DYNAMIC HASHING TECHNIQUE FOR BANDWIDTH REDUCTION IN IMAGE TRANSMISSION

ERFANEH NOROOZI

A thesis submitted in partial fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy

Advanced Informatics School
Universiti Teknologi Malaysia

MAY 2015

To my lovely mother and father, who gave me endless love, trust, constant encouragement over the years, and for their prayers.

To my Family for their patience, support, love, and for enduring the ups and downs during the completion of this thesis.
This thesis is dedicated to them.

ACKNOWLEDGEMENT

Foremost, I would like to express my greatest appreciation to my supervisor, Assoc. Prof. Dr. Salwani Mohd Daud for her precious guidance and encouragement during completion of my project. Even though she was busy with her daily tasks, she was always there to offer assistance and helping me with my project. Without her continual support and advices, this thesis would have not been the same as presented here.

I owe my loving thanks to my family for supporting me spiritually and financially throughout my life. Without their encouragement and understanding it would have been impossible for me to finish this project.

Last but not least, I offer my regards and blessings to all of those who supported me in any respect during the completion of this project.

I would like to express greatest appreciation to Ministry of Education (MOE), Malaysia and Universiti Teknologi Malaysia for providing the grant to carry out this research work with vot number R.K130000.7838.4F357. Last but not least, I would like to thank Advanced Informatics School, Universiti Teknologi Malaysia for their support of this project.

ABSTRACT

Hash functions are widely used in secure communication systems by generating the message digests for detection of unauthorized changes in the files. Encrypted hashed message or digital signature is used in many applications like authentication to ensure data integrity. It is almost impossible to ensure authentic messages when sending over large bandwidth in highly accessible network especially on insecure channels. Two issues that required to be addressed are the large size of hashed message and high bandwidth. A collaborative approach between encoded hash message and steganography provides a highly secure hidden data. The aim of the research is to propose a new method for producing a dynamic and smaller encoded hash message with reduced bandwidth. The encoded hash message is embedded into an image as a stego-image to avoid additional file and consequently the bandwidth is reduced. The receiver extracts the encoded hash and dynamic hashed message from the received file at the same time. If decoding encrypted hash by public key and hashed message from the original file matches the received file, it is considered as authentic. In enhancing the robustness of the hashed message, we compressed or encoded it or performed both operations before embedding the hashed data into the image. The proposed algorithm had achieved the lowest dynamic size (1 KB) with no fix length of the original file compared to MD5, SHA-1 and SHA-2 hash algorithms. The robustness of hashed message was tested against the substitution, replacement and collision attacks to check whether or not there is any detection of the same message in the output. The results show that the probability of the existence of the same hashed message in the output is closed to 0% compared to the MD5 and SHA algorithms. Amongst the benefits of this proposed algorithm is computational efficiency, and for messages with the sizes less than 1600 bytes, the hashed file reduced the original file up to 8.51%.

ABSTRAK

Fungsi hash digunakan secara meluas dalam sistem komunikasi selamat dengan menjana mesej hadam untuk mengesan perubahan yang tidak dibenarkan dalam fail. Mesej hash yang terenkrip atau tandatangan digital digunakan dalam banyak aplikasi seperti pengesahan untuk memastikan integriti data. Adalah sangat mustahil untuk memastikan mesej adalah sah apabila penghantaran dilakukan dalam rangkaian jalur lebar yang tinggi dan diakses dengan mudah terutama dalam saluran yang tidak selamat. Dua isu yang perlu ditangani adalah saiz besar data rahsia dalam tandatangan digital dan jalur lebar yang tinggi dalam penghantaran data rahsia ini. Pendekatan kolaboratif antara mesej hash terenkrip dan steganografi berupaya menghasilkan data tersembunyi yang sangat selamat. Tujuan kajian ini adalah untuk mencadangkan satu kaedah baru bagi menghasilkan mesej hash yang dikodkan yang dinamik dan saiz yang lebih kecil dengan jalur lebar yang lebih rendah. Mesej hash yang dikodkan akan dibenamkan ke dalam imej sebagai stego-imej untuk mengelak pertambahan fail dan seterusnya jalur lebar dapat dikurangkan. Penerima akan ekstrak mesej hash yang dikodkan dan dinamik daripada fail yang diterima pada masa yang sama. Jika penyahkodan hash terenkrip oleh kunci awam dan mesej hash daripada fail asal sepadan dengan fail yang diterima, ia dianggap sebagai sahih. Dalam meningkatkan keteguhan mesej hash, kami mampatkan atau kodkan atau lakukan kedua-dua operasi sebelum membenamkan data hash ke dalam imej. Algoritma yang dicadangkan telah mencapai saiz yang dinamik yang paling rendah (1 KB) daripada fail asal yang tidak tetap panjangnya berbanding algoritma hash MD5, SHA-1 dan SHA-2. Keteguhan mesej hash telah diuji terhadap serangan penggantian, pertukaran dan perlanggaran untuk memeriksa sama ada terdapat sebarang mesej yang sama pada output. Dapatan kajian ini menunjukkan bahawa kebarangkalian kewujudan mesej hash dalam output menghampiri kepada 0% berbanding dengan algoritma MD5 dan SHA. Di antara faedah algoritma yang dicadangkan ini adalah kecekapan pengkomputeran, dan untuk mesej dengan saiz kurang daripada 1600 bytes, fail hash dikurangkan sehingga 8.51% daripada fail asal.

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGEMENT	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vii
	LIST OF TABLES	xi
	LIST OF FIGURES	xiii
	LIST OF ABBREVIATIONS	xvi
	LIST OF APPENDICES	xviii
1	**INTRODUCTION**	**1**
	1.1 Overview	1
	1.2 Background of Problem	2
	1.3 Problem Statement	5
	1.4 Research Aim	6
	1.5 Research Questions	6
	1.6 Research Objectives	7
	1.7 Scope of Study	7
	1.8 Significance of Study	7
	1.9 Organization of the Thesis	8

2	**LITERATURE REVIEW**	**9**
	2.1 Introduction	9
	2.2 Digital Signature	10
	2.3 Authentication	12
	2.3.1 Related Works on Digital Signature	15
	2.3.2 Hash Algorithm	18
	2.3.2.1 MD5 Algorithm	18
	2.3.2.2 SHA-1 Algorithm	20
	2.3.2.3 SHA-2 Algorithm	21
	2.3.2.4 Related Works on Hash Algorithms	23
	2.4 Steganography	26
	2.4.1 Types of Steganography	28
	2.4.1.1 Image Steganography	29
	2.4.2 Image Steganography Techniques	31
	2.5 Popular Techniques Available to Hide Data	32
	2.6 Steganography Algorithm	35
	2.6.1 Spatial Domain Technique	35
	2.6.2 JSteg Algorithm	37
	2.6.3 F5 Algorithm	38
	2.7 Related Works on Image Steganography	38
	2.8 Hash Function Attacks	43
	2.8.1 Collision Attack	43
	2.9 Summary	43
3	**RESEARCH METHODOLOGY**	**45**
	3.1 Introduction	45
	3.2 Operational Framework	45
	3.2.1 Phase 1: Investigation Phase	47
	3.2.1.1 Activity 1: Dynamic Hashed Message in Digital Signature	47
	3.2.1.2 Activity 2: Embedded Data in Image	48
	3.2.2 Phase 2: Development of Proposed Algorithm	51
	3.2.2.1 Activity 1: Dynamic Hashed Message in Digital Signature	52

	3.2.2.2 Activity 2: Encrypted Dynamic Hash Message	52
	3.2.2.3 Activity 3: Embedded Data Process	55
	3.2.2.4 Encoded Embedding Function	56
	3.2.3 Phase 3: Implementation of the Proposed Algorithm	58
	3.2.4 Phase 4: Evaluation of the Proposed Algorithm	59
	3.3 Research Activity	59
	3.4 Summary	60
4	**DEVELOPMENT AND IMPLEMENTATION**	**62**
	4.1 Introduction	62
	4.2 Development of the Algorithm	62
	4.3 Implementation of the Algorithm	67
	4.4 Evaluation of the Hash Algorithms	67
	4.5 Imperceptibility Metrics	69
	4.5.1 Peak Signal to Noise Ratio (PSNR)	70
	4.5.2 Mean Square Error (MSE)	71
	4.5.3 Structural Similarity Measure (SSIM)	72
	4.6 Simulation Results of Imperceptibility Testing	73
	4.6.1 Embedded Data Compression Testing	78
	4.6.2 Encoded Embedded Data Testing	83
	4.6.3 Encoded Compress Embedded Data Testing	85
	4.7 Summary	92
5	**RESULTS AND DISCUSSION**	**93**
	5.1 Introduction	93
	5.2 Generating and Extracting Digital Signature for Authentication Purpose	94
	5.3 Tests of Extracting and Embedding Digital Signature in Image	95
	5.4 Experimental Results of Compressed and Encoded Stego-Image	99
	5.4.1 Comparison Results in Different Image Steganography Methods	113
	5.4.2 Significance of the Proposed Algorithm	114

	5.5 Collision Resistant Hash Function	117
	5.5.1 Hash Message Collision Attacks	118
	5.5.2 Robustness against Attacks	125
	5.6 Summary	130
6	**CONCLUSION**	**131**
	6.1 Introduction	131
	6.2 Achievement of the Research Objectives	132
	6.3 Novel Contributions	134
	6.4 Future Works	135
	6.5 Concluding Remarks	135
REFERENCES		**137**
Appendices A-B		152-172

LIST OF TABLES

TABLE NO.	TITLE	PAGE
2.1	Comparison of hash algorithm of size of output and logical operations and hardware complexity	25
2.2	Comparison of size of file in bytes	26
2.3	Comparison of techniques available to hide data securely	34
2.4	Three consecutive pixels for a 24-bits image	36
2.5	Least significant bit embedding scheme for (101101101)	36
2.6	Comparison of research works previously done for image steganography	42
3.1	Mapping Research Activities to Research Objectives and Research Questions	60
4.1	Comparison of hash algorithm of size of output and logical operations and finding collision and hardware complexity	67
4.2	Comparison of file size in bytes	69
4.3	(a) Attribute of image, (b) Imperceptibility values of stego-image	77
4.4	(a) Attribute of image, (b) Imperceptibility values of stego-image	77
4.5	(a) Attribute of image, (b) Imperceptibility values of stego-image	77
4.6	Attributes of cover and stego-compress image after compression	82
4.7	Attributes of cover and stego-compress image after compression	83
4.8	Attributes of cover image and stego-image (Baboon)	84
4.9	PSNR value of cover image and stego-image (Airplane)	88

4.10	PSNR value of cover image and stego-image (Lena)	90
5.1	PSNR and MSE values of stego-image (embedded data: digital signature)	97
5.2	PSNR and MSE values of stego-image (embedded data: digital signature)	98
5.3	PSNR and MSE values of stego-image (embedded data: digital signature)	98
5.4	PSNR and MSE and SSIM value of compressed and encoded stego- image	102
5.5	PSNR and MSE and SSIM value of compressed and encoded stego image	105
5.6	PSNR and MSE and SSIM values of compressed and encoded stego image	108
5.7	PSNR and MSE and SSIM value of compressed and encoded stego-image	110
5.8	Comparison of PSNR value of compressed and encoded stego-image	112
5.9	Comparison of MSE value of compressed and encoded stego-image	112
5.10	Comparison of SSIM of compressed and encoded stego-image	112
5.11	Comparison results of PSNR in the different methods	113
5.12	Comparison results of PSNR values	114
5.13	PSNR and MSE of encoded embedded (n= 1, 2)	115
5.14	PSNR and MSE of encoded embedded (n= 3, 4)	115
5.15	Comparison of size of file in bytes	116
5.16	Test of propose hash algorithm in different size	122
6.1	Achievement of the Research Objective	135

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
2.1	Block diagram of digital signature by private and public key	11
2.2	Process of digital signature for authentication	13
2.3	Verification of digital signature on the receiver side	15
2.4	Generation and verification of digital signature	17
2.5	One operation of MD5 algorithm	19
2.6	One operation of SHA-1 algorithm	20
2.7	One iteration in a SHA-2 family function	22
2.8	Block diagram of steganography for data hiding	27
2.10	Types of steganography	28
2.11	Color image steganography based on pixel value	30
2.12	Block diagram of information hiding systems	34
2.13	Framework algorithms for embedding data	40
3.1	Operational Framework	46
3.2	Literature study in phase 1	47
3.3	Block diagram of digital signature	48
3.4	Pixel of image from (R, G and B)	49
3.5	Divided one pixel of image into primary colors (Red, Green and Blue)	49
3.6	Block Diagram of Activity 1 and Activity 2 in Phase 2	53
3.7	Operation steps for hash and encoded hash message	54
3.8	Block diagram of steganographic system in pubic channel	55
3.9	Process of embedded data in spatial domain	55
3.10	Encoded embedded function before embedding data	56
3.11	Array of encoded matrix in steganographic system	57
3.12	Matrix of encoded function in embedded digital signature	58

4.1	A sample of 100 hashed files in digital signature	65
4.2	Generating and embedding digital signature	66
4.3	(a) Cover image, (b) Embedded data, (c) Stego-image and (d) PSNR value (embedded image: ship)	74
4.4	(a) Cover image, (b) Embedded data, (c) Stego-image and (d) PSNR value (embedded image: zhekond)	75
4.5	(a) Cover image, (b) Embedded data, (c) Stego-image and (d) PSNR value (embedded image: Diamond)	76
4.6	Capacity of Airplain cover image (512×512)	79
4.7	Embedded data into cover image before compression	79
4.8	Embedded data into cover image after compression	80
4.9	Export file from normal buffer in the receiver	80
4.10	(a) Cover image, (b) Embedded data, (c) Stego-image after compression	81
4.11	(a) Cover image, (b) Embedded data, (c) Stego-image after compression	82
4.12	Process of encoded embedding data into image	83
4.13	PSNR value of encoded compress embedding data	85
4.15	PSNR value of stego-image and stego-compress and stego-compress encoded and stego-encoded image	88
4.16	PSNR value of stego-image and stego-compress and stego-compress encoded and stego-encoded image	90
4.17	PSNR value of stego-image and stego-compress and stego-compress encoded and stego-encoded image	92
5.1	Block diagram of generation and embedding of digital signature into image	94
5.2	Block diagram of verification and extracting of digital signature from image	95
5.3	Generating and embedding of digital signature into image	96
5.4	PSNR value of cover image and stego-image	96
5.5	Generating and embedding of digital signature into image	97
5.6	PSNR value of cover image and stego-image	97
5.7	PSNR value of cover image and stego-image	98
5.8	Generating and embedding of digital signature into image	99

5.9	Stego-image produced by using hidden information	100
5.10	PSNR value of (a)Stego-image, (b)Stego-compress image, (c)Stego-encoded compress image, (d)Stego-encoded image	102
5.11	Stego-image produced by using hidden information	103
5.12	PSNR value of(a)Stego-image, (b)Stego-compress image, (c) Stego-encoded compress image, (d)Stego-encoded image	105
5.13	Stego-image produced by using hidden information	106
5.14	PSNR value of (a) Stego-image,(b)Stego-compress image, (c)Stego-encoded compress image,(d)Stego-encoded image	108
5.15	Stego-image produced by using hidden information	109
5.16	PSNR value of (a)Stego-image, (b)Stego-compress image, (c)Stego-encoded compress image, (d)Stego-encoded image	111
5.17	PSNR value of compressed	117
B.1	Running menus in proposed software	158
B.2	Generate private key in steganographic system	159
B.3	(a) Block diagram of normal embedded image, (b) Execution of software implementation of normal embedded image	161
B.4	(a) Block diagram of compress embedded image, (b) Execution of software implementation of compress embedded image	163
B.5	(a) Block diagram of encoded embedded image, (b) Execution of software implementation of encoded embedded image	165
B.6	(a) Block diagram of encoded compress embedded image, (b) Implementation of encoded compress embedded image	168
B.7	Export file from normal buffer	169
B.8	Export uncompressed file from normal buffer	171
B.9	Export decoded file from uncompressed buffer	172
B.10	Export decoded uncompressed file from compress buffer	173

LIST OF ABBREVIATIONS

AWST	-	Authentication Watermarking by Self-Toggling
AWT	-	Authentication Watermarking Technique
B	-	Blue
BMP	-	Bitmap
CA	-	Certificate Authority
CB-PKC	-	Certificate-Based Public Key Cryptosystem
CS	-	Certificate Signature
db	-	decibel
DB	-	Data Base
DCT	-	Discrete Cosine Transform
DHPT	-	Data Hiding Pair Toggling
DHSPT	-	Data Hiding by Smart Pair Toggling
DHST	-	Data Hiding by Self-Toggling
DWT	-	Discrete Wavelet Transformation
FFT	-	Fast Fourier Transform
G	-	Green
GIF	-	Graphical Interchange Format
GMR	-	Goldwasser, Micali and Rivest
HVS	-	Human Visual System
JFIF	-	JPEG File Interchange Format
KB	-	Kilo Byte
LSB	-	Least Significant Bit
MSE	-	Mean Squared Error
NSA	-	National Security Agency
POVS	-	Pair of Values
PKI	-	Public Key Infrastructure

PSNR	-	Peak Signal-to-Noise Ratio
QIM	-	Quantization Index Modulation
R	-	Red
RB	-	Read Binary
RGB	-	Red, Green and Blue
RMSE	-	Root Mean Square Error
RSA	-	Rivest, Shamir and Adlemen
SHA	-	Secure Hash Algorithm
SNR	-	Signal-to-Noise Ratio
SRSA	-	Strong RSA
SSIM	-	Structural Similarity Measure

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	Programming language source code of Unit 1	152
B	Implementation interface of hash data into image	155

CHAPTER 1

INTRODUCTION

1.1 Overview

Since people have been succeeded in making connections among themselves, the issue of confidential (private) connection came to the attention, too. At first; the application of confidential connection was mostly in martial issues. With the development of civilization, the use of ciphering in issues like politics became essential. In one division, the ciphering systems are divided to block cipher systems and stream cipher systems. In stream ciphering systems, the ciphering and deciphering is done on every single bit. In another division, the ciphering systems are divided into two sections of symmetric ciphering systems and asymmetric ciphering systems (public key). In one symmetric ciphering system, ciphering and deciphering are done via one key. Therefore, supplying the authentication and safety of the message is done together. In public key systems, ciphering and deciphering is done via two keys. These two keys are in a way that without having special information, reaching from one to the other is impossible. Therefore, in these systems one key can be spread as public.

In addition, public key encryption technique is the desired encryption technique that each input bytes into exactly one byte as output. The secret key can be any string such as a word, a number, or just a string of random letters. Then the secret key is used to change the content of the information in the method. Asymmetric algorithms require both the sender and the receiver have the secret key for encrypting and decrypting of data. Another category of hiding information is steganography that is a way of inserting information in host image and its end is protecting copyright law, validation and legitimization of image (Shin and Ruland, 2013). In all the cases, manipulation of image for inserting information should be in a licensed limit, so that there would be no damage to the image. Nowadays, various applications of steganography like monitoring the way of product distribution, ownership validation, copy control and concealed communication are introduced (Saadi *et al.*, 2009).

Because of the same application of these two methods (cryptography and steganography) in protecting confidential information, they are often confused (Turner *et al.*, 2010). Cryptography is a method that focuses on securing the secrecy of the message and expanding different techniques to encode and decode data for the sake of maintaining the secrecy of the contents of communication and message but steganography's focus is on maintaining the secrecy of the existence of the message (Salehi *et al.*, 2009). When the message is revealed or suspicions of the existence of the secret message emerge, steganography has been unsuccessful in its purpose. Both of the techniques are protectors against wicked attacks but not perfect and the combination of them can augment the data strength in a cover media.

1.2 Background of Problem

Text, image, sound and video can be expressed as digital data. Incremental learning and rapid growth of Internet led people to digital world and communication via digital data. Whenever there is talk of communication, the security of communication channel is introduced (Serret-Avila and Boccon-Gibod, 2012). In structure of public key systems and digital signature, one-way functions are used F(O) is one-way; if for any x belonging to F(O) range, computation of F(x) is done easily and computation of x from F(x) from the computational point be impossible. In addition, increasing the volume of the sent messages and specially using insecure channels, sending authentic messages via this way seemed difficult or impossible (Park *et al.*, 2002). The solution used was applying symmetric cipher systems. In these systems, the sender and receiver agree on a private key. The sender sends and ciphers his message with this key and the receiver, knowing the key, receives the message from the cipher text (Mahdi *et al.*, 2012). The main condition in the above system is confidentiality (privacy) of the key and the mutual trust between the sender and the receiver. If one of the parts intends to deceive the other, there is no way to prevent it. For solving this problem, the message is signed. The signature should be in a way that any changes in the message are apparent. If there is no possibility for fake signature, then the identity of the sender can be investigated. This kind of signature is called digital signature.

Digital signature scheme and steganography are the popular techniques available to hide data securely. In fact, in a communication channel, steganography is a method of sending confidential information in a way that the existence of the channel in this communication remains secret (Thomas and Singh, 2013). Computer steganography is a steganography method that provides the image security in digital media and its end is inserting and sending a confidential message via digital media in a way that no doubt is exited based on the sending of the information (Fridrich *et al.*, 2011). Confidential message can be as an image or text or control signal and on the whole anything that can be expressed as a bit chain of 0 and 1. It should be noted that there is a possibility that confidential message should come under compression or cryptography before steganography (Biham *et al.*, 2011).

The three most important parameters for image steganography are: i) payload, ii) imperceptibility, iii) robustness (Makbol and Khoo, 2013), and imperceptibility should be observed in applying the techniques which attempt to enhance the payloads or robustness. Steganography capacity is the maximum number of bits that can be embedded in a particular cover file, making the possibility of detection by an adversary inconsiderably low (Prabakaran *et al.*, 2013). Embedding capacity, that is more than steganography capacity, is the amount of information that can be inserted in a cover medium. When the amount of secret data is high, the form and specification of the cover media will be changed (An *et al.*, 2012). At the times of changing the data such as the changes in the facade of the cover data in message embedded, a technique called imperceptibility is applied. After concealing the secret data, the appearance or format of cover files must remain unchanged. If a hacker can distinguish the existence of a secret message, steganographic system has lost its mission (An *et al.*, 2012). So, methods like PSNR and MSE are used for measuring the imperceptibility.

A collaborative approach between steganography and cryptography is suggested by Islam *et al.* (2010). Using Public Key Infrastructure (PKI) method, the approach provides a high secure hidden data, although the size of the cipher-text is a genuine problem for the steganography. In order to preserve integrity, PKI encryption has been proposed by Wang *et al.* (2009). By using a hash function of digital signature instead of PKI, we can obtain faster processing and less size for authentication of the message. Collaboration of these two methods can empower system for sharing messages, but cryptography produces message sizes larger than the original message (plaintext) that is known as cipher-text (Malik, 2010).

By using encryption in cryptography, a stage of decryption is also required, and when the message is detected, another protector shield is available (Johnson, 2010). In steganography, the original message remains without any change and it is just concealed by using an embedding technique into a cover medium. By doing the reverse function, we can retrieve the original data. In cryptography, the attacker being aware of the existence of the communication will break this encryption algorithm with enough time and resources at any cost (Kae-por, 2008). But in steganography, we accept that the attacker can detect the cover without being able to identify the information besides the original cover content (Makbol and Khoo, 2013). Public key encryption is the basis of digital signature scheme (O'Neill, 2011).

A hashed message value, also called a message digest, is a number generated from a string of the text. A message digest $\{0,1\}^n$ is an algorithm H that uses non constant size message as input $\{0,1\}^*$ to produce a dynamic hashed message output. Dynamic hashed amount is not fixed and depends on the original file as the input file. The hashed message is substantially smaller than the text itself, and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value. For encrypting hashed message, a private key is used. Only the one signing the image is aware of this private key used to encrypt the file and a related public key is used to decrypt the encoded hash message (Fridrich *et al.*, 2011). We can hash this image by using the same hashing function that is used at first and when these hashes correspond, the image authentication is verified.

There are two main approaches for hiding data: (i) image steganography and (ii) digital watermarking (Zaidan *et al.*, 2009); most of these approaches have limitations with the size and the robustness of image steganography (Naji *et al.*, 2009).

In computer networks, bandwidth or data transfer rate is the amount of information that can be transmitted from sender to the receiver side in the specific given time (Chen *et al.*, 2001). In digital signature scheme after generating digital signature, original file with the digital signature have to be send to the receiver side, separately. Consequently, a high bandwidth (Jansirani *et al.*, 2011) is required. Thus, for solving this issue, the data was transformed into encoded format and then these data were embedded in an image file, finally the image file with the much lower bandwidth is transmitted. By this scheme not only the authenticity and the integrity of images can be verified, but also the illegal modifications can be located.

1.3 Problem Statement

The ability to create dynamic hashed message is highly related with the integrity and robustness of the image steganography. As a significant verification method, digital signature algorithm introduces a technique to endorse the contents of the message. This message has not been altered throughout the communication process (Filler *et al.*, 2009). Thus, it increases the receiver confidence that the message was unchanged. Two drawbacks when using digital signature schemes are extra bandwidth and large file size during transmission. Implementing an encryption algorithm in the spatial domain steganographic method can contribute to increasing the degree of security. Unfortunately, there is wide variety of attacks that affect on quality of image steganography, although there are methods for data hiding but they are still very weak in resisting these attacks.

In Kae-por (2008) study, they had combined three steganography algorithms on the image through StegCure system; they succeeded in implementing StegCure which hides around 33% by using Public Key Infrastructure (PKI) which has a high level of security. Hmood *et al.* (2012) illustrated the relation between the quantity of hidden data and quality of the image by using human vision system property and pure steganography. The main purpose of their research works is to evaluate the effect of increasing the amount of data on the quality of the image. They concluded these findings: first, the images that include a simple texture can hide only 33.3% of the image size. Second, images that do not include any simple texture can hide up to 50% of the image size.

Robustness is an important concern in developing multimedia authentication techniques (Shin and Ruland, 2013). Without robustness, an authentication method can only verify the images or videos at the final stage of transcoding processes, but not authenticate them. Robustness refers to the amount of distortion that the digital cover can endure before the hidden message is destroyed. Since the purpose of steganography process is to hide the existence of the secret data, the message should be embedded in such way that it cannot be easily extracted from the cover medium (Makbol and Khoo, 2013).

1.4 Research Aim

The aim of the research is to propose a new method for producing a dynamic hashed message algorithm in digital signature and then embedded into image with reduced bandwidth. A digital signature with smaller hash length is developed for authentication purpose.

1.5 Research Questions

In order to achieve the aim objective, the questions used to guide the study are as follows:

i. Why embedded image without dynamic hashed message of digital signature is not robust for image authentication purpose?

ii. Why hashed message of digital signature in current algorithms have a fix length output?
iii. How to generate dynamic hashed message of digital signature?
iv. How to evaluate the robustness performance of the proposed algorithm against hashed message attacks such as collision attacks?

1.6 Research Objectives

The objectives of the study are:

i. To analyze the robustness of dynamic digital signature in image steganography for authentication purpose.
ii. To analyze the current algorithms in producing hashed message of digital signature with a fix length output.
iii. To develop and implement the algorithm that can generate dynamic hashed message of digital signature.
iv. To evaluate the performance of proposed algorithm against hashed message attacks such as collision attacks.

1.7 Scope of Study

The scope of the research is limited to the following:

i. Key management is done by using asymmetric-key concept.
ii. Embedded digital signature is in bitmap format image (*.bmp)
iii. Dynamic hashed message file with the text format works better rather than image format.

1.8 Significance of Study

Digital signature and image steganography are two techniques used for data authentication. This project focuses on developing new algorithm in hiding data to enhance robustness of image steganography for image authentication purpose. Results of this study are an efficient and robust stenographic technique which can avoid various image attacks. We proposed a new algorithm for producing a dynamic hashed message algorithm in digital signature by generating an encoded hash message and then embedded into image for enhancing robustness of image steganography. Thus to produce a cipher text size closer to an original file; digital signature can be embedded into the image as stego-image. This is a new approach for dynamic hashed message in digital signature, based on the divided input using a fixed block of byte sequences but we emphasize that the output of proposed hash function need not be of fixed length and size of hashed message output depends on the size of original file, consequently generate dynamic hashed output.

1.9 Organization of the Thesis

The thesis is divided into six chapters. After this introduction and problem statement in Chapter 1, a literature review on digital signature and image steganography scheme and comparing on previous related researches for authentication purpose is proposed in Chapter 2. In Chapter 3, the methodology and operational framework that guides the research consists of four phases is described in this chapter. Chapter 4 discusses about development and implementation of the research. Chapter 5, evaluation of the results in term of imperceptibility by using Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Structural Similarity Measure (SSIM). The robustness performance of the algorithm is investigated against hashed message attacks such as collision attacks and finally Chapter 6 contains novel contributions and suggestions for the future work.

REFERENCES

Aarumugam, G., & Rajan, B. (2011). Independent Domain of Symmetric Encryption using Least SignificantBit: Computer Vision, Steganography and Cryptography Techniques (Doctoral dissertation, Dalarna University).

Abeyratne, R. (2013). The ePassport-new technology to counter security threats. *Journal of Transportation Security*, 6(1), 27-42.

Ahmad, M. A., & Al, I. F. (2012). Protection of the Texts Using Base64 and MD5. *Journal of Advanced Computer Science and Technology Research*, 2, 22-34.

Ahmed, K., Sampath, R., & Khan, M. S. (2006). Current trends in the diagnosis and management of renal nutcracker syndrome: a review. *European journal of vascular and endovascular surgery*, 31(4), 410-416.

Ahmed, M. A., Kiah, M. L. M., Zaidan, B. B., & Zaidan, A. A. (2010). A novel embedding method to increase capacity and robustness of low-bit encoding audio steganography technique using noise gate software logic algorithm. *Applied Sci*, 10, 59-64.

Al-Khouri, A. M. (2012). PKI in Government Digital Identity Management Systems. *European Journal of ePractice*, 4, 4-21.

Al-Taani, A. T., & Al-Issa, A. M. (2009). A Novel Steganographic Method for Gray-Level Images. *International Journal of Computer, Information and Systems Science, and Engineering*, 3(1).

Alam, G. M., Kiah, M. M., Zaidan, B. B., Zaidan, A. A., & Alanazi, H. O. (2010). Using the features of mosaic image and AES cryptosystem to implement an extremely high rate and high secure data hidden: Analytical study. *Sci. Res. Essays*, 5(21), 3254-3260.

Alkhathami, M., Han, F., & van Schyndel, R. (2013). Fingerprint image protection protection using two watermarks without corrupting minutiae. *ICIEA 2013*, 1151.

Al-Othmani, A. Z., Manaf, A. A., & Zeki, A. M. (2012). A Survey on Steganography Techniques in Real Time Audio Signals and Evaluation.

Amin, M. M., Salleh, M., Ibrahim, S., Katmin, M. R., & Shamsuddin, M. Z. I. (2003, January). Information hiding using steganography. In Telecommunication Technology, 2003. *NCTT 2003 Proceedings. 4th National Conference on* (pp. 21-25). IEEE.

An, L., Gao, X., Yuan, Y., & Tao, D. (2012). Robust lossless data hiding using clustering and statistical quantity histogram. *Neuro computing*, 77(1), 1-11.

Andreeva E. Mennink B. Preneel B. & Skrobot M. (2012), Security Analysis and Comparison of the SHA-3 Finalists BLAKE, Grostl, JH, Keccak, and Skein.fromKatholiekeUniversiteit Leuven.

Andrew, J. P. (2009). *European Patent No. EP* 0971544. Munich, Germany: European Patent Office.

Antony, J., Sobin, C. C., & Sherly, A. P. (2012). Audio Steganography in Wavelet Domain–A Survey. *International Journal of Computer Applications*, 52(13), 33-37.

Au, M. H., Tsang, P. P., & Kapadia, A. (2011). PEREA: Practical TTP-free revocation of repeatedly misbehaving anonymous users. *ACM Transactions on Information and System Security* (TISSEC), 14(4), 29.

Bai, L., Zhang, Y., & Yang, G. (2012, April). SM2 cryptographic algorithm based on discrete logarithm problem and prospect. *In Consumer Electronics, Communications and Networks* (CECNet), (pp. 1294-1297). IEEE.

Banerjee, I., Bhattacharyya, S., & Sanyal, G. (2014, March). Robust image steganography with pixel factor mapping (PFM) technique. In Computing for Sustainable Global Development (INDIACom), *2014 International Conference on* (pp. 692-698). IEEE.

Bellare, K., Druck, G., & McCallum, A. (2009, June). Alternating projections for learning with expectation constraints. *In Proceedings of the Twenty-Fifth Conference on Uncertainty in Artificial Intelligence* (pp. 43-50). AUAI Press.

Bhat, P., Zitnick, C. L., Cohen, M., & Curless, B. (2010). Gradientshop: A gradient-domain optimization framework for image and video filtering. *ACM Transactions on Graphics* (TOG), 29(2), 10.

Biham, E., Dunkelman, O., Keller, N., & Shamir, A. (2011). New data-efficient attacks on reduced-round IDEA. *Cryptology ePrint Archive, Report* 2011/417.

Biswas, R., Chowdhury, G. D., & Bandhyopadhyay, S. K. (2014). Perspective Based Variable Key Encryption in LSB Steganography. *In Advanced Computing,* Networking and Informatics-Volume 2 (pp. 285-293). Springer International Publishing.

Camenisch, J., & Grob, T. (2012). Efficient Attributes for Anonymous Credentials. *ACM Transactions on Information and System Security* (TISSEC), 15(1), 4.

Cao, F., & Cao, Z. (2009). A secure identity-based proxy multi-signature scheme. *Information Sciences*, 179(3), 292-302.

Chakraborty, K., & Mehta, J. (2012). A Stamped Blind Signature Scheme based on Elliptic Curve Discrete Logarithm Problem. *IJ Network Security*, 14(6), 316-319.

Chang, C. C., Chen, T. S., & Chung, L. Z. (2002). A steganographic method based upon JPEG and quantization table modification. *Information Sciences*, 141(1), 123-138.

Chang, Chin-Chen, and Hsien-Wen Tseng. "A steganographic method for digital images using side match." *Pattern Recognition Letters* 25.12 (2004): 1431-1437.

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

Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal processing*, 90(3), 727-752.

Cheddad, A., Nord, C., Hörnblad, A., Prunskaite-Hyyryläinen, R., Eriksson, M., Georgsson, F., & Ahlgren, U. (2013). Improving signal detection in emission optical projection tomography via single source multi-exposure image fusion. Optics express, 21(14), 16584-16604.

Chen, T., Wang, J., & Zhou, Y. (2001). Combined digital signature and digital watermark scheme for image authentication. *In Info-tech and Info-net,* 2001. Proceedings. ICII 2001-Beijing. 2001 International Conferences on (Vol. 5, pp. 78-82). IEEE.

Chen, S. W., Huang, S. Y., Wang, C. C., & Tsai, Y. C. (2013). U.S. *Patent Application* 14/033,516.

Chen, M. Q., Wen, Q. Y., Jin, Z. P., & Zhang, H. (2014). Secure and Efficient Certificateless Signature and Blind Signature Scheme from Pairings. Applied *Mechanics and Materials*, 457, 1262-1265.

Chung, L., & do Prado Leite, J. (2009). On non-functional requirements in software engineering. Conceptual modeling: *Foundations and applications*, 363-379.

Chung, H., Laforte, J. P., Reifschneider, D., & Williams, J. C. (2011). Estimating the macroeconomic effects of the fed's asset purchases. *FRBSF Economic Letter*, 3.

Damasevicius, R., Ziberkas, G., Stuikys, V., & Toldinas, J. (2012). Energy Consumption of Hash Functions. *Electronics and Electrical Engineering*, 18(10), 81-84.

Desmedt, Y., Pieprzyk, J., Steinfeld, R., Sun, X., Tartary, C., Wang, H., & Yao, A. C. C. (2012). Graph coloring applied to secure computation in non-Abelian groups| Macquarie University ResearchOnline.

Dewangan, U., Sharma, M., & Bera, S. (2013). Development and Analysis of Stego Image Using Discrete Wavelet Transform. *International Journal of Science and Research (IJSR)*, 2, 142-148.

Diffie, W., & Hellman, M. (1976). New directions in cryptography. Information Theory, *IEEE Transactions* on, 22(6), 644-654.

Ding, J., Yang, B. Y., Chen, C. H., Chen, M. S., & Cheng, C. M. (2008). New differential-algebraic attacks and reparametrization of rainbow. *In Applied Cryptography and Network Security* (pp. 242-257). Springer Berlin/Heidelberg.

Dinolt, G., Allen, B., Canright, D., & Garfinkel, S. (2012). Parallelizing SHA-256, SHA-1 and MD5 and AES on the *Cell Broadband Engine*.

Duffy, D. G., Goodwin, C. C., Johnes, A. W., & Binks, D. F. J. (2010). *U.S. Patent Application* 12/896,101.

El-Ghoneimy, M. M. (2008). Comparison between two Watermarking Algorithms Using DCT Coefficient and LSB Replacement. *Journal of Theoretical and Applied Information Technology*, 4(2), 132-139.

Elkamchouchi, H., Elshenawy, K., & Shaban, H. (2002, November). Extended RSA cryptosystem and digital signature schemes in the domain of Gaussian integers. In *Communication Systems*, 2002. ICCS 2002. The 8th International Conference on (Vol. 1, pp. 91-95). IEEE.

Eskander, G. S., Sabourin, R., & Granger, E. (2013). A Dissimilarity-Based Approach for Biometric Fuzzy Vaults–Application to Handwritten Signature Images. *In New Trends in Image Analysis and Processing–ICIAP* 2013 (pp. 95-102). Springer Berlin Heidelberg.

Ferguson, N., Schneier, B., & Kohno, T. (2012). *Cryptography Engineering*: Design Principles and Practical Applications. Wiley.

Filler, T., Ker, A. D., & Fridrich, J. (2009, February). The square root law of steganographic capacity for Markov covers. In IS&T/SPIE Electronic Imaging (pp. 725408-725408). *International Society for Optics and Photonics*.

Filler, T., Judas, J., & Fridrich, J. (2010). Minimizing embedding impact in steganography using trellis-coded quantization. *Proceedings of Media Forensics and Security III, SPIE*, 7451, 715405-1.

Fridrich, J., & Long, M. (2000). Steganalysis of LSB encoding in color images. In Multimedia and Expo, 2000. ICME 2000. 2000 IEEE *International Conference on* (Vol. 3, pp. 1279-1282). IEEE.

Fridrich, J., & Goljan, M. (2002, April). Practical steganalysis of digital images-state of the art. *In Proceedings of SPIE* (Vol. 4675, pp. 1-13).

Fridrich, J., Goljan, M., & Hogea, D. (2003). Steganalysis of JPEG images: Breaking the F5 algorithm. *In Information Hiding* (pp. 310-323). Springer Berlin/Heidelberg.

Fridrich, J. (2005). Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes. *In Information Hiding* (pp. 67-81). Springer Berlin/Heidelberg.

Fridrich, J., Kodovsky, J., Holub, V., & Goljan, M. (2011). Steganalysis of content-adaptive steganography in spatial domain. *In Information Hiding* (pp. 102-117). Springer Berlin/Heidelberg.

Goljan, M., Fridrich, J., & Filler, T. (2009). Large scale test of sensor fingerprint camera identification. Proc. *SPIE, Electronic Imaging, Security and Forensics of Multimedia* Contents XI, San Jose, CA.

Goyal, H., & Chutani, S. (2012). LSB Embedding in Spatial Domain-A Review of Improved Techniques. *International Journal of Computers & Technology*, 3(1), 153-157.

Gupta, P. B., Onder, T. T., Jiang, G., Tao, K., Kuperwasser, C., Weinberg, R. A., & Lander, E. S. (2009). Identification of selective inhibitors of cancer stem cells by *high-throughput screening*. Cell, 138(4), 645-659.

Hamid, N., Yahya, A., Ahmad, R. B., & Al-Qershi, O. M. (2012). Image Steganography Techniques: An Overview. *International Journal of Computer Science and Security (IJCSS)*, 6(3), 168.

Heidelmann, M., Barthel, J., & Houben, L. (2009). StripeSTEM, a technique for the isochronous acquisition of high angle annular dark-field images and monolayer resolved electron energy loss spectra. *Ultramicroscopy*, 109(12), 1447-1452.

Hmood, A. K., Kasirun, Z. M., Jalab, H. A., Alam, G. M., Zaidan, A. A., & Zaidan, B. B. (2010). On the accuracy of hiding information metrics: Counterfeit protection for education and important certificates. *Int. J. Phys. Sci*, 5(7), 1054-1062.

Hmood, A., Kadhim, A., & Abu Hassan, H. (2012). Enhancement of electrical transport through the anisotropic nanostructure performance of heavily Yb-doped thin films. *Materials Chemistry and Physics*.

Hu, G., Ma, J., & Huang, B. (2009, December). High throughput implementation of md5 algorithm on gpu. In Ubiquitous Information Technologies & Applications, 2009. ICUT'09. *Proceedings of the 4th International Conference on* (pp. 1-5). IEEE.

Huang, J., & Manning, B. D. (2009). A complex interplay between Akt, TSC2, and the two mTOR complexes. *Biochemical Society Transactions*, 37(Pt 1), 217.

Huang, C. C., & Lo, C. C. (2010, January). Threshold based group-oriented nominative proxy signature scheme for digital rights management. *In Consumer Communications and Networking Conference* (CCNC), 2010 7th IEEE (pp. 1-5). IEEE.

Huang, L. C., & Hwang, M. S. (2013). Two-party Authenticated Multiple-key Agreement Based on Elliptic Curve Discrete Logarithm Problem. *International Journal of Smart Home*, 7(1).

Homsirikamol E. Rogawski M. & K. Gaj (2010), Comparing Hardware Performance of Fourteen Round Two SHA-3 Candidates Using FPGAs. Retrieved December 21, 2010, from George Mason University.

Hossain, M., Al Haque, S., & Sharmin, F. (2009, December). Variable rate steganography in gray scale digital images using neighborhood pixel information. In Computers and Information Technology, 2009. ICCIT'09. *12th International Conference on* (pp. 267-272). IEEE.

Imad F. Alshaikhli, M. A. Ahmad. (2011). "Security Threats of Finger Print Biometric in Network System Environment." Advanced Computer Science and Technology Research 1(1): 15.

Indesteege, S. (2010). Analysis and Design of Cryptographic Hash Functions (Doctoral dissertation, PhD thesis, Katholieke Universiteit Leuven).

Isobe, T., & Shibutani, K. (2009). Preimage attacks on reduced Tiger and SHA-2. In *Fast Software Encryption* (pp. 139-155). Springer Berlin/Heidelberg.

Islam, R., Naji, A. W., Zaidan, A. A., & Zaidan, B. B. (2010). New System for Secure Cover File of Hidden Data in the Image Page within Executable File Using Statistical Steganography Techniques. *arXiv preprint arXiv*:1002.2416.

Jansen, J. (2009). Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC.

Jansirani, A., Rajesh, R., Balasubramanian, R., & Eswaran, P. (2011). Hi-tech authentication for palette images using digital signature and data hiding. *The International Arab Journal of Information Technology,* 8(2), 117-123.

Johnson, L., Levine, A., Smith, R., & Stone, S. (2010). The 2010 Horizon Report. New Media Consortium.

Joshi, R., Gagnani, L., & Pandey, S. (2013). Image Steganography. *International Journal of Advanced Research in Computer Engineering & Technology* (IJARCET), 2(1), pp-224.

Juneja, M., & Sandhu, P. S. (2014). Improved LSB based Steganography Techniques for Color Images in Spatial Domain. *IJ Network Security*, 16(4), 366-376.

Kae-por, F. C. (2008). U.S. Patent No. 7,328,344. Washington, DC: U.S. *Patent and Trademark Office*.

Kakvi, S. A., Kiltz, E., & May, A. (2012). Certifying rsa. *In Advances in Cryptology–ASIACRYPT* 2012 (pp. 404-414). Springer Berlin Heidelberg.

Kaur, J. S. (2014). TPA Ensuring Data Integrity in Cloud Environment. *Global Journal of Computer Science and Technology*, 13(13).

Karapanos, N., & Capkun, S. (2014). On the Effective Prevention of TLS Man-In-The-Middle Attacks in Web Applications. IACR Cryptology ePrint Archive, 2014, 150.

Keromytis, A. (2010). X. 509 Key and Signature Encoding for the KeyNote Trust Management System.

Kessler, G. C., & Hosmer, C. (2011). An Overview of Steganography. Advances in *Imaging and Electron Physics*, 83, 51-107.

Kim, P. S., & Han, J. S. (2006). New authorizing binding to reduce binding latency during mobile ipv6 handover procedure. *International Journal of Computer Science and Network Security*, 6(8B), 202-208.

Kim, K. S., Zhao, Y., Jang, H., Lee, S. Y., Kim, J. M., Kim, K. S., ... & Hong, B. H. (2009). Large-scale pattern growth of graphene films for stretchable transparent electrodes. *Nature*, 457(7230), 706-710.

Kirsch, S. T. (2012), *U.S. Patent* No. 20,120,323,717. Washington, DC: U.S. *Patent and Trademark Office.*

Koff, D., Bak, P., Brownrigg, P., Hosseinzadeh, D., Khademi, A., Kiss, A., ... & Volkening, A. (2009). Pan-Canadian evaluation of irreversible compression ratios ("lossy" compression) for development of national guidelines. *Journal of digital imaging*, 22(6), 569-578.

Kolesnikov, V., Sadeghi, A. R., & Schneider, T. (2009). Improved garbled circuit building blocks and applications to auctions and computing minima. *Cryptology and Network Security*, 1-20.

Koscielny, C., Kurkowski, M., & Srebrny, M. (2013). An Electronic Signature and Hash Functions. *In Modern Cryptography Primer* (pp. 127-145). *Springer Berlin Heidelberg.*

Kumar, A. (2011). Image Retrieval From Repository using Overlapping Approach (Doctoral dissertation, DELHI COLLEGE OF ENGINEERING).

Kumar, A. (2013, August). An efficient text extraction algorithm in complex images. In Contemporary Computing (IC3), 2013 *Sixth International Conference* on (pp. 6-12). IEEE.

Kumari, M., Khare, A., & Khare, P. (2010). JPEG Compression Steganography & Crypography Using Image-Adaptation Technique. *journal of advances in information technology*, 1(3), 141-145.

Lee, L. G., Chen, C. H., & Chiu, L. A. (2005). Thiazole orange: a new dye for reticulocyte analysis. Cytometry, 7(6), 508-517.

Lee, J. W., Kim, S. L., Kim, C. H., Koch, R. H., Lee, C. U., Kim, H. I., & Park, J. H. (2009). The sdB+ M eclipsing system HW Virginis and its circumbinary planets. *The Astronomical Journal*, 137(2), 3181.

Lee, C. F., & Huang, Y. L. (2011). Reversible data hiding scheme based on dual stegano-images using orientation combinations. *Telecommunication Systems*, 1-11.

Li, Y., He, B., Luo, Q., & Yi, K. (2009, March). Tree indexing on flash disks. In Data Engineering, 2009. ICDE'09. *IEEE 25th International Conference on (pp. 1303-1306). IEEE.*

Li, C., Zhou, Q., Liu, Y., & Yao, Q. (2011, July). Cost-efficient data cryptographic engine based on FPGA. In Ubi-Media Computing (U-Media), *2011 4th International Conference on (pp. 48-52). IEEE.*

Lin, C. H., Yang, C. Y., & Chang, C. W. (2012, July). An Efficient Algorithm for Protecting and Authenticating Medical Image. In Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), *2012 Eighth International Conference on (pp. 67-70). IEEE.*

Liu, Y. F., Guo, J. M., & Lee, J. D. (2011). Halftone Image Classification Using LMS Algorithm and Naive Bayes. Image Processing, *IEEE Transactions on*, 20(10), 2837-2847.

Liu, S., Hennelly, B. M., & Sheridan, J. T. (2013). Digital image watermarking spread-space spread-spectrum technique based on Double Random Phase Encoding. *Optics Communications*, 300, 162-177

Luo, W., Huang, F., & Huang, J. (2010). Edge adaptive image steganography based on LSB matching revisited. *Information Forensics and Security*, *IEEE Transactions on,* 5(2), 201-214.

Mahdi, O. A., Mohammed, M. A., Mohamed, A. J., & Baghdad, I. (2012). Implementing a Novel Approach an Convert Audio Compression to Text Coding via Hybrid Technique.

Makbol, N. M., & Khoo, B. E. (2013). Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. *AEU-International Journal of Electronics and Communications*, 67(2), 102-112.

Malik, M. Y. (2010, February). Efficient implementation of elliptic curve cryptography using low-power digital signal processor. In Advanced Communication Technology (ICACT), 2010 *The 12th International Conference on* (Vol. 2, pp. 1464-1468). IEEE.

Mazumder, J. A., & Hemachandran, K. (2012). Review Of Different Techniques Used In Recent Steganography Researches. *International Journal of Engineering*, 1(8).

Morkel, T. (2012). IMAGE STEGANOGRAPHY APPLICATIONS FOR SECURE COMMUNICATION (Doctoral dissertation, University of Pretoria).

Naccache, D. (2011). Reverse public key encryption. *In Encyclopedia of Cryptography and Security* (pp. 1044-1044). Springer US.

Naji, K. (2008). Ahmadinejad: the secret history of Iran's radical leader (Vol. 1). University of California Press.

Naji, A. W., Gunawan, T. S., Zaidan, A. A., Zaidan, B. B., Al-Khateeb, W. F., & Hameed, S. A. (2009). New approach of hidden data in the portable executable file without change the size of carrier file using statistical technique. *International Journal of Computer Science and Network Security* (IJCSNS), 9(7), 218-224.

Naji, A. W., Hameed, S. A., Zaidan, B. B., Al-Khateeb, W. F., Khalifa, O. O., Zaidan, A. A., & Gunawan, T. S. (2009). Novel Framework for Hidden Data in the Image Page within Executable File Using Computation between Advanced Encryption Standard and Distortion Techniques. *arXiv preprint arXiv*:0908.0216.

Nandi, M. and S. Paul (2010). Speeding up the wide-pipe: Secure and fast hashing. Progress in Cryptology-INDOCRYPT 2010, Springer: 144-162.

Nasr, D., Bahig, H., & Daoud, S. (2011). Visualizing Secure Hash Algorithm (SHA-1) on the Web. *Active Media Technology*, 101-112.

Naredla, H. K. (2010). Digital image steganography: Survey and analysis of current methods more.

Nixon, M., & Aguado, A. S. (2012). Feature Extraction & Image Processing for *Computer Vision*. Academic Press.

Nazaryan, L., Panaousis, E., & Politis, C. (2010). End-to-End Security Protection. Vehicular Technology Magazine, IEEE, 5(1), 85-90.

Noroozi, E., Salwani, M., Sabouhi, A and SalehNamadi M. (2012), New Implementation of Hashing and Encoding in Digital Signature, *International Conference on Security Science and Technology* – ICSST, Hong Kong, March 2012.

Noroozi, E., Salwani, M., Sabouhi, A., Hafiza, A. (2012), A New Dynamic Hash Algorithm in Digital Signature, First International Conference on *Advanced Machine Learning Technologies and Applications* (AMLTA12), published by LNCS/CCIS series, Egypt, December 2012.

Noroozi, E., Salwani, M., & Sabouhi, A. (2013). Secure digital signature schemes based on hash functions. *International Journal of Innovative Technology and Exploring Engineering*, 2(4), 321-325.

Noroozi, E., Daud, S. M., & Sabouhi, A. (2014). Enhancing Secured Data Hiding Using Dynamic Digital Signature for Authentication Purpose. *Jurnal Teknologi*, 68(2).

Osborne, M. C., & Visegrady, T. (2012). *U.S. Patent No*. 20,120,324,230. Washington, DC: *U.S. Patent and Trademark Office*.

Othman, S., Trad, A., & Youssef, H. (2012, March). Performance evaluation of encryption algorithm for wireless sensor networks. In Information Technology and e-Services (ICITeS), 2012 *International Conference* on (pp. 1-8). IEEE.

O'Neill, A., Peikert, C., & Waters, B. (2011). Bi-deniable public-key encryption. *Advances in Cryptology*–CRYPTO 2011, 525-542

Pandey, A. K., Mirdha, V., & Hembram, S. S. (2011). Digital image watermarking based on FPGA and spintronic logic and study of some aspects of spintronic logic based circuits (Doctoral dissertation).

Park, J. M., Chong, E. K., & Siegel, H. J. (2002). Efficient multicast packet authentication using signature amortization. *In Security and Privacy,* 2002. Proceedings. 2002 IEEE Symposium on (pp. 227-240). IEEE.

Perwej, Y., Parwej, F., & Perwej, A. (2012). An Adaptive Watermarking Technique for the copyright of digital images and Digital Image Protection. *arXiv preprint arXiv:*1205.2800.

Potdar, V. M., Han, S., & Chang, E. (2005, August). A survey of digital image watermarking techniques. In Industrial Informatics, 2005. INDIN'05. 2005 3rd *IEEE International Conference* on (pp. 709-716). IEEE.

Prabakaran, G., Bhavani, R., & Kanimozhi, K. (2013, February). Dual transform based steganography using wavelet families and statistical methods. In Pattern Recognition, Informatics and Medical Engineering (PRIME), 2013 *International Conference on* (pp. 287-293). IEEE.

Rao, T. D. K. (2012). Implementation and performance analysis of JPEG2000, JPEG, JPEG-LS, JPEG-XR and H. 264/AVC Intra frame coding.

Reddy, M. I., Bhat, P. J., Chetwavani, R., & Reddy, M. P. (2011). Establishment of Public Key Infrastructure for Digital Signatures. *Computer Engineering and Intelligent Systems*, 2(6), 33-43.

Reinhard, E., Heidrich, W., Debevec, P., Pattanaik, S., Ward, G., & Myszkowski, K. (2010). High dynamic range imaging: acquisition, display, and image-based lighting. Morgan Kaufmann.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120-126.

Saadi, K. A., Bouridane, A., & Guessoum, A. (2009). Combined Fragile Watermark and Digital Signature for H. 264/AVC Video Authentication. *In EUSIPCO* (Vol. 9, pp. 1-4).

Salehi, H., Shirazi, H., & Moghadam, R. A. (2009, April). Increasing overall network security by integrating Signature-Based NIDS with Packet Filtering Firewall. In Artificial Intelligence, 2009. JCAI'09. *International Joint Conference on* (pp. 357-362). IEEE.

Sara, K. (2011). A new steganography method based on HIOP (Higher Intensity Of Pixel) algorithm and Strassen's Matrix Multiplication. *Journal of Global Research in Computer Science,* 2(1).

Satish, K., Jayakar, T., Tobin, C., Madhavi, K., & Murali, K. (2004). Chaos based spread spectrum image steganography. Consumer Electronics, *IEEE Transactions on*, 50(2), 587-590.

Schuldt, J. C., & Matsuura, K. (2011). Efficient convertible undeniable signatures with delegatable verification. IEICE *transactions on fundamentals of electronics, communications and computer sciences*, 94(1), 71-83.

Serret-Avila, X., & Boccon-Gibod, G. (2012). U.S. Patent No. 8,099,601. Washington, DC: U.S. *Patent and Trademark* Office.

Selbrede, M. G., Van Ostrand, D. K., & Essman, L. (2011). U.S. Patent No. 8,014,057. Washington, DC: U.S. *Patent and Trademark* Office.

Shah, V., Rao, N. N., Agrawal, A., Sarkar, S., Subramanian, K., & Shukla, H. (2010). U.S. Patent No. 7,694,009. Washington, DC: U.S. *Patent and Trademark* Office.

Shen, A. N., Guo, S., Zeng, D., & Guizani, M. (2012, April). A lightweight privacy-preserving protocol using chameleon hashing for secure vehicular communications. *In Wireless Communications and Networking Conference* (WCNC), 2012 IEEE (pp. 2543-2548). IEEE.

Shin, J., & Ruland, C. (2013, October). A survey of image hashing technique for data authentication in WMSNs. *In Wireless and Mobile Computing, Networking and Communications (WiMob),* 2013 IEEE 9th International Conference on (pp. 253-258). IEEE.

Shirali-Shahreza, S., & Shirali-Shahreza, M. (2008, August). Identifying child users: Is it possible?. *In SICE Annual Conference*, 2008 (pp. 3241-3244). IEEE.

Shin, J., & Ruland, C. (2013, October). A survey of image hashing technique for data authentication in WMSNs. *In Wireless and Mobile Computing, Networking and Communications (WiMob),* 2013 IEEE 9th International Conference on (pp. 253-258). IEEE.

Singh, S., & Agarwal, G. (2010). Use of image to secure text message with the help of LSB replacement. *international journal of applied engineering research*, 1(2).

Sinha, A., & Singh, K. (2003). A technique for image encryption using digital signature. *Optics Communications*, 218(4), 229-234.

Sivaraja, S., & Baburaj, E. (2011). Survey of Steganoraphic Techniques in Network Security. *International Journal of Research and Reviews in Computer Science* (IJRRCS), 2(1).

Soumi, C. G., George, J., & Stephen, J. (2014). Genetic Algorithm based Mosaic Image Steganography for Enhanced Security. *ACEEE International Journal on Signal & Image Processing,* 5 (1), 15-26.

Stern, J., Pointcheval, D., Malone-Lee, J., & Smart, N. (2002). Flaws in applying proof methodologies to signature schemes. *Advances in Cryptology*—CRYPTO 2002, 215-224.

Sudia, F. W., Freund, P. C., & Huang, S. T. (2013). U.S. Patent No. 8,364,967. Washington, DC: U.S. Patent and Trademark Office.

Swathi, B., Shalini, K., & Prasanthi, K. N. (2012). A REVIEW ON STEGANOGRAPHY USING IMAGES. *Asian Journal of Computer Science and Information Technology*, 2(8).

Taqa, A., Zaidan, A. A., & Zaidan, B. B. (2009). New framework for high secure data hidden in the MPEG using AES encryption algorithm. *International Journal of Computer and Electrical Engineering* (IJCEE), 1(5), 589-595.

Thomas, P., & Singh, A. K. (2013). A Novel Steganographic Approach for Enhancing the Security of Images.

Thomson, K., Purcell, K., & Rainie, L. (2013). Arts organizations and digital technologies. Washington, DC: Pew Research Centergies. Accessed November, 22, 2013.

Turner, D. M., Prevelakis, V., & Keromytis, A. D. (2010). A market-based bandwidth charging framework. *ACM Transactions on Internet Technology* (TOIT), 10(1), 1.

Turner, S., Chen, L., Polk, T., & Hoffman, P. (2011). Security Considerations for the SHA-0 and SHA-1 Message-Digest Algorithms.

Venkatraman, S., Boey, F., & Lao, L. L. (2008). Implanted cardiovascular polymers: Natural, synthetic and bio-inspired. *Progress in Polymer Science*, 33(9), 853-874.

Walker, M. A. (2010). Standard Method of Evaluating Cryptographic Capabilities and Efficiency for Devices with the Android Platform.

Wang, Z., & Li, Q. (2007). Video quality assessment using a statistical model of human visual speed perception. JOSA A, 24(12), B61-B69.

Wang, Q., Wang, C., Li, J., Ren, K., & Lou, W. (2009). Enabling public verifiability and data dynamics for storage security in cloud computing. *Computer Security–ESORICS* 2009, 355-370.

Wang, Y., Zhao, Q., Jiang, L., & Shao, Y. (2010). Ultra high throughput implementations for MD5 hash algorithm on FPGA. High Performance Computing and Applications, 433-441.

Westfeld, A., & Pfitzmann, A. (2000). Attacks on steganographic systems. In Information Hiding (pp. 61-76). Springer Berlin/Heidelberg.

Westfeld, A. (2009). Fast Determination of Sensitivity in the Presence of Countermeasures in BOWS-2. In Information Hiding (pp. 89-101). Springer Berlin/Heidelberg.

Westfeld, P., Maas, H. G., Pust, O., Kitzhofer, J., & Brücker, C. (2010, July). 3-D least squares matching for volumetric velocimetry data processing. In Proceedings of *the 15th International Symposium on Appliocations of Laser Techniques to Fluid Mechnaics* (pp. 5-8).

Wu, D. C., & Tsai, W. H. (2003). A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters*, 24(9), 1613-1626.

Wu, C. H. (2010, December). Self-Generated-Certificate Digital Signature. In Genetic and Evolutionary Computing (ICGEC), 2010 *Fourth International Conference on* (pp. 379-382). IEEE.

Wong, K. W., Man, K. P., Li, S., & Liao, X. (2005). A more secure chaotic cryptographic scheme based on the dynamic look-up table. *Circuits, systems, and signal processing*, 24(5), 571-584.

Yan, G., Yue-Fei, Z., Chun-Xiang, G., Jin-long, F., & Xin-Zheng, H. (2013). A Framework for Automated Security Proof and its Application to OAEP. *Journal of Networks,* 8(3).

Yao, A. C., & Zhao, Y. (2011). A New Family of Practical Non-Malleable Diffie-Hellman Protocols. *arXiv preprint arXiv*:1105.1071.

Zaidan, A. A., Zaidan, B. B., Abdulrazzaq, M. M., Raji, R. Z., & Mohammed, S. M. (2009). Implementation stage for high securing cover-file of hidden data using computation between cryptography and steganography. *International Association of Computer Science and Information Technology* (IACSIT), indexing by Nielsen, Thomson ISI (ISTP), IACSIT Database, British Library and EI Compendex, 20.

Zaidan, A. A., Othman, F., Zaidan, B. B., Raji, R. Z., Hasan, A. K., & Naji, A. W. (2009). Securing Cover-File Without Limitation of Hidden Data Size Using Computation Between Cryptography and Steganography. In Proceedings of the *World Congress on Engineering* (Vol. 1).

Zaidan, A. A., Zaidan, B. B., Taqa, A. Y., Mustafa, K. M. S., Alam, G. M., & Jalab, H. A. (2010). Novel multi-cover steganography using remote sensing image and general recursion neural cryptosystem. *Int. J. Phys*. Sci, 5(21), 3254-3260.

Zaidan, A. A., Zaidan, B. B., Alanazi, H. O., Gani, A., Zakaria, O., & Alam, G. M (2010). Novel approach for high (secure and rate) data hidden within triplex space for executable file. *Sci. Res. Essays*, 5(15), 1965-1977.

Zaidan, A. A., Zaidan, B. B., Al-Fraja, A. K., & Jalab, H. A. (2010). Investigate the capability of applying hidden data in text file: An overview. *J. Appl. Sci*, 10(17), 1916-1922.