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.

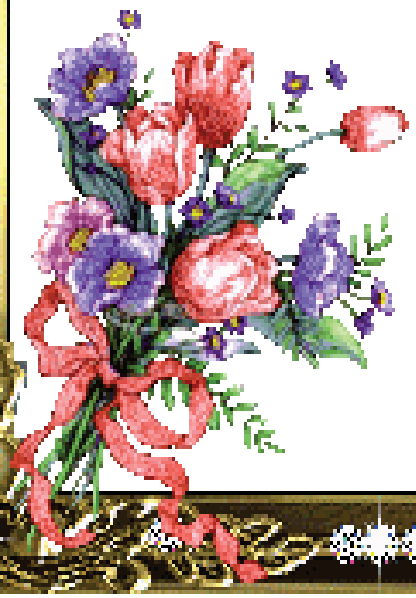
بسم الله الرحمن الرحيم

﴿فأما الزَّبَدُ فَيَذْهَبُ جُفَاءً وإمَّا مَا ينَفعُ الناسَ فيَمكُثُ في الأرضِ ﴾

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

# 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

# List of Tables

# 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

# 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, …, n3 in a (n x n x 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.