FEATURE BASE FUSION FOR SPLICING FORGERY DETECTION BASED ON NEURO FUZZY

HABIB GHAFFARI HADIGHEH

UNIVERSITI TEKNOLOGI MALAYSIA

FEATURE BASE FUSION FOR SPLICING FORGERY DETECTION BASED ON NEURO FUZZY

HABIB GHAFFARI HADIGHEH

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 2014

I lovingly dedicate this thesis to my family, specially my father and my wife who supported me each step of the way.

ACKNOWLEDGEMENT

A major research project like this is never the work of anyone alone. The contributions of many different people, in their different ways, have made this possible. I would like to extend my appreciation especially to the following.

All Praise For Allah, Creator Of This Universe Thanks For The Precious Iman & Islam You Blessed On Me Thanks For All The Strength And Knowledge You Granted On Me And Also Peace Be Upon The Holy Prophet Muhammad.

Prof. Dr. Ghazali Bin Sulong, for making this research possible. His support, guidance, advice throughout the research project are greatly appreciated. Indeed, without his guidance, I would not be able to put the topic together. Thanks Prof.

In particular, I would like to thank my father, Prof. Dr. Alireza Ghaffari, for his unconditional support, both financially and emotionally throw my master. His contribution and advices in the process of doing this project is undeniable.

Of course, this project would not have been possible without the participation of the subjects.

Last but not least, I would like to thank my mum, my wife and my sister. The patience and understanding that you show during these years are greatly appreciated.

ABSTRACT

Most of image forensics researches have mainly focused on detection of artifacts introduced by a single processing tool. Thus, they have lead in the development of many specialized algorithms looking for one or more particular footprints under distinct settings. Naturally, the performance of such algorithms are not perfect and accordingly the provided output they might be noisy, inaccurate and only partially correct. Furthermore, in practical scenarios, a forged image is often the result of utilizing several tools made available by the image-processing softwares. Therefore, reliable tamper detection requires developing several tools to deal with various tampering scenarios. Fusion of forgery detection tools based on Fuzzy Inference System has been used before for addressing this problem. Adjusting the Membership Functions and defining proper fuzzy rules for getting optimal results are a time consuming processes. This can be accounted as main disadvantage of Fuzzy Inference Systems. In this study, a Neuro Fuzzy Inference System for fusion of forgery detection tools is developed. The Neural Network characteristic of Neuro Fuzzy Inference Systems provide appropriate tool for automatically adjusting Membership Functions. Moreover, initial Fuzzy inference system is generated based on fuzzy clustering techniques. The purposed framework is implemented and validated on a benchmark image splicing dataset in which three forgery detection tools are fused based on Adaptive Neuro Fuzzy Inference System. The final outcome of the purposed method reveals that applying Neuro Fuzzy Inference systems could be a proper approach for fusion of forgery detection tools. On the best of our knowledge, this is the first time that Neuro Fuzzy Inference Systems employed for fusion of forgery detection tools. Therefore, more researches should be conducted to make it more practical and to increase the effectiveness of methodology.

ABSTRAK

Kebanyakan imej forensik kajian telah memberi tumpuan kepada pengesanan artifak yang diperkenalkan oleh alat pemprosesan tunggal. Oleh itu, mereka telah menerajui pembangunan banyak algoritma khusus mencari satu atau lebih kesan tertentu di bawah keadaan yang berbeza. Secara semula jadi, pelaksanaan algoritma tersebut tidak sempurna dan berdasarkan hasil yang diberi ia mungkin kabur, tidak tepat dan hanya sebahagiannya betul. Tambahan pula, dalam senario praktikal, kebanyakkan imej palsu adalah hasil daripada menggunakan beberapa alat yang disediakan oleh perisian pemprosesan imej. Oleh itu, pengesanan pengubahsuaian yang dipercayai memerlukan beberapa pembangunan alat untuk menangani pelbagai senario yang diubah suai. Gabungan alat pengesanan pemalsuan berdasarkan Fuzzy Inference System telah digunakan sebelum ini untuk menangani masalah ini. Melaraskan Membership Functions dan menentukan hukum fuzzy yang betul untuk mendapatkan hasil yang optimum adalah proses yang memakan masa. Ini boleh diambil kira sebagai kelemahan utama Fuzzy Inference System. Dalam kajian ini, satu Neuro Fuzzy Inference System untuk gabungan alat pengesanan pemalsuan dibangunkan. Ciri Neural Network daripada Neuro Fuzzy Inference Systems menyediakan alat yang sesuai secara automatik untuk menyesuaikan Membership Functions. Selain itu, pada awalnya Fuzzy inference system dihasilkan berdasarkan teknik fuzzy clustering. Tujuan rangka kerja dilaksanakan dan disahkan berdasarkan pada imej penanda aras splicing set data di mana tiga alat pengesanan pemalsuan adalah bergabung berdasarkan Adaptive Neuro Fuzzy Inference System. Hasil dapatan daripada kaedah yang bertujuan bagi mendedahkan bahawa mengguna pakai Neuro Fuzzy Inference Systems boleh dijadikan pendekatan yang sesuai untuk gabungan alat pengesanan pemalsuan. Pada pengetahuan kami, ini adalah kali pertama Neuro Fuzzy Inference Systems digunakan untuk gabungan alat pengesanan pemalsuan. Oleh itu, lebih banyak kajian perlu dijalankan untuk menjadikannya lebih praktikal dan untuk meningkatkan keberkesanan metodologi.

TABLE OF CONTENTS

CHAPTER	TITLE		PAGE
	DECLARATION		ii
	DEDICATION		iii
	ACKNOWLEDGEMENT		iv
	ABSTRACT		v
	ABSTRAK		vi
	TABLE OF CONTENTS		vii
	LIST OF TABLES		x
	LIST OF FIGURES		xi
	LIST OF ABBREVIATIONS		xiii
	LIST OF APPENDICES		xv
1	**INTRODUCTION**		
	1.1	Introduction	1
	1.2	Problem Background	4
	1.3	Problem Statement	7
	1.4	Objectives	8
	1.5	Project Scope	8
	1.6	Significance of Project	9
	1.7	Dissertation Organization	9
2	**LITERATURE REVIEW**		
	2.1	Introduction	11
	2.2	Different Color Spaces	11
	2.3	Different Image Formats	14
	2.4	How Digital Cameras Work?	15
		2.4.1 Color Filter Array Interpolation	18
		2.4.2 Standard Joint Photographic Experts Group (JPEG) Compression Scheme	19

2.5	Different Image Forgery Types		21
2.6	Different Forgery Detection Techniques		22
	2.6.1	Active Forgery Detection	22
		2.6.1.1 Passive Forgery Detection	23
	2.6.2	Splicing Detection Techniques	24
	2.6.3	Splicing Detection Features	25
2.7	Fuzzy Logic		30
	2.7.1	Fuzzy Sets	31
	2.7.2	Fuzzy Logic Operations	32
	2.7.3	Linguistic variables and hedges	33
2.8	Neural Network		35
2.9	Neuro Fuzzy		37
	2.9.1	Fuzzy Neurons	38
	2.9.2	Neuro Fuzzy Learning	43
	2.9.3	Input Space Partitioning	47
2.10	Forgery detection based on fusion		48
2.11	Summary		49

3 RESEARCH METHODOLOGY

3.1	Introduction		51
3.2	Research Framework and Processes		51
	3.2.1	Problem Formulation	53
	3.2.2	Literature Review	53
	3.2.3	Pre-Preparation	54
		3.2.3.1 Benchmark Image Dataset	55
		3.2.3.2 Reading the images	56
		3.2.3.3 Feature Extraction	57
		3.2.3.4 Boosting Feature Selection (BFS) alghorithm	63
		3.2.3.5 Support Vector Machine (SVM)	65
		3.2.3.6 Training and Testing process for SVM	67
	3.2.4	Fusion of forgery detection tools	68
		3.2.4.1 Converting Decision Value to Probability	68
	3.2.5	Neuro-Fuzzy Inference Systems	69
	3.2.6	Training and Testing ANFIS system	70
	3.2.7	Evaluation	71

			3.2.7.1 Sensitivity and specificity	72
			3.2.7.2 Area Under ROC Curve	74
	3.3	Implementation Tools		75
	3.4	Summary		76
4	**EXPERIMENTAL RESULTS AND DISCUSSION**			
	4.1	Introduction		77
	4.2	Pre-Preparation Results		77
		4.2.1	Discrete Wavelet Transform based feature extraction	78
		4.2.2	Edge Image based feature extraction	81
		4.2.3	N-Run Length feature extraction	86
		4.2.4	Discussion on the results	92
	4.3	Fusion of forgery detection tools		93
		4.3.1	Converting Decision Value to Probability Results	93
		4.3.2	Fusion based on Neuro-Fuzzy Inference System (NFIS) results	96
		4.3.3	Discussion on the results	100
	4.4	Comparisons and Evaluation		101
	4.5	Discussion		102
5	**CONCLUSION**			
	5.1	Introduction		104
	5.2	Dissertation Summary		104
	5.3	Dissertation Contribution		105
	5.4	Feature Works		106
REFERENCES				108
Appendices A – C				113 – 117

LIST OF TABLES

TABLE NO.	TITLE	PAGE
2.1	Different image forgery types	21
2.2	List of splicing forgery detection algorithms based on illumination analysis	26
2.3	List of splicing detection algorithms	27
2.4	List of Fuzzy Logic Operations	33
2.5	List of rules applicable for Fuzzy sets	33
2.6	Different kinds of Fuzzy neurons	39
2.7	Output of Fuzzy Logic system	40
2.8	List of training methods for Neuro-Fuzzy systems	46
3.1	List of the used Hardware	75
3.2	List of Softwares	75
4.1	DWT Forgery Detection Results.	81
4.2	Sample of a feature vector generated using Gray Level Co-occurrence Matrix and BFS by 30 element length.	83
4.3	Edge Based Forgery Detection Results.	86
4.4	Sample of features vector for N-Run Length forgery detection tool.	91
4.5	N-Run Length based forgery detection tool results	91
4.6	Evaluation Results based on NFIS fusion	100

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
1.1	Sample of an image forgery	3
1.2	Steps of Image Splicing	5
2.1	Liturature Review	12
2.2	Standard Red,Green,Blue (RGB) and Cyan,Magenta, Yellow (CMY) color spaces	13
2.3	Hue,Saturation,Value (HSV) color space	13
2.4	Initial optical-path block diagram for a digital camera	16
2.5	Single-sensor optical-path block of digital camera	17
2.6	A schematic view of a standard digital image acquisition pipeline	17
2.7	A popular CFA	19
2.8	Standard Discrete Cosine Transform (DCT)-Based compression processing steps	20
2.9	Fuzzy Logic diagrams demonstration	30
2.10	Basic Neural Network System	35
2.11	Adaptive-Network-based Fuzzy Inference System architecture for Sugenos reasoning method	41
3.1	Research Framework	52
3.2	Pre-Preparation Framework	55
3.3	Sample of image splicing forgery evaluation dataset	55
3.4	Process of image splicing	56
3.5	DWT based feature extraction pipeline	58
3.6	Prediction Context	59
3.7	Edge Image based feature extraction pipeline	61
3.8	Run-Length based feature extraction pipeline	64
3.9	Process of training/testing for SVM	67
3.10	Sample of sigmoidal base function curve	69
3.11	ANFIS training/testing process	71
3.12	Sample of Receiver Operating Curve (ROC) curve	74

4.1	Sample of the Prediction and the Error Images	79
4.2	Samples of the subbands calculated for an image	80
4.3	ROC plots of the results provided by DWT based Forgery Detection Tool	82
4.4	Sample of edge images calculated for an Original image	84
4.5	Sample of Edge images for a forged Image	85
4.6	ROC plots of the results obtained by Edge Image Based Forgery Detection Tool	87
4.7	Run-Length Histogram (RLH)s and Discrete Fourier Transform (DFT) calculated for an original image	89
4.8	RLHs and DFT calculated for a forged image.	90
4.9	ROC curves of N-Run Length results	91
4.10	Sigmoid functions for Run 1	94
4.11	Sigmoid function plots for Run 1	95
4.12	Sigmoid functions for N-Run Length based forgery detection tool, plotted for different Runs	96
4.13	Sample of distribution of input/output pairs for Binary classification	97
4.14	Grid partitioning Graphical User Interface (GUI) for generating an Fuzzy Inference System (FIS) system.	98
4.15	Structure of initial FIS.	98
4.16	Sample of an ANFIS training process	99
4.17	Comparison in Terms of Sensitivity	101
4.18	Comparison in Terms of Specificity	102

LIST OF ABBREVIATIONS

ANFIS	–	Adaptive-Network-based Fuzzy Inference System
AUC	–	Area Under Curve
AI	–	Artificial Intelligent
BFS	–	Boosting Feature Selection
BACM	–	Blocking Artifact Characteristics Matrix
CCD	–	Charged Coupled Device
CMY	–	Cyan,Magenta,Yellow
CF	–	Characteristic function
CFA	–	Color Filter Array
DCT	–	Discrete Cosine Transform
DIF	–	Detect Image Forgery
DFT	–	Discrete Fourier Transform
DWT	–	Discrete Wavelet Transform
FIS	–	Fuzzy Inference System
FS	–	Feature Selection
GPS	–	Geographical Positioning System
GLCM	–	Gray Level Co-occurrence Matrix
GUI	–	Graphical User Interface
HHT	–	Hilbert-Hang Transform
HSV	–	Hue,Saturation,Value
HSB	–	Hue,Saturation,Brightness
IQM	–	Image Quality Metrics
JPEG	–	Joint Photographic Experts Group
LZW	–	Lempel-Ziv-Welch
LDA	–	Linear Discriminant Analysis
MBDCT	–	Multi-size Block Discrete Cosine Transform
MF	–	Membership Function
NFIS	–	Neuro-Fuzzy Inference System

OSF	–	Order Statistic Filter
PKCS	–	Public Key Crypto Systems
RBF	–	Radial Basis Function
RGB	–	Red,Green,Blue
RLRN	–	Run-Length Run-Number
RL	–	Run length
RLH	–	Run-Length Histogram
ROC	–	Receiver Operating Curve
SVM	–	Support Vector Machine
TP	–	True Positive
FP	–	False Positive
TN	–	True Negative
FN	–	False Negative

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	Purposed BFS system	113
B	Grid search process	116
C	NFIS complete results	117

CHAPTER 1

INTRODUCTION

1.1 Introduction

Nowadays, so many devices exist for producing digital images. Almost, every communication device has access to the Internet and is equipped with a digital camera. Digital cameras with different qualities and capabilities which produce very high resolution digital images are available for both professionals and amateurs.

Currently, individuals spend considerable amount of time surfing the Internet and digital images appear to be an inevitable aspect of this context. The exploitation of digital images and photos taken by various smart recording devices is getting more tangible as the number of social networks such as Facebook, Twitter and Instagram increases and users tend to share every moments of their lives as well as some interesting occasions which happen in their countries, cites and neighbourhoods.

Moreover, images might be used to convey special messages deliberately. For instance, an image taken from a protest may be intended to show the power of numerous individuals supporting an idea which is ignored by the government. Or a picture taken form the private moments of famous people might be intended to reveal secretes about them which can change their lives dramatically or to put them in a situation in which they are forced to do things in favor of a third party that otherwise they would refuse to do in a normal condition. This innate and potential quality of an

image in general and digital image in particular would increase abuses such as image forgery and manipulation within the realm of digital image editing and postprocessing.

Editing and postprocessing operations are no longer limited to computer science laboratories and are not restricted to the researches. Now, with not too expensive softwares like Photoshop, it becomes an easy task to make different kind of changes on photos even by the persons with limited information on image processing. Most of the devices have some sort of free image processing softwares that helps people to convert and demonstrate the taken image as they intended. Softwares like 3D-max helps to create completely virtual images independent of other real photos. Most of the times, manipulation of images is done with the aim of increasing their performance, however it sometimes could be used to transfer an untrue message or disfigure an existing fact. Figure 1.1 illustrates a very famous forged image that shows a very famous celebrity next to a politician. This image affected the Senator John Kerry's destiny in the United State of America presidential election on 2004. The person who created this image by composting two different images was arrested and this image itself was used as a clue and proving evidence of the criminality in the court.

According to the above mentioned intentions, it is easily seen that finding the integrity of images is very important and attracted many researches to work on detecting the possible forgery on images. In general, there are two forgery detection categories, the active detection methods and the passive ones which are known as blind detection methods (Farid, 2009).

Active forgery detection methods follow the idea of inserting information inside the images and use them for authentication and showing the integrity of the images. These methods include two common techniques, *digital watermarking* and *digital signature*. The problem in using these techniques is that, these information must be inserted into the image during taking the photos or just during the post processing operations. Inserting these information needs special kind of softwares as well as specialized hardwares included in devices. For this reason, it is almost impossible to discover the trace of forgery and it is almost a hard task to authenticate the originality

Figure 1.1: This is one of the most famous sample of image forgery. This picture belongs to John Kerry and Jane Fonda at Anti-War Rally which is a faked image and its purpose is to show that these two persons standing together at podium during 1970s anti-war rally.

of the most daily taken images. On the other hand, it is a very hard task to remove and reinsert these information on photos (Katzenbeisser *et al.*, 2000; Cox *et al.*, 2003).

Unlike the active methods, passive methods use the information of the image itself to detect the forgery. For this purpose, these methods search the image to find any trace of forgery and it makes these methods more practical than the active ones because most of the images in real life is not accompanied with a watermark inside (Farid, 2009).

There are different kinds of passive methods for detecting possible forgeries and none of them claims to have 100% accuracy (Kirchner and Bohme, 2008), because forgers sometimes do it with such proficiency that makes the detection very hard and even an impossible job (Kirchner and Böhme, 2007; Kirchner and Bohme, 2008). There are many types of image forgery methods such as image splicing, copy-paste attack, and image retouching. It is almost impractical to use a single method for detecting different kinds of forgeries, because there should be a common characteristics or features to be used for detecting them (Avcibas *et al.*, 2004; Hsiao and Pei, 2005). Therefore, most of the researches just focus on one type of forgery.

The main objective of image splicing is is to develop a new image from two or more images, and it is wildly used for image forgery. Image splicing detection is the main difficulty in image forensics. However, there is almost no ultimate solution for the problem(Ms. Sushama, 2014). Therefor, the current research concentrates on the splicing forgery attacks.

1.2 Problem Background

Image splicing is a technology of image forgery carried out by combining image fragments from the same image or others without further postprocessing such

as smoothing of boundaries among adjacent fragments (Zhang *et al.*, 2008). Figure 1.2 depicts the steps of generating a splicing forgery. $F(x, y)$ and $G(x, y)$ are two images and $H(x, y)$ is a fragment of F intended to be moved into the G and the $I(x, y)$ is the resulted image. It is important to mention that F and G might be identical.

Many researches carried out on detecting the splicing forgery. First group of researches focused on detecting the possible forgery using statistical analysis of pixel information and the second group diverted their focus on detecting the inconsistency of the light directions to trace the potentially existent splicing forgery (Redi *et al.*, 2011).

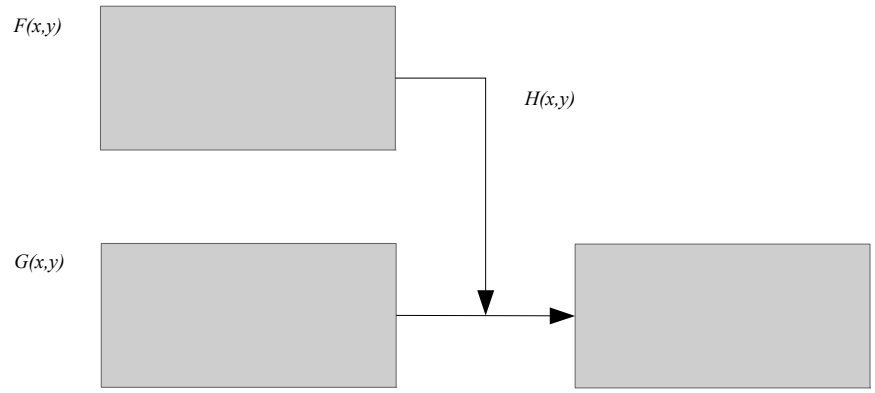

Figure 1.2: Steps of Image Splicing.

Simple splicing operation itself, even when visually masked with blending techniques, leaves its traces in the image statistics. Thus, it seems possible to use these traces for detecting the splicing forgery. This is the idea of the first group of researches.

Ng *et al.* (2004a) work was one of the early researches in this area. They used the idea initiated by Farid (1999) as a base of their work. Farid (1999) work is also one of the first studies for finding the traces of forgery in digital signals. The authors idea is as, when deformation in digital data happens, it would be possible to detect traces of this distortion using the spectrum analysis. The auther showed that power spectrum (1'st order correlation) is unable to detect this kind of traces and he recommended

to apply higher order correlations and as a result, he used bispectrum (Third-order correlation) for detecting audio signals forgery. Ng *et al.* (2004a) generalized the Farid (1999) idea in image processing and considered the information of pixels as a 2d signal. By using bispectrum of harmonically related Fourier frequencies of a signal, it is possible to capture quite discontinuities introduced in an image after splicing.

On the other hand, second group focused on detecting forgery using illumination analysis. The main idea is, when an authenticated image is processed for illumination direction, majority of objects in the image would have the same or very similar lighting direction. Illumination direction could be detected by processing the intensity of the colors in the neighboring pixels (Redi *et al.*, 2011). Though modern editing tools allow to conceal the traces of splicing in a convincing way, it is not always possible for the forger even for the professional one to match the lighting conditions of the regions that make up the composite, as in the well-known case of the Kerry and Fonda photomontage(Figure1.1). Several studies are dedicated to forgery detection through the scene illumination analysis. A first attempt was proposed by Johnson and Farid (2005), in which they estimated the incident light direction for different objects in order to highlight the mismatches. Similar approaches could be find in Johnson and Farid (2007b) and Zhang *et al.* (2009).

Even though very good studies have been done in the area of splicing forgery detection and lots of techniques have been introduced for this purpose, it is still not an easy task to detect forgeries with reasonable accuracy. The imperfection of accuracy might happen due to performing post processing operations for hiding the traces of forgery or utilizing lossy compression formats. This is the problem that could be referred to as “Uncertainty”(Barni and Costanzo, 2012).

One approach for dealing with uncertainty in detecting splicing forgery attack is using more than one detection tool simultaneously. This could be done by using fusion. In the area of splicing detection by the use of fusion, there are two approaches. One which use it before decision making process, and the other use fusion after making the decision.

The (Fu *et al.*, 2006; Dong *et al.*, 2009; Chetty and Singh, 2010) are the studies which use fusion of features before decision making process. On the best of our knowledge there is only one experiment that has used fusion after decision making process of forgery detection tools(Barni and Costanzo, 2012).

Using fuzzy for fusion of forgery detection tools has been remained on touched for a long time Chetty and Singh (2010); Barni and Costanzo (2012) and there is still good chance to use it in this area. The term "Fuzzy logic" was introduced in 1965 by (Zadeh, 1965). Fuzzy logic has been applied in many fields, from control theory to artificial intelligence. The main advantage of fuzzy inference systems is the ability of dealing with incomplete information. This makes fuzzy logic a good choice for solving the problem of uncertainty in forgery detection.

The problem of fuzzy logic based systems is that adjusting of Membership Function (MF) for getting accurate results is a time consuming process. The hypothesis in this study is using NFIS system instead of FIS. By fusing splicing forgery detection tools using NFIS, adjustment of MF could be done automatically and this option would decrease the time required for forgery detection. According to the provided literature, this is the first time that NFIS based approach is used for splicing forgery detection and it is anticipated that the obtained results would be better using this method.

1.3 Problem Statement

Very good researches have been done in this area and lots of features have been introduced for this purpose, it is still not an easy task to detect forgeries with reasonable accuracy is referred to as uncertainty. One approach for addressing the uncertainty is to use FIS for combining some forgery detection techniques. To the best of our knowledge, there are only two published works exist that use FIS addressing the uncertainty Chetty and Singh (2010); Barni and Costanzo (2012). Limitation on

using the fuzzy based system is, for having better results, the MFs should be adjusted manually and different kinds of fuzzy rules should be tested which is a very time consuming process.

1.4 Objectives

Based on the problem statement, the following objectives are stated:

1. To investigate feature extraction and decision making by SVM for splicing forgery detection tools.
2. To Enhance the accuracy of detection by fusion of splicing detection tools based on DWT decompositions analysis, Edge Image analysis using GLCM and N-Run Length matrices analysis.
3. To evaluate the performance of proposed method compare to each forgery detection tool individually.

1.5 Project Scope

The dissertation is bounded to the following scopes:

1. We focus on one type of image forgery; the splicing attack.
2. DWT decompositions analysis, Edge Image analysis using GLCM and N-Run Length matrices analysis are three forgery detection tools that are used for feature extraction and fusion.
3. MATLAB will be used to implement the proposed algorithms.

4. We are focusing on detecting the forgery images. Targeting the forgery location is out of our scope.

1.6 Significance of Project

One of the techniques for fusion of forgery detection tools is using fuzzy inference systems. To the best of our knowledge, there are two experiments that used this approach for fusion. Chetty and Singh (2010) relies on Fuzzy integrals applied to the features extracted by forensic algorithms and Barni and Costanzo (2012) uses Fuzzy rule-based system in which the input of system is the final decision regarding each forensic tool.

The disadvantage of using Fuzzy based system is that the MFs should be adjusted manually which is time consuming. Also, it is necessary to define good fuzzy rules in order to obtain good results. Moreover, these adjustments of MFs and defining the fuzzy rules depend on the expert idea. A Neural Network characteristic of the purposed approach helps MFs to be adjusted automatically. Also, the characteristic of grid partitioning helps the NFIS systems to define the whole FIS automatically. This will save considerable amount of time.

1.7 Dissertation Organization

This dissertation is organized as follows. Chapter 2 includes the literature review. It consist of fundamental information of image processing, fuzzy logic, NFIS as well as thoroughly study of forgery attacks, different forgery detection and splicing forgery detection techniques. Chapter 3 presents the proposed methodology of this dissertation . Chapter 4 includes the experimental results and discussions based on the

proposed methodology. Chapter 5 describe the overall conclusion of the dissertation and feature works.

REFERENCES

Adams, J., Parulski, K. and Spaulding, K.1998. Color processing in digital cameras. *Micro, IEEE*. 18(6), 20–30.

Avcibas, I., Bayram, S., Memon, N., Ramkumar, M. and Sankur, B.2004. A classifier design for detecting image manipulations. In *Image Processing, 2004. ICIP'04. 2004 International Conference on*, vol. 4. IEEE, 2645–2648.

Barni, M. and Costanzo, A.2012. A fuzzy approach to deal with uncertainty in image forensics. *Signal Processing: Image Communication*.

Carlsson, C. and Fullér, R.1998. *Optimization with linguistic values*. Technical report. TUCS Technical Reports.

Castillo, O., Melin, P., Kacprzyk, J. and Pedrycz, W.2007. Type-2 Fuzzy Logic: Theory and Applications. In *Granular Computing, 2007. GRC 2007. IEEE International Conference on*. Nov. 145–145. doi:10.1109/GrC.2007.118.

Chang, C.-C. and Lin, C.-J.2011. LIBSVM: a library for support vector machines. *ACM Transactions on Intelligent Systems and Technology (TIST)*. 2(3), 27.

Chen, W., Shi, Y. Q. and Su, W.2007. Image splicing detection using 2-d phase congruency and statistical moments of characteristic function. In *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series*, vol. 6505. Citeseer, 26.

Chetty, G. and Singh, M.2010. Nonintrusive image tamper detection based on fuzzy fusion. *International Journal of Computer Science and Network Security*. 10, 86–90.

Cox, I., Miller, M. and Bloom, J.2003. Digital Watermarking Morgan Kaufmann Publishers. *San Francisco, CA*.

Curry, H. B.1944. The method of steepest descent for nonlinear minimization problems. *Quart. Appl. Math.* 2(3), 250–261.

Dong, J., Wang, W., Tan, T. and Shi, Y. Q.2009. Run-length and edge statistics based approach for image splicing detection. In *Digital Watermarking*. (pp. 76–87). Springer.

Fang, Y., Dirik, A. E., Sun, X. and Memon, N.2009. Source class identification for DSLR and compact cameras. In *Multimedia Signal Processing, 2009. MMSP'09. IEEE International Workshop on*. IEEE, 1–5.

Farid, H.1999. Detecting digital forgeries using bispectral analysis.

Farid, H.2004. Creating and detecting doctored and virtual images. *Implications to The Child Pornography Prevention Act*, 280–291.

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

Fu, D., Shi, Y. Q. and Su, W.2006. Detection of image splicing based on hilbert-huang transform and moments of characteristic functions with wavelet decomposition. In *Digital Watermarking*. (pp. 177–187). Springer.

Fullér, R.2000. *Introduction to neuro-fuzzy systems*. vol. 2. Springer.

Fullér, R. and Zimmermann, H.-J.1993. On Zadehs compositional rule of inference. In *Fuzzy Logic*. (pp. 193–200). Springer.

Hájek, P.1998. *Metamathematics of fuzzy logic*. vol. 4. Springer.

Hirota, K. and Pedrycz, W.1994. OR/AND neuron in modeling fuzzy set connectives. *Fuzzy Systems, IEEE Transactions on*. 2(2), 151–161.

Hsiao, D.-Y. and Pei, S.-C.2005. Detecting digital tampering by blur estimation. In *Systematic Approaches to Digital Forensic Engineering, 2005. First International Workshop on*. IEEE, 264–278.

Hsu, Y.-F. and Chang, S.-F.2006. Detecting image splicing using geometry invariants and camera characteristics consistency. In *Multimedia and Expo, 2006 IEEE International Conference on*. IEEE, 549–552.

Hsu, Y.-F. and Chang, S.-F.2010. Camera response functions for image forensics: an automatic algorithm for splicing detection. *Information Forensics and Security, IEEE Transactions on*. 5(4), 816–825.

Hulsurkar, S., Biswal, M. P. and Sinha, S. B.1997. Fuzzy programming approach to multi-objective stochastic linear programming problems. *Fuzzy Sets and Systems*. 88(2), 173–181.

Ichihashi, H.1991. Iterative fuzzy modeling and a hierarchical network. In *Proceedings of the Fourth IFSA Congress, Vol. Engineering, Brussels*. 49–52.

Jang, J.-S.1993. ANFIS: adaptive-network-based fuzzy inference system. *Systems, Man and Cybernetics, IEEE Transactions on*. 23(3), 665–685.

Jing Dong, W. W.2011. *CASIA Tampering Detection Dataset*. Retrievable at http://forensics.idealtest.org.

Johnson, M. K. and Farid, H.2005. Exposing digital forgeries by detecting inconsistencies in lighting. In *Proceedings of the 7th workshop on Multimedia and security*. ACM, 1–10.

Johnson, M. K. and Farid, H.2007a. Exposing digital forgeries in complex lighting environments. *Information Forensics and Security, IEEE Transactions on*. 2(3), 450–461.

Johnson, M. K. and Farid, H.2007b. Exposing digital forgeries through specular highlights on the eye. In *Information Hiding*. Springer, 311–325.

Katzenbeisser, S., Petitcolas, F. A. *et al.*2000. *Information hiding techniques for steganography and digital watermarking*. vol. 316. Artech house Norwood.

Kirchner, M. and Böhme, R.2007. Tamper hiding: Defeating image forensics. In *Information Hiding*. Springer, 326–341.

Kirchner, M. and Bohme, R.2008. Hiding traces of resampling in digital images. *Information Forensics and Security, IEEE Transactions on*. 3(4), 582–592.

Lin, H.-T., Lin, C.-J. and Weng, R. C.2007. A note on Platts probabilistic outputs for support vector machines. *Machine learning*. 68(3), 267–276.

Lin, Z., Wang, R., Tang, X. and Shum, H.-Y.2005. Detecting doctored images using camera response normality and consistency. In *Computer Vision and Pattern Recognition, 2005. CVPR 2005. IEEE Computer Society Conference on*, vol. 1. IEEE, 1087–1092.

Liu, Q. and Sung, A. H.2009. A new approach for JPEG resize and image splicing detection. In *Proceedings of the First ACM workshop on Multimedia in forensics*. ACM, 43–48.

Majid Valiollahzadeh, S., Sayadiyan, A. and Nazari, M.2008. Face Detection Using Adaboosted SVM-Based Component Classifier.

Malvar, H. S., He, L.-w. and Cutler, R.2004. High-quality linear interpolation for demosaicing of Bayer-patterned color images. In *Acoustics, Speech, and Signal Processing, 2004. Proceedings.(ICASSP'04). IEEE International Conference on*, vol. 3. IEEE, iii–485.

Mathias, E. and Conci, A.1998. Comparing the influence of color spaces and metrics in content-based image retrieval. In *Computer Graphics, Image Processing, and Vision, 1998. Proceedings. SIBGRAPI'98. International Symposium on*. IEEE, 371–378.

Ms. Sushama, G. R.2014. Review of Detection of Digital Image Splicing Forgeries with illumination color Estimation. *International Journal of Emerging Research in Management &Technology*. 3(3).

Negnevitsky, M.2005. *Artificial intelligence: a guide to intelligent systems*. Pearson Education.

Ng, T.-T., Chang, S.-F. and Sun, Q.2004a. Blind detection of photomontage using higher order statistics. In *Circuits and Systems, 2004. ISCAS'04. Proceedings of the 2004 International Symposium on*, vol. 5. IEEE, V–688.

Ng, T.-T., Chang, S.-F. and Sun, Q.2004b. A data set of authentic and spliced image blocks. *Columbia University, ADVENT Technical Report*, 203–2004.

Nomura, H., Hayashi, I. and Wakami, N.1992. A learning method of fuzzy inference rules by descent method. In *Fuzzy Systems, 1992., IEEE International Conference on*. IEEE, 203–210.

Platt, J. *et al.*1999. Probabilistic outputs for support vector machines and comparisons to regularized likelihood methods. *Advances in large margin classifiers*. 10(3), 61–74.

Qu, Z., Qiu, G. and Huang, J.2009. Detect digital image splicing with visual cues. In *Information Hiding*. Springer, 247–261.

Redi, J. A., Taktak, W. and Dugelay, J.-L.2011. Digital image forensics: a booklet for beginners. *Multimedia Tools and Applications*. 51(1), 133–162.

Shaw, S.1999. JISC Technology Applications Programme (JTAP)Overview of Watermarks, Fingerprints, and Digital Signatures. *The University of Edinburgh*.

Shi, Y. Q., Chen, C. and Chen, W.2007. A natural image model approach to splicing detection. In *Proceedings of the 9th workshop on Multimedia & security*. ACM, 51–62.

Tieu, K. and Viola, P.2004. Boosting image retrieval. *International Journal of Computer Vision*. 56(1-2), 17–36.

Turevskiy, A.2014. *Design and simulate fuzzy logic systems*. Retrievable at http://www.mathworks.com/products/fuzzy-logic/.

Wang, W., Dong, J. and Tan, T.2009. Effective image splicing detection based on image chroma. In *Image Processing (ICIP), 2009 16th IEEE International Conference on*. IEEE, 1257–1260.

Wolfgang, R. B. and Delp, E. J.1996. A watermark for digital images. In *Image Processing, 1996. Proceedings., International Conference on*, vol. 3. IEEE, 219–222.

Yager, R. R. and Zadeh, L. A.1992. *An introduction to fuzzy logic applications in intelligent systems*. Kluwer Academic Publishers.

Yu-Feng Hsu, S.-F.2006. *Columbia Image Splicing Detection Evaluation Dataset*. Retrievable at http://www.ee.columbia.edu/ln/dvmm/downloads/AuthSplicedDataSet/AuthSplicedDataSet.htm.

Zadeh, L. A.1965. Fuzzy sets. *Information and control*. 8(3), 338–353.

Zhang, C. and Zhang, H.2007. Detecting digital image forgeries through weighted local entropy. In *Signal Processing and Information Technology, 2007 IEEE International Symposium on*. IEEE, 62–67.

Zhang, W., Cao, X., Zhang, J., Zhu, J. and Wang, P.2009. Detecting photographic composites using shadows. In *Multimedia and Expo, 2009. ICME 2009. IEEE International Conference on*. IEEE, 1042–1045.

Zhang, Z., Zhou, Y., Kang, J. and Ren, Y.2008. Study of Image Splicing Detection. In *Advanced Intelligent Computing Theories and Applications. With Aspects of Theoretical and Methodological Issues*. (pp. 1103–1110). Springer.

Zhao, X., Li, J., Li, S. and Wang, S.2011. Detecting digital image splicing in chroma spaces. In *Digital Watermarking*. (pp. 12–22). Springer.