier detection method using DCT algorithm
ii. To implement the proposed method using the CoMoFoD dataset

iii. To analyze the effectiveness of the proposed method in terms of precision, recall, the combination of precision and recall, and runtime factor.

1.6 Research Scope

The scope of the project will include:

i. The work based on the forgery detection based on DCT method by Fridrich *et al.* (2003)

ii. Copy-move forgery detection on images with plain copy-move objects and no post-processing attacks or forgery object overlaps

iii. Effectiveness of the proposed method is only compared to the implementation of the traditional DCT method using large block size of 16x16 and the small block size of 2x2 and not with any other block sizes in between

iv. The implementation of the method is using MATLAB on Windows platform

1.7 Organization of Dissertation

The rest of this dissertation is organized as follows. Chapter 2 discussed the literature review which closely related to the existing work in the field of study involved. In chapter 3, the methodology of the conducted research is explained in terms of its framework. In Chapter 4, the algorithm of the proposed method is described in details. Chapter 5 presents the results of the proposed method when applied on the standard dataset of copy-move forged images. Chapter 6 concludes this dissertation.

REFERENCES

Al-Qershi, O. M., and Khoo, B. E. (2013). Passive detection of copy-move forgery in digital images: State-of-the-art. *Forensic Science International. 231*(1), 284-295.

Ali Qureshi, M., and Deriche, M. (2014). *A review on copy move image forgery detection techniques.* Multi-Conference on Systems, Signals & Devices (SSD), 2014 11th International. 11-14 Feb. 2014. 1-5

AlSawadi, M., Muhammad, G., Hussain, M., and Bebis, G. (2013). *Copy-Move Image Forgery Detection Using Local Binary Pattern and Neighborhood Clustering.* Modelling Symposium (EMS), 2013 European. 20-22 Nov. 2013. 249-254

Anand, V., Hashmi, M. F., and Keskar, A. G. (2014). A copy move forgery detection to overcome sustained attacks using dyadic wavelet transform and sift methods *Intelligent Information and Database Systems* (pp. 530-542): Springer.

Bayram, S., Sencar, H. T., and Memon, N. (2008). *A survey of copy-move forgery detection techniques.* IEEE Western New York Image Processing Workshop. Citeseer, 538-542

Bayram, S., Sencar, H. T., and Memon, N. (2009). *An efficient and robust method for detecting copy-move forgery.* Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on. 19-24 April 2009. 1053-1056

Bo, X., Junwen, W., Guangjie, L., and Yuewei, D. *Image Copy-Move Forgery Detection Based on SURF.* 2010. 889-892

Bravo-Solorio, S., and 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.

Chihaoui, T., Bourouis, S., and Hamrouni, K. (2014). *Copy-move image forgery detection based on SIFT descriptors and SVD-matching.* Advanced

Technologies for Signal and Image Processing (ATSIP), 2014 1st International Conference on. 17-19 March 2014. 125-129

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

Farid, A., and Popescu, A. (2004). Exposing digital forgeries by detecting duplicated image regions: Technical Report, TR2004-515, Department of Computer Science, Dartmouth College, Hanover, New Hampshire.

Farid, H. (2009). Image forgery detection. *Signal Processing Magazine, IEEE. 26*(2), 16-25.

Fridrich, A. J., Soukal, B. D., and Lukáš, A. J. (2003). *Detection of copy-move forgery in digital images.* in Proceedings of Digital Forensic Research Workshop. Citeseer,

Gharibi, F., RavanJamjah, J., Akhlaghian, F., Azami, B. Z., and Alirezaie, J. (2011). *Robust detection of copy-move forgery using texture features.* Electrical Engineering (ICEE), 2011 19th Iranian Conference on. 17-19 May 2011. 1-4

Ghorbani, M., Firouzmand, M., and Faraahi, A. *DWT-DCT (QCD) based copy-move image forgery detection.* 2011. 1-4

Gupta, A., Saxena, N., and Vasistha, S. (2013). Detecting Copy move Forgery using DCT. *International Journal of Scientific and Research Publications. 3*(5).

Hailing, H., Weiqiang, G., and Yu, Z. (2008). *Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm.* Computational Intelligence and Industrial Application, 2008. PACIIA '08. Pacific-Asia Workshop on. 19-20 Dec. 2008. 272-276

Huang, H. L., Guo, W. Q., and Zhang, Y. (2008). Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm. *Paciia: 2008 Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Vols 1-3, Proceedings.* 1241-1245.

Kang, X., Kang, X., Wei, S., and Wei, S. *Identifying Tampered Regions Using Singular Value Decomposition in Digital Image Forensics.* 2008. IEEE, 926-930

Li, G., Wu, Q., Tu, D., and Sun, S. (2007). *A Sorted Neighborhood Approach for Detecting Duplicated Regions in Image Forgeries Based on DWT and SVD*. 2007. IEEE, 1750-1753

Li, L., Li, S., Zhu, H., Chu, S.-C., Roddick, J. F., and Pan, J.-S. (2013). An efficient scheme for detecting copy-move forged images by local binary patterns. *Journal of Information Hiding and Multimedia Signal Processing*. *4*(1), 46-56.

Li, L. D., Li, S. S., and Wang, J. (2012). Copy-Move Forgery Detection Based on PHT. *Proceedings of the 2012 World Congress on Information and Communication Technologies*. 1061-1065.

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

Lin, S. D., and Tszan, W. (2011). *An integrated technique for splicing and copy-move forgery image detection*. Image and Signal Processing (CISP), 2011 4th International Congress on. 15-17 Oct. 2011. 1086-1090

Luo, W.-Q., Huang, J.-W., and Qiu, G.-P. (2007). Robust detection of region-duplication forgery in digital image. *Jisuanji Xuebao/Chinese Journal of Computers*. *30*(11), 1998-2007.

Mahdian, B., and Saic, S. (2007). Detection of copy-move forgery using a method based on blur moment invariants. *Forensic Science International (Online)*. *171*(2), 180-189.

Mahdian, B., and Saic, S. (2007). Detection of copy-move forgery using a method based on blur moment invariants. *Forensic Science International*. *171*(2-3), 180-189.

Mohamadian, Z., and Pouyan, A. A. *Detection of Duplication Forgery in Digital Images in Uniform and Non-uniform Regions*. 2013. IEEE, 455-460

Muhammad, N., Hussain, M., Muhammad, G., and Bebis, G. (2011). *Copy-Move Forgery Detection Using Dyadic Wavelet Transform*. Computer Graphics, Imaging and Visualization (CGIV), 2011 Eighth International Conference on. 17-19 Aug. 2011. 103-108

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

Ryu, S.-J., Lee, M.-J., and Lee, H.-K. (2010). Detection of Copy-Rotate-Move Forgery Using Zernike Moments (Vol. 6387, pp. 51-65). Berlin, Heidelberg: Springer Berlin Heidelberg.

Singh, A. B., Barma, S. D., and Singh, K. M. (2013). Review of copy-move forgery detection of images using discrete cosine transform. *International Journal of Computer Applications. 84*(15).

Sunil, K., Jagan, D., and Shaktidev, M. (2014). *DCT-PCA based method for copy-move forgery detection.* ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-Vol II. Springer, 577-583

Thajeel, S. A., and Sulong, G. B. (2013). STATE OF THE ART OF COPY-MOVE FORGERY DETECTION TECHNIQUES: A REVIEW. *International Journal of Computer Science Issues (IJCSI). 10*(6).

Tralic, D., Zupancic, I., Grgic, S., and Grgic, M. (2013). *CoMoFoD—New database for copy-move forgery detection.* ELMAR, 2013 55th International Symposium. IEEE, 49-54

Ustubioglu, B., Ulutas, G., Ulutas, M., Nabiyev, V., and Ustubioglu, A. (2016). LBP-DCT Based Copy Move Forgery Detection Algorithm *Information Sciences and Systems 2015* (pp. 127-136): Springer.

Wang, J.-W., Liu, G.-J., Zhang, Z., Dai, Y.-W., and Wang, Z.-Q. (2009). Fast and robust forensics for image region-duplication forgery. *Zidonghua Xuebao/ Acta Automatica Sinica. 35*(12), 1488-1495.

Yang, J., Ran, P., Xiao, D., and Tan, J. (2013). Digital image forgery forensics by using undecimated dyadic wavelet transform and Zernike moments. *Journal of Computational Information Systems. 9*(16), 6399-6408.

Yang, Y., Yixu, S., Fangwen, Z., Zhaozhou, F., Yue, M., and Jiaxin, W. (2009). *A High-Precision Localization Algorithm by Improved SIFT Key-Points.* Image and Signal Processing, 2009. CISP '09. 2nd International Congress on. 17-19 Oct. 2009. 1-6

Zhang, T., and Wang, R.-d. (2009). *Copy-Move Forgery Detection Based on SVD in Digital Image*. 2009. 1-5

Zhao, J., and Guo, J. (2013). Passive forensics for copy-move image forgery using a method based on DCT and SVD. *Forensic Science International.* *233*(1), 158-166.

Zimba, M., and Xingming, S. (2011). DWT-PCA (EVD) based copy-move image forgery detection. *International Journal of Digital Content Technology and its Applications.* *5*(1), 251-258.