



Republic of Iraq
Ministry of Higher Education
and Scientific Research
University of Diyala
College of Science



Improvement of Data Security System Using Magic Cube

A Thesis
Submitted to College of Science/ University of Diyala in a Partial
Fulfillment of the requirements for the Degree of Master in computer
Science

By

Nuha Salim Mohammed

Supervised By

Prof. Dr. Ziyad Tariq Mustafa

2019 A.D.

1439 A.H.

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ
﴿فَأَمَّا الزَّبَدُ فَيَذْهَبُ جُفَاءً وَإِنَّمَا مَا
يَنْفَعُ النَّاسَ فَيَمْكُتُ فِي الْأَرْضِ﴾
صدق الله العظيم

سورة الرعد

الآية 17



Dedication

I would like to dedicate this

Work To:

*Whom taught me that the champions
will never be defeated, but they
convert it to victory.*

Our Prophet Mohammed

Peace be Upon Him (PBH)

*My Father and my Mother, my
husband, my sister and my brothers,
and my son
(Abdallah).*

Acknowledgments

Firstly, all my prayers go to (Allah), the Almighty, for the successive blessings, divine providence, and my success in this research.

I would like to extend my sincere thanks and gratitude to my supervisor **Prof. Dr. Ziyad Tariq Mustafa** for their invaluable guidance, constructive suggestions, advice and assistance during the writing of this research. Thanks are also due to all staff members at computer science Department in the University of Diyala for their encouragement and support.

Special thanks are extended to my father and my mother for their patience and moral support that helped me finish this study.

Also many thanks are extended to my brothers and sister and my husband for their support.

Finally, I would like to thank all my friends for their support and Willingness to listen and comment on different aspects of this Research.



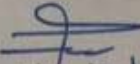
Nuha S. Mohammed

Publication Papers

Nuha S. Mohammed, Ziyad T. Mustafa “Using Magic Cube And a modified LSB for Audio Steganography” International Journal of Engineering & Technology, 8 (1.5) (2019) 283-289.

Linguistic Certification

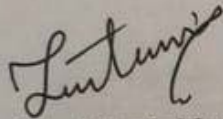
I certify that this thesis entitled "**Improvement of Data Security system Using Magic Cube**" was prepared by **Nuha Salim Mohammed** and was reviewed linguistically. Its language is amended to meet the style of English language.

Signature: 
Name: *Shatha Haleem*
Date: *6/3/2019*

Supervisor's Certification

I certify that this thesis entitled "**Improvement of Data Security System Using Magic Cube**" Was prepared by **Nuha Salim Mohammad** under my Supervision at the Department of Computer Science University of Diyala as a partial fulfilment of requirements for the Degree of **Master of Sciences in Computer Science**.

Signature:



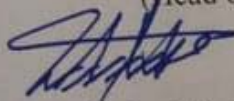
Name: Prof. Dr. Ziyad Tariq Mustafa

Date: 5/3/2019

Approved by the computer sciences department, college of science,
university of Diyala.

(Head of the Department)

Signature:



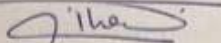
Name: Prof. Dr. Taha Mohammed Hasan

Date: 5/3/2019

Examination Committee Certificate

We certify that this thesis entitled "**Improvement of Data Security system Using Magic Cube**" and as an examining committee, examined the student **Nuha Salim Mohammad** in its contents, and that in our opinion it has adequate fulfill the requirements for the Degree of Master of Science in Computer Science department.

(Chairman)

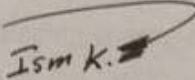
Signature: 

Name: Dr. Dhahair A. Abdulah Salma

Title: Professor

Date: 5/3/2019

(Member)

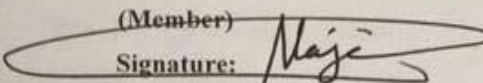
Signature: 

Name: Dr. Ismail Khalil Ali

Title: Assistant Professor

Date: 9/3/2019

(Member)

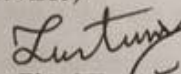
Signature: 

Name: Naji M. Sahib

Title: Assistant Professor

Date: 5/3/2019

(Member/Supervisor)

Signature: 

Name: Prof. Dr. Ziyad Tariq Mustafa

Title: Professor

Date: 5/3/2019

Approved by the Dean of College of Science, University of Diyala.

(The Dean)

Signature: 

Name: Dr. Tahseen Hussein Mubarak

Title: Professor

Date: 17/3/2019

Abstract

It is axiomatic that most of encryption systems are relied on keys, because of they are easier to protect and easier to change, this also applies to steganographic systems. Therefore, the security of the encryption systems and steganographic systems is linked to the method of generating the keys to these systems.

As a result, this thesis presents magic cube as a mathematical technique for generating keys in a proposed secure system. The proposed secure system consists of transmitter side and receiver side. The transmitter side includes three phases: (the first phase is constructing the magic cube in order to generate random uncorrelated keys, the second phase is encrypting secret plaintext messages by using (RC4 or RSA) algorithm depending on magic cube keys (from phase one), and the third phase is hiding the (RC4 or RSA) encrypted messages using least significant bit (LSB) method depending on magic cube keys. The receiver side extracts the secret plaintext messages by using the reverse way of the transmitter side.

NIST Package and correlation tests prove that the keys (which are generated by the constructed magic cube) are random, unpredictable and uncorrelated, so they are robustness against the attacks. The magic cube keys are passed most of the NIST tests with high success rates. The improved of RC4 with IKSA is tested for its secrecy, randomness and performance over the variable key length and different plaintext size with respect to those of the original RC4. The results show that the improved RC4 with IKSA is better than the original RC4 with KSA.

The average security of the (RC4) encrypted messages is between (0.116801555631564 - 0.296875), while the average security of the (Improved RC4 (IRC4)) encrypted messages by using magic cube keys is

between (0.15283203125 - 0.558364648336087). Implementation RSA with Big Integer Calculations of modular exponential, modular inverse, Greatest common divisor, modulus n, Big Integer p and Big Integer q.

The PSNR of audio stegocovers without using magic cube keys for embedding (32 bits) is between (74.93983862- 80.44353577) dB, while the PSNR of audio stegocovers by using magic cube keys for embedding (32 bits) is between (78.08175304- 83.01604649) dB.

List of CONTENTS

	Contents	<i>Page No.</i>
	<i>Chapter One: Introduction</i>	1-8
1.1	overview	1-3
1.2	Problems Statement	3-4
1.3	Aim of The Thesis	4
1.4	Related Works	5-7
1.5	Outline of thesis	7-8
	<i>Chapter Two: Theoretical Background</i>	9- 42
2.1	Introduction	9
2.2	Cryptography	9-10
2.2.1	Symmetric Cipher (RC4)	10-12
2.2.2	Random Number Generators	12-13
2.2.3	RC4 Weakness Point	13
2.3	Asymmetric Cipher (RSA)	13-14
2.3.1	Attacks on RSA	14-15
2.3.2	RSA Weakness Point	15
2.3.3	Library Big Integer c#	15-17
2.3.4	Number Theory and Prime Generation	17-18
2.3.5	Primality Testing	18-19
2.3.6	Integer factorization	19
2.4	Steganography	20-21
2.5	Magic square	21-23
2.5.1	Magic square properties	23-24
2.5.2	Magic square construction	24
2.5.2.1	Magic Squares as Odd Order	24-27
2.5.2.2	Magic Squares as Double Even Order	27-29
2.5.2.3	Magic Squares as Single Even Order	29-33
2.6	The probability of the magic squares	33-34
2.7	Magic cube	34-36
2.8	Magic cube construction	36-37

2.9	Randomness Tests	38-39
2.10	Audio Quality Metrics	39-40
2.11	Correlation test	41
2.12	Average Security	41
	<i>Chapter Three: The Proposed System</i>	42- 67
3.1	Introduction	42
3.2	Design Objectives	43
3.3	Proposed System	43- 44
3.3.1	Transmitter Side	45
3.3.1.1	Constructing magic cube	46- 53
3.3.1.2	Select Approach (RC4 or RSA)	53- 62
3.3.1.3	LSB Embedding Steganography	62- 64
3.3.2	Receiver Side	64
3.3.2.1	Constructing Magic Cube	65
3.3.2.2	LSB Extraction Steganography	65
3.3.2.3	Select Approach (RSA or RC4)	66
	<i>Chapter Four: Analysis and Results</i>	67-95
4.1	Introduction	67
4.2	Initialization	67
4.3	Results of the proposed system	67
4.3.1	Results of Magic cube (Random keys)	67-68
4.3.2	Results of Cipherring with RC4 Algorithm	68-71
4.3.3	Results of Cipherring with RSA Algorithm	71-77
4.3.4	Results of LSB Steganography	78
4.3.4.1	Test Histogram Samples	78-79
4.3.4.2	Quality Metrics Results	79-80
4.3.4.3	LSB Hiding	80-81
4.4	Analysis	81
4.4.1	Tests on Magic Cube	81-82
4.4.2	Correlation Test	83-84
4.4.3	Analysis for the Results of RC4 Cipherring	85
4.4.4	Average Security	85-90
4.4.5	Analysis for the Results of RSA Cipherring	90-91

4.4.5.1	Merge prime numbers	91
4.4.5.2	Primality Testing with Miller and Rabin Algorithm	91
4.4.6	Analysis of LSB Steganography	92-94
4.5	Time span	94
	<i>Chapter Five: Conclusions and Suggestions</i>	95-97
5.1	Introduction	95
5.2	Conclusions	95-96
5.3	Suggestions for Future Works	96-97
	<i>References</i>	98-105

LIST OF ABBREVIATIONS

Abbreviations	Meaning
NIST	National Institute of Standards and Technology
IFP	Integer Factorization Problem
DES	Data Encryption Standard
PRN	Pseudo Random Numbers
TRN	True Random Numbers
RNGS	Pseudo Random Numbers Generators
TRNGS	True Random Numbers Generators
RSA	Rivest Shamir and Adelman
LSB	Least Significant Bit
RC4	Rivest Cipher 4
MC	Magic Constant
MS	Magic Sum
KSA	Key scheduling algorithm
PRGA	pseudo-random generation algorithm

List of Figures

<i>Figure No.</i>	<i>Caption</i>	<i>Page No.</i>
2.1	Magic Square of Order(3)	22
2.2	Steps of Construction Odd Order Magic Square	26
2.3	Pyramid Magical Square with order Three	26
2.4	Pyramid Magical Square with order Five	27
2.5	Example of Durer Approach	28
2.6	Other Example of Durer Approach	29
2.7	Some Reflection and Rotations for the Durer approach	29
2.8	de la Hire Technique of Order Six	31
2.9	de la Hire Technique of Order 6,10 and 14	32
2.10	Example of de la Hire with Order Six	33
2.11	Rotations and Reflections of Magic Square	34
2.12	Magic Cube of Order Three	34
2.13	Magic Cube of Three Layers	35
3.1	General Block Diagram of the Proposed System	44
3.2	The Detailed Block Diagram of the Transmitter Side	45
3.3	Magic Cube with Order Three	47
3.4	Magic Cube of Order Four	48
3.5	Sequence cube with order six	51
3.6	Zigzag cube with order six	52
3.7	Block Diagram of Generate Magic Cube	52
3.8	Block Diagram of Testing Magic Cube Keys	53
3.9	Block Diagram of RC4 Algorithm	54
3.10	Pseudo Code of KSA	54
3.11	Pseudo Code of PRGA	55

3.12	The method of getting the key stream(k)	56
3.13	Overall Operation of RC4 algorithm	56
3.14	The Detailed Block Diagram of the Receiver Side	64
4.1	Statistical Tests of NIST on the Keys	82
4.2	Results of the Correlation Test the keys (vertical)	84
4.3	Results of the Correlation Test the keys (Horizontal)	84
4.4	Average Security With Original RC4	85
4.5	Average Security With IRC4	86
4.6	Average Secrecy Value vs. Key length	87-88
4.7	Average Secrecy Value vs. plaintext	89-90
4.8	Distribution of Hided Locations with 32-bit Encrypted Secret Message for Audio Cover	92
4.9	Distribution of Hided Locations with 64-bit Encrypted Secret Message for Audio Cover	92
4.10	Distribution of Hided Locations with 128-bit Encrypted Secret Message for Audio Cover	93
4.11	Distribution of Hided Locations with 256-bit Encrypted Secret Message for Audio Cover	93
4.12	Distribution of Hided Locations with 512-bit Encrypted Secret Message for Audio Cover	93
4.13	Distribution of Hided Locations with 1024-bit Encrypted Secret Message for Audio Cover	94

List of Tables

<i>Table No.</i>	<i>Caption</i>	<i>Page No.</i>
4.1	Sixty Random Keys created by Magic Cube with Different Orders using (10) Iterations	68
4.2	The ASCII Values of Secret Plain Text Message	69
4.3	Byte Keys(256)	69
4.4	First Permuted 256-Byte Keys	70
4.5	Second Permuted Key Stream	70
4.6	RC4 process	71
4.7	the ASCII Values of Secret Plain Text Message	71
4.8	the no of prime number	71
4.9	the no of prime number with Big Integer	73
4.10	mod operation	76
4.11	Result of addition Big Integer	76
4.12	Result of division Big Integer	77
4.13	Histograms of Audio Covers	78
4.14	Histogram for Audio Stegocovers	79
4.15	Evaluation of Audio Stegocovers	80
4.16	LSB Hiding of Encrypted Secret Message	80-81
4.17	The Statistical Tests of NIST on The Keys of the Proposed Magic Cube	82
4.18	Results of the Correlation Test the keys of the Magic Cube seven order	83
4.19	Average Secrecy Value vs. Plaintext size	86
4.20	Average Secrecy Value vs. Plaintext	88-89
4.21	Comparison in time span	94

SYMBOLS TABLE

Symbol	Meaning
*	Multiplication operation
+	Addition operation
/	Division operation
-	Subtraction operation
C#	C sharp
==	Equality sign
!=	Inequality sign
++	Increment
--	Decrement
~	Negation
&	AND
	OR
^	exclusive OR
<<	left shift
>>	Right shift
<	Less than
<=	Less than or equal to
>=	Greater than or equal to
>	Greater than
\sum	Summation - sum of all values in range of series
X	The absolute value bars
Log	Logarithm
%	modulus
\oplus	Circled plus / oplus - xor
(a,b)	Ordered pair, collection of 2 elements

()	Parentheses, calculate expression inside first
----	--

List Algorithms

<i>Algorithm no.</i>	<i>Title</i>	<i>Page No.</i>
1	Chapter two	
2.1	RC4 Algorithm	9
2.2	Miller and Rabin	12
2	Chapter three	
3.1	Siamese Method (Odd order) Magic cube Creation	37
3.2	Strachney Method (Single even order) Magic cube Creation	38
3.3	Albrecht Durer's Method (Double even order) Magic cube Creation	39
3.4	Implemented RSA Algorithm with Big Integer	45
3.5	an embedding of Ciphersed Secret Message Using LSB	52
3.6	Extraction of Ciphersed Secret Audio using LSB	54

Chapter One

Introduction

Chapter One

Introduction

1.1 Overview

In nowadays, security is required to transmit confidential information on public network. The need for data security and the privacy increased rapidly and become very important to transmit secret information over the network [1]. Two important technologies cryptography and steganography are used for Information safety of digital reality for today .The process of combining encryption and embedding help for increasing in power work or the digital information protection and security that it will be difficult to limit and find hiding in sender file. These two technologies are known very well and depended on techniques that encryption\decryption or hiding the data [2][3]. Cryptography system can be classified into two parts first is Symmetric key Cryptography and second is public key cryptography. Symmetric key cryptography: In symmetric key cryptography system sender and receiver share a single key which is used to encrypt and decrypt a message. It is also called secret key cryptography. The algorithms used for symmetric key cryptography is called symmetric- key algorithms. There are two types of symmetric algorithms such as stream cipher and block cipher. Stream ciphers encrypt the bits of information one at a time and Block ciphers encrypt the information by breaking down into blocks [1][2][3]. True Random Number (TRN) and Pseudorandom numbers (PRN) are so important in many applications of cryptographic. In any cryptosystems use Keys that must be generated in a random style .Random Numbers Generators (RNGs) are classified into Pseudo Random Numbers Generators (PRNGs) and True Random Numbers Generators (TRNGs) [2][3]. Algorithms in Cryptographic play an important role in providing

the data security against malicious attacks. Random numbers technique applies to many fields such as, network security, cryptographic algorithms. Cryptographic methods utilize algorithmic techniques to generate random number, these are deterministic and product series of numbers that are not statistically random. However, if algorithmic works perfect, the obtained result will exceed many sensible tests of randomness; these numbers are called pseudorandom numbers [2] [4].

The efficiency of cryptographic algorithm is not only depending on its time taken for encryption and decryption, and it also accounts for number of stages used to obtain the cipher-text from a plain-text. RSA is one of the most common encryption algorithms, which guarantees authenticity, confidentiality and data integrity through a risky connection channel; however, various attackers attempt to break algorithm security due to certain constraints. Furthermore, RSA not be guaranteed that the cipher plan is perfectly secured. Therefore, magic cube and Magic Square are introduced to improve the security due to its complexity of the encryption procedure [1].

A randomness concept is used widely in this field; also the power and strong argument of any encryption algorithm, build upon the encryption Key attributes; its length and randomness. The security of all application of this field depends essentially on making unpredictable Key[5]. Some cryptographic systems which has high security depends on unpredictable components generation, such as strong large prime randomly p and q in the RSA, secret key in the DES, key stream that generated by one-time pad etc. In these systems, quantities of generated keys must be sufficient in random and the size, that the probability of any selected value must be sufficiently small [6].

Therefore, different methods are used for the security development system such as: double even, single even, odd magic squares of order n and magic cubes.

The construction of magic square and magic cube are based on the start number, different number, and size of cube, number of cubes according to the size of secret message, magic sum and magic constant. These values are very difficult to follow and predicate because of their randomness.

Magic cube helps to identify the existing issues of secret-key cryptosystem.

Magic cube is technique mathematics with 3-dimension called magic square. The pattern of this technique is a number arranged from 1, 2, ..., n^3 in a $(n \times n \times n)$, n is integer, the summation of the numbers on row, column, pillar and of the 4- main space diagonals equivalent to the same number, the so-called magic constant of the cube[7]

Magic cube cryptography and steganography are new techniques. These techniques are adopted in this thesis in order to build complete secure system.

1.2 Problem Statement

The major problem of this work is to design secure system with high secrecy keys by to overcome on the weakness points in RC4 (Rivest Cipher 4) algorithm and Integer Factorization Problem (IFP) focuses on the factoring the number to its factors prime numbers. The RSA public key is considered a good paradigm that is based on factoring problem of analyzing the composite n number to its factors of two distinct large prime's numbers p and q , in order to find the e^{th} root. Thus, the main difficult waylays if the factoring of n is known, so it's computational

mathematics will be easy to solve the RSA problem .This secure system has two different security models such as: cryptography and steganography, but both of them depend on a magic cube as a random keys generator. The minor one is a comparison between magic cube symmetric encryption and magic cube asymmetric encryption.

1.3 Aim of Thesis

The aims of the study:

- 1- Design and implement magic cube with size (n), any type and any order, and both cryptographic and LSB steganographic system are depended on magic cube.
- 2- Design and implement symmetric magic cube encryption using RC4 algorithm.
- 3- Design and implement asymmetric magic cube encryption using RSA algorithm.
- 4- Design and implement asymmetric magic cube encryption using RSA algorithm with Big Integer.
- 4- Make an enhancement of RC4 magic cube encryption using average security and RSA magic cube encryption using Big Integer.
- 5- Design and implement complete multilevel secure system consists of cryptographic system (RC4 system) to encrypt plain-text message using RC4 magic cube encryption or RSA magic cube encryption, and steganographic system (LSB system)for hiding the output cipher-text inside audio cover using magic cube random keys.