SOURCE IDENTIFICATION OF CAPTURED VIDEO USING PHOTO RESPONSE NON-UNIFORMITY NOISE PATTERN AND SVM CLASSIFIERS

ROYA ESMAEILANI

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

Faculty of Computing
Universiti Teknologi Malaysia

JUNE 2014

This dissertation is dedicated to my beloved parents and sister for their endless support and encouragement.

ACKNOWLEDGEMENT

First and foremost, I would like to express heartfelt gratitude to my supervisor **Prof. Dr. Ghazali Bin Sulong** for his constant support during my study at UTM. He inspired me greatly to work on this project. His willingness to motivate me contributed tremendously to our project. I have learned a lot from him and I am fortunate to have him as my mentor and supervisor. Also, I would like to thank my sister for her help facilities and for her nice guidance during my project preparation. Furthermore, I would like to thank my parents and all my friends that have given their moral support during the ups and down of my project work life cycle.

Last but not least, I would like to thank the authority of Universiti Teknologi Malaysia (UTM) for providing me with a good environment and facilities such as Computer laboratory to complete this project with software which I need during process.

ABSTRACT

Recent works have shown that passive capturing source detection methods based on Photo-Response-Non-Uniformity (PRNU) extraction are the most reliable ones in comparison with techniques that based on lens properties or compression artifacts. Some important issues in this field include: employing an effective method for extracting PRNU, calculating the similarity and categorizing videos according to source of camera. In this study, a comprehensive algorithm is proposed to compare and evaluate the performance of different source detection methods in terms of filters used and partitioning process applied for PRNU extraction coupled with SVM classifier. Moreover, in consideration of observations, a new method is proposed for sampling selection using SVM classifier. Furthermore, the capabilities of employing and combining the results of different color parts of videos are used instead of changing them to grayscale. The proposed algorithm is based on three essential steps: Firstly, fingerprint of each camera, which is regarded as reference PRNU, is calculated by extracting PRNU of blue-sky videos. Secondly, the PRNU similarities of sample videos with reference PRNU are measured by calculating cross correlation and Peak to Correlation Energy (PCE) metrics. Finally, the sample videos are classified based on calculated PCE with SVM classifier. Experimental results revealed that Zero-mean and Wiener filters have small influences on PRNU, thus they can be ignored. Experimental results also revealed that eliminating the partitioning step considerably increases the performance of detection success rate by 15%. Among SVM classifiers, “RBF” and “MLP” types have the best identification rate of 75%.

ABSTRAK

Pengkajian terbaharu telah menunjukkan bahawa kaedah pengesanan sumber rakaman pasif berdasarkan *Photo-Response-Non-Uniformity* (PRNU) adalah sangat boleh dipercayai berbanding dengan teknik yang berdasarkan sifat-sifat kanta atau artifak mampatan. Beberapa isu penting dalam bidang ini termasuklah penggunaan kaedah yang lebih berkesan untuk pengekstrakan PRNU, pengiraan kesamaan dan pengkategorian video menurut sumber kamera. Dalam kajian ini algoritma komprehensif dicadangkan bagi membandingkan dan menilai prestasi kaedah pengesanan sumber yang berbeza dari segi penapis yang digunakan dan proses pembahagian yang diterapkan untuk pengekstrakan PRNU. Selanjutnya, dalam pertimbangan pemerhatian kaedah baharu dicadangkan untuk pemilihan pensampelan menggunakan pengkelas *SVM*. Selain itu keupayaan menggunakan dan menggabungkan hasil video bagi bahagian-bahagian warna yang berbeza digunakan bukannya mengubah hasil video tersebut kepada skala kelabu. Algoritma ini berdasarkan tiga langkah penting: Pertama, cap jari setiap kamera dikira dengan pengekstrakan PRNU video langit biru. Kedua, kesamaan PRNU video sampel dengan cap jari kamera diukur dengan metrik korelasi tenaga *PCE*. Akhir sekali, video sampel dikelaskan berdasarkan *PCE* yang dikira dengan pengkelas *SVM*. Keputusan eksperimen menunjukkan bahawa penggunaan *zero-mean* dan penapis *Wiener* mempunyai pengaruh yang kecil kepada ketepatan PRNU dan boleh diabaikan. Sementara itu, langkah menghapuskan pembahagian secara ketara meningkatkan prestasi kadar kejayaan pengesanan sebanyak 15%. Tambahan lagi, antara jenis pengkelas *SVM*, "*RBF*" dan "*MLP*" memiliki kadar kejayaan yang terbaik, iaitu sebanyak 75%

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Nowadays, digital file producing devices like several kinds of cell phones, camcorders, cameras and scanners and the possibility of sharing information through internet causes usage of digital videos to increase in different aspects of human lives such as surveillance cameras, home video and so on. The improvements in digital technology with providing easy access to digital video, besides a lot of advantages can create some problems which are the results of illegal activities and may lead to creating diverse origins or some alterations to contents of video files.

Video authentication can be defined as a process which proves the given video content is exactly same as when it was captured by camera and due to its usage can be achieved by searching and detecting different types of forensics which maybe done about video through several ways (Upadhyay and Singh, 2012).

A video clip can be doctored by several forensics such as altering, combining, or creating new video contents. All these forgery activities that are done usually with criminal goals lead to producing a fake video which conceals or changes the determinative facts, events and important details in the recorded scene; So that, authenticity of video data can be considered as an important factor in cases such as forensic investigation, law enforcement, video surveillance and content ownership.

For example, in surveillance videos which usually are used as legal evidences in many courts, the accuracy of content is essential. These surveillance videos can be easily forged using video editing tools such as Premier, Vegas, etc. Moreover, the forger might replace the whole video taken by the surveillance camera with another video. In the cases that forged surveillance videos are used as court evidence, it may potentially cause the wrong person to be convicted mistakenly. Generally, the most important and sensitive cases which clarify the necessity of video authentication are related to scenarios in which video clips used as evidence in court law and even a little modification can change the sentence(Pradeep K et al, 2009;Upadhyay and Singh, 2012; Pradeep K et al,2004).

Digital forensics often leaves some traces in resulting signal which called "fingerprints". Fingerprints are usually hidden in digital video and it is needed to complex signal processing for analyzing and detecting them. Uncovering and inspecting these fingerprints provide a kind of reverse engineering to find and understand the processing steps which is performed on video from its first generation to its actual form and can be employed for finding tampering areas(Bestagini et al, 2012; Tsai and Shih, 2009).

1.2. Problem Background

Nowadays, fast improvements in digital technologies and widely use of digital video recording systems together with sophisticated video editing software, high quality processing tools and algorithms, and accessibility of low-cost and easy-operable digital multimedia devices, increase the trend for tampering videos and make the authenticating multimedia content as a challenging issue.

There are two general approaches for authenticating video clips. In the first approach of forgery detection, a watermark or digital signature is embedded into the video. These determinant files can be saved into video content, header file or even as independent files. By using embedded watermarks in video content, whenever a

video is forged, this watermark also be modified and can be processed by authentication systems as a clue of forgery. In the cases of using digital signatures, tampering in videos can be determined by extracting the digital signature and matching the data of video content with information obtained from the digital signature. In these methods, the requirement of a preprocessing modules which should be embedded in the device and it can influence on video quality, can be considered as an important drawback (Upadhyay and Singh, 2012).

In the second approach, in comparison to first one, there is no need to any pre-processing activities. These methods rely on intrinsic features like pixel value and statistical features and characteristics of video files. The main steps of these approaches is extracting different types of fingerprints and then applying pattern recognition techniques in order to detect forgery. Some fingerprints which can be used in these techniques include: noise patterns, lens distortion, double compression artifacts, inconsistence-related artifacts and so on (Kancherla and Mukkamala, 2012).

One of the methods which is considered in recent years in order to detect video forgery, are techniques that are based on identifying of acquisition device and able to detect whether two video clips originate from the same source. Based on Alex C. Kot and Hong Cao, because of statistical source features fragile nature toward tampering and manipulations, it can be used to address tamper issue.

Researches on camera model identification focus on certain stages of processing pipeline inside digital cameras because each part of this process could be implemented differently in various camera types. An overview of this processing pipeline is illustrated in Figure 1.1(Xu and Shi, 2012).

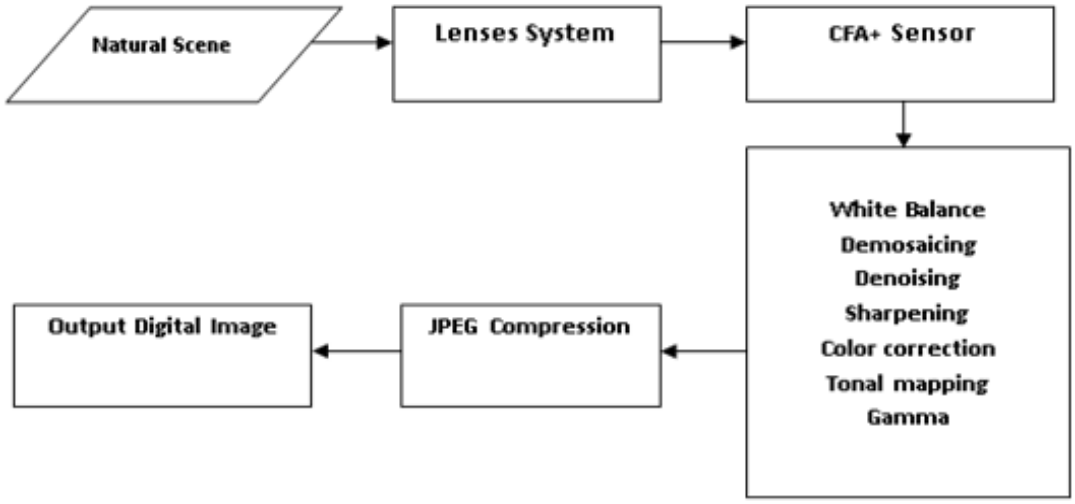

Figure 1.1 Processing pipeline diagram inside digital cameras

Processing pipeline stages that are shown in Figure 1.1 can be divided into two main categories: Software stages and hardware parts. Camera identification methods rely on software parts consists of compression procedure parameters and examining the digital file's header which contains the information about camera type, date and time and exposure. But these methods are not so reliable and not widely used because each camera could be adjusted in different settings and the resulted image could be compressed even more by additional software on computers before usage.

Because of that, it's better to switch on hardware parts and identify the source of digital files based on the imperfections of camera hardware. These hardware parts consist of lens and CCD or CMOS sensors. Each of these hardware devices leave some fingerprints in resulted images or videos which can be used as intrinsic features of each camera type (Van Lanh et al., 2007; Irie et al., 2008).

Lens distortion parameters, can capture the geometric fingerprints which are left by the camera (lens system) on the digital files. Among different types of lens aberrations, lens radial distortion seems more suitable for camera source identification; however the lens distortion parameter is affected by manual zooming and this causes the performance of this method to limit (Choi et al., 2006).

As, it is mentioned above, another set of video source identification methods are based on extracting and measuring noise characteristics which are resulted of camera sensors. Generally, noise is a random, unwanted and fluctuation of pixel values in digital file such as images and videos that is produced by sensors. The noise patterns which are mostly used as one part of source identification process because of their deterministic properties, come from CCD sensors (Bayram et al., 2005).

Among all CCD's noise types which can be detected in a captured video, PRNU can be used as an effective fingerprint for camera identification because of some its properties such as resistance against humidity, temperature, light refraction on dust particles, optical surfaces and optical zoom setting and also its source that is camera sensor (Chen et al., 2007).

1.3. Problem Statement

As it is mentioned in the last section, capturing source detection methods is considered as an effective approach in authenticating video files. Based on previous studies which are performed in this area, PRNU noise is determined as one of the best deterministic fingerprint for identifying the source (Bayram et al., 2005; Chen et al. 2007; Peng et al.,2013; Goljan et al. 2009). One of the challenging issues which raises in these studies, is implementing an appropriate method for evaluating the accuracy of extracted PRNUs. In this study, the efficiency of PRNU-based identification methods is investigated by proposing the comprehensive evaluating algorithm. Moreover, the best and most effective methodology in order to identify the videos' capturing source by means of PRNU is introduced. The presented algorithm in comparison with the last study in which videos should belong enough to obtain more reliable results, is independent of videos' length (Chen and et al., 2007). Finally, the proposed method uses artificial intelligence classifiers for classifying a

large number of videos in consideration to extracted PRNUs. The success rates of these classifiers can be considered for evaluating the accuracy of extracted PRNU.

1.4. Research Questions

1. How to detect of PRNU noise from captured video by digital cameras?
2. How to extract PRNU noise? Is it efficient to use filters? Is it efficient to use partitioning process?
3. How to authenticate the source of the video by using PRNU noise?
4. What is the best classifier for classifying videos based on extracted PRNU?

1.5. Aim of Study

The aim of this study is to propose and implement a comprehensive evaluating algorithm for video forgery detection method based on source of camera used and classify videos according to similarity metric (Peak to Correlation Energy).

1.6. Objectives

1. To detect PRNU noise from captured video by digital cameras.
2. To extract PRNU noise by employing different filters.
3. To classify videos based on captured PRNU noise and similarity metrics using the SVM classifier.

1.7. Scope of Study

1. Prior knowledge of the camera used is known.
2. SVM (Support Vector Machine) tools are used for classifying the video based on similarity metric (PCE).
3. Several numbers of videos which are taken by four types of camera and included “SONY DSC-W390”, ”CANON POWERSHOT GX1”, “CANON G12” and “SONY DSC-HX5V, are used for providing training and testing dataset.
4. Matlab2011a software is used as the processing tool for capturing the video noise pattern and implementing the evaluating phase.

1.8. Significance of Study

In recent years, increasing trend of using digital videos and sharing video clips easily throughout internet on one hand, and accessible enhanced tools and software tools which are produced in order to tamper videos on the other hand create an essential need to authenticate the video files. Authenticating of video files can be considered as an important issue since they can be used as critical evidences to prove criminal activities which are done by individuals and can change the sentence in court of law.

1.9 Thesis Organization

The research is comprised of five chapters. Chapter one presents an introduction to the research which includes the problem background, problem statements, research questions, aim of the study, the main objectives, scope and significance of the study. Chapter two reviews the literature about video

authentication and investigates the methods used in video forgery detection. Chapter three describes the methodology for the research. Chapter four looks into the design of algorithms and displays the results. Lastly, the conclusion is presented in chapter five.

REFERENCES

Bayram, S., Sencar, H. T., Memon, N., and Avcibas, I., 2006. Improvements on Source Camera-model Identification Based on CFA Interpolation. *Proceeding of 2006 WG*

Bayram, S., Sencar, H.T., Memon, N., and Avcibas, I.,2005. Source Camera Identification Based on CFA Interpolation, *Proceedings of the 2005 IEEE International Conference on in Image Processing*. III-69-72.

Bennett, K. P., and Campbell, C.,2000. Support Vector Machines: Hype or Hallelujah? *ACM SIGKDD Explorations Newsletter. 2(2),*1-13.

Bestagini, P., Fontani, M., Milani, S., Barni, M., Piva, A., Tagliasacchi, M., andTubaro, S., 2012. AN OVERVIEW ON VIDEO FORENSICS. *Proceedings of the 2012 IEEE EuropeanConference onSignal Processing.*1229–1233.

Brereton, R. G., and Lloyd, G. R., 2010. Support Vector Machines for Classification and Regression. *Analyst,*135(2), 230-267.

Chang, C. C., and Lin, C. J., 2011. LIBSVM : a library for support vector machines. *ACM Transactions on Intelligent Systems and Technology*, 2:27:1-27:27.

Chen, M., Fridrich, J., Goljan, M., and Lukás, J.,2008. Determining Image Origin and Integrity Using Sensor Noise.*IEEE Transactions on Information Forensics and Security*. 3(1), 74-90.

Chen, M., Fridrich, J., Goljan, M., and Lukáš, J., 2007. Source Digital Camcorder Identification Using Sensor Photo Response Non-uniformity. *In Electronic Imaging 200,. International Society for Optics and Photonics.*65051G-65051G.

Choi, K. S., Lam, E. Y., and Wong, K. K., 2006. Automatic Source Camera Identification Using the Intrinsic Lens Radial Distortion,*Optics Express*. 14(24), 11551-11565.

Conotter, V., O'Brien, J. F., and Farid, H., 2012.Exposing Digital Forgeries in Ballistic Motion. *IEEE Transactions on Information Forensics and Security*.7(1), 283–296.

Cortes, C., and Vapnik, V., 1995. Support-Vector Networks.*Kluwer Academic*. 273–297.

Dong, Q., Yang, G., and Zhu, N., 2012. A MCEA Based Passive Forensics Scheme for Detecting Frame-Based Video Tampering. *Digital Investigation*. 9(2), 151-159.

Fridrich, J., 2009. Digital Image Forensics,*Signal Processing Magazine, IEEE*. 26(2) , 26 - 37

Goljan, M., Fridrich, J., and Filler, T., 2009. Large Scale Test of Sensor Fingerprint Camera Identification. *InIS&T/SPIE Electronic Imaging*.1-12.

Helmberg, C., Rendl, F., Vanderbei, R. J., and Wolkowicz, H., 1996. An interior-point method for semidefinite programming. *SIAM Journal on Optimization*. 6(2), 342-361.

Hsu, C. C., Hung, T. Y., Lin, C. W., and Hsu, C. T., 2008. Video Forgery Detection Using Correlation of Noise Residue., *2008 IEEE 10th Workshop in Multimedia Signal Processing*. 170-174.

Irie, K., McKinnon, A. E., Unsworth, K., and Woodhead, I. M., 2008. A Technique for Evaluation of CCD Video-Camera Noise. *IEEE Transactions on Circuits and Systems for Video Technology*. 18(2), 280 - 284.

Kee, E., Johnson, M. K., and Farid, H., 2011. Digital Image Authentication from JPEG Headers.*IEEE Transactions on Information Forensics and Security*. 6(3), 1066-1075.

Kharrazi, M., Sencar, H. T., and Memon, N., 2004. Blind Source Camera Identification.*Proceedings ofthe 2004 international Conference in Image Processing.(ICIP04)*.1, 709-712.

Kobayashi, M., Okabe, T., and Sato, Y., 2010. Detecting Forgery from Static-Scene Video Based on Inconsistency in Noise Level Functions.*IEEE Transactions on Information Forensics and Security*. 5(4), 883-892.

Lukas, J., Fridrich, J., and Goljan, M., 2006. Digital Camera Identification from Sensor Pattern Noise.*IEEE Transactions on Information Forensics and Security*. 1(2), 205–214.

Peng, F., Shi, J., and Long, M., 2013. Comparison and Analysis of the Performance of PRNU Extraction Methods in Source Camera Identification.*Journal of Computational Information Systems*. 9(14), 5585-5592.

San Choi, K., Lam, E. Y., and Wong, K. K., 2006. Source Camera Identification Using Footprints from Lens Aberration. *Proceeding of the 2006 SPIE - The International Society For Optical Engineering*. 6069, 1–8.

Shawe-Taylor, J., and Sun, S., 2011. A Review of OptimizationMethodologies in Support Vector Machines, *Neurocomputing, 74(17). Elsevier*.3609‑3618.

Su, Y., Zhang, J., and Liu, J.,2009. Exposing Digital Video Forgery by Detecting Motion-Compensated Edge Artifact.*Proceedings of the 2009 IEEEInternational Conference on Computational Intelligence and Software Engineering*. 1–4.

Swaminathan, A., Wu, M., and Liu, K. R., 2007. Nonintrusive Component Forensics of Visual Sensors Using Output Images.*IEEE Transactions onInformation Forensics and Security*. *2(1),*91-106.

Tsai, J. C., and Shih, T. K., 2011.Video Forgery and Motion Editing.*In Visual Informatics: Sustaining Research and Innovations*. *Springer Berlin Heidelberg*. 7066.

Upadhyay, S., and Singh, S. K., 2012. Video Authentication: Issues and Challenges. *IJCSI International Journal of Computer Science Issues*. 9(1), 409–418.

Van Lanh, T., Chong, K. S., Emmanuel, S., and Kankanhalli, M. S.,2007. A Survey on Digital Camera Image Forensic Methods. *Proceedings of the 2007 IEEE International Conference On Multimedia and Expo*. 16–19.

Xu, G., Gao, S., Shi, Y. Q., Hu, R., and Su, W., 2009. Camera-Model Identification Using Markovian Transition Probability Matrix.*in Digital Watermarking.*Springer Berlin / Heidelberg. 294-307

Xu, G., and Shi, Y. Q., 2012. Camera Model Identification Using Local Binary Patterns, *Proceedings of the* 2012 *IEEE International Conference on Multimedia and Expo(ICME)*. 392–397.

Yin, P., and Hong, H. Y.,Classification Of Video Tampering Methods and Countermeasures Using Digital Watermarking Image. *In ITCom 2001: International Symposium on the Convergence of IT and Communications*,239-246.

Zhang, J., Su, Y., and Zhang, M., 2009. Exposing Digital Video Forgery by Ghost Shadow Artifact. *Proceedings of the First ACM workshop on Multimedia in forensics.* 49-54.