SPLICING IMAGE FORGERY IDENTIFICATION BASED ON ARTIFICIAL NEURAL NETWORK APPROACH AND TEXTURE FEATURES

NUR FAREHA AMIRA BINTI MOHD OMAR

FSKTM 2019 30

SPLICING IMAGE FORGERY IDENTIFICATION BASED ON ARTIFICIAL NEURAL NETWORK APPROACH AND TEXTURE FEATURES

By

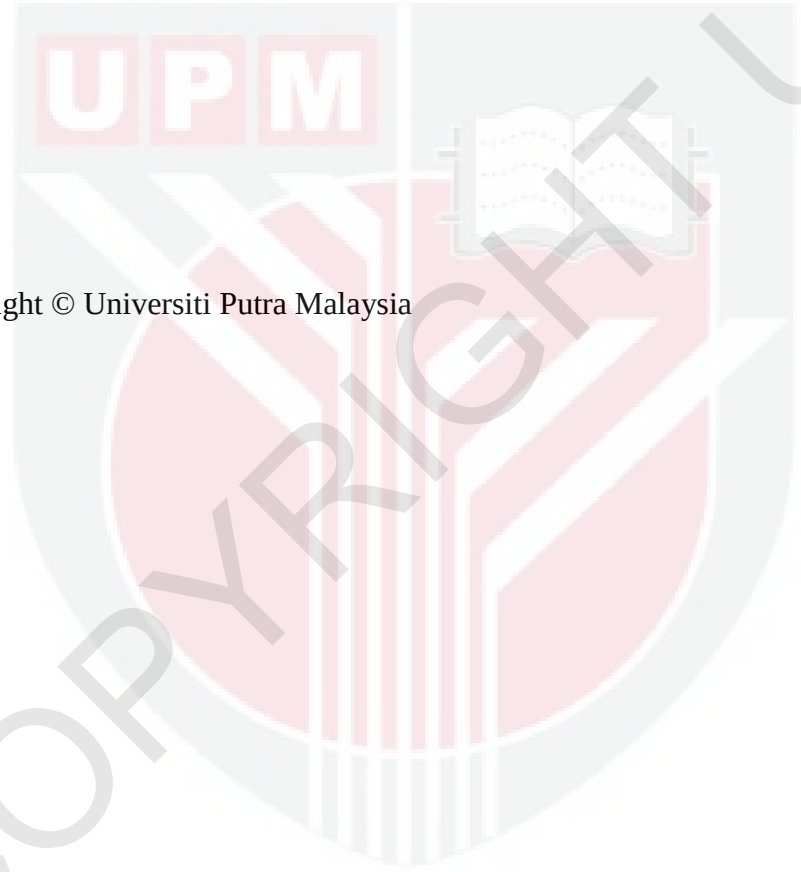
NUR FAREHA AMIRA BINTI MOHD OMAR

Thesis submitted to the School of Graduate Studies,

Universiti Putra Malaysia,

in Fulfilment of the Requirements for the Master of Information Security

JANUARY 2019



ABSTRACT

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Information Security

SPLICING IMAGE FORGERY IDENTIFICATION BASED ON ARTIFICIAL NEURAL NETWORK APPROACH AND TEXTURE FEATURES

By

NUR FAREHA AMIRA BINTI MOHD OMAR

January 2019

Supervisor: Puan Zaiton Binti Muda

Faculty: Faculty of Computer Science and Information Technology

Abstract:

In this technology area, manipulation an image become an easy task due to the availability of open source image handling software and becomes a great challenge to determine whether an image has been manipulated or not. Moreover, the authenticity of digital image experience extreme dangers because the capable of altering images software that effectively adjust the image without leaving any obvious hint of such change. Therefore, image integrity is becoming questionable especially when images have influential power for example, in a court of law or news report. Manipulating the original image content is called digital image forgery. Splicing image forgery is one of technique to forgery an image. The splicing image forgery is replicated one or more are from source image and paste into an objective picture to create a composite image.

This study present combination of features extraction to produce good vector to describe the image and feed the image to the multilayer perceptron. This study is try to improve the accuracy identification on splicing image based on anchor paper. The finding outcome from this study have shown improved approach for identification splicing image. The identification accuracy in the technique used is about 100% and 98% based on dataset.

ABSTRAK

Abstrak tesis yang dikemukan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Sarjana Keselamatan Maklumat

IDENTIFIKASI KE ATAS PEMALSUAN GAMBAR CANTUMAN BERDASARKAN PENDEKATAN RANGKAIAN NEURAL BUATAN DAN CIRI-CIRI TEKSTUR

Oleh

NUR FAREHA AMIRA BINTI MOHD OMAR

Januari 2019

Penyelia: Puan Zaiton Binti Muda

Fakulti: Fakulti Sains Komputer dan Teknologi Maklumat

Abstrak:

Di dalam era teknologi kini, memanipulasi gambar menjadi tugas mudah kerana ketersediaan perisian pengendalian gambar sumber terbuka dan menjadi satu cabaran besar untuk menentukan sama ada gambar telah dimanipulasi atau tidak. Lebih-lebih lagi, keaslian gambar digital berada dalam keadaan bahaya kerana terdapat perisian gambar yang mampu mengubah secara efektif memalsukan gambar tanpa meninggalkan sebarang petunjuk jelas dari perubahan tersebut. Oleh itu, integriti gambar menjadi persoalan terutamanya apabila gambar mempunyai kuasa yang berpengaruh, contohnya dalam mahkamah undang-undang atau laporan berita.

Memanipulasi kandungan gambar asal dipanggil pemalsuan gambar digital. Pemalsuan gambar cantuman adalah salah satu teknik untuk memalsukan gambar. Pemalsuan gambar cantuman ditiru satu atau lebih dari gambar asal dan mencantumkan ke dalam gambar lain untuk membuat gambar palsu. Kajian ini mempersembahkan ciri-ciri pengekstrakan untuk menghasilkan vektor yang baik untuk menggambarkan gambar dan akan melalui rangkaian neural buatan untuk klafikasi gambar. Oleh kerana kajian ini cuba untuk meningkatkan pengenalan ketepatan pada gambar cantuman berdasarkan hasil dari rujukan kertas utama. Hasil penemuan dari kajian ini telah memperolehi pendekatan yang lebih baik untuk mengenalpasti gambar cantuman. Ketepatan pengenalan teknik yang digunakan adalah kira-kira 100% dan 98% berdasarkan data yang digunaka

ACKNOWLEDGEMENTS

Alhamdulillah praise to Allah for His blessing, I can finish writing this thesis for my degree of Master of Information Security.

First and foremost, I would like to thank my parents for their countless supports in my journey to complete my year as a Master student.

Especially, I would like to express my appreciation to my supervisor, Puan Zaiton Binti Muda who have guiding and assisting me in my journey. Thank you for all the knowledge, advice and effort during the research period.

Additionally, I would like to extend my thankful to all lecturer and my friends who involved directly or indirectly in this work.

APPROVAL

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Master of Information Security. The members of the Supervisory Committee were as follows:

PN. ZAITON BINTI MUDA
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Supervisor)

Date :

DECLARATION

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustration and citation have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, report, lecturer notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia(Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012.

Signature: _____ Date: _____

Name and Matric No.: **NUR FAREHA AMIRA BINTI MOHD OMAR**

GS48638

TABLE OF CONTENTS

LIST OF TABLES

Table No.

LIST OF FIGURES

Figure No.

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND

Since the advancement of technology, there a lot of new development of devices, application or software have been develop due to demand of interest. Nowadays, digital image have experienced incredible growth and been widely used in our daily life. Based on that, application or software that related to image editing are quickly develop such as Adobe Photoshop that can forged an image. Once it been forged, we basically cannot compare whether it original image or manipulated through the naked eye. Image forgery or image tempering is defined as adding, changing or deleting some important features from an image without leaving any obvious trace of tempering (Abhishek et al., 2017). Therefore, image forgery is categorized as intentional manipulation of images for malicious purpose (Toqeer et al., 2016). In recent year, digital image forensics has raised which to finds the evidence or proof of forgeries in digital image (Toqeer et al., 2016). According to Abhishek et al, when a digital images being used as evidence in court during criminal investigation the integrity of visual data is important for the credibility of news. The main focus of digital image forensics is to investigate the images for the presence of forgery by applying either the active or passive technique. Active and passive are two approaches are commonly used for image forgery detection (Abhishek et al., 2017). The active techniques such as watermarking and digital signature depend on the information embedded in the images. However, the inaccessibility of the information may boundary the application

of active techniques in practice. While, passive technique no needs to insert information in the image for authentication.

According to several previous researches, there have three different techniques on image forgery. Copy-Move forgery or cloning is a technique copied from original image and pasted to another area on the same image. The second of image forgery technique is known as image splicing, which is a technique uses cut and paste from one or more images to create another fake images. And the third technique is known as image resampling or retouching in which certain image or feature being enhance or reduce in order to make the image more attractive. In addition, this technique is less harmful to security issue as it used mostly by editor. Among all the possible image tempering techniques, image splicing is the most common.

For example, according to Nistha. et al, one forged image that being published by western media that showed four missiles instead of three released by Iran. Similarly, in Abhishek T. et al, an image of tiger in forest required the people to believe in the existence of tiger in China while according to forensics analysis, it just "paper tiger".

1.2 PROBLEM STATEMENT

In today's worlds, people are depending on getting information or news through internet without knows is real or not and simply make story based on picture they seen. Moreover, digital image provides the convincible and easiest way to convey any message more impactful. Digital image forgery can be perform by manipulating features of digital images. With the easiness of use and availability of software tool

and low-cost hardware, make it very simple to forge digital image and leaving almost no trace that it has been tempered. While, the tempered image also can create malicious purpose to spread huge rumour or fake information based on images that people will see. This give a huge challenge of the trustworthiness in digital images offered as medical diagnosis, as evidence in courts, as newspaper items or as legal documents because of difficulty in differentiating original and modified contents. This problem will make people easy to trust what they see than the truth one. Furthermore, today's people like to use social media or application message to spread news easily without thinking it fake or not. Just one image, people will assume different opinions mostly negative comment or information.

There is compulsion to take an immediate action. Nevertheless, the dilemma with authenticity of digital image appeal for the verification of legitimacy of the digital image in diverse application. As it is important to prevent integrity and authenticity of image as it really play important role in our daily life as evidence in courts, medical fields as medical report.

1.3 RESEARCH OBJECTIVE

The objective of this research is to study and improve the accuracy of identification on image forgery based current proposed. The extracted features are used as the key to distinguish between splicing image and non-splicing image. The accuracy need to be achieved about 99.43%, 97.4% and 98.6% based on the dataset they used.

1.4 RESEARCH SCOPE

The scope of this work is to identify splicing image forged to overcome the objective by using WEKA Software. The dataset of this study use the available online image data that mainly used in forgery detection. Which are collect at Tampered Image Detection Evaluation Dataset CASIA TIDE V1.0 , V2.0 and The Columbia Image Splicing Detection Evaluation Dataset.

1.5 THESIS STRUCTURE

This thesis is structured as follow:

Chapter 1 - Briefly describes about introduction, problem statement, objective, research scope in conducting a research work on detection on splicing images forgery.

Chapter 2 - This chapter provides the literature review from others publications to understand more about digital image forgery and comparison of existing solution on image splicing forgery detection.

Chapter 3 - This section cover a full phase of methodology that will using through this research.

Chapter 4 - The details analysis of result by using the proposed solution.

Chapter 5 - As the final chapter for the thesis, the summary of research works will be elaborated here.

REFERENCES

Abhishek Kashyap, Rajesh Singh Parmar, Megha Agrawal, Hariom Gupta. (2017). An Evaluation of Digital Image Forgery Detection Approaches. ArXiv.

Abshishek Kashyap, Megha Agarwal, Hariom Gupta. (n.d.). Detection of Copy-Move Image Forgery using SVD and Cuckoo Search Algorithm.

Alahmadi A.A, Hussain M., Aboalsamh M., Muhammad G, Bebis G. (2013). Splicing Image Forgery Detection Based on DCT and LBP. *Global Conference on Signal and Information Processing.* IEEE.

Alahmadi A.A., Hussain, M., Aboalsamh M., Muhammad, G., Bebus, G., Mathkor, H.,. (2016). Passive Detection of Image Forgery using DCT and LBP. *Springer-Verlag London* .

Amol Prataprao Bhatkar, Dr.G.U.Kharat. (2015). Detection of Diabetic Retinopathy in Retinal Images using MLP Classifier. *International Symposium on Nanoelectronic and Information System*.

Araz R. A., Mohd S. M. R., Ghazali S., . (2018). Splicing Image Forgery Identification Based on Artificial Neural Network Approach and Texture Features. *Cluster Computeing, Springer*.

Emre Avuclu, Fatih Basciftci. (2018). New Approaches To Determine Age and Gender in Image Processing Techniques using Multilayer Perceptron Neutral Network. *Elsevier B.V.*

Hakimi F., Hairi M. (2015). Image Splicing Forgery Detection Based on Improved LBP and K-Nearest Neighboor Algorithm. *Article in Electronic Information and Planning*.

Hicham Amakdouf, Mostafa El Mallahi, Amal Zouhri, Ahmed Tahiru, Hassan Qjidaa. (2018). Classification and Recognition of 3D Image of Charlier Moments using a Multilayer Perceptron Achicture. *The First International Conference on Intelligent Computing in Data Sciences.* Science Direct.

Jalab, H. A. (2011). Image Retrieval System Based on Color Layout Descriptor and Gabor Filter. *IEEE Conference on Open System (ICO 2011).*

Jharna Majumdar, Santhosh Kumar K L, Venkatesh G M. (2015). Analysis of Video Shot Detection using Color Layout Descriptor and Video Summarization based on Expectation-Maximization Clustering. *International Conference on Cognitive Computing and Information Processing (CCIP).* Noida, India: IEEE.

Jong G. H., Tae H. P., Yong H. M., II K. E. (2018). Quantization-based Markov Feature Extraction Method For Image Splicing Detection. *Spring-Verlag GmbH Germany*.

Kaur, H., Kaur, K. (2015). Image Forgery Detection using Steerable Pyramid Transform and Lab Color Space. *International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5*.

Kotoulas L., Andreadis I. (2003). Colour Histogram Content-Based Image Retrieval and Hardware Implementation. *IEE proceedings-Circuit, Devices and System (Volume: 150, Issue: 5, 6 OCt 2003).* IET.

Kunika Verma, Ajay Khunteta. (20017). Facial Expression Recognition using Gabor Filter and Multi-layer Artificial Neural Network. *International Conference on Information, Communication, Instrumentation and Control (ICICIC).* Indore, India: IEEE.

Lu Wang, Zhiming Qiu. (2012). Combining Color Histogram and ORB Features for Robust Visual Tracking. *8th International Conference on Natural Computation* . Chongqing, China: IEEE.

Lumin, Zheng Ling Xiang. (2007). Contour Detection based on Gabor filter and directional DoG filter. *14th International Conference on Mechatronic and Machine Vision in Practice.* Xiamen, China: IEEE.

Marius C. P., Valentina E. B., Liliana P. P., Nikos M.,. (2009). Multilayer Perceptron and Neural Networks. *WSEAS Transactions on Circuits and Systems*.

Muhammad Imran, Rathiah Hashim, Noor Elaiza Abd Khalid. (2015). Segmentation-based Fractal Texture Analysis and Color Layout Descriptor for Content Based Image Retrieval. *14th International Conference on Intelligent System Design and Application.* Okinawa, Japan: IEEE.

Nikita Kashyap, Dr. Dharmendra Kumar Singh. (2017). Color Histogram Based Image Retrieval Technique for Diabetic Retinopathy Detection. *2nd International Conference for Convergency in Technology*. Mumbai, India: IEEE.

Nistha Parashar, Nirupama Tiwari, Deepika Dubey. (2016). A Survey of Digital Image Tempering Technique. *Internal Journal of Signal Processing, Image Processing and Pattern Recognittion Volume 9,2,*.

P.Sabeena Burvin, J.Monica Esther. (2014). Detection of Digital Image Splicing Using Luminance. *International Journal of Engineering Research and Application (IJERA)*.

Peerapon Chantharainthron, Sasipa Panthuwadeethorn, Suphakant Phimoltares. (2017). Robust Video Editing Detection Using Scalable Color and Color Laout Descriptor. *14th International Joint Conference on Computer Science and Software Engineering (JCSSE).* Nakhon Si Thammarant, Thailand: IEEE.

Priyadarsan Parida, Nilamani Bhoi. (2016). 2-D Gabor Filter Based Transition Region Extraction and Morphological Operation for Image Segmentation. *Elsevier Ltd*.

Ravichandran.K, Arulchelvan.S. (2017). The Model of Multilayer Perceptron Analysed The Crime News Awareness in India. *International Conference on Advanced Computing and Communication Syatem* . Coimbatore, India: IEEE.

Rishav Chakravarti, Xiannong Meng. (2009). A Study of Color Histogram Based Image Retrieval. *Sixth International Conference on Information Technology.*

Rohit Arora, Suman. (2012). Comparative Analysis of Classification Algorithm on Different Datasets using WEKA. *International Journal of Computer Apllication, Volume 54,*.

Rui Zhao, Yan Wu, Junbo Zhu, Zhihua WEi. (2011). Efficient Vehicle Identification using MPEG-7 Color Layout Descriptor. *International Conference on Business Management and Electronic Information.* Guangzhou, China: IEEE.

Ruziana Mohamad Rasli, T Zalizam T Muda, Yuhanis Yusof, Juhaida Abu Bakar. (2012). Comparative Analysis of Content Based Image Retrieval Technique using Color histogram. A case Study of GLCM and K-Means Clustering. *Third International Conference on Intelligent Systems Modelling and Simulation.* Kota Kinabalu, Sabah: IEEE.

Swagota Bera, Dr. Monisha Sharma, Dr. Bikesh Singh. (n.d.). Feature Extraction and Analysis using Gabor Filter and Higher Order Statistics for the JPEG Steganography. *International Journal of Applied Engineering Research ISSN vOLUME 13*, 2018.

Toqeer Mahmood, Tabassam Nawaz, Aun Irtaza, Rehan Ashraf, Mohsin Shah, Muhammad Tariq Mahmood. (2016). Copy-Move Forgery Detection Technique for Forensic Analysis in Digital Images. *Hindawi Publishing Corporation Mathematical Problem in Engineering Volume 2016*.

Vignesh T., Thyagharajan K. K. (2017). Water Bodies Identification from Multispectral Images using Gabor Filter, FCM, and Canny Edge Detection Methods. *International Conference on Information, Communication and Embedded System)ICICES).* Chennai, India: IEEE.

Weikang Yuan, Murat Hamit, Abdugheni Kutluk, Chuanbo Yan, Li Li, jianjun Chen, Yanting Hu, Fang Yang. (2013). Feature Extraction and Analysis on Xinjiang Uygur Medicine Image by using Color Histogram. *IEEE International Conference on Medical Imaging Physics and Engineering.* Shenyang, China: IEEE.

WEKA Open Source Software, Version 3.8.3, 1999-2018

Worapan Kusakunniran, Nantawat Prachasri, Nattaporn Dirakbussarakom, Duangkamol Yangchaem. (2017). Distinguishing ACL Patients from Healthy Individual using Multilayer Perceptron on Motion Pattern. *9th International Conference on Knowledge and Smart Technology (KST).* Chonburi, Thailand: IEEE.

Yoo Joo Choi, Ku Jin Kim, Yunyoung nam, We-Duke Cho. (2008). Retrieval of identical Clothing Images based on Local Color Histogram. *Third International Conference on Convergence and Hybrid Information Technology*. Busan, South Korea: IEEE.

Yuren Du, Yuan Feng. (2009). Vehicle Detection From Video Sequence Based on gabor Filter. *9th International Conference on Electronic Measurement and Instrument.* Beijing, China: IEEE.

Zanaty, E. A. (2012). Support Vector Machines (SVMs) versus Multilayer perception (MLP) in data classification. *Egyptian Information Journal*.