IMAGE FORENSIC FOR DIGITAL IMAGE COPY MOVE FORGERY DETECTION

YEAP YONG YEW

A project report submitted in partial fulfilment of the
requirements for the award of the degree of
Master of Engineering (Computer and Microelectronic Systems)

Faculty of Electrical Engineering
Universiti Teknologi Malaysia

JANUARY 2018

For my beloved parents, aunt, sister and family members.

ACKNOWLEDGEMENT

Firstly, I would also like to express my deepest gratitude to my supervisor, Dr. Usman Ullah Sheikh for his support and guidance. Dr. Usman has been instrumental in the completion of the research by providing timely advice and feedback that ensured that the research is of high quality. Furthermore, I would like to thank Dr. Usman for his frequent trips to Penang for sync up and research discussion purposes. The research would not have been possible without Dr. Usman's assistance.

I would like to recognize and thank the panel of judges, namely Associate Professor Muhammad Mun'im Ahmad Zabidi and Dr. Ab Al Hadi Ab Rahman for their constructive feedback during the presentation. The feedback is critical as it enhances the research quality.

Lastly, I would like to thank my family members, especially my parents, aunt and sister, who have been nothing but supportive of me. They were understanding and constantly showered me with words of encouragement throughout the research. I would also like to recognize and thank my colleagues who provided work coverage during the research duration and also my fellow course mates who are always there to lend a helping hand.

ABSTRACT

In recent years, digital image forgery detection has become an active research area due to the advancement of photo editing software. In general, image forgery detection can be classified into two types, namely active and passive detection. Active forgery detection relies on embedded authentication code in the image while passive forgery detection relies solely on the images for authentication. The forgery detection techniques are used to identify images tampered with common techniques such as copy move, slicing, contrast alteration and sharpening/blurring. This project focuses on passive forgery detection on images tampered using copy move technique, better known as Copy Move Forgery Detection (CMFD). A CMFD technique consisting of oriented Features from Accelerated Segment Test and rotated Binary Robust Independent Elementary Features (Oriented FAST and rotated BRIEF) as the feature extraction method and 2 Nearest Neighbour (2NN) with Hierachical Agglomerative Clustering (HAC) as the feature matching method is proposed. The ORB parameters, namely the number of features to retain and patch size are optimized using Particle Swarm Optimization (PSO). The optimization is essential in obtaining a balance between performance and runtime. Evaluation of the proposed CMFD technique is performed on images which underwent various geometrical attacks. With the proposed technique, an overall accuracy rate of 84.33% and 82.79% is obtained for evaluation carried out with images from the MICC-F600 and MICC-F2000 databases. Forgery detection is performed accurately, with True Positive Rate of 91% and above, for tampered images with object translation, different degree of rotation and enlargement. However, the performance degraded for tampered images with reduced copied object size and asymmetrical scaling, with True Positive Rate of 73.68% and 38.15% respectively.

ABSTRAK

Dalam beberapa tahun kebelakangan ini, kemajuan perisian penyuntingan foto telah menjadikan pengesanan pemalsuan imej digital sebagai satu bidang penyelidikan yang aktif. Pengesanan pemalsuan imej boleh diklasifikasikan kepada dua jenis, pengesanan aktif dan pasif. Pengesanan pemalsuan aktif bergantung kepada kod pengesahan yang tertanam dalam imej sementara pengesanan pemalsuan pasif hanya bergantung kepada imej untuk menjalankan pengesahan. Cara-cara pengesanan pemalsuan imej digunakan untuk mengesan pemalsuan imej termasuk salinan langkah, penyalinan dari imej lain, pengubahan kontras dan pengaburan. Projek ini memberi tumpuan kepada pengesanan pemalsuan pasif pada imej yang dicemari menggunakan teknik salinan langkah. Teknik tersebut dikenali sebagai Pengesanan Pemalsuan Salinan Langkah (CMFD). Teknik CMFD yang dicadangkan dalam projek ini terdiri daripada *oriented Features from Accelerated Segment Test* dan *rotated Binary Robust Independent Elementary Features (Oriented FAST dan rotated BRIEF)* sebagai kaedah pengekstrakan ciri dan *2 Nearest Neighbor (2NN)* dengan *Agglomerative Hierachical Clustering (HAC)* sebagai kaedah pencocokan ciri. Parameter ORB, iaitu bilangan ciri untuk dikekalkan dan saiz patch telah dioptimumkan dengan mengguna cara Particle Swarm Optimization (PSO). Pengoptimuman adalah penting dalam menyeimbangkan antara prestasi dan tempoh masa yang diperlukan. Penilaian teknik CMFD yang dicadangkan dilakukan pada imej yang mengalami pelbagai serangan geometri. Dengan teknik yang dicadangkan, kadar ketepatan keseluruhan adalah 84.33% dan 82.79% bagi penilaian yang dijalankan dengan imej dari pangkalan data MICC-F600 dan MICC-F2000. Pengesanan pemalsuan imej dilakukan dengan tepat dan kadar positif sebenar sebangai 91% dan ke atas diperolehi untuk imej dengan terjemahan objek, tahap putaran yang berbeza dan pembesaran. Walau bagaimanapun, prestasi menyusut bagi imej di mana saiz objek yang disalin dikurangkan dan penskalaan tak simetri, dengan kadar positif benar masing-masing sebanyak 73.68% dan 38.15%.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

2NN	-	2 Nearest Neighbour
BAG	-	Block Artifacts Grids
BRIEF	-	Binary Robust Independent Elementary Features
CMFD	-	Copy Move Forgery Detection
DoG	-	Difference of Gaussian
DCT	-	Digital Cosine Transform
DWT	-	Discrete Wavelet Transform
FN	-	False Negative
FP	-	False Positive
FPR	-	False Positive Rate
FWHT	-	Fast Walsh-Hadamard Transform
HAC	-	Hierarchical Agglomerative Clustering
ORB	-	Oriented FAST and rotated BRIEF
PCA	-	Principal Component Analysis
PCT	-	Principal Component Transformation
SURF	-	Speeded Up Robust Feature
SIFT	-	Scale-Invariant Feature Transform
SVD	-	Singular Value Decomposition
SVM	-	Support Vector Machine
TN	-	True Negative
TP	-	True Positive
TPR	-	True Positive Rate

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

This chapter introduces this research work by providing the project background and potential impact. It focuses on the research motivation and the research gap, before concluding the chapter with the organization of the thesis.

1.1 Problem Background

In this day and age, digital images tampering has been made easy with widely available image editing softwares, such as Adobe Photoshop. The advancement of image editing softwares has reached a level such that image tampering can be done without degrading its quality or leaving obvious traces. This is alarming as images are now being presented as supported evidences and historical records in various fields, such as in forensic investigation, law enforcement, journalistic photography and medical images.

Moreover, in many instances tampered images have appeared in the news or social media, such as the manipulated images of Iranian missile test released on the 9th of July 2008 by Sepah News, the official media arm of Iran's Revolutionary Guard. The tampered image, shown in Figure 1.1 is aimed at exaggerating the country's military capabilities. The tampered image made its way into media circulation, making the front page of notable newspapers, such as The Financial Times and The Los Angeles Times. The forgery is detected a day later when the same source released another image taken from the same angle at almost the same time, but with different content.

The scientific community is also not spared from image tampering. Farid et al. [1] stated that 20% of accepted manuscripts of the Journal of Cell Biology contains inappropriate figure manipulation. Hence, image tampering and detection

have garnered substantial attention as manipulated images can be used to misrepresent their meaning with malicious intent.

Figure 1.1: (a) Original image of Iranian Missile Test (b) Forged image of Iranian Missile Test

Among the image manipulation techniques in the literature, Abd Warif et al. [2] stated that copy-move forgery and copy-move forgery detection (CMFD) is one of the most widely studied field. In general, CMFD involves the manipulation of an image where an object, texture or letter is copied from one region of an image and inserted into another region of the same image.

1.2 Problem Statement

The project focuses on applying widely used keypoint based algorithms in the field of object recognition for CMFD. The proposed CMFD technique, consisting of both feature extraction and feature matching, would serve as an alternative to the current state of the art CMFD method using Speeded Up Robust Features (SURF).

Before SURF was introduced in the field of CMFD, Scale-invariant Feature Transform (SIFT) is widely regarded as one of the best keypoint based algorithm for CMFD. With SURF, the algorithm proposed multiple optimization which successfully reduced the computation time by 3 times. However, the improvement came at the expense of the accuracy rate.

Hence, this work aims to identify a Copy Move Forgery Detection technique, consisting of both feature extraction (descriptor) and feature matching, capable of obtaining better accuracy rate while maintaining the computational time seen with SURF.

1.3 Project Objective

The object of this project is to identify a Copy Move Forgery Detection technique, with both feature extraction and feature matching technique, capable of obtaining better accuracy rate while maintaining the computational time seen with SURF. Also, the proposed CMFD method is compared with existing CMFD techniques in terms of performance.

1.4 Scope of Study

The scope of this project focuses on proposing a CMFD technique, with both descriptor and feature matching methods, and its performance on accurately detecting tampered images. Apart from the proposed CMFD techniques, an existing CMFD technique, namely SURF, which is the state of the art feature extraction method is also reproduced.

The performance of the proposed CMFD technique is evaluated using images which have underwent different geometrical attacks, namely translation, different degrees of rotation, symmetrical and asymmetrical scaling. The proposed CMFD technique is also tested on images with multiple copy-move regions. The proposed work is implemented using MATLAB and tested on the following dataset: MICC-F600 and MICC-F2000.

1.5 Organization

The thesis is organized as follows: Chapter 2 presents the literature review on Copy-Move Forgery Detection, focusing on block based and keypoint based CMFD techniques. Chapter 3 presents the research methodology of the proposed CMFD technique, focusing on SURF and ORB as the feature extraction methods and 2 Nearest Neighbour (2NN) and Hierarchical Agglomerative Clustering (HAC) as the feature matching method. Chapter 4 presents the result of our proposed CMFD technique with a summary of the contribution and achievements of the project. Lastly, we conclude the project by a conclusion and a discussion on potential future works to build on the project.

REFERENCES

1. Farid, H. Exposing digital forgeries from JPEG ghosts. *IEEE Transactions on Information Forensics and Security*, 2009. 4(1): 154–160.
2. Bakiah, N., Warif, A., Wahid, A., Wahab, A., Yamani, M., Idris, I., Ramli, R., Salleh, R. and Shamshirband, S. Copy-move forgery detection : Survey , challenges and future directions. *Journal of Network and Computer Applications*, 2016. 75: 259–278.
3. Lucchese, L. and Cortelazzo, G. M. A noise-robust frequency domain technique for estimating planar roto-translations. *IEEE Transactions on Signal Processing*, 2000. 48(6): 1769–1786.
4. Fridrich, J., Soukal, D. and Lukáš, J. Detection of Copy-Move Forgery in Digital Images. *International Journal*, 2003. 3(2): 652–663.
5. Li, W., Yu, N. and Yuan, Y. Doctored JPEG image detection. *IEEE International Conference on Multimedia and Expo*, 2008: 253–256.
6. Ye, S., Sun, Q. and Chang, E. C. Detecting Digital Image Forgeries by Measuring Inconsistencies of Blocking Artifact. *2007 IEEE International Conference on Multimedia and Expo*, 2007: 12–15.
7. Huang, Y., Lu, W., Sun, W. and Long, D. Improved DCT-based detection of copy-move forgery in images. *Forensic Science International*, 2011. 206(1-3): 178–184.
8. Cao, Y., Gao, T., Fan, L. and Yang, Q. A robust detection algorithm for copy-move forgery in digital images. *Forensic Science International*, 2012. 214(1-3): 33–43.
9. Zhao, J. and Guo, J. Passive forensics for copy-move image forgery using a method based on DCT and SVD. *Forensic Science International*, 2013. 233(1-3): 158–166.
10. Shao, H., Yu, T., Xu, M. and Cui, W. Image region duplication detection based on circular window expansion and phase correlation. *Forensic Science International*, 2012. 222(1-3): 71–82.

11. Yang, B., Sun, X., Chen, X., Zhang, J. and Li, X. An efficient forensic method for copy-move forgery detection based on DWT-FWHT. *Radioengineering*, 2013. 22(4): 1098–1105.

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

13. Lin, H.-J., Wang, C.-W. and Kao, Y.-T. Fast Copy-Move Forgery Detection. *Signal Processing*, 2009. 5(5): 188–197.

14. Hsu, H. C. and Wang, M. S. Detection of copy-move forgery image using Gabor descriptor. *Proceedings of the International Conference on Anti-Counterfeiting, Security and Identification, ASID*, 2012: 1–4.

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

16. Ojala, T., Pietikäinen, M. and Harwood, D. A comparative study of texture measures with classification based on featured distributions. *Pattern Recognition*, 1996. 29(1): 51–59.

17. AlSawadi, M., Muhammad, G., Hussain, M. and Bebis, G. Copy-move image forgery detection using local binary pattern and neighborhood clustering. *Proceedings - UKSim-AMSS 7th European Modelling Symposium on Computer Modelling and Simulation, EMS 2013*, 2013: 249–254.

18. Nandi, S. B.-S. and K., A. Exposing Duplicated Regions Affected by Reflection, Rotation and Scaling. *Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on*, 2011: 1880–1883.

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

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

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

22. Kashyap, A. and Joshi, S. D. Detection of copy-move forgery using wavelet decomposition. *2013 International Conference on Signal Processing and*

Communication, ICSC 2013, 2013: 396–400.

23. Liu, G., Wang, J., Lian, S. and Wang, Z. A passive image authentication scheme for detecting region-duplication forgery with rotation. *Journal of Network and Computer Applications*, 2011. 34(5): 1557–1565.

24. Hu, M.-K. Visual pattern recognition by moment invariants. *Information Theory, IEEE Transactions on*, 1962. 8: 179–187.

25. Ryu, S. J., Lee, M. J. and Lee, H. K. Detection of copy-rotate-move forgery using zernike moments. *Int'l Journal of Computer Vision*, 2010: 51–65.

26. Kang, X. and Wei, S. Identifying Tampered Regions Using Singular Value Decomposition in Digital Image Forensics. *International Conference on Computer Science and Software Engineering*, 2008: 926–930.

27. Li, C., Yang, S. and Nguyen, T. T. A self-learning particle swarm optimizer for global optimization problems. *IEEE transactions on systems, man, and cybernetics. Part B, Cybernetics : a publication of the IEEE Systems, Man, and Cybernetics Society*, 2012. 42(3): 627–46.

28. Christlein, V., Riess, C., Jordan, J., Riess, C. and Angelopoulou, E. An evaluation of popular copy-move forgery detection approaches. *IEEE Transactions on Information Forensics and Security*, 2012. 7(6): 1841–1854.

29. Lowe, D. G. Distinctive image features from scale invariant keypoints. *Int'l Journal of Computer Vision*, 2004. 60: 91–110.

30. Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A. and Serra, G. A SIFT-based forensic method for copy-move attack detection and transformation recovery. *IEEE Transactions on Information Forensics and Security*, 2011. 6(3): 1099–1110.

31. Popescu, A. C. and Farid, H. Exposing digital forgeries by detecting duplicated image regions. *Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515*, 2004. (2000): 1–11.

32. He, H., Huang, X. and Jun, K. Exposing copy-move forgeries based on a dimension-reduced sift method. *Information Technology Journal*, 2013. 12(14): 2975–2979.

33. Mohamadian, Z. and Pouyan, A. A. Detection of duplication forgery in digital images in uniform and non-uniform regions. *Proceedings - UKSim 15th International Conference on Computer Modelling and Simulation, UKSim 2013*, 2013. 1: 455–460.

34. Bay, H., Ess, A., Tuytelaars, T. and Van Gool, L. Speeded-Up Robust Features

(SURF). *Computer Vision and Image Understanding*, 2008. 110(3): 346–359.

35. Xu, B., Wang, J., Liu, G. and Dai, Y. Image copy-move forgery detection based on SURF. *Proceedings - 2010 2nd International Conference on Multimedia Information Networking and Security, MINES 2010*, 2010: 889–892.

36. Mishra, P., Mishra, N., Sharma, S. and Patel, R. Region Duplication Forgery Detection Technique Based on SURF and HAC. *The Scientific World Journal*, 2013. 2013: 10–18.

37. Hashmi, M. F., Anand, V. and Keskar, A. G. A copy-move image forgery detection based on speeded up robust feature transform and wavelet transforms. *Proceedings - 5th IEEE International Conference on Computer and Communication Technology, ICCCT 2014*, 2015: 147–152.

38. Rublee, E., Rabaud, V., Konolige, K. and Bradski, G. ORB: An efficient alternative to SIFT or SURF. *Proceedings of the IEEE International Conference on Computer Vision*, 2011: 2564–2571.

39. Rosin, P. L. Measuring Corner Properties. *Computer Vision and Image Understanding*, 1999. 73(2): 291–307.

40. Calonder, M., Lepetit, V., Strecha, C. and Fua, P. BRIEF: Binary robust independent elementary features. *European Conference Computer Vision*, 2010. (6314): 778–792.

41. Kennedy, J. and Eberhart, R. Particle swarm optimization. *Neural Networks, 1995. Proceedings., IEEE International Conference on*, 1995. 4: 1942–1948.

42. Kaur, R. and Kaur, A. Copy-Move Forgery Detection Using ORB and SIFT Detector. *International Journal of Engineering Development and Research*, 2016. 4(4): 804–813.