



شبكة المعلومات الجامعية
التوثيق الإلكتروني والميكروفيلم

بسم الله الرحمن الرحيم



MONA MAGHRABY



شبكة المعلومات الجامعية
التوثيق الإلكتروني والميكروفيلم



شبكة المعلومات الجامعية التوثيق الإلكتروني والميكروفيلم



MONA MAGHRABY



شبكة المعلومات الجامعية
التوثيق الإلكتروني والميكروفيلم

جامعة عين شمس

التوثيق الإلكتروني والميكروفيلم

قسم

نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها
علي هذه الأقراص المدمجة قد أعدت دون أية تغيرات



يجب أن

تحفظ هذه الأقراص المدمجة بعيدا عن الغبار



MONA MAGHRABY



Ain Shams University
Faculty of Engineering
Department of Engineering Physics and Mathematics

MATHEMATICAL TECHNIQUES FOR MULTIPLE LAYER SECURITY SCHEMES

A Thesis Submitted
for the Degree of Master of Science in Engineering
Mathematics

Prepared by:
Eng. Abeer Samir Khalifa Abd-Allah

Under the supervision of
Assoc. Prof. Dr. Ahmed Mohamed Ibrahim El-Rafei
Department of Engineering Physics and Mathematics
Faculty of Engineering, Ain Shams University

Dr. Ramy Farouk Taki Eldin
Department of Engineering Physics and Mathematics
Faculty of Engineering, Ain Shams University

Dr. Wassim Joseph Alexan
Department of Information and Engineering Technology
German University in Cairo

2021



Ain Shams University
Faculty of Engineering
Department of Engineering Physics and Mathematics

MATHEMATICAL TECHNIQUES FOR MULTIPLE LAYER SECURITY SCHEMES

A thesis submitted to the Faculty of Engineering, Ain Shams University in
partial fulfillment of the requirements for the M.Sc. degree in
Engineering Mathematics

Prepared by:

Eng. Abeer Samir Khalifa Abd-Allah

Bachelor in Communication Engineering
Department of Communication
Helwan University

Examination Committee

Title, Name and Affiliation

Signature

Prof. Dr. Hamdy Mohamed Ahmed

Department of Engineering Physics and Mathematics
El-Sherouk Academy

Prof. Dr. Salwa Hussein El-Ramly

Department of Electronics and Electrical Communication Engineering
Faculty of Engineering, Ain Shams University

Assoc. Prof. Dr. Ahmed Mohamed Ibrahim El-Rafei

Department of Engineering Physics and Mathematics
Faculty of Engineering, Ain Shams University

Date: / /

TABLE OF CONTENTS

Abstract.....	IV
Acknowledgment.....	VI
List of Tables.....	VIII
List of Figures.....	IX
List of Symbols.....	XII
List of Abbreviations.....	XIV
Publications Extracted from this Thesis.....	XVI
CHAPTER 1 INTRODUCTION	1
1.1 Overview	1
1.2 Problem Statement.....	1
1.3 Research Motivation.....	3
1.4 Objective.....	4
1.5 Scope and Contribution	4
1.6 Thesis Outline.....	5
CHAPTER 2 STEGANOGRAPHY AND DATA SECURITY	7
2.1 Information Security Main Concepts	7
2.2 Basics of Security Implementation.....	8
2.3 Cryptography Overview	9
2.3.1 Cryptography Main Concept.....	9
2.3.2 Basic Contents of Cryptography System	10
2.3.3 The Main Types of Cryptography	10
2.3.4 Some Examples for Cryptography Techniques.....	11
2.3.5 Cryptography Main Aims.....	13

2.4	Steganography Overview	14
2.4.1	Steganography Definition	14
2.4.2	Basic Contents of Steganography System.....	14
2.4.3	Steganography Main Aims and Requirements.....	15
2.4.4	Classifications of Steganography	17
2.4.4.1	Hiding Method Steganography	17
2.4.4.2	Cover Medium Steganography	18
2.5	3D Image Steganography	24
2.5.2	Some Applications of Steganography	28
2.6	Cryptography and Steganography	29
2.7	Stego-Image Quality Evaluation Metrics	30
2.8	Summary.....	33
CHAPTER 3 LITERATURE REVIEW ON STEGANOGRAPHY		34
3.1	Summary.....	46
CHAPTER 4 MATHEMATICAL BASICS FOR RANDOMNESS		47
4.1	Statistical Properties of Random Number Generation	47
4.2	General Requirements of Random Number Sequences	48
4.3	Categories of Random Number Generator	49
4.3.1	True Random Number Generation	50
4.3.2	Pseudo-Random Number Generation (PRNG)	50
4.3.3	Quasi-Random Number Generation.....	55
4.4	Logistic (Chaos) Equation Based on PRN Generation.....	57
4.4.1	Chaotic System Dynamical Properties	62
CHAPTER 5 MULTI-LEVEL DATA SECURITY SCHEME.....		64
5.1	Introduction	64
5.2	Multi-Level Data Security Implementation Through 3D Image Steganography	64
5.2.1	Blowfish Cryptography	65

5.2.1.1	Blowfish General Features and Advantages	66
5.2.2	3D Image Steganography	66
5.2.3	Modular Equation for Random Sequence Generation	68
5.2.4	Slicing and Shuffling of the 3D Image Contents	70
5.3	Steganography algorithm pseudo code	74
5.4	Performance Evaluation Metrics	75
5.5	Experimental Results and Discussion.....	77
5.5.1	Numerical Structure and Results.....	78
5.5.2	Comparative Study	80
CHAPTER 6 CONCLUSION AND FUTURE WORK		83
6.1	Conclusion	83
6.2	Future Work.....	84
REFERENCES.....		86

ABSTRACT

The massive development in information transmission and communication technology requires several potentials for information security. Many methods have been developed and enhanced for exchanging information protection such as steganography and cryptography. Steganography is the art of hiding secret information within an appropriate visible cover media, such that only the authorized recipient, can know about the hiding of the information. The hidden information can exist on the form of text, image, audio or video. The approaches used in concealing secret data are seeking to select suitable cover media to these secret data in each approach. On the other hand, cryptography can be defined as the process where data or messages are converted into secret code for exchanging over a public channel. The main objective of this thesis is to develop and propose a new hybrid technique for data security through the integration between cryptography and improved steganography algorithms. The proposed system will be used to embed an encrypted secret message into a 3D cover image with minimal change and error in the received stego-image. The embedding is performed using the Least Significant Bit (LSB) approach into 3D grayscale image in its spatial domain. In this hybrid approach the secret message is encrypted first before being hidden, using Blowfish encryption technique that is chosen due to its proven security and efficiency. Steganography is implemented through slicing the 3D cover image into 2D slices. These 2D slices are randomly shuffled according to certain keys. Then the pixels in each slice are randomly shuffled with other keys. After that, the LSB data embedding takes place. Finally, re-shuffling of Shuffled pixels and slices are performed to obtain the stego-image. In this work, after performing the proposed techniques, several steganography performance evaluation metrics are incorporated including the peak signal to noise ratio (PSNR), Mean Square Error (MSE) and structural similarity index (SSIM). A comparison between the original image file (cover image) and the stego-image is carried out through these metrics. Also, the developed scheme is compared to some of its counterparts from the literature and the results show its superior performance and simplicity over the methods in comparison.

This is to ensure less distortion of the original cover file after embedding the secret message. Experimental results presented at the end of the thesis confirm a relative improvement and efficiency in the used approaches.

Keywords: 3D image Steganography, Data Security, Information Hiding, Shuffling, Blowfish algorithm.

ACKNOWLEDGEMENT

At first and before all, I want to express all my praises to ALLAH for all the blessings and bounties He has bestowed on me through this long journey. Without ALLAH, nothing can be achieved.

I would like to convey my utmost gratitude, deep thanks and blessing to my supervisor **Assoc. Prof. Dr. Ahmed Ibrahim**, Department of Engineering Physics and Mathematics, Faculty of Engineering, Ain Shams University and **Dr. Ramy Farouk**, Department of Engineering Physics and Mathematics, Faculty of Engineering, Ain Shams University, for their unwavering support of my research, supervising this project, their constant feedbacks as well as their patience, inspiration and enthusiasm, they really have made this a wonderful learning opportunity. Also, I would like to send my deepest thanks to **Dr. Wassim Alexan**, Department of Information and Engineering Technology, German University in Cairo, for his invaluable guidance, continuous support and motivation throughout the dissertation work. Without their helps and advices, I would not write these words for this thesis.

I am deeply thankful and blessed for the special, unique, amazing man; I have never forgotten in my life, **my faraway Dad** “May ALLAH bestow blessings upon his soul”. He might be dead, but I believe he is heaven, happy with this progress and success more than I am. His good works will be remembered forever. He was the one who gave me the first push to this work and was always providing me with great support and encouragement. Although he is no longer with us in this world, thoughts of him will never leave our memories.

The acknowledgement will surely still incomplete without expressing my deep indebtedness and cordial thanks to my family’s encouragement and love: **my husband, my mother, my brother, and my sister**, so I would like to express my deep gratitude and appreciation to them for their continuous support and encouragement. They have aided and helped me a lot in successfully completing my thesis.

I would also like to thank my friends, colleagues and anyone who has helped me even with thoughts and opinions or contributed in some way to this project.

Last but not least, I'd like to express my advanced grateful thanks to the **Examination Committee** for their important role in the accomplishment of this thesis.

Abeer Samir Khalifa
2021

LIST OF TABLES

Table 4.1: Output results of the PRNG using linear congruential method $x_0 = 7, a = 5, c = 3$ and $m = 16$	51
Table 4.2: Output results of the PRNG using linear congruential method $x_0 = 7, a = 1, c = 3$ and $m = 16$	52
Table 4.3: Output results of the PRNG using linear congruential method with different $x_0, a = 13, c = 0$ and $m = 64$	54
Table 4.4: Van der Corput-sequence generation consecutive outputs.....	57
Table 5.1: Output results of Equation 5.2 at $q = 2$ and $B = 10$	70
Table 5.2: Output results of Equation 5.2 at $q = 3$ and $B = 10$	70
Table 5.3: Proposed Scheme Metrics for Various 3D Images.	80
Table 5.4: Performance Comparison with Other Schemes from the Literature.....	81

LIST OF FIGURES

Figure 1.1: Block diagram of general steganography model.	3
Figure 2.1: The three main requirements for any security system.	8
Figure 2.2: Basic cryptography block diagram. It shows the sequenced stages for data ciphering in cryptography system.	9
Figure 2.3: The basic structure of general steganography model.	16
Figure 2.4: Steganography classification based on data hiding method...18	
Figure 2.5: Steganography classification based on the cover types.	19
Figure 2.6: 2D array of pixels for a digital image. Each pixel has (x, y) coordinates and intensity value.	22
Figure 2.7: Color image with an example for color values in addition to the LSB embedding.	23
Figure 2.8: Slicing of 3D object into a number of 2D slices.	25
Figure 2.9: Spikey Image in its spatial domain and after transformation to frequency the domain.	26
Figure 2.10: The successive operations for 3D object domain transformation and its recovery.	26
Figure 2.11: Point Cloud (shown on the left) and Mesh (shown on the right) representations of the Stanford bunny.....	27
Figure 2.12: The basic levels of a general steganography technique.	28
Figure 2.13: Relation between cryptography and steganography main concepts.....	29
Figure 3.1: Block diagram of the full procedures for message in [36]:.....	36
Figure 3.2: Flowchart of: a) Hiding data in cover image and b)Recovering data from stego-image [37].....	38

Figure 3.3: Block diagram of New Hybrid Security Allocation Algorithm (NHSA) [38].	39
Figure 3.4: The embedding flow chart of algorithm [39].	41
Figure 3.5: Block diagram of the MST: a) data embedding method	42
Figure 3.6: Block diagram of system model to: a) Embed secret data and b) Extract secret data from 3-D image in [43].	43
Figure 3.7: Flowchart of: a) Embedding process and b) Extracting process in [45].	45
Figure 3.8: Block diagram of the proposed algorithm in [46].	45
Figure 4.1: Types of random numbers generation with some examples.	49
Figure 4.2: Different chaotic behaviors of the logistic equation, substituting $r = 1, r = 2, r = 3$ and $r = 4$.	59
Figure 4.3: The chaotic behavior diagram of difference logistic equations, showing the three phases of bifurcation process.	61
Figure 4.4: Plotting of dynamics of the Henon map that results on (x_n, x_{n+1}) plane.	62
Figure 5.1: Cryptographic Blowfish algorithm with working of round structure.	67
Figure 5.2: Blowfish F-function hardware implementation with 4 S-boxes.	68
Figure 5.3: “CT-engine” 3D-grayscale cover image: The original image before the data embedding	71
Figure 5.4: 2D slices of the 3D object. Starting from left to right: slice1, slice 2, slice 3, ..., slice110.	72
Figure 5.5: The sequential outputs of the 3D Image contents’ shuffling and re-shuffling processes.	72
Figure 5.6: Least Significant Bit (LSB) embedding Samples into shuffled pixels of a single 2D slice.	73
