WATERMARK REDUNDANCY USING SUDOKU

SHAMSUL KAMAL BIN AHMAD KHALID

A thesis submitted in
fulfillment of the requirement for the award of the
Doctor of Philosophy

Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia

APRIL 2018

DEDICATION

For my beloved family and the ummah.

ACKNOWLEDGMENT

All thanks to Allah S.W.T. Peace be upon Muhammad S.A.W. I am greatly in debt to my supervisors, particularly the most respected Professor Dr. Mustafa bin Mat Deris, Dr. Kamarudin Malik bin Mohamad, and my research buddies at the fifth floor of FSKTM. And, last but not least I am so grateful for the unceasing supports from my wife Dr. Noor Azah binti Samsudin and all my children – Aishah Amirah, Muhammad Muadz and Asma' Athirah - to bear the psychological cost of my PhD roller coaster rides. Ironically, although this is an arduous and long journey, not to anyone's liking, I felt it was all necessary process to break and reconstruct my new self. If you cannot see, you cannot be.

ABSTRACT

In today's world, designer of a watermarking system had to constantly faced with determined attacks to remove copyright information from a watermarked cover image. Due to these attacks, a watermark could be seriously corrupted and not detectable anymore or the watermark could be so noisy that it's proof of ownership is questionable. Many redundant watermarking systems have been proposed to address these problem. However, they are not designed with adequate redundancies to protect the watermark, and existing metrics merely disregard noisy watermarks for proof of ownership. In this thesis, a new watermark redundancy using Sudoku watermarking is proposed. In Sudoku watermarking, an 81-digit Sudoku "serial" numbers are embedded into a cover image. These numbers are represented in the form of series of small image tiles, constructed from a given watermark. The 81 tiles were divided into halves or more and hidden into the cover image using multiple schemes (composite schemes) that would complementarily protect the watermark from different attacks. During retrieval process, the image tiles are converted back to its Sudoku number. Due to attacks, some numbers may be missing. However, as other numbers will likely remain protected due to the composite schemes, these missing numbers can be regenerated back to its full Sudoku key by using a Sudoku solver. As a result, the image tile usage, the composite schemes and the Sudoku solver collaboratively enable verification of watermark for noisy and missing watermark. Using the classic 9×9 Sudoku puzzle, the proposed approach has been implemented and tested with Salt and Pepper, Cropping, Gaussian, compression, Poisson, speckle, low pass filter, high pass filter and contrast attacks on standard test images. The approach is found to be able to improve detection by 19% as compared to existing methods when attacked by random cropping and by 10% improvement with Salt and Pepper attack. For the rest of the attacks, the average correct number of tiles recovered (NoT) and correct Sudoku key (CoK) are 75% and 100%, respectively. The result indicates that the new layers of

redundancy improve detection of watermark. Furthermore, the binary metric (CoK) can be used to standardize evaluation of watermarking systems.

ABSTRAK

Pada masa kini, pereka bentuk sistem tera air terpaksa mendepani pelbagai serangan untuk membuang maklumat hakcipta daripada sesebuah imej yang telah ditera air. Kesan daripada serangan-serangan ini, sesebuah tera air boleh rosak dengan teruk dan kemungkinan tidak dapat dikesan lagi atau tera air itu boleh menjadi sangat bising sehingga tidak dapat digunakan sebagai bukti hakcipta. Banyak sistem tera air lebihan telah dicadangkan untuk mengatasi masalah ini. Tetapi, sistem-sistem ini tidak direkabentuk dengan lebihan yang mencukupi untuk melindungi tera air, dan pengukur semasa tidak mengambil kira tera air bising dalam proses pengesahan hakcipta. Didalam tesis ini, lebihan tera air yang baru menggunakan sistem tera air Sudoku telah dicadangkan. Didalam sistem tera air Sudoku, beberapa salinan tera air akan dipecahkan kepada jubin-jubin kecil dan jubin-jubin ini dikaitkan dengan kekunci Sudoku yang tertentu. Jubin-jubin kecil ini pula akan dibahagikan kepada dua bahagian atau lebih dan disembunyikan didalam imej hos menggunakan skim-skim penanaman tera air yang berbeza yang akan saling melindungi tera air itu mengikut kekuatan skim masing-masing. Semasa proses mendapatkan semula tera air, jubin-jubin yang rosak akan ditukar semula kepada nombor-nombor Sudoku. Kesan daripada serangan tera air, sebahagian kecil nombor-nombor mungkin hilang. Walaubagaimana pun, oleh kerana nombor-nombor lain akan tetap terpelihara akibat penggunaan skim komposit, nombor-nombor Sudoku yang tidak lengkap akan dapat dihasilkan semula kepada kekunci penuh Sudoku menggunakan sebuah penyelesai Sudoku. Penggunaan jubin, skema komposit dan penyelesai Sudoku secara kerjasama yang efektif telah membolehkan pengesahan tera air bagi tera air yang rosak dan tidak lengkap dapat dilakukan. Menggunakan Sudoku klasik berkonfigurasi 9×9, kaedah yang dicadangkan telah dilaksanakan dan diuji dengan serangan *Salt and Pepper*, pemotongan, *Gaussian*, mampatan, *Poisson*, speckle, tapisan rendah dan tapisan tinggi

dan juga serangan *contrast* menggunakan imej-imej pengujian piawai yang biasa digunakan dalam penyelidikan tera air. Kaedah ini didapati mampu meningkatkan pengesanan tera air sehingga 19% berbanding kaedah semasa apabila diserang oleh pemotongan rawak dan sehingga 10% apabila diserang oleh serangan *Salt and Pepper*. Untuk serangan-serangan lain yang tersenarai diatas, purata jumpaan semula jubin yang betul (NoT) dan purata kekunci yang betul (CoK) adalah tinggi iaitu pada tahap 75% dan 100%, masing-masing. Keputusan ini menunjukkan penggunaan beberapa lapis lebihan didalam sistem tera air Sudoku dapat meningkatkan pengesanan tera air. Selain itu, metric perduaan (CoK) boleh digunakan untuk mempiawaikan penilaian sistem-sistem tera air.

TABLE OF CONTENTS

TITLE			**i**
DECLARATION			**ii**
DEDICATION			**iii**
ACKNOWLEDGEMENT			**iv**
ABSTRACT			**v**
ABSTRAK			**vii**
TABLE OF CONTENTS			**ix**
LIST OF TABLES			**xii**
LIST OF FIGURES			**xiv**
LIST OF SYMBOLS AND ABBREVIATIONS			**xvi**
LIST OF APPENDICES			**xvii**
CHAPTER 1	**INTRODUCTION**		**1**
	1.1	Background	1
	1.2	A Watermarking System	2
	1.3	Network Redundancy	4
	1.4	Problem Statement	5
	1.5	Research Objectives	6
	1.6	Contributions	6
	1.7	Research Scope	8
	1.8	Thesis Organisation	8
CHAPTER 2	**LITERATURE REVIEW**		**9**
	2.1	Introduction	9
	2.2	Overview of Watermarking	9
	2.3	Origin of Watermarking	10

2.4	Watermarking for the Digital Age	11
2.5	Applications of Watermarking	11
2.6	Requirements of a Watermarking System	13
2.7	Attacks on Watermarking	13
2.8	Current Approaches to Watermarking	14
2.9	Types of Watermarking System	16
2.10	How Existing Schemes Perform Against Cropping and Salt and Pepper Attacks	17
2.11	Redundancy as an Important Strategy	20
2.12	Sudoku	22
2.13	Sudoku Approach in Security and Data Hiding	23
2.14	Comparison of Approaches in Watermark Redundancy	24
2.15	Chapter Summary	33
CHAPTER 3	**RESEARCH METHODOLOGY**	**34**
3.1	Introduction	34
3.2	Research Framework	34
3.3	Promising Redundant Characteristics in Sudoku	37
3.4	Conceptual Model of the Proposed Solution	38
3.5	Performance Evaluation	40
3.6	Experimental Setup and Tools	40
3.7	Benchmarking	41
3.8	Chapter Summary	41
CHAPTER 4	**SUDOKU WATERMARKING (SW)**	**43**
4.1	Introduction	43
4.2	Sudoku Theory	43
4.3	Hopfield Networks	49
4.4	Composite Functions	53
4.5	Sudoku Watermarking	54
4.6	Numbered Image Tiles	57

	4.7	Composite Watermarking Schemes	58
	4.8	Support for Noisy and Missing Watermark Regeneration	59
	4.9	Basic 4-bits Tiles SW Variant	61
	4.10	Advanced 64-bits Image Tiles SW Variant	72
	4.11	Comments on the New Performance Metrics	79
	4.12	Chapter Summary	81
CHAPTER 5	**RESULTS AND ANALYSIS**		**82**
	5.1	Introduction	82
	5.2	Fusion of Image Watermark with a Sudoku Key	82
	5.3	Experiment 1: Salt and Pepper Attacks	83
	5.4	Experiment 2: Cropping Attacks	88
	5.5	Experiment 3: Compression, Gaussian, Poisson, Speckle, Low pass filter, High Pass Filter and Contrast Attacks	92
	5.6	Analysis of Results	94
	5.7	Chapter Summary	96
CHAPTER 6	**CONCLUSION**		**97**
	6.1	Research Summaries	97
	6.2	Research Contributions	98
	6.3	Future Works	99
REFERENCES			**100**
APPENDICES			**111**
LIST OF PUBLICATIONS			**124**
VITA			**125**

LIST OF TABLES

2.1	Comparison of Watermarking Schemes against Cropping Attacks	17
2.2	Comparison of Approaches against Salt and Pepper Attacks	19
2.3	Usage of Sudoku	24
2.4	Comparison of Various Approaches in Watermark Redundancy	25
4.1	Table of Schemes	60
4.2	Sudoku Number Representation	60
4.3	Set of Skeys per function as listed in MoS	62
4.4	Sample Pixel values (partial)	63
4.5	The RInfo table retrieved from RInfo	66
4.6	An Example of Tiles to Sudoku number Translation Table	71
5.1	Experiment 2B: Salt & Pepper	84
5.2	Comparison of Sudoku-based Redundant Watermarking Schemes	85
5.3	Watermark with cropping ratio & detection result	87

5.4 Comparison of anti cropping with other watermarking schemes 90

5.5 Detection of tiles under different attacks 91

LIST OF FIGURES

1.1	A watermarking communication model	3
2.1	A Sudoku solution	22
2.2	A Summary of Redundant Mechanisms in Existing Multiple Watermarking Approach	31
3.1	Research Framework	33
3.2	Noisy Watermarks are Discarded	35
3.3	Sudoku Characteristics	36
3.4	Sudoku Watermarking Conceptual Model	38
4.1	A Sudoku puzzle of rank 3 with 17 filled cells	46
4.2	A Sudoku solution for Figure 3.1	46
4.3	A Hopfield Network Configuration	47
4.4	An Example of a 10x12 pattern	47
4.5	Numbered Tiles are Used and Flattened to form Sudoku Serial Number	55
4.6	Composite Watermarking Scheme	56
4.7	Converting Noisy Tiles to Sudoku Numbers	57
4.8	Missing Tiles Regeneration using Sudoku Solver	58

4.9	Embed 4-bits Tiles SW	59
4.10	An Skey (a Sudoku solution)	61
4.11	Matrix of Schemes	61
4.12	Retrieve 4-bits Tiles SW	65
4.13	A corrupted retrieved Skey due to watermarking attack	70
4.14	Embed 64-bits Tiles SW	70
4.15	An image being cut into 9 pieces and assigned with a tile number	71
4.16	An augmented watermark is created using a Sudoku key	73
4.17	Embedding Procedure	74
4.18	Retrieve 64 bits Tiles SW	75
4.19	Detection Procedure	77
5.1	Watermark Image Fusion with a Sudoku Key	81
5.2	Sample watermarked image and the noisy watermarks	82
5.3	A Sudoku key embedded into the cover image	83
5.4	Recovered Tiles	83
5.5	The effect of different image content on the recovery rates	85
5.6	Graph of Cropping vs tiles detectors	89

LIST OF ABBREVIATIONS AND SYMBOLS

CWS	-	Composite Watermarking using Sudoku
DCT	-	Discrete Cosine Transform
DWT	-	Discrete Wavelet Transform
LSB	-	Least Significant Bit
MoS	-	Matrix of Scheme
Skey	-	Sudoku Key
RInfo	-	Retrieval Information
MSE	-	Mean Square Error
PSNR	-	Peak Signal to Noise Ratio
SSIM	-	Structural Similarity Index Measurement
BER	-	Bit Error Rate
NoT	-	Number of Correct Tiles
PoC	-	Percentage of Completed Tiles
CoK	-	Completeness of Sudoku Key

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	Sample Codes	111
B	List of Publications	124
C	Vita	125

CHAPTER 1

INTRODUCTION

1.1 Background

The availability of broadband and smartphone technology has contributed significantly to the growth and transmission of digital information. This availability and the introduction of social media applications have accelerated the popularity of communicating digital content over the Internet. Digital content such as images, video, and audio have been revolutionized in a way that they can be easily captured, stored, transmitted, and manipulated. Some of these digital content is freely accessible via YouTube, Google Images, Flickr, blogs and websites. But these access channel also unfortunately provides virtually unprecedented opportunities to illegally use copyrighted material (Shivani et al., 2017).

A number of techniques can be used to protect a copyrighted document. The first and probably the most common method of protecting a document is cryptography. It is essentially a very well developed method with strong fundamentals and concepts that has evolved due to war needs. Nowadays, business documents such as account records can be securely shared between a seller and a customer over the Internet. For example, Choi et al. (2014) designed a framework with multiple security mechanisms that includes watermarking of government documents for secure sharing. Without appropriate key, an attacker cannot open the document even if they manage to capture the document during transit. However, this protection of a document ends once it is decrypted. For example, a person may purchase commercial images via a legal channel. He will be given a key to open the images. After decryption, the person can now copy and distribute these images as he wishes.

Thus, a technology that can protect documents beyond decryption is needed. This requirement can be fulfilled by using a method called watermarking. In this method, an image, for example, can be discretely inserted as a mark into an image, whether visibly or invisibly. The mark can be some pertinent information that can be used to identify the owner of the image. This mark could be logos or serial numbers. Therefore, digital watermarking is a great way to protect a document. The insertion or embedding of the watermark can be made in such a way that it cannot be easily removed via normal processing.

Besides watermarking documents, there are other application domains where watermarking has been successfully used. For example, digital watermark has been used for wireless sensor network (Harjito et al., 2012), video (Gao et al., 2017), mobile application components (Ren et al., 2014), social media texts (Rizzo et al., 2017), image electronic patience records (Sharma et al., 2017) and digital forensics (Fujiyoshi and Kiya, 2017).

Therefore, the idea of using a digital mark to detect and trace copyright violations has stimulated significant interests among engineers, scientists, lawyers, artists, and publishers, to name a few. On the other hand, using signal processing techniques, adversaries have tried various methods in order to remove the watermark. As a result, the research in watermarking is primarily focused on achieving robustness with respect to variety of attacks like compression, image-processing operations, and cryptographic attacks. Research in this field has become very active in recent years, and many techniques have been developed and improved to a great extend.

In the following sections, the working of a watermarking system and also the concept of redundancy in networking field are explained.

1.2 A Watermarking System

The term watermarking comes from the history of traditional paper making industry. In the industrial processing, a water-coated metal stamp is pressed unto a paper to expel the water, and the enhanced contrast between watermarked and non watermarked areas of the paper forms a certain pattern that is visible. This is due to thickness or density changes in the pressed area. Watermarking starts to be used in

the West by the paper industry in the late middle ages – estimated to be in the 13th century (Harris, 2017). There is a clear record on the earliest usage of watermark including the names of paper brand and manufacturing mill (Harris, 2017). Later, watermarking was used to certify the composition of paper. Nowadays, watermark is used by many countries to protect their official documents, currencies, and postage stamps to make counterfeiting more difficult.

The digitation of our world has supplemented traditional watermarking with digital forms. While paper watermarks were originally used to differentiate between different paper manufacturers, today's digital watermarks have more widespread uses. Stemming from the legal need to protect intellectual property of the creator from unauthorized usage, digital watermarking technology attempts to reinforce the copyright by embedding a digital message that can identify the original creator or the intended recipients. Unauthorized usage is usually contained by using encryption. When encryption is broken, watermarking is essentially the remaining technology that is able to protect unencrypted multimedia content.

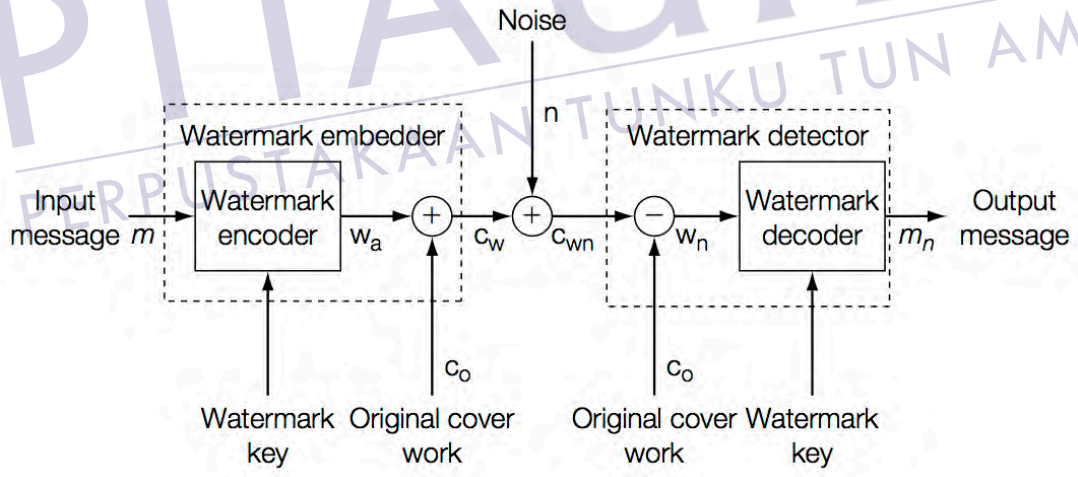

Figure 1.1: A watermarking communication model (Cox et al., 2008). Plus sign means "added" and negative sign means "deduct".

Figure 1.1 shows a watermarking system consisting of a message, a cover image and a key to be supplied to the encoder, which essentially hides the message in a hiding channel of the cover image. Using a decoder, the receiver will retrieve back the embedded watermark using the same key and the original cover image. As much as the designer of a watermarking system tries to embed a watermark, an adversary may

also put efforts to remove the watermark. An attacker may inject white noise to overwrite the embedded watermark. In the case of digital image, a watermarked image can be put under several attacks like cropping, filtering, noise addition or geometric distortions to destroy the embedded watermark (Qassim et al., 2018).

Therefore, a watermarking system that can sustain these attacks is required. Watermarks designed to survive legitimate and everyday usage are referred to as robust watermarks (Cox et al., 2008; Qassim et al., 2018; Parah et al., 2015). In other words, if the embedded watermark remains detectable or retrievable under various attacks on the watermarked host, it is considered robust.

It is important to note the difference between robust watermarking and secure watermarking. Robust watermarking is designed to survive probable range of processing that could remove a watermark, while secure watermarking is designed to survive all possible attacks (Cox et al., 2008; Qassim et al., 2018; Parah et al., 2015). In reality, there is no such thing as totally secure watermark that can survive all possible attacks.

1.3 Network Redundancy

Network redundancy is a mechanism in which alternative instances of network devices, equipment and communication mediums are installed within a network infrastructure (Oppenheimer, 2010). Its primary goal is to provide increased network availability in case of a network device or path failure. Such design provides reliable fail over mechanism to support a more robust infrastructure.

Network redundancy is usually implemented in enterprise network infrastructure to provide a redundant source of communication channels (Techopedia, 2018). This mechanism allows for quickly swapping of network operations onto redundant infrastructure in the event of unplanned network outages. Network redundancy is provided through the addition of alternate network paths, which are implemented through redundant standby routers and switches. When the primary path is not available, an alternate path can be instantly deployed to ensure continuity of network services.

In the following section, the problem of "single point of failure" in watermarking is presented. Borrowing from networking field, the solution to this problem lies in creating some form of redundancy in the process of watermarking.

1.4 Problem Statement

Traditional and recent direction of research in watermarking are mostly focused on developing a single hiding place that can sustain all types of common attacks. However, a hiding place reacts differently to different types of attacks. In this thesis, hiding scheme and hiding location can be used interchangeably. Techniques like spread spectrum, embedding in perceptively significant coefficients, and attack reversal at the embedder and detector are all helpful to make the watermark more or less robust. However, most techniques suffered from four significant weaknesses:

i. Most watermarking techniques rely on a single hiding scheme (i.e. hiding location). If this hiding scheme gets compromised, they would not have anywhere else to go to retrieve the watermark. Obviously, this is unavoidable since researchers usually focus on a particular design to pacify the effects from a group of attacks.
ii. Most watermarking techniques are relatively stronger against certain types of attacks but in compensation, weaker against other types of attacks. It is unlikely that there exists a scheme that is strong against all types of attacks (Qassim et al., 2017).
iii. An attacker does not need to know exactly how you arrange your watermark in a hiding place. They may comb all possible spaces in the hiding area with destructive write ups once they figure out where the hiding area is.
iv. Most watermarking techniques determine proof of ownership by retrieving the embedded image. If the mean square error (MSE) of this image is low (perhaps, below 10%), we say that it is "proven" that the host image has been marked by our method. Such embedded image however can be noisy or simply vanished due to well-calculated attacks. Besides, there is no specific watermark noise value that is considered acceptable among researchers. This

makes comparison between different watermarking systems becomes inconclusive.

Due to the above problems, relying on a single scheme to mark an image is a fundamentally weak approach. Having redundant copies distributed to different hiding locations may enhance the survivability of the watermark against various attacks. Such redundancy must be designed to survive well-coordinated attacks on those hiding channels. Under sizable attacks, it is generally safe to assume that some watermarks will get very noisy and may not be retrievable at all after an attack.

1.5 Research Objectives

The research aim is to improve the robustness of a watermarking system using a new form of watermark redundancy. To support this aim, the objectives of this research are as follows:

i. To propose a new watermarking approach based on Sudoku numbered image tiles.
ii. To propose a Sudoku based composite scheme to enhance watermarking tiles survivability.
iii. To propose a reliable conversion technique from watermark tiles to Sudoku numbers using existing quality metrics and Associative Neural Networks.
iv. To implement a new watermarking approach that would enable the verification of proof of ownership using noisy or missing watermarks.
v. To compare the recoverability rate of the proposed approach with the existing approaches.

1.6 Contributions

This research contributes to the body of knowledge in the field of image watermarking in the following ways:

i. A new type of watermark is proposed. The watermark is made of "Sudoku numbered image tiles." These tiles virtually act as holders or hosts for Sudoku numbers. In other words, the cover image hosts the tiles and the tiles host Sudoku numbers. The tiles can be viewed as first order watermarks; the Sudoku numbers on this tiles are second order watermarks. During retrieval process, the primary goal is to retrieve the Sudoku numbers, not the tiles. The advantage of this approach as compared to regular watermark is that the Sudoku numbers are still recoverable even though with varying level of noise affecting the tiles. The tiles can take a larger range of noise intensity when attacked. Although the tiles can get damaged due to attacks, specific numbers associated with the tiles can still be retrieved from the noisy tiles using some convergence pattern algorithm like associative neural network (Hopfield Neural Network). As a result, the technique extends the overall recoverability of a watermark compared to the existing approach.

ii. An improved composite watermarking is proposed. Breaking a watermark into small pieces and distributing them over complementary defense planes (i.e. using different hiding schemes) help high recoverability of the watermark. As a note, multiple small watermarks have been earlier experimented by Lach et al.(1999), but for FPGA IP (field-programmable gate array intellectual property) domain. Furthermore, recent multiple watermarking systems have shown increased robustness (Bajaj, 2014; Gunjal and Mali, 2014; Jamali et al., 2015; Cao et al.,2016). Watermarks are broken into smaller pieces and distributed via different hiding schemes into the cover media to ensure its survivability when attacked.

iii. A new application of Sudoku to recover missing watermarks is proposed. Due to attacks, some watermark pieces are expected to be destroyed, while others will survive. However, damaged watermark pieces can be reconstructed back from surviving pieces. This is possible due to the inherent redundancy in Sudoku numbers. Incomplete watermarks can be reconstructed back from the remaining watermarks pieces, similar to filling up a partially filled Sudoku puzzle.

iv. A new binary metric to measure the performance of a watermarking system is proposed. The above contributions inadvertently lead to the discovery of a new performance metric which is solely based on the recoverability of a Sudoku

key from a watermarked image. Existing verification metrics rely on the analog, inconclusive PSNR and MSE values. There are no "agreeable" thresholds as to these values among researcher. In contrast, the proposed metric evaluates the quality of a watermark to only 2 values– unsuccessful (0) or successful (1) recovery of the Sudoku key.

1.7 Research Scope

This study focuses on developing Sudoku watermarking using images. Other cover objects such as video and text are not covered. Although other configurations are possible, the approach will be implemented and tested in 9×9 Sudoku configuration. Furthermore, the study does not propose any new scheme. It instead created a new approach to watermarking using existing schemes. A limited number of well known watermarking schemes are considered in the proposed approach, specifically when creating composite watermarking schemes. A more comprehensive composition of watermarking schemes requires another study.

1.8 Thesis Organisation

This thesis is organised as follows: Chapter 2 discusses pertinent reviews of basic watermarking concepts, approaches and methods to achieve robustness, existing redundancy concepts, Sudoku and evaluations of a watermarking system. Chapter 3 explains the research methodology. Chapter 4 elaborates on the design of a Sudoku watermarking together with its mathematical preliminaries. Chapter 5 presents experimental results and analysis using 9×9 Sudoku watermarking configuration. Finally, Chapter 6 concludes the achievement of the thesis objectives and its impact on the body of knowledge in watermarking research.

REFERENCES

A. Aggarwal & M. Singla (2011). Robust watermarking of color image under noise and cropping attack in spatial domain. *International Journal of Computer Science and Information Technologies, 2(5)*, pp. 2036- 2041.

S. K. Ahmad Khalid, M. Mat Deris & K. M. Mohamad (2013). Anti-cropping digital image watermaking using Sudoku. *International Journal of Grid and Utility Computing, 4(2/3)*, pp. 169-177.

A. K. Al-Asmari and F. A. Al-Enizi (2009). A Pyramid-Based Watermarking Technique for Digital Color Images Copyright Protection. *Proceedings of the International Conference on Computing, Engineering and Information*. Fullerton, pp. 44-47.

P. Arya, D.S. Tomar & D. Dubey (2015). A review on different digital watermarking techniques. *International Journal of Signal Processing, Image Processing and Pattern Recognition, 8*, pp. 129-136.

A. Bajaj (2014). Robust and reversible digital image watermarking technique based on RDWT-DCT-SVD. *Proceedings of the International Conference on Advances in Engineering & Technology Research (ICAETR2014)*. Unnao. pp. 1-5.

P. Bas, T. Furon, F. Cayre, G. Doërr & B. Mathon (2016). *Watermarking security: fundamentals, secure designs, and attacks*. France: Springer.

N. Bi, Q. Sun, D. Huang, Z. Yang & J. Huang (2007). Robust image watermarking based on multiband wavelets and empirical mode decomposition. *IEEE Transactions on Image Processing, 16(8)*, pp. 1956-1966.

G. Bhatnagar & Q. M. J. Wu (2013). A new logo watermarking based on redundant fractional wavelet transform. *Mathematical and Computer Modelling, 58(1–2)*, pp. 204-218.

N. Boston (2001). A mathematical foundation for watermarking. *Information Protection Seminar*, University of Illinois at Urbana-Champaign. (www.math.uiuc.edu/~boston/mark2.pdf).

M. Cao, C. Li, Z. Wu, L. Tian, & S. Du (2016). Novel robust audio watermarking scheme against synchronization attacks. *Proceedings of the International Conference on Internet Multimedia Computing and Service (ICIMCS2016)*. New York: ACM. pp. 9-13.

C. C. Chang, P. Y. Lin, Z. H. Wang & M. C. Li (2010). A sudoku-based secret image sharing scheme with reversibility. *Journal of Communications, 5(1),* pp. 5-12.

L. Chen & J. Zhao (2015). Adaptive digital watermarking using RDWT and SVD. *Proceedings of the IEEE International Symposium on Haptic, Audio and Visual Environments and Games (HAVE2015).* Ottawa. pp. 1-5.

L. Çerkezi & G. Çetinel (2016). RDWT and SVD based secure digital image watermarking using ACM. *Proceedings of the 24th Signal Processing and Communication Application Conference (SIU).* Zonguldak, pp. 149-152.

K. Chitra & V. P. Venkatesan (2016). Spatial domain watermarking technique: an introspective study. *Proceedings of the ACM International Conference on Informatics and Analytics (ICIA2016).* New York. pp. 50:1-50:6.

J. (J. U.) Choi, S. A. Chun & J. W. Cho (2014). Smart SecureGov: mobile government security framework. *Proceedings of the 15th ACM Annual International Conference on Digital Government Research (DG.O 2014)*. New York. pp. 91-99.

Y. C. Chou, C. H. Lin, P. C. Li & Y. C. Li (2010). A (2,3) threshold secret sharing scheme using Sudoku. *Proceedings of the IEEE Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. Washington. pp. 43-46.

I. J. Cox (2000). *Watermarking of image data using mpeg/jpeg coefficients*. United States Patent 6069914.

I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich & T. Kalker (2008). *Digital Watermarking and Steganography*. Burlington, MA: Morgan Kaufmann.

V. Diaconu (2014). An image encryption algorithm with a chaotic dynamical system based Sudoku Grid. *Proceedings of the 10th International Conference on Communications (COMM2014),* Bucharest. pp. 1-4.

Y. M. Fang, J. W. Huang & S. Q. Wu (2004). CDMA-based watermarking resisting to cropping. *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS2004).* Vancouver. pp.25–28.

B. Felgenhauer & F. Jarvis (2006). Mathematics of Sudoku I. *Mathematical Spectrum, 39(1),* pp. 15-22.

X. Feng & Y. Chen (2012). Digital image watermarking based on super resolution image reconstruction. *Proceedings of the International Conference on Fuzzy Systems and Knowledge Discovery*. Sichuan. pp. 1778-1782.

Y. G. Fu & R. M. Shen (2008). Color image watermarking scheme based on linear discriminant analysis. *Computer Standards and Interfaces, 30(3),* pp. 115-120.

M. Fujiyoshi & H. Kiya (2017). A blind reversible data hiding method for high dynamic range images taking advantage of sparse histogram. in C. Kraetzer, Y. Q. Shi, J. Dittmann, H. Kim (Eds.) *Digital Forensics and Watermarking*. Lecture Notes in Computer Science, vol 10431. Cham: Springer.

C. W. H. Fung, A. Gortan & W. Godoy Jr. (2011). A review study on image digital watermarking. *Proceedings of the 10th International Conference on Networks.* pp. 24-28.

Q. Gao, Z. Li, & S. Chen (2017). A video dual watermarking algorithm against geometric attack based on Integer Wavelet and SIFT. *Proceedings of the ACM International Conference on Cryptography, Security and Privacy (ICCSP2017).* New York. pp. 33-37.

H. Garg & S. Agrawal (2014). Uniform repeated insertion of redundant watermark in 3D object. *Proceedings of the International Conference on Signal Processing and Integrated Networks (SPIN2014).* Noida. pp. 184-189.

B. M. Garlapati & S. R. Chalamala (2016). A symbol based watermarking approach for spread spectrum audio watermarking methods. *Proceedings of the 7th International Conference on Intelligent Systems, Modelling and Simulation (ISMS2016).* Bangkok. pp. 180-184.

M. L. Pérez Gort, C. F. Uribe & J. Nummenmaa (2017). A minimum distortion: high capacity watermarking technique for relational data. *Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security*. New York. pp. 111-121.

B. L. Gunjal & S. N. Mali (2014). Comparative performance analysis of digital image watermarking scheme in DWT and DWT-FWHT-SVD domains. *Proceedings of the Annual IEEE India Conference (INDICON2014)*. Pune. pp. 1-6.

R. Gunjan, V. Laxmi & M. S. Gaur (2012). Detection attack analysis using partial watermark in DCT domain. *Proceedings of the Fifth ACM International Conference on Security of Information and Networks (SIN2012)*. New York. pp. 188-192.

D. Groupe (2007). *Principles of Artificial Neural Networks*. Singapore: World Scientific Publishing.

L. R. Haddada, B. Dorizzi & N. E. B. Amara (2017). A combined watermarking approach for securing biometric data. *Signal Processing: Image Communication, 55*, pp. 23-31.

F. A. Haight (1967). *Handbook of the Poisson distribution*. New York: John Wiley & Sons.

B. Harjito, V. Potdar & J. Singh (2012). Watermarking technique for copyright protection of wireless sensor network data using LFSR and Kolmogorov complexity. *Proceedings of the 10th ACM International Conference on Advances in Mobile Computing & Multimedia (MoMM 2012)*. New York. pp. 208-217.

N. Harris (2017). *Paper and Watermarks as Bibliographical Evidence*. Lyon: Institut D'Histoire Du livre. ISBN: 97829560427161.

M. Heidari, N. Karimi & S. Samavi (2016). A hybrid DCT-SVD based image watermarking algorithm. *Proceedings of the 24th Iranian Conference on Electrical Engineering (ICEE2016)*. Shiraz. pp. 838-843.

J. J. Hopfield (1982). Neural networks and physical systems with emergent collective computational abilities. *Proceedings of the National Academy of Sciences of the USA, 79(8)*, pp. 2554–2558.

A. Iacovazzi & Y. Elovici (2017). Network flow watermarking: a survey. in *IEEE Communications Surveys & Tutorials, 19(1)*, pp. 512-530.

A. K. Jain, J. Mao & K. M. Mohiuddin (1996). Artificial neural networks: a tutorial. *Computer, 29(3)*, pp. 31-44.

M. Jamali, S. Samavi & N. Karimi (2015). Robust image watermarking by multi resolution embedding in wavelet transform coefficients. *Proceedings of the 23rd Iranian Conference on Electrical Engineering*. Tehran. pp. 478-482.

J. Jang, B. Kim & Y. Cho (2013). Impact of software watermarking on smart devices. *Proceedings of the ACM Research in Adaptive and Convergent Systems (RACS2013).* New York. pp. 361-362.

N. Jussien (2007). *A to Z of Sudoku*. London: ISTE Ltd.

J. Hämmerle, A. Uhl & H. Wernisch (2008). Multiple re-watermarking using varying non-stationary MRA with parameterized wavelet filters. *Proceedings of the 10th ACM workshop on Multimedia and security (MM&Sec2008).* New York. pp. 63-68.

S. K. A. Khalid, M. M. Deris & K. M. Mohamad (2014). A systematic redundancy approach in watermarking using Sudoku. *Proceedings of the International Conference on IT Convergence and Security (ICITCS2014)*. Beijing. pp. 1-5.

M. Khalili (2011). A novel effective, secure and robust CDMA digital image watermarking in YUV color space using DWT2. *International Journal of Computer Science Issues, 8(3),* pp. 70-78.

V. Khanduja, S. Chakraverty & O. P. Verma (2016). Enabling information recovery with ownership using robust multiple watermarks. *Journal of Information Security and Applications, 29*, pp. 80-92.

B. Kim & J. Jung (2013). Impact of multiple watermarks for protecting copyright of applications on smart mobile devices. *Proceedings of the ACM Research in Adaptive and Convergent Systems (RACS2013).* New York. pp. 359-360.

D. Kundur & D. Hatzinakos (2004). Towards robust logo watermarking using multi-resolution image fusion. *IEEE Transactions on Multimedia, 6(1),* pp. 185-197.

J. Lach, W. H. Mangione-Smith & M. Potkonjak (1999). Robust FPGA intellectual property protection through multiple small watermarks. *Proceedings of the 36th annual ACM/IEEE Design Automation Conference (DAC1999).* Mary Jane Irwin (Ed.). New York. pp. 831-836.

C. Lala (2013). *Graph theory of Sudoku*. Indian Institute Of Science Education And Research Bhopal: Master's Thesis.

K. Loukhaoukha, A. Refae & K. Zebbiche (2017). Ambiguity attacks on robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. *Journal of Electrical Systems and Information Technology, 4(3),* pp. 359-368.

N. Lazarov & Z. Ilcheva (2016). A fragile watermarking algorithm for image tamper detection based on chaotic maps. *Proceedings of the IEEE 8th International Conference on Intelligent Systems (IS2016)*. Sofia. pp. 723-728.

R. V. Mahule & C. A. Dhawale (2016). An analytical study of digital image watermarking in frequency domain. *Proceedings of the Second ACM International Conference on Information and Communication Technology for Competitive Strategies (ICTCS2016).* New York. pp. 31:1-31:6.

A. K. Maji & R. K. Pal (2015). A novel biometric template encryption scheme using sudoku puzzle. in R. Chaki, K. Saeed, S. Choudhury & N. Chaki. (Eds.) Applied Computation and Security Systems. *Advances in Intelligent Systems and Computing, vol 305*. New Delhi: Springer.

G. N. Mohammed, A. Yasin & A. M. Zeki (2014). Robust image watermarking based on Dual Intermediate Significant Bit (DISB). *Proceedings of the 6th International Conference on Computer Science and Information Technology (CSIT2014)*. Amman. pp. 18-22.

N. Mohananthini & G. Yamuna (2016). Comparison of multiple watermarking techniques using genetic algorithms. *Journal of Electrical Systems and Information Technology, 3(1),* pp. 68-80.

S. M. Mousavi, A. Naghsh & S. Abu-Bakar (2014). Watermarking techniques used in medical images: a survey. *Journal of Digital Imaging, 27*, pp. 714-729.

T. Munakata (2008). *Fundamentals of the New Artificial Intelligence: Neural, Evolutionary, Fuzzy and More (Texts in Computer Science)*. London: Springer-Verlag.

P. M. Naini, S. M. Fakhraie & A. N. Avanaki (2010). Sudoku bit arrangement for combined de-mosaicking and watermarking in digital camera. *Proceedings of the 2nd IEEE International Conference on Advances in Databases, Knowledge, and Data Applications.* Menuires, pp. 41-44.

I. Nasir, F. Khelifi, J. M. Jiang & S. S. Ipson (2010). A robust image watermarking scheme based on normalized circular image in DWT domain. *Proceedings of the 10th International Conference on Information Sciences, Signal Processing and their Applications (ISSPA2010).* Kuala Lumpur. pp. 33-36.

R. Naskar, A. Raju & R. S. Chakraborty (2013). A single pass, high throughput reversible watermarking scheme for audio based on redundant embedding. *Proceedings of The International Conference on Signal Processing and Communication (ICSC2013)*. Noida. pp. 303-308.

I. Natgunanathan, Y. Xiang, G. Hua, G. Beliakov, J. Yearwood (2017). Patchwork-based multilayer audio watermarking. *IEEE/ACM Transactions on Audio, Speech and Language Processing, 25(11),* pp. 2176-2187.

T. Nguyen & C. Chang (2015). A reversible data hiding scheme based on the Sudoku technique. *Displays, 39,* pp. 109-116.

P. Oppenheimer (2010). *Top-down Network Design,* 3rd Edition, Cisco Press.

K. Pal, G. Ghosh & M. Bhatarcharya (2012). Biomedical image watermarking in wavelet domain for data integrity using bit majority algorithm and multiple copies of hidden information. *American Journal Of Biomedical Engineering, 2(2),* pp. 29-37.

S. A. Parah, F. Ahad, J. A. Sheikh & G. M. Bhat (2015). On the realization of robust watermarking system for medical images. *Proceedings of the Annual IEEE India Conference (INDICON2015).* New Delhi. pp. 1-5.

A. F. Qasim, F. Meziane & R. Aspin (2018). Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review. *Computer Science Review, 27,* pp. 45-60.

N. Ramamurthy & S. Varadarajan (2012). The robust digital image watermarking using quantization and fuzzy logic approach in DWT domain. *International Journal of Computer Science and Network, 1(5),* pp. 13-19.

S. Rawat & B. Raman (2010). A new robust watermarking scheme for color images. Proceedings of the IEEE 2nd International Advance Computing Conference. Patiala. pp. 206–209.

V. P. Reddy & S. Varadarajan (2010). An effective wavelet-based watermarking scheme using human visual system for protecting copyrights of digital images, *International Journal of Computer and Electrical Engineering, 2(1)*, pp. 24-27.

C. Ren, K. Chen & P. Liu. (2014). Droidmarking: resilient software watermarking for impeding android application repackaging. *Proceedings of the 29th ACM/IEEE International Conference on Automated Software Engineering (ASE2014)*. New York. pp. 635-646.

S. G. Rizzo, F. Bertini, D. Montesi & C. Stomeo (2017). Text watermarking in social media. Proceedings of the IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM2017). in J. Diesner, E. Ferrari, and G. Xu (Eds.). New York. pp. 208-211.

S. Rohith & K.N.H. Bhat (2012). A simple robust digital image watermarking against salt and pepper noise using repetition codes. *International Journal on Signal and Image Processing, 3(1)*, pp. 47-54.

S. Rohith, K. N. H. Bhat & B. K. Sujatha (2014). A secure and robust digital image watermarking scheme using repetition codes for copyright protection. *Proceedings of the International Conference on Advances in Electronics Computers and Communications*. Bangalore. pp. 1-8.

B. R. Roshan Shetty, J. Rohith, V. Mukund & H. Rohan (2009). Steganography using Sudoku puzzle. *Proceedings of the IEEE International Conference on Advances in Recent Technologies in Communication and Computing*. Kerala. pp. 623-626.

S. Roy & A. K. Pal (2017). A blind DCT based color watermarking algorithm for embedding multiple watermarks. *AEU - International Journal of Electronics and Communications, 72*, pp. 149-161.

E. Russell & F. Jarvis (2007). Mathematics of Sudoku II. *Mathematical Spectrum, 39(2)*, pp. 54-58.

A. Samčović & M. Milovanović (2015). Robust digital image watermarking based on wavelet transform and spread spectrum techniques. *Proceedings of the 23rd Telecommunications Forum Telfor (TELFOR2015)*. Belgrade. pp. 811-814.

V. Santhi, N. Rekha and S. Tharini (2008). A hybrid block based watermarking algorithm using DWT-DCT-SVD techniques for color images. *Proceedings of the International Conference on Computing, Communication and Networking*. St. Thomas. pp. 1-7.

M. Sharkas, D. ElShafie, N. Hamdy (2005). A dual digital-image watermarking technique. Proceedings of the 3rd World Enformatika Conference. Istanbul. pp. 136-139.

N. P. Sheppard, R. Safavi-Naini & P. Ogunbona (2001). On multiple watermarking. Proceedings of the 2001 ACM Workshop on Multimedia and Security: New Challenges (MM&Sec2001). New York. pp. 3-6.

S. S. Shankar & A. Rengarajan (2017). Puzzle based highly secure steganography. *Proceedings of the International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET2017).* Chennai. pp. 1-5.

A. Sharma, A. K. Singh & S. P. Ghrera (2017). Robust and secure multiple watermarking for medical image. *Wireless Personal Communications: An International Journal, 92(4)*, pp. 1611-1624.

F. Shih (2017). *Digital Watermarking and Steganography: Fundamentals and Techniques*, 2nd ed., Florida: CRC Press.

S. Shivani, P. Singh & S. Agarwal (2017). A dual watermarking scheme for ownership verification and pixel level authentication. *Proceedings of the 9th ACM International Conference on Computer and Automation Engineering (ICCAE2017).* New York. pp. 131-135.

A. K. Singh, B. Kumar, G. Singh & A. Mohan (2017). *Medical Image Watermarking: Techniques and Applications*, Springer International Publishing.

R. Srinivasan, T. Gopalakrishnan & B. Krishnasamy. (2011). SVD Based Robust Digital Watermarking For Still Images Using Wavelet Transform. *Computer Science & Information Technolog, 2*, pp. 155-167.

W. Stallings (2016). *Cryptography and network security: principles and practice*, 7th ed., New York: Pearson.

Su Doku (2017). A Su Doku Solver. Retrieved on July 21, 2017, from http://sudoku.sourceforge.net

Sudoku Tutor and Solver (2017). Retrieved on July 20, 2017, from https://www.sudoku-solutions.com

Sudokuwiki.org (2017). Sudoku Solver. Retrieved on July 21, 2017, from http://www.sudokuwiki.org/sudoku.htm

Techopedia (2018), Network Redundancy. Retrieved on February 15, 2018, from https://www.techopedia.com/definition/29305/network-redundancy

The USC-SIPI Image Database (2013), Retrieved on Mac 15, 2013 from http://sipi.usc.edu/database/

A. M. Widodo & B. Tjahjono (2017). Implementation of image fusion method for watermark on color image using wavelet transformation domain. *Proceedings of the ACM International Conference on Computer Science and Artificial Intelligence (CSAI2017)*. New York. pp. 100-108.

W. C. Wu & G. R. Ren (2009), A New Approach to Image Authentication using Chaotic Map and Sudoku Puzzle. *Proceedings of the IEEE Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2009. Kyoto. pp. 628-631.

Q. Wu, C. Zhu, J. Li, C. Chang & Z. Wang (2016). A magic cube based information hiding scheme of large payload. *Journal of Information Security and Applications, 26*, pp. 1-7.

Y. Xiang, I. Natgunanathan, D. Peng, G. Hua & B. Liu (2018). Spread spectrum audio watermarking using multiple orthogonal pn sequences and variable embedding strengths and polarities. *IEEE/ACM Transaction on Audio, Speech and Language Processing, 26(3)*, pp. 529-539.

Y. Xiang, I. Natgunanathan, Y. Rong & S. Guo (2015). Spread spectrum-based high embedding capacity watermarking method for audio signals. *IEEE/ACM Transactions on Audio, Speech and Language Processsing, 23(12)*, pp. 2228-2237.

J. Xiaolin, Y. Zhou, Q. Yanli & S. Liping (2016). The anti-geometric attack digital watermarking algorithm based on image normalization of local information. *Proceedings of the IEEE Information Technology, Networking, Electronic and Automation Control Conference.* Chongqing. pp. 1120-1124.

T. Yato & T. Seta (2003). Complexity and completeness of finding another solution and its application to puzzles, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 86(5)*, pp. 1052-1060.

L. Zhang (2013). A Improve Robust Watermarking Algorithm for Binary Images. *Advanced Materials Research, 756*, pp. 3775-3780.

L. Zhang & H. Zheng (2015). A high capacity watermarking scheme based on fourier descriptor and Sudoku. *Proceedings of the 8th International Symposium on Computational Intelligence and Design (ISCID2015)*. Hangzhou. pp. 637-642.

S. S. M. Ziabari (2015). Intelligent image watermarking robust against cropping attack. *Proceedings of the 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI2015)*. Tehran. pp. 1203-1206.

T. Zong, Y. Xiang, S. Elbadry & S. Nahavandi (2013). A modified moment-based image watermarking method robust to cropping attack. *Proceedings of the IEEE 8th Conference on Industrial Electronics and Applications (ICIEA2013)*. Melbourne. pp. 881-885.

F. Zou, Z. Lu & H. Ling (2004). A multiple watermarking algorithm based on CDMA technique. *Proceedings of the 12th annual ACM international conference on Multimedia (MULTIMEDIA2004)*. New York. pp. 424-427.

Y. Zou, X. L. Tian, S. W. Xia & Y. Song (2011). A novel image scrambling algorithm based on Sudoku puzzle. *Proceedings of the IEEE Forth International Congress on Image and Signal Processing*. Shanghai. pp. 737-740.