DESIGN OF NEW IMAGE ENCRYPTION SYSTEMS USING CHAOS THEORY AND FRACTALS

By

Sherif Hamdy AbdElHaleem Mohamed

A Thesis Submitted to the
Faculty of Engineering at Cairo University
in Partial Fulfillment of the
Requirements for the Degree of
MASTER OF SCIENCE
in
Engineering Mathematics

FACULTY OF ENGINEERING, CAIRO UNIVERSITY
GIZA, EGYPT
2015

DESIGN OF NEW IMAGE ENCRYPTION SYSTEMS USING CHAOS THEORY AND FRACTALS

By
Sherif Hamdy AbdElHaleem Mohamed

A Thesis Submitted to the
Faculty of Engineering at Cairo University
in Partial Fulfillment of the
Requirements for the Degree of
MASTER OF SCIENCE
in
Engineering Mathematics

Under the Supervision of

Prof. Salwa Kamal Abd-El-Hafiz

Professor of Engineering Mathematics
Engineering Mathematics and Physics Department
Faculty of Engineering, Cairo University

Assoc. Prof. Ahmed Gomaa Ahmed Radwan

Associate Professor of Engineering Mathematics
Engineering Mathematics and Physics Department
Faculty of Engineering, Cairo University

FACULTY OF ENGINEERING, CAIRO UNIVERSITY
GIZA, EGYPT
2015

Engineer’s Name:	Sherif Hamdy AbdElHaleem Mohamed
Date of Birth:	10 / 4 / 1978
Nationality:	Egyptian
E-mail:	SherifHamdynet@hotmail.com
Phone:	+2010-0315-0157
Registration Date:	1 / 10 / 2011
Awarding Date:	/ /
Degree:	Master of Science
Department:	Engineering Mathematics and Physics Department

Supervisors:

Prof. Salwa Kamal Abd-El-Hafiz
Dr. Ahmed Gomaa Ahmed Radwan

Examiners:

Prof. Salwa Kamal Abd-El-Hafiz	(Main Supervisor)
Dr. Ahmed Gomaa Ahmed Radwan	(Supervisor)
Prof. Hany Lamey Abdel-Malek	(Internal Examiner)
Prof. Galal Ahmed M. Elkobrosy	(External Examiner, Alexandria Univ.)

Title of Thesis:

Design of New Image Encryption Systems Using Chaos Theory and Fractals

Key Words:
Cryptography; Cryptanalysis; Image Encryption; Information Security; Fractional-Order; Fractals; Generalized Feistel Networks; Linear Feedback Shift Register; S-Boxes; Keystream Generator; Chess; Horse Movement; Permutation Matrix; Chaotic equations; Chaotic Maps.

Summary:

This thesis introduced seven new encryption designs based on different methodologies such as: chaotic differential equations of integer and fractional-orders, nonlinear generalized chaotic maps, fractals with their fine details, mixing the generalized Fiestel network with the Linear Feedback Shift Register (LFSR) and, also, a new encryption system based on the chess-based horse-move to generate the permutation matrix. Many standard images were discussed and evaluated using the international measures such as NIST. Seven international papers were published (2 journal papers with IF + five international conferences).

Acknowledgments

I would never imagine myself writing these lines without the great support from everyone around me. Starting with my family who has encouraged me to continue this work and to take this step in my life, then my colleagues who have supported me and made me feel that I am just one of them, finally my professors who have enlightened me with their knowledge and experience.

I would like to express my deepest gratitude to Prof. Magdy Abd El-Aty El-Tawil, may GOD bless his soul and grant him paradise. He was the first person I met in the mathematics department. With his experience, he was able to direct me in selecting the correct branch to do my thesis in (based on my knowledge and work experience). He gave me the best chance when he nominated me to Prof. Salwa Abd-El-Hafiz.

Prof. Abd-El-Hafiz is more than an advisor to me; she has given me unlimited support during my work in this thesis and she has been a very kind person. She treated me as a son; I learned from her more than what could be written in words. She simply deserves more than what could be written in this acknowledgement.

Dr. Ahmed Radwan is just like my big brother. He has been very kind, supportive, motivating and encouraging. His long experience added to this thesis a valuable value. Words are not enough to thank him for his great ideas that have enriched this thesis.

Dedication

I dedicate this work to my family. Their support and encouragement have been very inspiring to me. Many thanks are due to my mother who pushed me forward to continue this thesis. Many thanks are also due to my father, who is my role model in life.

I would also like to dedicate this work to my wife who has supported and withstood all the hard times we have had together. I cannot forget my little daughter who has spent a lot of time without me so that I could do my work.

Very special dedication goes to my sisters Eman and Asmaa and my brother Adel. I hope that this work would encourage and inspire them to continue their postgraduate education in the future.

Finally, I would like to dedicate this work to the soul of my brother Mohamed and mother in law Nadia, may GOD bless their souls and grant them paradise.

Table of Contents

ACKNOWLEDGMENTS .... **I**

DEDICATION .... **II**

TABLE OF CONTENTS .... **III**

LIST OF TABLES .... **VI**

LIST OF FIGURES .... **VIII**

NOMENCLATURE .... **XI**

ABSTRACT .... **XII**

CHAPTER 1 : INTRODUCTION **1**

1.1. ORGANIZATION OF THE THESIS 3

CHAPTER 2 : BACKGROUND AND RELATED LITERATURE **4**

2.1. HISTORY OF CRYPTOGRAPHY 4
2.2. OVERVIEW OF CRYPTOGRAPHY 6
2.2.1. Symmetric and asymmetric key cryptography 7
2.2.2. Stream and block ciphers 9
2.2.3. Block ciphers modes of operation 9
2.3. IMAGE ENCRYPTION 12
2.3.1. Digital image 12
2.3.2. Encryption evaluation techniques 18
2.3.2.1. Statistical tests 18
2.3.2.2. Sensitivity tests 24
2.4. ENCRYPTION SYSTEMS 27
2.4.1. System key 27
2.4.2. Encryption blocks 29
2.4.3. Pseudo random number generator (PRNG) 31
2.4.3.1. Discrete maps 34
2.4.3.2. Continuous systems 36
2.5. RELATED LITERATURE 38

CHAPTER 3 : NEW STREAM CIPHERS BASED ON NON-CHAOTIC GENERATORS **42**

3.1. IMAGE ENCRYPTION BASED ON LFSR AND FEISTEL NETWORKS 43
3.1.1. The simplified system 43
3.1.1.1. LFSR 43
3.1.1.2. Simulation Results 44
3.1.2. The proposed encryption system 45
3.1.2.1. Generalized Feistel network 46
3.1.2.2. Substitution box (S-box) 46
3.1.2.3. System key 47
3.1.3. Analysis results 48
3.2. A FRACTAL-BASED IMAGE ENCRYPTION SYSTEM 51

3.2.1. Fractal images 51
3.2.2. A simplified encryption system 54
3.2.3. The proposed encryption system 56
3.2.3.1. System block diagrams 56
3.2.3.2. System key 58
3.2.4. Multi-fractal encryption 60
3.2.4.1. Sensitivity analysis 63
3.2.4.2. Comparison with previous work 66
3.3. A PSEUDO RANDOM KEY GENERATOR 67
3.3.1. The proposed PRKG 67
3.3.1.1. SPN 67
3.3.1.2. Fractal images 68
3.3.1.3. The proposed PRKG based on fractals 69
3.3.2. PRKG results 70
3.3.3. Image encryption using the proposed PRKG 73
CHAPTER 4 : NEW STREAM CIPHERS BASED ON CHAOTIC GENERATORS 76
4.1. IMAGE ENCRYPTION BASED ON GENERALIZED DISCRETE MAPS 77
4.1.1. Generalized logistic, tent and sine maps 78
4.1.1.1. Logistic map 78
4.1.1.2. Tent map 79
4.1.1.3. Sine map 79
4.1.2. System block diagram 80
4.1.3. Encryption results 81
4.1.4. Encryption based on the generalized sine map 85
4.1.4.1. System key 86
4.1.4.2. Encryption results 87
4.1.4.3. Sensitivity analysis 89
4.1.4.4. Additional results and comparisons 90
4.2. IMAGE ENCRYPTION IN THE FRACTIONAL-ORDER DOMAIN 92
4.2.1. Fractional-order chaotic systems 92
4.2.1.1. Chaotic maps 92
4.2.1.2. Fractional-order derivatives 93
4.2.1.3. Fractional-order lorenz map 94
4.2.1.4. Strange attractors 94
4.2.2. The encryption algorithm 94
4.2.3. Analysis results 95
4.2.3.1. System parameters and initial values 95
4.2.3.2. Histogram analysis 96
4.2.3.3. Pixel correlation analysis 96
4.2.3.4. Sensitivity analysis 99
4.2.3.5. Differential attacks 99
CHAPTER 5 : NEW SYSTEMS FOR BLOCK-BASED ENCRYPTION 100
5.1. CHESS-BASED IMAGE ENCRYPTION 101
5.1.1. The proposed chess-based chaotic cipher 101
5.1.1.1. Substitution process 101
5.1.1.2. Chess-based permutation process 103
5.1.1.3. System key 104
5.1.2. Evaluation of the encryption system 105
5.1.2.1. Substitution and permutation processes analysis results 106

5.1.2.2. Proposed block cipher analysis results 106
5.1.2.3. Sensitivity analysis 108
5.2. COMPARISON OF DIFFERENT PERMUTATION TECHNIQUES AND THEIR EFFECT ON IMAGE ENCRYPTION 110
5.2.1. Permutation techniques 110
5.2.1.1. Matrix generation using discrete chaos 111
5.2.1.2. Matrix generation using permutation vectors 111
5.2.1.3. Arnold's cat map 112
5.2.1.4. Matrix generation using continuous chaos 112
5.2.1.5. Matrix generation using chess-based horse move 113
5.2.2. Permutation comparisons 115
5.2.2.1. Permutation matrix analysis 115
5.2.2.2. Algorithm results and analysis 117
5.2.3. Image encryption using the five techniques 121
5.2.3.1. System key design 122
5.2.3.2. Case 1: analysis results when $S = 0$ 123
5.2.3.3. Case 2: analysis results when $S = 1$ 125
DISCUSSION AND CONCLUSIONS 133
REFERENCES 135

List of Tables

Table 2.1: Comparison between symmetric and asymmetric cryptography 8
Table 2.2: Image types vs. bit depth 12
Table 2.3: “Peppers” 256×256 image sizes in different formats 13
Table 2.4: Basic colors decomposition 14
Table 2.5: Statistical properties for standard images 16
Table 2.5: Statistical properties for standard images (Cont.) 17
Table 2.6: Correlation coefficients for “Peppers” 1024 × 1024 19
Table 2.7: Entropy values for “Peppers” and “Lena” (1024 × 1024) 22
Table 2.8: NIST SP-800-22 statistical test [89].. 23
Table 2.9: NIST test results for encrypted “Peppers” and encrypted “Lena” 24
Table 2.10: Example of differential attacks results 25
Table 2.11: Mean square error values... 26
Table 2.12: Maximum period LFSR feedback polynomials 32
Table 2.13: Step by step output of a 5-bit LFSR 33
Table 3.1: Correlation and differential attack measures for the simplified system 44
Table 3.2: NIST results for the simplified system 44
Table 3.3: Truth table for the multiplexing operation... 45
Table 3.4: Analysis results for the proposed system... 49
Table 3.5: Comparison to other related systems.. 49
Table 3.6: NIST results for the proposed system 49
Table 3.7: Wrong decryption results for one bit change in the key............................. 50
Table 3.8: Correlation results 55
Table 3.9: Differential attack results... 55
Table 3.10: Simplified system NIST results when encrypting Peppers image 56
Table 3.11: Shift values used for seven-fractals encryption 61
Table 3.12: Correlation and differential attack results for the Peppers image using two and seven fractals... 61
Table 3.13: NIST results when encrypting Peppers image using two and seven fractals 62
Table 3.14: Wrong decryption for the Peppers image using seven fractals................. 64
Table 3.15: Results for colored images from USC-SIPI image database 65
Table 3.16: Comparison between the proposed system and other reported chaotic based systems 66
Table 3.17: Pixel correlation 69
Table 3.18: Entropy values... 69
Table 3.19: Pixel correlation results for the three cases.. 72
Table 3.20: Entropy values results for the three cases... 72
Table 3.21: NIST results for fractal 2 73
Table 3.22: Analysis measures for encrypted image 74
Table 3.23: Entropy values for encrypted image... 75
Table 3.24: NIST results for encrypted image 75
Table 4.1: Correlation coefficients of the proposed system.. 82
Table 4.2: Differential attack measures of the proposed system................................. 83
Table 4.3: NIST test suite results of the proposed system 83
Table 4.4: MSE and entropy as measures of sensitivity analysis 84
Table 4.5: Comparison with other systems 85

Table 4.6: Analysis results of the proposed system 88
Table 4.7: NIST suite results of the proposed encryption system 88
Table 4.8: MSE and entropy as measures of sensitivity 89
Table 4.10: Comparison with other systems 90
Table 4.9: Results of encrypting different standard images 91
Table 4.11: Correlation coefficients for the source image and the encrypted image when α = 0.8 and c = 4 97
Table 4.12: Results for all correlation coefficients in the used ranges of α and c 98
Table 4.13: Results for the differential attacks analysis 99
Table 5.1: Substitution only results (Peppers image, L = 64) 106
Table 5.2: Permutation only results (Peppers image, L = 64) 106
Table 5.3: Proposed block cipher results (Peppers image, L = 64) 107
Table 5.4: NIST results for the encryption process 108
Table 5.5: Mean Square Error and entropy values 109
Table 5.6: Comparison with other systems 109
Table 5.7: Permutation matrix analysis results 117
Table 5.8: Adjacent pixels correlation results for Lena 256 × 256 118
Table 5.9: Execution time ratios for the five algorithms 120
Table 5.10: Case 1 ($S = 0$) encryption results for images with resolution 1024 × 1024 124
Table 5.11: Case 2 ($S = 1$) encryption results for Lena 1024 × 1024 127
Table 5.12: Case 2 NIST results for encrypted Lena (1024 × 1024) 128
Table 5.13: Case 2 NIST results for encrypted Peppers (1024 × 1024) 129
Table 5.14: Case 2 Mean Square Error and entropy results 131
Table 5.15: Permutation algorithms comparison for matrix size M × N 132

List of Figures

Figure 2.1: Historical encryption devices (a) Scytale and (b) Engima machine 5

Figure 2.2: Block diagram for a typical cryptosystem 6

Figure 2.3: Block diagram for asymmetric algorithm 7

Figure 2.4: Block diagram for symmetric algorithms 8

Figure 2.5: Stream ciphering and block ciphering 9

Figure 2.6: Block cipher modes of operation (a) ECB mode, (b) CBC mode, (c) CFB mode, (d) OFB mode and (e) CTR mode 11

Figure 2.7: Encryption process 11

Figure 2.8: Typical image cryptosystem using symmetric-key 12

Figure 2.9: Typical image pixels representation 13

Figure 2.10: Pixel value representation 14

Figure 2.11: RGB color system 14

Figure 2.12: Statistical tests 18

Figure 2.13: Adjacent pixels in (a) “Peppers” image and (b) Encrypted “Peppers” 20

Figure 2.14: Histogram analysis 21

Figure 2.15: Sensitivity tests 24

Figure 2.16: Typical encryption system 27

Figure 2.17: 8 bit P-box 30

Figure 2.18: One round of an SPN 30

Figure 2.19: One round Fiestel network (a) classical Fiestel and (b) unbalanced fiestel 31

Figure 2.20: LFSR with maximum period connections (a) 5-bit and (b) 8-bit 32

Figure 2.21: Output of a 5-bit LFSR with maximum period $T = 31$ 33

Figure 2.22: Logistic map bifurcation diagram 34

Figure 2.23: Logistic map chaotic behavior when $\lambda = 3.999$ and $x1 = 0.5$ 35

Figure 2.24: Bifurcation diagram for (a) sine map and (b) tent map 35

Figure 2.25: Lorenz attractor when $\sigma = 10, \rho = 28\ and\ \beta = 83$ 36

Figure 2.26: Lorenz attractor 37

Figure 2.27: Rössler attractor 37

Figure 2.28: Encryption system design elements 41

Figure 3.1: Simplified system block diagram 43

Figure 3.2: System block diagram. 45

Figure 3.3: Generalized Feistel network internal structure. 46

Figure 3.4: S-box generation using an 8-bit LFSR initialized with the value 179. 47

Figure 3.5: System key details. 47

Figure 3.6: Key values (a) for M = 1 and (b) M = 4. 48

Figure 3.7: Peppers image and its encryption for (b) M = 1and (c) M = 4. 48

Figure 3.8: (a) Histogram and (b) Adjacent horz. pixels of the blue channel in the original Peppers image (top) and encrypted image for M = 4 (bottom). 50

Figure 3.9: Wrong decryption for the Peppers image. 50

Figure 3.10: Examples of fractal images 51

Figure 3.11: Mandelbulb creation using Eq. (17) for different values of n (a) n = 4, (b) n = 6, (c) n = 8 and (d) n = 10 54

Figure 3.12: Fractal images used in testing the proposed system; numbered 1 to 8 from left to right and from top to bottom 54

Figure 3.13: The simplified block diagram 55

Figure 3.14: Keystream generation using fractals 57
Figure 3.15: System block diagrams (a) encryption system and (b) decryption system. 58
Figure 3.16: Key construction details 59
Figure 3.17: Example of key identification when using two fractals 59
Figure 3.18: Key length for different values of K and S when $M = 10$; black points are safe points where key length ≥ 128 60
Figure 3.19: (a) Peppers image, (b) encrypted Peppers image using two fractals, (c) encrypted Peppers image using seven fractals and (d) encrypted Peppers image using seven fractals after changing one pixel in the plain image 61
Figure 3.20: (a) Lena image, (b) encrypted Lena image using two fractals, (c) encrypted Lena image using seven fractals and (d) encrypted Lena image using seven fractals after changing one pixel in the plain image 61
Figure 3.21: Histogram for red, green and blue components of (a) Peppers image, (b) encrypted Peppers image using seven fractals, (c) Lena image and (d) encrypted Lena image using seven fractals 63
Figure 3.22: Wrong decryption of Peppers image (a) Test I, (b) Test II, (c) Test III and (d) Test V 64
Figure 3.23: SPN internal structure 68
Figure 3.24: Fractal images numbered 1 to 5 from left to right, top to bottom 68
Figure 3.25: Histogram analysis for (a) fractal 1 and (b) fractal 2 69
Figure 3.26: The proposed block diagram of the PRKG based on fractals 70
Figure 3.27: Histogram analysis for the output stream when using fractal 2 in (a) Case A, (b) Case B and (c) Case C 71
Figure 3.28: The processed fractals after the different cases of post-processing 71
Figure 3.29: Block diagram for the encryption system. 73
Figure 3.30: (a) Peppers image and (b) encrypted Peppers image. 74
Figure 3.31: Histogram analysis for (a) Peppers image and (b) encrypted image. 74
Figure 4.1: The conventional logistic, tent and sine maps. 77
Figure 4.2: The generalized logistic map when $\lambda = 3.99$; (a) function fg versus xn and d when $c = 0.9$, (b) chaotic output in the $c - d$ plane, and (c) the MLE values versus the $c - d$ plane. 78
Figure 4.3: The generalized tent map; (a) function ft versus xn and b when $a = 1.3$, (b) chaotic output in the $a - b$ plane when $rt = 1.99$, and (c) the MLE values versus the $rt - b$ plane when $a = 1.3$. 79
Figure 4.4: The generalized sine map; (a) function fs versus xn and β when $\gamma = 1.1$, $rs = 0.9$ and $\alpha = 0.95$, (b) chaotic output and (c) the MLE values in the $\beta - \gamma$ plane when $rs = 0.9$ and $\alpha = 0.95$. 80
Figure 4.5: Encryption block diagram based on generalized maps. 80
Figure 4.6: Encryption key. 81
Figure 4.7: The original Peppers image and its histograms and the second row is the encrypted TSG-image with its histograms. 82
Figure 4.8: Decrypted Lena image with one bit change in the key (a) Case I, (b) Case II, (c) Case III, (d) Case IV and (e) Case V 85
Figure 4.9: Encryption block diagram (left) and decryption block diagram (right). 86
Figure 4.10: Example utilization of the system key in constructing the parameters and initial conditions of the three maps. 87
Figure 4.11: Histogram distributions for the original Lena image (first row) and its encrypted image (second row). 88
Figure 4.12: Decrypted Lena image with one bit change in the key for (a) Case I, (b) Case II and (c) Case IV. 89

Figure 4.13: Strange attractor for the Lorenz system while fixing c at 4; (a) α = 0.75 (b) α = 0.8 (c) α = 0.95 (d) α = 1 94
Figure 4.14: Block diagram of the encryption process using the fractional-order Lorenz map 95
Figure 4.15: (a) Original image (Lena), and encrypted image at c=4 with (b) α = 0.75, (c) α = 0.8, and (d) α = 0.95 95
Figure 4.16: Histogram for red, green and blue components (a) of Lena (b) of the encrypted image shown in Fig. 4.15(c) 96
Figure 4.17: Adjacent pixels values in horz., vert. and diag. directions in source (first row) and encrypted image (second row) for red component. 97
Figure 4.18: Decryption with different values of α, (a) decrypted image with α = 0.799 and c = 4, Δα = -0.001, and (b) decrypted image with α = 0.801 and c = 4, Δα = +0.001 99
Figure 5.1: Block diagram of the chess-based chaotic block cipher 102
Figure 5.2: Block diagram of the decryption system 102
Figure 5.3: Flowchart for generating the permutation matrix 103
Figure 5.4: (a) Valid horse moves and (b) permutation matrix generated using the proposed algorithm 104
Figure 5.5: System key details 105
Figure 5.6: (a) Peppers image (1024 × 1024), (b) encrypted Peppers image, (c) Lena image (1024 × 1024) and (d) encrypted Lena image 107
Figure 5.7: Histograms for Peppers image (first row) and encrypted Peppers image using L = 64 (second row) 107
Figure 5.8: Decrypted Peppers image with one bit change in the key (a) case I, (b) case II, (c) case III and (d) case IV 109
Figure 5.9: The permutation phase: (a) pixel processing indices, (b) an example of a permutation matrix T and (c) new pixel locations after applying equation (56). 111
Figure 5.10: Permutation vectors mapping row and column indices. 112
Figure 5.11: Modified horse move algorithm. 114
Figure 5.12: Valid horse moves with start value = 1 and step value = 1. 114
Figure 5.13: Permutations effect for the five different techniques. 115
Figure 5.14: (a) $\mathrm{ADOPM} - \mathrm{M}/2$ and (b) $\mathrm{ADBTAPav} - \mathrm{M}/2$. 116
Figure 5.15: (a) Lena. Scrambled Lena using: (b) Discrete Chaos, (c) Permutation Vectors, (d) Arnold's Cat Map, (e) Continuous Chaos and (f) Chess-based. 118
Figure 5.16: The execution time ratios (a) for a single block of size M and (b) for a complete “Lena”1024 × 1024 with different block sizes M. 120
Figure 5.17: Block diagrams of (a) encryption system and (b) decryption system. 121
Figure 5.18: Structure of the system key. 122
Figure 5.19: Case 2 encryption and wrong decryption for Lena and Peppers images. 130

Nomenclature

ADBTAP	The Average Distance Between Two Adjacent Pixels
ADOPM	The Average Distance One Pixel Moved
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining Mode
CFB	Cipher Feedback Mode
CTR	Counter Mode
DCT	Discrete Cosine Transformation
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
ECB	Electronic Codebook Mode
GFN	Generalized Feistel Network
IDEA	International Data Encryption Algorithm
IFS	Iterated Function Systems
IV	Initialization Vector
KG	Keystream Generator
LDE	Linear Diophantine Equation
LFSR	Linear Feedback Shift Register
LSB	Least Significant Bit
MAE	Mean Absolute Error
MLE	Maximum Lyapunov Exponent
MSE	Mean Square Error
NIST	The National Institute of Standards and Technology
NPCR	Number Of Pixels Change Rate
ODE	Ordinary Differential Equations
OFB	Output Feedback Mode
P-box	Permutation Box
PP	The Proportion Of Passing Sequences
PRKG	Pseudo Random Keystream Generator
PRNG	Pseudo Random Number Generator
PV	P-value Distribution
RSA	Rivest-Shamir-Adleman
S-box	Substitution Box
SPN	Substitution-Permutation Network
UACI	Unified Average Change Intensity
XOR	Modulo 2 Sum

Abstract

Recently, the huge dependence on electronic communication has lead to an increased demand for data security in order to achieve privacy. The security of data transmission is a vital issue since it is easy to detect the information sent across the internet. Hence, a lot of research is performed in the field of data security in general and, consequently, image encryption arises as an important research field. A typical symmetric-key image encryption system usually consists of two main substitution and permutation phases to accomplish Shannon's confusion and diffusion properties. Therefore, this thesis introduces new encryption systems that utilize chaotic and non-chaotic generators in different designs of the aforementioned two phases.

Several stream-based image encryption systems are proposed and analyzed using chaotic as well as non-chaotic generators. Using non-chaotic generators, three stream-based systems are presented. The first system is designed by combining a Linear Feedback Shift Register (LFSR) with a generalized form of a Feistel-like structure in order to provide a strong keystream. The second system is based on fractal images where a set of fractal images is selected and processed in a form that achieves strong encryption. The third system proposes a different design of a pseudo random keystream generator based on fractal images.

In addition, two stream-based encryption systems are designed using chaotic generators. The first system is based on generalized forms of three discrete maps, which are the logistic map, the sine map and the tent map. By combining the three maps, a strong keystream is generated that helps in achieving the required encryption quality. The second system is based on the fractional-order Lorenz attractor. This system makes use of the extra degrees of freedom, which arise from the new fractional powers, and shows that the fractional order system exhibits a wider range in the new parameters that can achieve a chaotic behavior and helps in increasing the system key length and maintaining sensitivity to only one bit change.

On the other hand, two block-based image encryption systems are proposed and analyzed. The first system includes a novel chess-based permutation stage. The presented encryption algorithm is very sensitive to the input parameters, which helps in maintaining a very sensitive system key. The second system discusses five different algorithms for generating permutation matrices. The generated permutation matrices are, then, used in an encryption system in order to compare and evaluate the proposed permutation algorithms.

To evaluate the proposed encryption systems, the quality of the resulting ciphers is tested using adjacent pixels correlation coefficients, histogram distributions, differential attack measures and the NIST statistical test suite. Furthermore, sensitivity of the system key to one bit change is also examined using the mean square error and entropy values of the wrong decrypted images. Results achieved by the proposed cryptosystems are very promising and show great potential as compared to other systems in recent literature.