A COMPARATIVE STUDY OF IMAGE ENCRYPTION TECHNIQUES

A thesis submitted to the
Institute of Graduate Studies and Research
Alexandria University
In Partial Fulfillment of the Requirements for the Degree

of

Master of Science

In

Information Technology

By

Marwa Mohamed Mohamed Abd El-Wahed

B.Sc. Civil Engineering (2001)

Diploma in IT (2005)

October, 2009

بسم الله الرحمن الرحيم

قالوا سبحانك لا علم لنا إلا ما علمتنا إنك أنت العليم الحكيم

صدق الله العظيم

سورة البقرة – آية رقم (٢٣)

بسم الله الرحمن الرحيم

وعلمك ما لم تكن تعلم وكان فضل الله عليك عظيما

صدق الله العظيم

سورة النساء – آية رقم (١١٣)

A COMPARATIVE STUDY OF IMAGE ENCRYPTION TECHNIQUES

A Thesis

Presented by

Marwa Mohamed Mohamed Abd El-Wahed

For the Degree of

Master of Science

In

Information Technology

Examining Committee Members **Approved**

Prof. Dr. Amin Fahmy Shoukry
Professor
Head, Dept. of Computer and Systems Engineering
Faculty of Engineering, Alexandria University

Prof. Dr. Shawkat Kamal Guirguis
Professor
Head, Dept. of Information Technology
Institute of Graduate Studies and Research
Alexandria University

Prof. Dr. Khaled Mohamed Mahar
Professor
Head of College of Computing and Information Technology - Arab Academy for Science and Technology - Alexandria

Date: 15 / 10 / 2009

Advisor's Committee:

Prof. Dr. Amin Fahmy Shoukry
Professor,
Head, Dept. of Computer and Systems Engineering,
Faculty of Engineering,
Alexandria University

Dr. Saleh Mesbah EL-Kaffas
Assistant Professor,
Dept. of Information Technology,
Institute of Graduate Studies and Research,
Alexandria University

ACKNOWLEDGMENT

Foremost thanks to Allah for his blessings at every stage of my life.

Thanks to Prof. Dr. Amin Shoukry, Professor of Computer and Systems Engineering, Faculty of Engineering, Alexandria University, for his help to carry out the study. His assistance facilitated to accomplish of this work.

I would like also to express my sincere appreciation and gratitude to Dr. Saleh Mesbah, Assistant Professor of Information Technology, Department of Information Technology, Institute of Graduate Studies and Research, Alexandria University, for his continuous guidance, supervision and constructive criticism.

The special thanks are due to my mother (ask Allah the mercy to her), for her deep prays, endless love, patience, and support. I owe her more than I can possibly express.

DECLARATION

This thesis submitted to the Institute of Graduate Studies and Research, Alexandria University, for the degree of Master of Science in Information Technology.

The work included in this thesis was out by the author at Information Technology Department, Alexandria University.

No part of this thesis has been submitted for a degree or qualification at other university or institution.

Name: Marwa Mohamed Mohamed Abd El-Wahed

Signature:

Date: 15/ 10 /2009

ABSTRACT

With the widely use of images in various applications, it is important to protect a confidential image using encryption techniques. Many research works on image encryption techniques have been done in an attempt to enhance the security and efficiency of cryptosystems. To be accepted by both practitioners and cryptanalysts, a cryptosystem must achieve security without neglecting efficiency.

This thesis suggests measuring criteria for the evaluation of image encryption algorithms. Specifically, this work focuses on efficiency evaluation by measuring the encryption quality, the memory requirements, and the execution time of encryption techniques. The security analysis of these techniques is investigated for both statistical and differential attacks. The results of these evaluation criteria show that each algorithm has its own strengths and weaknesses and no single encryption mechanism is able to get the high level of security with high efficiency performance.

TABLE OF CONTENTS

Page

Acknowledgment ---- i
Declaration ---- ii
Abstract ---- iii
Table of Contents ---- iv
List of Figures ---- vi
List of Tables ---- vii
List of Abbreviations ---- viii

1. CHAPTER 1: INTRODUCTION

1.1 Overview ---- 1
1.2 Research Problem ---- 1
1.3 Research Objective ---- 1
1.4 Research Methodology ---- 2
1.5 Thesis Organization ---- 2

2. CHAPTER 2: LITERATURE REVIEW

2.1 Introduction ---- 3
2.2 Concept of Cryptography ---- 4
2.2.1 Cryptographic Systems ---- 5
2.2.2 Characteristics of Cryptosystem ---- 9
2.2.3 Encryption Key ---- 10
2.2.4 Cryptanalysis ---- 11
2.2.5 Confusion and Diffusion ---- 13
2.2.6 Applications of Cryptography ---- 14

3. CHAPTER 3: DATA ENCRYPTION

3.1 Textual Data Encryption ---- 15
3.1.1 Classical Cipher ---- 15
3.1.2 Modern Cipher ---- 18
3.2 Image Encryption ---- 21
3.2.1 The Digital Images ---- 21
3.2.2 Classification of Image Encryption ---- 23
3.2.3 Survey of Image Encryption Cryptosystem ---- 24

4. CHAPTER 4: IMPLEMENTATION OF SELECTED IMAGE ENCRYPTION ALGORITHMS AND EVALUATION CRITERIA

4.1 Data Collection and Execution Environment ---- 27
4.1.1 Image Files Used ---- 27
4.1.2 Platform ---- 29
4.2 Selected Image Encryption Algorithms ---- 29
4.2.1 Transposition Techniques (Position Permutation) ---- 29
4.2.2 Substitution Techniques (Value Transformation) ---- 32
4.2.3 Transposition-Substitution Techniques ---- 33
4.3 Evaluation Criteria ---- 39
4.3.1 Efficiency Evaluation ---- 39

4.3.2 Security Analysis ---------- 41

5. CHAPTER 5: RESULTS AND DISCUSSION

5.1 Results ---------- 43
5.2 Discussion ---------- 46

6. CHAPTER 6: CONCLUSION AND FUTURE WORK

6.1 Conclusion ---------- 50
6.2 Recommendations ---------- 50
6.3 Future Work ---------- 51

References ---------- 52
Arabic Summary

LIST OF FIGURES

Figure		Page
2.1	The Different Between Major Ways of Securing Communications	4
2.2	A Cryptosystem	5
2.3	Classification of Cryptosystems	7
2.4	A Block Cipher	8
2.5	A Stream Cipher	8
3.1	Blowfish Algorithm	20
3.2	Graphic Representation of F	20
3.3	Rijndael Round	21
3.4	The Structure of a Digital Image	23
3.5	The Image is Encrypted by AES Directly	24
4.1	The Test Images	28
4.2	Gray-level Histogram of the Test Images	28
4.3	Encryption Using a Permutation Technique Followed by Encryption	30
4.4	Diagram of Combinational Permutation Schemes	31
4.5	Results of Block, Bit, and Pixel Permutations	32
4.6	Image Encryption Using Block-Based Transformation Algorithm	32
4.7	Image Encryption Using Matrix Transformation	33
4.8	Image Encryption Based on Strange Attractor	34
4.9	Examples of Clifford Attractors	35
4.10	Encryption Using Enhanced 1-D Chaotic Key-Based Algorithm	36
4.11	Basic SCAN Patterns	37
4.12	Encryption Using SCAN Patterns	38
5.1	Encryption Quality	47
5.2	Memory Requirements	47
5.3	Execution Time	48
5.4	Correlation Coefficient	48
5.5	Differential attack	49

LIST OF TABLES

Table		Page
2.1	Example of Keystream	11
3.1	Caesar Cipher Mapped	16
3.2	Example of Caesar Cipher	16
3.3	Example of poly-alphabetic substitution ciphers	18
5.1	Encryption Quality	43
5.2	Memory Requirements	44
5.3	Execution Time of Image Encryption Algorithms	44
5.4	Correlation Coefficient Factor	45
5.5	Number of Pixels Change Rate	45
5.6	Unified Average Changing Intensity	46

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
C.C	Correlation Coefficient
CKBA	Chaotic Key Based Algorithm
DES	Data Encryption Standard
ECKBA	Enhance the Chaotic Key Based Algorithm
FIPS	Federal Information Processing Standard
NIST	National Institute for Standards and Technologies
NPCR	Number of Pixels Change Rate
PRNG	Pseudo Random Number Generator
PWLCM	Piecewise Linear Chaotic Map
RCES	Random Control Encryption Subsystem
RDTSC	Read Time-Stamp Counter
RSES	Random Seed Encryption Subsystem
UACI	Unified Average Changing Intensity

CHAPTER 1
INTRODUCTION

CHAPTER 1: INTRODUCTION

1.1 Overview

With the growth of the communication technology industry, the current need for data security is ever growing. Cryptography is one of the ways to enhance security. The basic principle of cryptography is that a plaintext is converted into a ciphertext through encryption. Because of widely using images in various applications, it is important to protect a confidential image from unauthorized access using encryption techniques.

Image encryption technique uses special image data structure, which leads to get efficient encryption with minimum time encryption requirement. Traditional encryption techniques such as Data Encryption Standard (DES) treat the image data as the traditional text data. Because, images are different from texts in some intrinsic properties such as large amount of data and strong correlation among pixels, using traditional encryption techniques are not suitable to encrypt images for two reasons. The first one is that the traditional encryption technique needs much time to encrypt the image data. The second reason is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable [1].

1.2 Research Problem

The protection against different types of attacks is considered the basic challenge of this era. New cryptosystem which is easy to carry out, works efficiently, and provides a high level of security, is the key to this problem.

Many research works on image encryption techniques have been done in an attempt to enhance the security and efficiency of cryptosystems. Considering that it is significant to achieve secure cryptosystem without neglecting efficiency, to be accepted by both practitioners and cryptanalysts.

1.3 Research Objective

The objective of this thesis suggests measuring criteria for the evaluation of image encryption algorithms. Specifically, this work focuses on evaluating efficiency by measuring the encryption quality, the memory requirements, and the execution time of the encryption. The security analysis has been performed on the image encryption schemes (statistical and differential attacks), demonstrates how much scheme provides a satisfactory security.