

**Multiple Pseudo Random Number Generators
Implementation for Watermarking Technique**

تطبيق مولدات الارقام العشوائية المتعددة لتكنولوجيا العلامة المائية

**Prepared By
Aysar Shamil Alsaadi**

**Supervisor By
Prof. HamzaAbbass Al-Sewadi**

Thesis Submitted In Partial Fulfillment of the Requirements

for the Degree of Master of Computer Science

Department of Computer Science

Faculty of Information Technology

Middle East University

May, 2017

Authorization statement

I, Aysar Shamil Alsaadi, authorize the Middle East University to provide hard copies or soft copies of my Thesis to libraries, institutions or individuals upon their request.

Name: Aysar Shamil Alsaadi

Date: 30/5/2017

Signature:



إقرار تفويض

انايسر شامل السعدي . افوض جامعة الشرق الاوسط بتزويد نسخ من رسالتي ورقياً و الكترونياً
للمكتبات، او المنظمات، او الهيئات و المؤسسات المعنية بالابحاث و الدراسات العلمية عند طلبها.

الاسم : ايسر شامل السعدي

التاريخ : 2017/5/30

التوقيع : 

Examination Committee Decision

This is to certify that the thesis entitled “Multiple Pseudo Random Number Generators Implementation for Watermark Technique” was successfully defended and approved on 30-5-2017.

Examination Committee Members

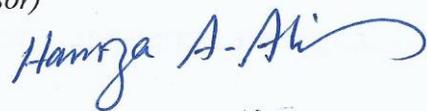
Signature

(Chairman of Examination Committee and Supervisor)

Prof. Hamza Abbass Al-Sewadi

Professor

Middle East University

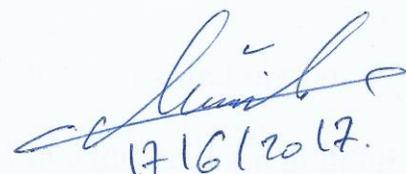


(Internal Committee Member)

Dr. Sharefa F. Murad

Assistant Professor

Middle East University



17/6/2017.

(External Committee Member)

Prof. Arafat Atwi Awajan

Professor

Princess Sumaya University for Technology



Acknowledgments

First, thanks to **ALLAH HIS ALMIGHTY** for enabling me to complete this work in spite of all the difficulties. I would like to sincerely thank Prof. Dr. Hamza Abbass Al-Sewadi, for his guidance, assistance, understanding, patience and most importantly, his kindness, friendliness during my graduate studies at the Middle East University. His mentorship was paramount in providing a well-round experience consistent with my long-term career goals. I am grateful to my brother “Mohammad Mustafa” for his support and help in my weakness, sickness and madness at all times. I want to thank Prof. Dr. Ali Makki Sagheer and Dr. Abdulkareem Al-Ibadi, for valuable advice and suggestions. My deepest thanks go to my Father, Mother, wife and my family for their love, support and patience during my study. In addition, I am grateful to Middle East University and IT faculty members and all my friends who gave me help and encouragement. Thanks for all.

The Researcher

Dedication

To My

Father, Mother, brother, wife, sisters and close friends for their full support, for their great patience, endless love, attention and pray for me.

I dedicate my effort

Table of Content

Cover Page	I
Authorization statement.....	II
اقرار تفويض.....	III
Examination Committee Decision.....	IV
Acknowledgments.....	V
Dedication.....	VI
Table of Content.....	VII
List of Tables.....	XI
List of figures.....	XII
List of Abbreviations.....	XIII
Abstract.....	XIV
الملخص.....	XV
Chapter 1: Introduction.....	1
1.1 Overview.....	2
1.2 Watermark Types.....	3
1.3 Random Number Generator.....	4
1.4 Watermark hiding and Steganography.....	5
1.4.1 Steganography Vs Watermarking.....	6
1.5 Problem Statement.....	7
1.6 Questions of the study.....	8
1.7 Objectives of the study.....	9
1.8 Motivation	9
1.9 Contribution and Significance of the research.....	10
1.10 Scope of the study.....	11
1.11 Thesis Organization.....	11

Chapter Two: Theoretical Background and Literature Review.....	12
2.1 Introduction.....	13
2.2 Watermark Purposes.....	13
2.3 Watermarking Chronology.....	14
2.4 Watermarking Classification.....	15
2.5 Watermarking Applications.....	16
2.6 Watermarking Requirements.....	20
2.6.1 Security.....	20
2.6.2 Invisibility	21
2.6.2.1 Perceptual Invisibility	21
2.6.2.2 Statistical Invisibility.....	21
2.6.3 Robustness.....	21
2.7 Watermarking Techniques.....	22
2.7.1 Spatial Domain Technique.....	23
2.7.1.1 Least Significant Bit (LSB).....	24
2.7.1.2 Limitation of Spatial Domain.....	24
2.7.2 Transform Domain Technique.....	24
2.7.2.1 Discrete Cosine Transform (DCT).....	25
2.7.2.2 Discrete Wavelet Transform (DWT).....	25
2.7.2.2.1 Merits of DWT over DCT.....	27
2.7.2.3 Discrete Fourier Transform (DFT).....	27
2.7.2.3.1 DFT Characteristics	27
2.7.3 DFT Advantage over DWT and DCT.....	28
2.7.4 Spread Spectrum Technique.....	28
2.8 General Digital Watermark Frameworks.....	29
2.9 Statistical Random and Pseudorandom Number Generators Tests.....	30
2.10 Related Work.....	31

2.1 Related Work Summary.....	35
Chapter Three: The Research Methodology.....	37
3.1 Introduction.....	38
3.2 Proposed Watermark Scheme.....	39
3.3 Modified Lorenz Attractor (LA) PRNG.....	44
3.3.1 Initial Secret Key for Modified Lorenz PRNG.....	47
3.4 The modified Trivium PRNG	47
3.4.1 PRNG Structure.....	48
3.4.2 Initialize generation Phase	49
3.4.3 Warm-Up Stage	49
3.4.4 Generation of modified Trivium PRNG.....	49
3.5 Secret Key Strength.....	52
Chapter Four: Implementation and Results.....	53
4.1 Introduction.....	54
4.2 Evaluation Metrics.....	55
4.3 Embedding Algorithm Tests.....	56
4.4 Short Definition of the metrics.....	59
4.4.1 PSNR Test.....	59
4.4.2 NPCR Test.....	60
4.4.3 MSE Test.....	61
4.4.4 Correlation Test.....	62
4.5 Grayscale.....	63
4.6 Summary of watermarking method results of robustness.....	64
4.7 Performed Attacks	66
4.7.1 Gaussian Noise.....	67
4.7.2 Localvar Noise.....	70

4.7.3 Salt and pepper Test.....	71
4.7.4 Speckle Noise Test.....	72
4.7.5 Poisson Noise Test	73
4.7.6 Cropping	74
4.7.7 Resizing.....	76
4.7.8 Rotating	76
4.8 PRNG Tests.....	77
4.8.1 Used PRNG test Results	78
5 Chapter Five: Conclusions and Future Work.....	85
5.1Conclusions.....	86
5.2Future Work.....	87
References.....	88
Appendices.....	94
Appendix A.....	94
Appendix B.....	96
Appendix C.....	98

List of Tables

Table 1.1	Steganography Vs Watermark	6
Table 2.1	Watermark Classification	15
Table 2.2	Related work Summary	35
Table 3.1	Trivium PRNG Parameters	49
Table 3.2	PRNG Workflow	51
Table 4.1	Used Images	56
Table 4.2	Embedding Tests	57
Table 4.3	HD (High Definition) Images	58
Table 4.4	Normal Quality Images	59
Table 4.5	Comparission with similar techniques	65
Table 4.6	Addition of Gaussian Noise	68
Table 4.7	Addition of Localvar Noise	70
Table 4.8	Addition of Salt and Pepper Noise	71
Table 4.9	Speckle Noise	72
Table 4.10	Poisson Noise Test	73
Table 4.11	Cropping	74
Table 4.12	Resizing	75
Table 4.13	Rotating	76
Table 4.14	Sample of the Frequency Test for the PRNG	79
Table 4.15	Sample of the Serial Test for the PRNG	80
Table 4.16	Sample of the Correlation Test for the PRNG	81
Table 4.17	Sample of the Run Test for the PRNG	83
Table 4.18	Sample of the Poker Test for the PRNG	84

List of Figures

Figure 2.1	Watermark Requirements	22
Figure 2.2	One level DWT	26
Figure 2.3	Two levels DWT	26
Figure 2.4	General Embedding Process	29
Figure 2.5	General Extracting Process	30
Figure 3.1	Embedding Process	42
Figure 3.2	Extracting Process	43
Figure 3.3	Proposed chaotic Image Encryption	46
Figure 3.4	Structure of modified Trivium PRNG	49
Figure 3.5	Trivium PRNG Implementation	52
Figure 4.1	Example of watermark steps	56
Figure 4.2	PSNR Istanbul City	60
Figure 4.3	NPCR Paris City	61
Figure 4.4	MSE Paris City	61
Figure 4.5	HCR Roma City	62
Figure 4.6	VCR Roma City	63
Figure 4.7	DCR Roma City	63
Figure 4.8	Grayscale PSNR	64
Figure 4.9	Grayscale MSE	64

List of Abbreviations

DW	Digital Watermark
LSB	Least Significant Bit
DCT	Discrete Cosine Transform
DFT	Discrete Fourier transform
DWT	Discrete Wavelet Transform
RNG	Random Number Generator
PRNG	Pseudo Random Number Generator
TRNG	True Random Number Generator
CSPRNG	Cryptographically Secure Pseudo Random Number Generator
IHW	Information Hiding Workshop
SPIE	Society of Photo-optical Instrumentation Engineers
NIST	National Institute of Standard and Technology
AC	Alternate Contents
HD	High definition
PSNR	Peak Signal to Noise Ratio
NPCR	Number of Pixels Change Ratio
MSE	Mean Square Error
H-CR	Horizontal Correlation
V-CR	Vertical Correlation
D-CR	Diagonal Correlation
UACI	Unified Average Change Intensity
CI	Chaotic Iteration
CIPRNG	Chaotic Iteration Pseudo Random Number Generator
TDES	Triple Data Encryption Standard
QIM	Quantization Index Modulation
ASCII	American Standard Code for Information Interchange
K	Number of Segmented Blocks
N	Pixels Length
IV	Initial Vector

Multiple Pseudo Random Number generators Implementation for Watermarking Technique

Prepared by

Aysar Shamil Alsaadi

Supervisor

Prof. Hamza Abbass Al-Sewadi

Abstract

Digital Watermarking is a technique for embedding personal or confidential information within an image, video or text. This paper proposes an embedding method that implements multiple pseudo random number generators (PRNGs). The cover image file will be segmented into number of blocks, each contains a specific pixel length. The first PRNG is used to generate secret key by chaotic map for encrypting the logo image before the embedding process. The second PRNG generates random number be used for randomly selecting the pixels from each block to be modified with watermark bits by LSB embedding method. Two seed keys were implemented, one for each PRNG, and they will represent the personal or the private keys for the watermarking process. The randomness of these keys has a strong impact on the system's security strength for being difficult to be predicted, guessed, reproduced, or discovered by a cryptanalyst. Experimental results of applying the proposed technique on embedding and extraction of logos of various types and sizes into vast number of images were satisfactory, as they resulted into fairly acceptable level of peak signal to noise ratio and low error values. Hence, this technique would be suitable for applications that involve cryptography, steganography, and copyright protection.

Keywords: PRNG, Copyright, Cryptography, Steganography, Digital watermarking.

تطبيق مولدات الأرقام العشوائية المتعددة تكنولوجيا العلامة المائية

إعداد

أيسر شامل السعدي

إشراف

الأستاذ الدكتور حمزة عباس السوادي

الملخص

العلامة المائية وهي تقنية تستخدم لتضمين المعلومات الشخصية او السرية داخل الصورة او الفيديو او داخل نص كتابي. طريقة الخوارزمية المقترحة هي تقسيم الصورة الاصلية التي سيتم اخفاء المعلومات داخلها الى عدة اجزاء متساوية بحيث ان كل جزء من الصورة يحتوي على طول معين من نقاط الصورة (pixel). تشتمل الخوارزمية المقترحة على مولدين للأرقام العشوائية حيث يستخدم المولد الاول للأرقام العشوائية في توليد مفاتيح سرية بواسطة خارطة عشوائية وذلك لكي تستخدم لتشفير المعلومات او العلامات قبل عملية اخفاءها داخل الصورة. بينما يستخدم المولد الثاني للأرقام العشوائية لتوليد سلسلة من الأرقام العشوائية تستخدم لتحديد موقع البايت داخل كل جزء من الصورة الاصلية ليتم التعديل على البتات فيها. اما المعلومات فيتم اخفاءها بواسطة تقنية البت الاقل اهمية (LSB). المفتاح العشوائي له تاثير قوي جدا على قوة امنية بيانات الأنظمة، ومن الصعب جداً على اي محلل شفرات اكتشافه او التنبؤ به. وبينت النتائج التجريبية لهذه الخوارزمية في هذا البحث ومنها نسبة الاشارة الى الضوضاء PSNR ومعدل مربع الخطأ MSE بانها تقنية مناسبة للتطبيقات الامنية (علم التشفير، علم

الاخفاء وكذلك حماية حقوق النشر) ومن خلال اخفاء معلومات مهمة او تواقع تخص المالك الفعلي

للسائط المتعددة

الكلمات المفتاحية: مولد الارقام العشوائية، حقوق النشر، علم التشفير، علم الاخفاء، العلامة المائية.

Chapter 1

Introduction

Chapter

Introduction

1.1 Overview

Data and information are very crucial to any organization or person. No one like his conversation or personal data being overheard or misused. Today's generation lives through the development of digital media which include photos that are captured by phones camera, text, audio, video, etc, and the internet is the fastest medium for transferring the data between the parties anywhere in the world. The most important point in this case is how to protect the data contents while transferred through the internet from any intruder attack to prevent unauthorized leakage or tampering with multimedia data. The answer to this question is that we have to use efficient techniques that can protect data. One of these techniques is the digital watermarking which provides a content authentication and copyright protection for digital contents over the internet.. A spatial domain algorithm and (LSB technique) would be employed with an encrypting pre-process in order to implement the watermark algorithm. In short, this study is planned to involve the design, test and implementation of PRNGs for encrypting and locating the embedding places the secret data, or watermark. The work will be concerned with invisible watermarks that will be useful for ownership and copyright protection, secure (embed) information.

[ref] Encryption is an obvious secure technique to converse data into a mingle code that can be distributed and decrypted through a private or public network. Generally speaking, in both research and application fields, encryption and cryptographic algorithms can serve watermarking technique which aims to copyright owners as an approach to protect the secure transmission of confidential multimedia data over public channels. Using

various encryption algorithms can be applied to prevent illegal access to digital private contents. When Applying the encryption technique within digital watermarking the content authentication of the secret data is increased (because the hacker task will be complex enough) to prevent any stealing or duplicating of the watermarked data. Multimedia content has been encrypted into its another style and the protection of information is validated for further manipulations, if there is any degradation of quality in subsequent works and no verification become from unauthorized replicating copy then transmission of multimedia data cannot be obstructed [Liang, H. Y., Cheng, C. H., Yang, C. Y., & Zhang, K. F. (2013)].

1.2 Watermark Types

Digital watermarking (DW) is a new technology for embedding (hiding) some multimedia such as audio, video, image and text inside any other multimedia. The importance of hiding the data comes from the concept of reliability over the medium through which the data is sent by insecure medium. In order for digital watermarking method to be effective, it should have two fundamental characteristics: perceptual transparencies which mean users cannot distinguish original from watermarked version and robust against attacks that may remove watermark or replace it with another one (Al-Qudsy, Z. N. 2011). The spatial domain is generally simple and faster than the frequency domain. Also it is a straight forward method and has the least complexity. The least significant bit (LSB) is the most widely used method for spatial domain technique. This method performs the information substitution in the LSB, since it provides the least effect on the carrier image. The frequency domain on the other hand is more robust but at the same time, more complex. The method requires transformation of the cover image into frequency domain.

Three types of transforms have been in use for transform domain, namely Discrete Cosine Transform (DCT), Discrete Fourier Transforms (DFT) and Discrete Wavelet Transforms (DWT) (Abbasfard, M , 2009).

1.3 Random Number Generator

Random number generators are useful for different purposes, such as generating data encryption keys, simulating and modeling complex phenomena and for selecting random samples from large data sets. With the advent of computers, programmers realized the need for introducing randomness into a computer application. However, surprisingly as it may seem, it is hard to get a computer to do something by chance. A computer follows the instructions blindly and is therefore completely predictable. There are three types of random number generators (RNG), (Paar, I. C., &Pelzl, I. J.2010). First one is True Random Number Generators (TRNG) which is characterized by the fact that their output cannot be reproduced. For instance, what happens when flipping a coin 100 times and recording the resulting sequence of 100 bits. The Second is Pseudo random number generators (PRNGs) which generate sequences that are computed from an initial seed value. Often they are computed recursively. Third, Cryptographically Secure Pseudorandom Number Generators (CSPRNG). These are special type of PRNG which generate unpredictable output. Informally, this means that given output bits of the key stream $s_i, s_i + 1, \dots, s_i + n - 1$, where n is some integer, it is computationally infeasible to compute the subsequent bits $s_i + n, s_i + n + 1, etc \dots$. A more exact definition is that which gives n consecutive bits of the key stream (Paar, I. C., &Pelzl, I. J.2010).

1.4 Watermarking, Information hiding and Steganography

Watermarking is related to the fields of information hiding and Steganography (Cox, I. et al, 2007). These three fields have a great deal of overlap and share many technical approaches of data hiding. However, there are fundamental differences that affect the requirements, and thus the design. Some examples of research in this field can be found in the International Workshops on Information Hiding, which have included papers on such topics as maintaining anonymity while using a network and keeping part of a database secret from unauthorized users.

Steganography is a term derived from the Greek word *stegano*, i.e. “covered,” and *graphia*, which means “writing”. It is the art of hidden communication. Hence, Steganographic system thus embeds secret content in unremarkable cover media so as not to arouse an eavesdropper’s suspicion. Tattoos or invisible ink to convey steganograph network technologies provide easy steganography. Essentially, the information system starts by identifying a cover medium’s redundant bits (those that can modify without destroying that medium’s integrity) (Provos, N., & Honeyman, P. 2003). Watermarking technology was developed along with protection of copyright. It is widely used for images copyright protection, audios and videos (Cox, I., Miller, M. L., & Bloom, J. A. 2001). These topics definitely fall outside our definition of watermarking.

1.4.1 Steganography Vs Watermarking

Table 1-1 Steganography Vs Watermarking

Criteria	Steganography	Watermarking
Goal	To hide a message in some (cover) data in order to obtain new data. To hide a message in one-to-one communications . (Amirtharajan,R.et.al,2010) (Techniques, S. ,2002)	To hide a secret data in some (cover) data to obtain hidden data. (Sharma, M. K. et.al, 2012).
Carrier	Mostly paper, image & audio. (Boyle, R., & Parvin, B. 2008).	Can be – text file, Image, audio, video etc. (Potdar, V., & Chang, E. 2004)
Different Methods	(Johnson, N. F.et.al, 2001). -Substitution techniques. -Transform domain techniques. -Spread spectrum techniques. -Statistical techniques. -Distortion techniques. -Cover generation techniques.	Private (non-blind) watermarking. Type I systems use the original cover data to extract the watermark. Type II systems require a copy of the embedded Watermark for extraction. Semi-private (semi-blind) Watermarking does not use the original cover-data for detection. Public (blind) watermarking - either cover data or embedded watermarks are required for extraction.
Objective	Secret communication. (Frączek, W, et.al. 2012)	Copyright, authentication and ownership. (Radharani, S.et.al ,2010)
Attack method	-Steganalysis (Johnson, N. F.et.al, 2001). Stego-only attack Only the stego object is available for stego analysis. Known message attack The hidden message may become known to the stegoanalyzer.	- Data processing (Cox,I. J.et.al, C. 2002) Unauthorized Embedding:(Attack against fragile watermark) – Forges a valid watermarked Work for new host data – Copy blocks of valid Work without understanding the content.. Unauthorized Removal

	<p>Chosen stego attack The stego analysis generates a stego-object from some steganography tool or algorithm from a chosen message. The goal in this attack is to determine corresponding patterns in the stego object that may point to the use of specific steganography tools or algorithms.</p> <p>Known stego attack The Steganography algorithm is known and the original and stego objects are available.</p>	<p>System Attack – Exploit the weakness of how the watermark is used.</p> <p>Preventing Unauthorized Detection – Decoding content: encrypt watermark before embedding. – Detecting watermark existence: currently hard to counterattack</p> <p>Pathological Distortions Copy Attack. Ambiguity Attack. Sensitivity Analysis Attack and Gradient Descendent Attack. Collusion Attack.</p>
Visibility	Invisible (Johnson, N. F.et.al, 2001).	visible and invisible(Cox,I. J.et.al, C. 2002)

1.5 Problem Statement

The problem of copyright protection and ownership judgment for digital images and videos is becoming of great concern nowadays. This is escalated due to the wide spread transfer of digital multimedia over the internet for various applications in various fields such as business, medical, industrial, commercial, education and personal use etc, (Sun Y. et.al, 2015). All data transfer through the internet are exposed to many kind of attacks or malicious acts that can duplicate, destroyed, claim ownership, steal the copyright, change or modify the original data. To solve this issue, lots of research works have resulted into several techniques and tools that can be used to overcome this problem. These techniques are termed digital watermarking as they involve the embedding of watermarks in the form of signatures or logos into the media to be protected. The embedded data can be either

visible or invisible depending on the application. Watermarking aims to protect the multimedia with little or no effect on its content. This research work focuses on invisible watermarking for still images. Several digital image watermarking techniques were developed with various levels of success in preserving its aim that include imperceptibility, content authentication, and security. Spatial techniques are fast and simple but give high imperceptibility, while transformation techniques are complicated but give better robustness. Therefore, there still be a great deal of interest in developing watermarking systems that have better performance. This research work is an effort to enhance the watermarking process by using multiple pseudo random number generators (PRNGs). The first PRNG is used to provide watermark content authentication and the other for randomly embedding this watermark into the digital image.

1.6 Questions of the study

- 1- Is it possible to design a watermarking scheme that enhances perceptibility and content authentication with low image quality degradation?
- 2- What would be the effectiveness of the common attacks on the watermark?
- 3- How would the use of PRNGs and secret seed keys length affect system technique?
- 4- Would the use of multiple PRNGs produce a reasonable improvement in the watermark perceptibility and content authentication?
- 5- How the use of multiple PRNGs would add value to the watermarking or steganography systems?

1.7 Objectives of the study methodology

- 2 Develop a new algorithm for digital data hiding implementing multiple PRNGs that will be used for digital images watermarking aiming to provide high content authentication.
- 3 Design and test two Pseudo random number generator PRNG algorithms to be implemented in the watermarking algorithm; one for encryption/decryption of the watermark data and the other for embedding/extraction into/out of the image.
- 4 The proposed technique improvements seek a high level of imperceptibility and low image quality degradation.
- 5 These sought improvements will be measured using the common data hiding and watermarking tests such as PSNR, MSE, NPCR and Correlation. Then they will compare with related previous works.
- 6 The performance of the system will be tested under the common types of image attacks such as cropping, rotation, cropping, and resizing, in addition to effect of various noise such Gaussian, poison, salt and pepper, etc.

1.8 Motivation

The main significance of the proposed system is to increase the imperceptibility and robustness of watermarking technique by using the spatial domain which is less complex than other techniques. The PRNG tool plays the most important part in this study in order to prevent illegal manipulation and distribution of the digital image. In addition to the secret keys strength which is concerned as back bone to the system technique. Although there are many ways to protect the images, the proposed system introduces an improved

approach to protect the image for the purposes of copyright, ownership and intellectual property.

1.9 Contribution and Significance of the research

- 1- The modification, design and testing of two types of PRNGs; Lorenz PRNG and Trivium PRNG. They are tested for randomness using the statistical test suite for random and pseudorandom number generators for cryptographic applications sets by the national institute for standard technology (NIST). As each of them requires different seed key, the security of the system is inherently increased.
- 2- Implementing the two PRNGs for encrypting and embedding of watermarks into images for copyright and ownership protection property system may provide a meaningful benefit in various protection applications. Digital watermark can create hidden label and annotation in medical application since watermark might be used for identifying patient records.
- 3- Using multiple PRNGs for encrypting and embedding the logo image into the carrier image and extract process.
- 4- The system is capable to be applied in many commercial, medical, personal, etc systems that giving the image a sense of ownership or authenticity.

1.10 Scope of the study

The watermarking technique is needed almost in every field, as it is the modern way to digitally protect copyright and ownership proof. The scope of the research will cover the embedding of signatures and logos in images, and will be limited to the involvement of random number generator in spatial mode watermarking. More concern will be given to the type of pseudo random number generators (PRNGs) that are to be implemented in the embedding and the extraction algorithms. Investigations are also planned for multiple PRNG's which might put more limitations. Moreover, the effect of various environment effecting factors on the developed mode will be studied. Some limitations are expected when different image formats are involved, but this will be examined and reported.

1.11 Thesis Organization

The thesis contains four chapters In addition to the first one. It's organized as follows: **Chapter 1** given definition of steganography and watermarking techniques and some comparison between them then stated the problem statement, project objectives, motivation and goals.

Chapter 2 Provides the Theoretical Literature and Previous Studies of watermarking techniques along with listing and explaining different related works that is most related to proposed system.

Chapter 3 Describes in detail the system methodology architecture and the different models and algorithms for the PRNGs that are used in all parts of the system.

Chapter 4. The Experimental results of the designed system are presented and discussed in detail.

Chapter 5 Includes conclusions and future work including recommendation.

Chapter Two
Theoretical Background
And Literature Review

Chapter Two

Theoretical Background And Literature Review

2.1 Introduction

A digital Watermark is the act of hiding data into the host multimedia in such a way that it is imperceptible to a human observer and inseparable from the data and it is resistant to many operations not degrading the host media (Khanzode,P et.al 2011), that can be detected or extracted later by means of computing efforts in order to make assertions about the data. This chapter presents a literature review and related work for watermarking techniques.

2.2 Watermarking Purposes

The importance of watermarking comes from the reliability concept over the medium. Basically the purpose of watermarking is:

- 1- Data Privacy.
- 2- Sensitive data.
- 3- Avoiding misuse of data.
- 4- Hiding crime traces.
- 5- Blackmail purposes.
- 6- Copyright.

2.3 Watermark Chronology

- In the 18th century, watermarks on paper are made in Europe and America. They used anti counterfeiting measures on money and other documents. It's also used to record the date, the paper was manufactured and to indicate the sizes of original sheets as trademarks (Simpson J. and E. Weiner, 2000).
- In 1954 the first example of a technology similar to digital watermarking is patented by Emil Hembrooke for identifying music works. (Komatsu, N., & Tominaga, H. 1988).
- The term watermark was introduced near the end of the 18th century. It was probably given because the marks resemble the effects of water on paper.
- In 1988, Komatsu and Tominaga raised to be the first to use the term "Digital Watermarking".
- Early 1990s the term digital watermarking really came into vogue.
- About 1995 interest in digital watermarking began to mushroom. The first Information Hiding Workshop was organized (IHW) (Petitcolas, F. A. et al, 1999)
- In 1996. Primary topics, were held as The Society of Photo-optical Instrumentation Engineers (SPIE) began devoting a conferences specifically to Security.
- Watermarking of Multimedia Contents began to be employed in 1999 (Wong, P. W., & Delp, E. J, (2000)

2.4 Watermarking Classification

Digital watermarking can be classified into various types, based on several criteria as summarized in the following table. (Saini, L. K., & Shrivastava, V. 2014).

Table (2.1) Watermark Classification

No	Criteria	Classification
1	Watermark Type	1. Noise: pseudo noise, Gaussian random and chaotic sequences 2. Image: Any logo, Stamp Image etc.
2	Robustness	1. Fragile: Easily Manipulated. 2. Semi-Fragile: Resist by some type of Attacks. 3. Robust: not affected by attacks.
3	Domain	1. Spatial: e.g. LSB. 2. Frequency: e.g. DWT, DCT, DFT, SVD. 3. Spread Spectrum.
4	Perceptivity	1. Visible Watermarking: e.g . TV Channel logo 2. Invisible Watermarking: like Steganography.
5	Host Data	1. Image Watermarking. 2. Text Watermarking. 3. Audio Watermarking. 4. Video Watermarking.
6	Data Extraction	1. Blind. 2. Semi-Blind. 3. Non- Blind.

2.5 Watermarking Applications

Digital Watermarks is used in many applications, including Ownership assertion, in applications where multimedia content is electronically distributed over a network, the content owner would like to discourage unauthorized duplication and distribution by embedding a distinct watermark (or a fingerprint) in each copy of the data, Copy prevention or control, Fraud and tamper detection and ID card security. Information in a passport or ID (e.g., passport number, person's name, etc.). (Goyal, et.al 2014).

Digital watermarking is well established research area with growing of applications (Bartolini, F., et.al (2001). Although the essential motivation point behind the digital watermarking is the copyright protection, its applications are not that restricted. There is a wide application area of digital watermarking, including broadcast monitoring, fingerprinting, authentication and cover communication, etc... (Maes, M. et.al, 2000). For example, by embedding watermarks into commercial advertisements, the advertisements can be monitored when they are broadcasted at the correct instants by means of an automated system (Cox, I. J., et.al, 2000), (Langelaar, G. C. et.al, 2000),The system receives the broadcast, and then starts searching these watermarks in order to identify where and when the advertisement is broadcasted. The same process can be used for video and sound clips. Musicians, actors and famous persons may request to ensure that they receive accurate ownership for broadcasts of their performances. Serious number of watermarking techniques can be found in the literature used in the diversity of applications because of their advantages over the alternate methods. For example, copyright protection needs robust watermarking but authentication needs fragile watermarking, etc. The requirements that a watermarking system needs to respond depends on the specific type of

application. Digital watermarking has so many applications. In this section, we discuss some more common applications of digital watermarking as below:

- **Copyright Protection:** Most important and common application of watermarking, especially in image watermarking, is to insert copyright information and prevent the modification, stealing or copying the copyright data. The rules of using and copying the contents into digital objects without any loss of quality need high robustness applications. Protection, especially in image watermarking is to insert copyright information.
- **Broadcast Monitoring:** A commercial advertisers use this kind of application to ensure control of the air time which they purchased from broadcasters. It's applied by putting a unique watermark in each commercial sound or video that is aired by the broadcasters at the time and location those they want. According to the contracts, watermarks can be embedded in any type of data to be broadcasted on the network by automated systems, which are able to monitor distribution channels to track, identifying and check the content in the time and the place that they appear. Thus, there should be an auto-identification system, which may store the identification codes to the broadcast. There are several techniques like cryptography that store the identification code in the file header but the data is unlikely to survive any sort of modifications even format change. The watermark exists within the content and is compatible with the installed base of broadcast equipment. Although, embedding the identification code is very complicated compared to cryptography as the code is placed in the file header. It also, affects the visual quality of the work.

However, many companies protect their broadcasts through watermarking techniques.

- **Authentication /Content Verification:** The main goal of the authentication is to be able to detect any manipulations or modification of the original data, so that the information required to authenticate the content should be watermarked. The essential characteristics of the authentication requirements are Imperceptibility, Fragility, Security, Efficient Computation, and Capacity depending on the necessity of the application. To avoid tampering with the original data without even being detected which can be easily happen, and maintain the originality of the data, a watermark like signature, or a set of words, may be embedded into this data. If the image is being tampered with it can be easily detected as the pixel values of the embedded data would change and do not match the original pixel values. But If the image is being copied it would lose its authentication as the embedded data would not be copied along with the image.
- **Transactional Watermarks/Fingerprinting:** Transaction tracking is also called fingerprinting. It is a technique that can be used to trace the source of illegal copying. Every copy available can be watermarked with a unique bit sequence, if a copy is made illegal, the source can be easily traced since each original copy had a unique bit sequence embedded into it where each copy of the work is uniquely identified, similar to the fingerprint that identifies an individual. The watermark might record the recipient for each legal distribution of the work. The owner embeds different watermarks in each copy. If the work is misused then the owner will be able to find the traitor. Visible watermarking is adopted for transaction

tracking but invisible watermarking is much better. For example, in movie making, the daily videos are distributed to the persons who are concerned with the movie. Sometimes, the videos are disclosed to the press, so the studios use visible text on corner of the screen, which identifies the copy of dailies.

- **Medical applications:** All names of the patients printed on the X-ray and MRI reports, using specific techniques of visible watermarking. The medical reports play a very important role in the treatment offered to the patient. If there is a mix up in the reports of two patients this could lead to a disaster.
- **Copy Control:** Techniques of copy prevention, is to have a copy and consumer control mechanism to prevent illegal copying or recording of the content by inserting a never-copy watermark or limiting the number of times of copying.
- **Owner Identification:** Owner identification is a label, logo, name, symbol or anything else that can be printed on the covers or mentioned somewhere on the item. Many examples exist refer to the identification mark of an audio company on the CD case or the mark of the paper manufacturer on top corner of the paper. These types of watermarks can be easily removed by cropping the image or by tearing the part that has the identification. Digital watermarking helps to overcome this problem by embedding the watermark in the form of bits that form an integral part of the content. Watermark on the CD can be identified, and their use should be licensed.

2.6 Watermarking requirements

The efficiency of a digital watermarking process can be evaluated according to the perceptual transparency, computational cost, robustness, recovery of data, embedding and retrieval process, ability of the embedding and retrieval module to be integrated into standard encoding and decoding process etc. (Delaigle, J. F, 2000). ,(Cox, I. J, 1997). One of the challenges for researchers in the watermarking field is that these requirements compete with each other. The most significant requirements is the security, visibility and robustness, see figure 2.1 they areas follow:

2.6.1 Security

Watermark security mean How much the watermark and cover work are safe. In other words refers to its ability to resist hostileattacks. A hostile attack is any process specifically intended to thwart the watermark's purpose, the types of attacks may be one of the three broad categories (Cox, I., et.al, 2007):

- 1- Unauthorized removal: referred to as active attacks because these attacks modify the cover work.
- 2- Unauthorized embedding: referred to as active attacks because these attacks modify the cover work.
- 3- Unauthorized detection: referred to as a passive attack because it does not modify the cover work.

2.6.2- Invisibility

Two types of invisibility that concern with watermark, perceptual invisibility and Statistical Invisibility.

2.6.2.1 Perceptual Invisibility

Hide the watermark in such a way that the watermark is impossible to be noticed. However, this requirement conflicts with other requirements such as robustness, which is an important requirement when facing watermarking attacks. For this purpose, the characteristics of the human visual system (HVS) for images and the human auditory system (HAS) for audio signal are exploited in the watermark embedding process.

2.6.2.2 Statistical Invisibility

The hacker or the unauthorized person should not detect the watermark by means of statistical methods. If we say, the availability of a great number of digital works are watermarked with the same code should not allow the extraction of the embedded mark by applying statistically based attacks. A possible solution is to use a content dependent watermark (Voyatzis et al., 1998).

2.6.3 Robustness

Digital images commonly are target to many types of distortions. The mark should be detectable even after such distortions have occurred. Robustness against signal distortion is better achieved if the watermark is placed in perceptually significant parts of the image signal. For example, a watermark hidden among perceptually insignificant data is likely not to survive lossy compression. Moreover, resistance to geometric manipulations, such as

translation, resizing, rotation and cropping is still an open issue. These geometric manipulations are still very common. (Khanzode, P., Ladhake, S., et.al, 2011).

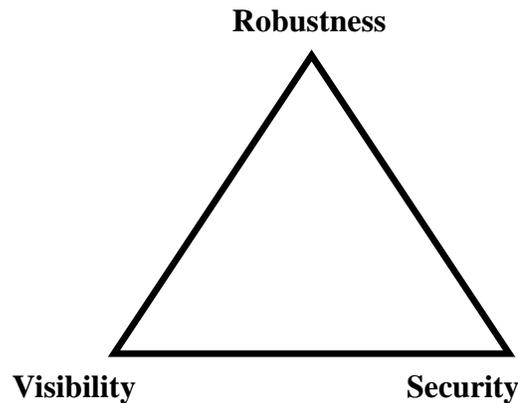


Figure 2.1 Watermark Requirement

2.7 Watermarking Techniques

Digital watermarking can be performed by various techniques which aim to protect the digital confidential contents. The common digital watermarking techniques work in two domains either spatial domain or frequency domain. Spatial domain works directly on the pixel, by modifying the carrier image pixel value to embedding the watermark data. The LSB is most commonly used with spatial domain. Transform domain is embedding the watermark by modifying the transform domain coefficients, using Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT). (Singh, P., &Chadha, R. S. (2013).

2.7.1 Spatial Domain Technique

This watermark technique is based on insertion of watermark data directly into pixels of a host image. This approach produces minor changes in the pixel intensity value, which are supposed to be imperceptible. The simplest example of the previous technique is to embed the watermark in the least significant bits (LSB) of image pixels. In other words, least significant bits have the lowest effect on the pixel value, and therefore any changes in these bits would have very low effect on the overall appearance on the image. Some LSB applications are embedded by splitting the image into blocks, and then a certain watermark data is added to the blocks by some procedures. It should be noted that this research project will be involved in the development of an improved embedding scheme in spatial domain. (Abbasfard, M. 2009).

Spatial domain is generally simple and faster than the frequency domain. The strength of the spatial domain is:

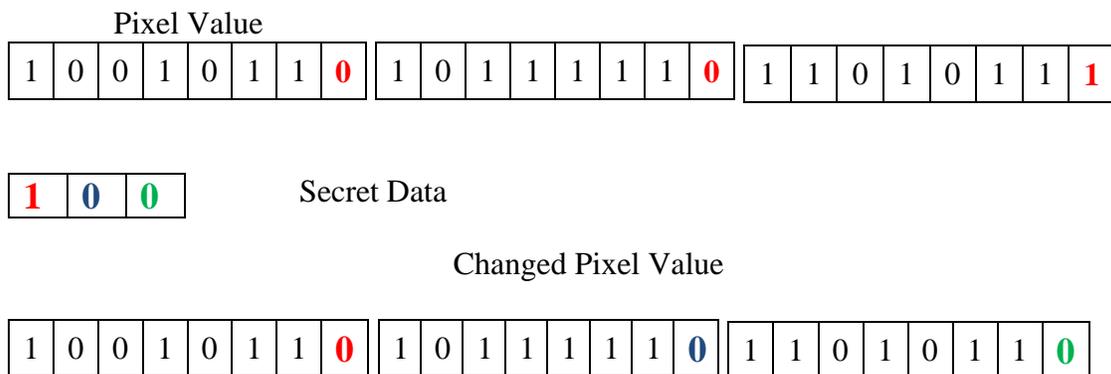
- A) Simplicity.
- B) Very Low mathematical Computational efforts.
- C) Less time consuming.

This technique of watermarking is easier and computing speed is higher than transform domain, but it is less robust against the attacks.

2.7.1.1 Least Significant Bit (LSB)

Easiest spatial domain watermarking is to hide a watermark data in the least significant bit of some randomly selected pixels of the carrier image. The LSB substitution method can be very powerful when subjected to cropping or any of the filters. Even if most of the multiple watermarks are lost in those attacks the retrieval of a single watermark would be considered as a success.

For example of performing the LSB:



2.7.1.2 Limitation of Spatial domain

Spatial domain is simple if compared with Transform domain. The robustness is the main limitation of spatial domain, it can survive simple operation such as cropping and addition of noise. The other limitation is that they do not allow for the subsequent processing in order to increase the watermarking robustness.

2.7.2 Transform Domain Technique:

The image is represented in the form of frequency. First, transform the image into another form that keeps the features, but not the intensity, embed the watermark data into the transformed image, and then transform it back to its original form. In this method,

transform coefficients are modified for embedding the watermark, to have imperceptibility as well as robustness. Transform domain is also called frequency domain because the values of frequency can be altered. The most important and widely used techniques in transform domain are Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Singular Value Decomposition (SVD) and Discrete Fourier Transform (DFT). (Tao, L. et.al 2014). The following a brief description of these techniques.

2.7.2.1 Discrete Cosine Transform (DCT)

This method is used for the signal processing by transforming a signal from spatial domain to frequency domain. DCT is applied in a lot of fields like pattern compression, data compression and all image watermarking fields. That's main DCT steps are:

- Segment the image.
- Applying DCT to each segment.
- Apply coefficient selection criteria.
- Embed the watermark.

2.7.2.2 Discrete Wavelet Transform (DWT)

Discrete Wavelet Transform is usually used in a wide variety of signal processing applications such as video and audio compression, removal of noise in audio and simulation of wireless antenna distribution. An example of one- level DWT is shown in Figure 2.2. Wavelets have their energy concentrated in time and are well suited for the analysis of transient, time-varying signals. DWT is also used to implement a simple watermarking scheme. 2-D (DWT) divided the image into sub-images, 3 details and 1 approximation as shown in Figure 2.3. The approximation looks just like the original; only

on 1/4 the scale. The 2-D DWT is an application of the 1-D DWT in both the horizontal and the vertical directions. It splits an image into four sub-images; lower resolution DWT.



Figure 2.2 One level DWT

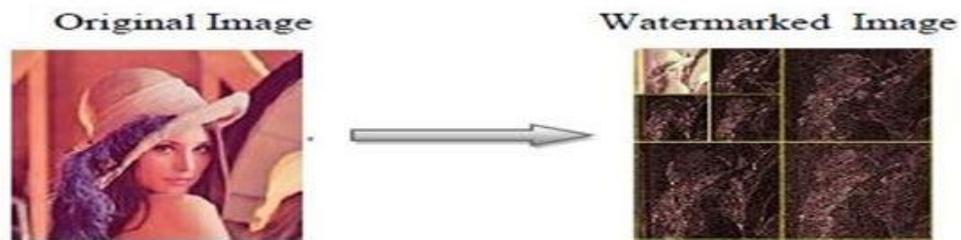


Figure 2.3 Two levels DWT

The fact is a multi-scale analysis can be used to the watermarking algorithm's benefit. Such process produces multi resolution representation of an image. The multi resolution representation provides a simple framework for interpreting the image information. DWT analyses the signal as multiple resolution by dividing the image into high frequency quadrants and low frequency quadrants. The low frequency quadrants are again split into two more parts of high and low frequency and this process is repeated until the signal has been entirely decomposed.

2.7.2.2.1 Merits of DWT over DCT

- The quality of visual image in DWT is better than DCT.
- In DWT, dividing the input coding into non overlapping 2-D block is not necessary; its higher compression ratios avoid blocking.
- Localization in DWT is better compared with DCT.
- DWT defines multi resolution details of the image, and the image can be shown on better levels of resolution and proceed from low to high resolution.

2.7.2.3 Discrete Fourier Transform (DFT)

Discrete Fourier Transform offers robustness against geometric attacks like rotation, scaling, cropping, translation etc. The DFT is used for the periodic digital signals or discrete time. DFT decomposes an image into sine and cosine form, and based watermark embedding techniques are divided in two types, first one is the direct embedding, second one is the template based embedding. According to the direct embedding technique the watermark is embedded by modifying DFT magnitude and phase coefficients. The template based embedding technique introduces the concept of templates. A template is structure which is embedded in the DFT domain to estimate the transformation factor.

2.7.2.3.1 DFT Characteristics

- Real time in DFT is complex valued, which results in phase and magnitude representation of an image.
- Strongest component is the central component because its contain low frequency.
- Resist the cropping; the main reason is that cropping effect leads to spectrum blurring.

- Scaling of image results in amplification of extracted signal and can be detected by correlation coefficient.

2.7.3 DFT advantages over DWT and DCT

DFT is Rotation Scaling Translation (RST) invariant. DFT can be used to recover from geometric distortion, but DCT and DWT are not invariant. Hence, it is hard to overcome geometric distortion.

DFT disadvantages over DWT and DCT

The main disadvantage of DFT is that its output is complex value and requires more frequency rate in addition to the computational efficiency is very poor.

2.7.4 Spread Spectrum Technique

This technique can be used for both spatial domain and frequency domain. The spread spectrum method has the advantage that the watermark extraction is possible without using the original unmarked image (Chopra, D. et.al, 2012). The watermark data must be placed in perceptually significant components of the signal if it is to be robust to any signal distortions and common attacks. However, it is well known that modification of these components can lead to perceptual degradation of the signal. The watermark is difficult for an attacker to remove, even when several individuals conspire together with independently watermarked copies of the data. The spread spectrum is used to embed the watermarking, the frequency components of the host image. First, Fourier Transform is applied to the host image. It is inserted to obtain the modified values. Verification of watermark presence relies on the cross correlation between extracted watermark and original watermark, It is also robust to common signal and geometric distortion like digital-

to-analog and analog-to-digital conversion, re sampling, translation, cropping, compression, rotation, quantization, dithering and scaling.(Goyal, R., &Kumar, N. 2014).

2.8 General Digital Image Watermarking Framework

Watermarking framework consists of two processes; embedding and extraction where:

- 1- Embedding the data in to the cover image.
- 2- Extract the date from the cover image.

The two processes are illustrated in fig. 2.4 and 2.5.

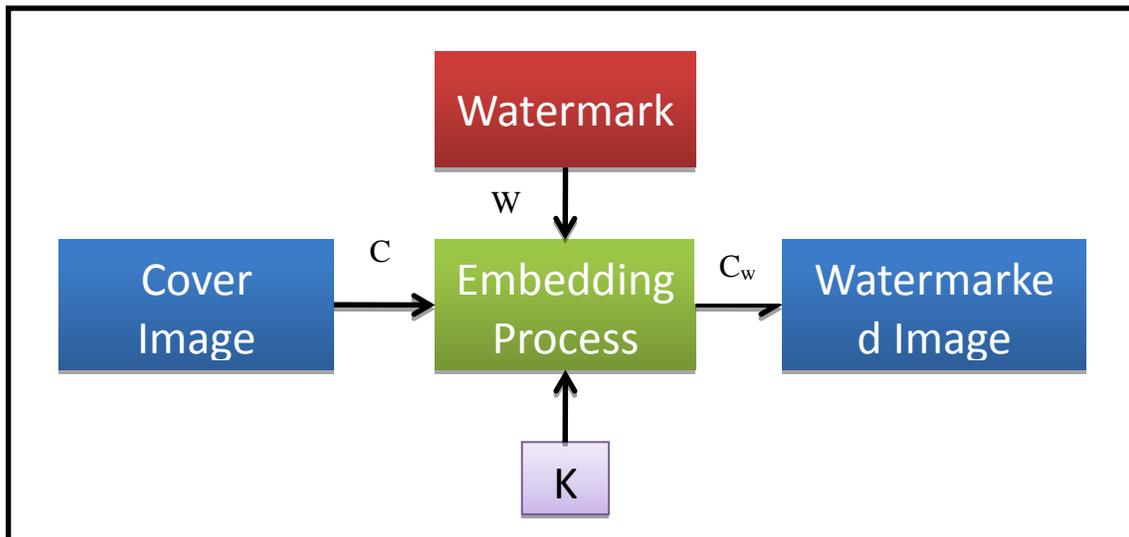


Figure 2.4 General Embedding Process

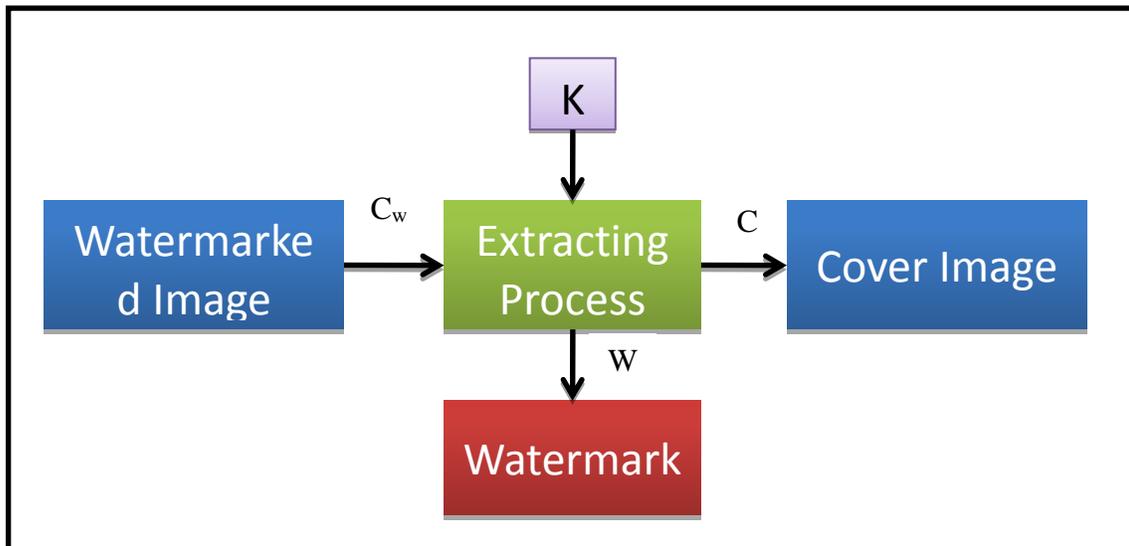


Figure 2.5 General Extracting

2.9 Statistical Random and Pseudo Random Number Generators Tests

In this study a number of statistical tests were used to check out the Pseudo Random Number Generators (PRNG's) strength. The quality of trust and security through the Internet has become an urgent need. To investigate the degree of randomness there are number of standard tests that can evaluate or test the RNG such as statistical tests which include: (Soto, J. 1999).

The Crypt-XS developed by researchers at the Information Security Research Centre at Queensland University of Technology in Australia. Crypt-XS tests include the frequency, change point, runs, linear complexity, sequence complexity and. binary derivative.

(Donald Knuth's book, 1999) illustrate several empirical tests which are: frequency, serial, gap, collision, birthday spacing, poker, coupon collector's, permutation, run, maximum-of-t, and serial correlation.

The initial test of Pseudo DIEHARD developed by George Marsaglia. suite of statistical tests consists of fifteen tests, monkey tests on 20-bit Words, birthday spacing, monkey tests, count the 1's in a stream of bytes, overlapping permutations, ranks of 31x31 and 32x32 matrices, ranks of 6x8 matrices count the 1's in specific bytes, parking lot, random spheres, squeeze, overlapping sums, runs, ,minimum distance, and craps.

The NIST Statistical Test includes fifteen tests:

Frequency (Monobit) test, frequency test within a Block, runs test, tests for the Longest-Run-of-Ones in a block, binary matrix rank test, discrete Fourier transform (Spectral) Test, Non-overlapping template matching test, Overlapping Template Matching Test, Maurer's "Universal Statistical" Test, linear complexity, test, serial test, approximate entropy test, cumulative sums (Cusums) test, random excursions test, and random excursions variant test.

2.10 Related Work

This section will illustrate number of related works in order to determine the major research techniques and methodologies used. Since this research is concern with PRNGs and LSB watermarking, the following literature survey describes only the previous work done on digital watermarking Spatial Domain with the PRNG researches.

(Behnia, S., et.al, 2008): In this paper, a way of improving the security of chaos-based cryptosystem is proposed, using a hierarchy of one dimensional chaotic maps and their coupling, which can be viewed as a high dimensional dynamical system. Mixture mechanism of chaotic maps, enhance the key space and security of algorithm. In regard to the tight relationship between cryptography and chaos theory, cryptosystem, encryption with this algorithm and could be helpful to reduce or even overcome cryptographical weaknesses of chaotic cryptosystems.

(Bamatraf, A.2010): In this paper a simple and robust watermarking algorithm is proposed a new LSB based digital watermarking scheme with the fourth and third LSB in the grayscale image. After embedded the secret data in the third and fourth LSB in the image in determine coordinates, then got watermarked image without noticeable distortion on it. Therefore, this digital watermarking algorithm can be used to hide data inside image.

(Sakthidasan, K., & Krishna, B. S. 2011): This paper, a new image encryption scheme which employs one of the three dynamic chaotic systems (Lorenz or Chen or LU chaotic system selected based on 16-byte key) to shuffle the position of the image pixels (pixel position permutation) and uses another one of the same three chaotic maps to confuse the relationship between the cipher image and the plain-image (pixel value diffusion), The proposed system has the advantage of bigger key space, smaller iteration times and high security analysis such as key space analysis, statistical analysis and sensitivity analysis were carried out. The results demonstrate that the proposed system is highly efficient and a robust system.

(Seyedzadeh, S. M., & Mirzakuchaki, S. 2012): This paper proposes a novel chaos-based image encryption algorithm to encrypt color images by using a Coupled Two-dimensional Piecewise Nonlinear Chaotic Map, called CTPNCM, and a masking process. Computer simulations confirm that the new algorithm has high security and is very fast for practical image encryption. Also the Experimental results reveal the fact that the proposed algorithm yields better security performance in comparison to the results obtained from other algorithms.

(Anees, A., & Siddiqui, A. M. 2013): This paper present a technique which is based upon spatial and frequency domains, and employ chaos to embed the watermark. With the employment of chaos in our technique, the results shown good as can be visualized through security statistical analysis, also the robustness of technique has checked through confidence measure. Results can say that the proposed technique lies between semi fragile and fragile watermarking schemes

Varkale, A & Sharma, 2014): The proposed technique used encryption key Pseudo random sequence consists of random bits is generated. Then used a chaotic sequence algorithm to create the pseudo-random sequence. 256-bit. By using the parameter additional data is inserted to encrypted image. With an encrypted image containing additional data, the proposed system demonstrated successful accuracy in recovering the original image.

(Sruthi, N., Sheetal, and et.al, 2014): In this study digital watermarking has been implemented in spatial domain using LSB method, in frequency domain using Discrete Cosine Transform with Gaussian noise as watermark. Various noise attacks done such as speckle, salt and pepper are modeled and the results are obtained with the extraction of the

watermark. This work further can be extended with combination of spatial and spectral domain, which is referred as hybrid domain watermarking.

(Maaita&Al_Sewadi. 2015): In this work, an algorithm for computationally fast, cryptographically secure pseudo-random key generation, a multi-stage algorithm based on mixing bitwise Boolean operations, integer modular operations, along with bit manipulations and displacements for secret splitting. The experimental part of the paper demonstrated that an average of 98.9% of the generated sequences were unpredictable and passed successfully six tests proposed by the NIST.

(Ghosh, Maity, et.al. 2015): This study proposed couple purpose robust algorithm in spatial domain for digital watermarking and image cryptography, this method gives a higher degree of imperceptibility without effecting robustness.

(Srivastava& Singh et.al. 2016): In their work, a digital watermarking embedding and extracting scheme based on Triple Data Encryption Standard Algorithm (TDES) and spatial domain technique is proposed. The main contribution of this work is to provide a robust digital watermarking scheme with high capacity, secrecy and also robust against various noise additions, Experimental results indicate that the proposed scheme has better imperceptibility, capacity and robustness against the noise addition.

(Dutta& Kumar, 2016): Block based on spatial domain digital watermarking technique is proposed in this study, in which formation is used to identifying the location(s) in the host image to which watermark is to be embedded, with the LSB substitution technique the experimental results showed good efficiency.

(Mathur,& Muralibabu et.al.2016): This paper implemented a watermarking technique and used various image testing of watermarking. The algorithm provides high level of security by generating key which is used to extract the watermark, the algorithm is able to randomize the location of the watermark by shell based pixel selection.

2.11 Related work Summary

Table (2.2) summarized some related work that shows the main parameters, advantages and drawbacks for each method.

Table 2.2 Related work summary

Authors	Parameters	Advantage	Drawbacks	Proposed work
(Varkale, A & Sharma, 2014)	Chaotic Algorithm, PRNG for encryption.	Proposed algorithm is good and obtained a good quality image.	The extraction process has an additional method in comparison with general data hiding scheme.	The PRNGs Used for encryption and embedding
(Sruthi, N., Sheetal, et.al, 2014)	Spatial and Spectral Digital Watermarking	This work further can extended with combination of spatial & spectral domain, which referred to hybrid watermarking	The PSNR and MSE result did not showing a high level of robustness, which it's the paper focusing point.	System is fragile, used a spatial domain and LSB.
(Behnia, S., et.al, 2008)	mixture of chaotic systems	Helpful to reduce or even overcome cryptographical weaknesses of chaotic cryptosystems	The algorithm used only two prototype of the hierarchy of one-dimensional chaotic maps.	The technique used single chaotic system.
Sakthidasan, K., & Krishna, B. S. (2011)	(Lorenz , Chen or LU chaotic system	bigger key space, smaller iteration times and high security analysis	Complex non-linearity was preserved by choosing suitable chaotic maps	Based on Lorenz chaotic map
(Ghosh, Maity, et.al. 2015)	dual purpose spatial domain robust algorithm for digital image	This method gives a higher degree of imperceptibility	The size of watermark increased.	Watermark kept same size

	watermark using Extended Hamming Code	without effecting robustness.		
(Srivastava& Singh et.al. 2016)	The scheme is based on Triple Data Encryption Standard Algorithm (TDES) and spatial domain technique	Proposed scheme has better imperceptibility, capacity and robust against the noise addition.	All the three used keys are identical in TDES, $K_1=K_2=K_3$.	Used two different keys K_1, K_2
(Seyedzadeh, S. M., & Mirzakuchaki, S. 2012)	based on Coupled Two-dimensional Piecewise Nonlinear Chaotic Map, called CTPNCM, and a masking process	Algorithm yields better security performance.	Key space equal to 2^{256} , not strong enough as the proposed technique.	Secret key space is $=2^{n+m}$ which come from K_1, K_2
(Mathur,&Muralibabu et.al.2016)	Spatial domain based image watermarking using shell based pixel selection	Provides high level of security by generating key which is used to extract the watermark later.	-Converting the watermark into binary image by local thresholding and then converted into a logical matrix. Consumes more time and computation effort.	Encrypt the watermark as first step, and then embed it inside image.
(Bamatraf, A. 2010)	Based on third and the fourth least significant bits (LSB) technique.	- Embedding is in the 3 rd & 4 th LSB in the image No noticeable distortion	Works on gray scale images only. It means less efficient with color images, and cannot applied on many applications.	Works on grayscale and color image by using LSB
(Anees, A., & Siddiqui, A. M. 2013)	Spatial, frequency domains, and employ chaos to embed the watermark	System can survive against unintentional attacks such as noise, compression and cropping	chaotic security system showing the flaws in the strength of secure algorithms and can be easily broken in short computer times.	Secret seed key strength increased the chaotic system security
(Dutta& Kumar, 2016)	combination of entropy block, and LSB substitution concepts	Efficiency of the proposed algorithm with the help standard performance measures using a varied image sets.	Proposed scheme should be robust with respect to a variety of possible attacks.	Watermark in spatial domain using LSB technique.

Chapter Three

The Research Methodology

Chapter Three

The Research Methodology

3.1 Introduction:

The main idea of the proposed research is to investigate the possible improvement of inserting watermarks into an image using a multiple Pseudo-random generators with LSB watermarking technique. This means modulating an image file as a cover to hide a logo file that can be a text or an image. LSB technique dictates that the cover file must be at least 8 times as long as the logo (hidden file) because a single bit of the hidden file will be embedded in single byte.

In this work two tasks are investigated and developed to achieve the hiding process. First, two Pseudo random number generator (PRNG) algorithms were designed and tested for randomness according to the available national standard (NIST) tests criterion. One of these PRNG algorithms is designed based on chaos theory principles which are sensitive to initial conditions. The chaos theory or chaotic map is used to generate sequence of number according chaos phenomena with randomness property (Chhibber, N., &Patra, G., 2015).This sequence of random number is used to encrypt the secret image which is logo image, before hiding it in the carrier image (Cover Image). The other PRNG algorithm will be utilized to produce random numbers that will govern the process of selecting the candidate pixel of the carrier image to be modified according to the data to be hidden, which will give the model more robustness against the common attacks by the randomness idea.

For more secure watermarking in LSB technique, not all bytes of the cover file will be used sequentially but only random byte positions in the cover image file will be selected.

3.2 The Proposed Watermarking Scheme

The proposed watermarking scheme consist a number of steps in order to give a proper, secure, and high authenticated model that serve the ownership or the personal data to be transferred through the internet.

The main objective of the proposed embedding algorithm is to increase the watermark content authentication in order to get high authentication copyright protection against many attacks that aim to copy, manipulate or damage the personal data. The algorithm relies on the randomness and secret keys strength concept by implementing multiple pseudo random number generators (PRNGs) for embed a logo image into the carrier image. Two PRNG's were implemented; the first PRNG is a modified Lorenz attractor. It is involved to encrypt the logo image before embedding process. The other PRNG is implemented for embedding the encrypted logo into the carrier image using LSB technique. They will be explained later in this chapter. To clarify the proposed algorithm, it consists of three processes; preparation, embedding and extraction as follow:

a. Preparation process

In this process, random numbers are generated to be used for embedding locations, logo image and carrier image were selected, and the parameters of compute the logo and carrier length are calculated to determine the number of segments and the length for each segment in the carrier image as in the following steps.

Step1: PRNG's preparations

Two PRNG's are selected and modified to be used for both encrypting the logo image and locating embedding places in the carrier multimedia. The chosen PRNG's were Lorenz and Trivium. They were chosen for their sound randomness, besides they were also modified to suit the intended purpose. One seed key (k_1) is selected as secret key for encryption and another seed key (k_2) is selected for embedding. The modified PRNG's will be explained later.

Step 2: Select a logo image (W) and calculate its length (L_w) in bits.

Step 3: Select a carrier image (C), and calculate its length(L_c) in bits.

Step 4: Segment the carrier image into a number of blocks (B), each of length N-bits according to equations (1) and (2).

$$B = \frac{(L_c)}{8*L_w} \dots\dots\dots (3.1)$$

$$N = \frac{(L_c)}{B} \dots\dots\dots (3.2)$$

The randomness of the keys has a strong impact on the system's security strength being difficult to be predicted, guessed, reproduced, or discovered by a cryptanalyst. In this study, PRNG algorithms are based on mathematically manipulating a publically agreed upon information. The random selection technique for embedding increases the robustness of the resulting watermarked multimedia. In addition to use of secret key seed and design of the PRNG algorithm enhances the security strength of the process. The used technique proved suitable for, copyright protection.

b. Embedding process

For the embedding of the logo image into the carrier image, the block diagram of Figure 3.1 is followed. It consists of the following steps.

Step1: use seed key k_1 to generate a sequence of random numbers by the modified Lorenz PRNG.

Step 2: Encrypt the logo W using the random numbers generated in step1.

$$W_e = E_{K1} (W) \dots \dots \dots (3.3)$$

Step 3: use seed key (k_2) to generate a sequence of random numbers by the modified Trivium PRNG.

Step 4: embed the resulting encrypted watermark (W_e) into the carrier image C using the random number sequence generated in step 3 to locating on the blocks, by equation 3.4.

$$C_{we} = E_{k2} (W_e) \dots \dots \dots (3.4)$$

Now C_{we} is the watermarked image which can be publicly used with its copyright protection measure. Figure 3.1 shows the steps for the embedding process.

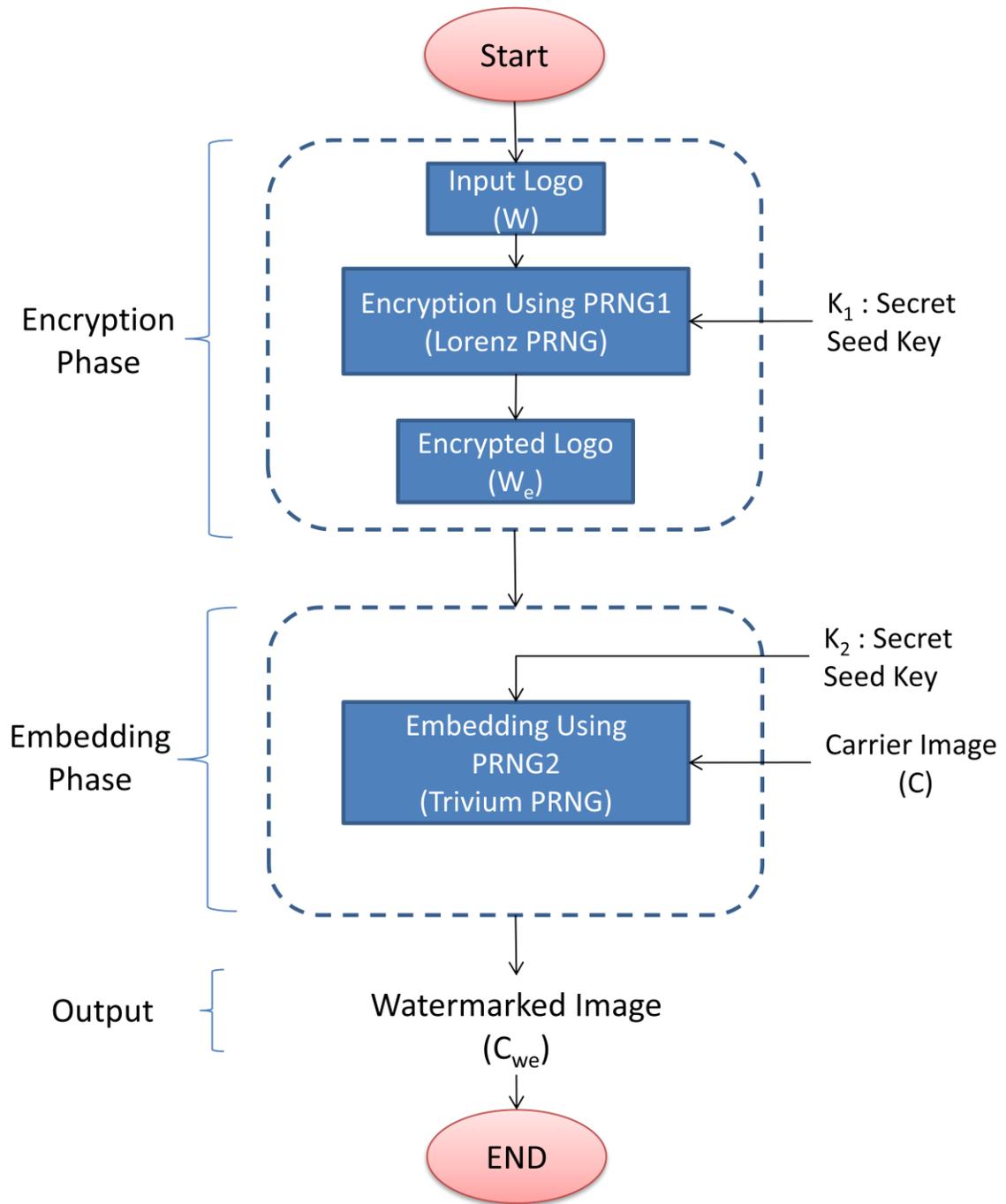


Figure 3.1 Embedding Process

b. Extraction process

To extract the embedded logo image from the watermarked image, a process similar to embedding process is conducted but in reverse order. It starts with watermarked image (C_{we}), using the same keys sequence generated by Trivium PRNG first to get W_e , then using the same keys sequence generated by Lorenz PRNG to decrypt W_e in order to produce W , figure 3.2 is illustrates the extraction process.

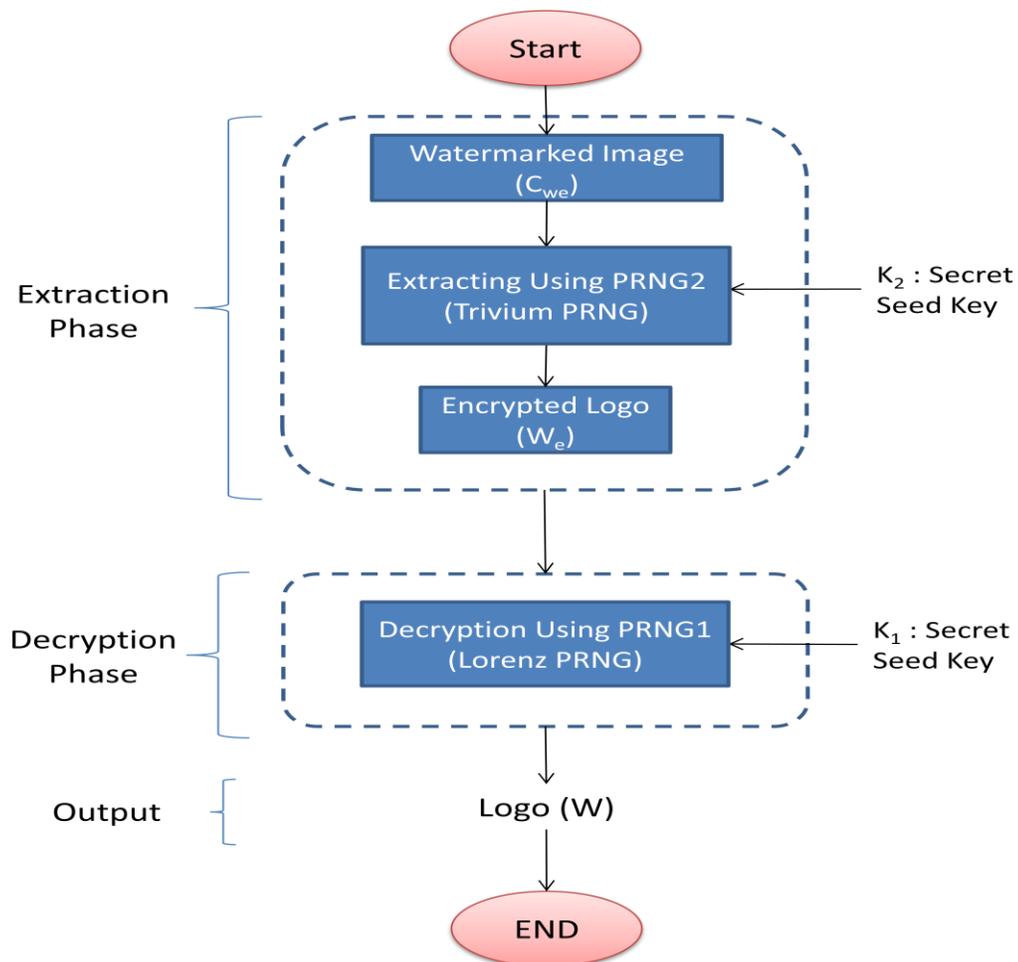


Figure 3.2 Extraction process

3.3 Modified Lorenz Attractor(LA) PRNG

The first step in this model, the encryption of the logo bits stream using modified Lorenz chaotic equation which is a 3D dynamical system defined by x , y and z . Lorenz equation is a model of thermally induced fluid convection in the atmosphere. It is among the classical chaotic systems (complex mathematical systems that show sensitivity to initial conditions. In such systems, any uncertainty in the beginning (no matter how small) will produce rapidly escalating patterns in the prediction of system's future behavior(Chhibber, N., & Patra, G. 2015)),and implies as the cause of the “butterfly effect” in the scientific studies due to the fact that the attractor has two wings as the butterflies. Therefore, it has been widely studied in chaos theory, dynamic system modeling, chaotic control and synchronization phenomenon. The equation system gives a chaotic behavior with regard to the initial system parameters. Apart from any 1D or 2D chaotic systems, the Lorenz system has a much complicated chaotic behavior. The equation system contains three differential equations (Cellk, K., & Kurt, E. 2016, June):

$$x_{i+1} = a(y_i - x_i) \dots \dots \dots (3.5)$$

$$y_{i+1} = rx_i - y_i - x_i z_i \dots \dots \dots (3.6)$$

$$z_{i+1} = x_i y_i - bz_i \dots \dots \dots (3.7)$$

Where x , y and z are the functions of time with the derivative forms (i.e. x , y and z) and a , b , r are the system parameters for the deterministic system.

All numbers in this technique represent real number with randomness property. The modifications are proposed to be more suitable in the random watermarking technique by convert the sequence of x, y and z into integer value to XOR it with carrier image according to the following equation.

Seq_j:

$$Seq_j = \lfloor x_{i+1} * 1000 \rfloor \bmod 256 \dots \dots \dots (3.8)$$

$$Seq_{j+1} = \lfloor y_{i+1} * 1000 \rfloor \bmod 256 \dots \dots \dots (3.9)$$

$$Seq_{j+2} = \lfloor z_{i+1} * 1000 \rfloor \bmod 256 \dots \dots \dots (3.10)$$

The following example clarifies the algorithm.

Example:-

$$X_0 = 0.9812628452745$$

$$Y_0 = 0.2121039012934$$

$$Z_0 = 0.3635463254264$$

$$Seq_0 = \lfloor 0.9812628452745 * 1000 \rfloor \bmod 256 = 981 \bmod 256 = 213$$

$$Seq_1 = \lfloor 0.212103906284 * 1000 \rfloor \bmod 256 = 212 \bmod 256 = 212$$

$$Seq_2 = \lfloor 0.3635463254264 * 1000 \rfloor \bmod 256 = 363 \bmod 256 = 107$$

In this operation the first three digit after floating point part are moved to integer side with truncate then the mod 256 operation convert these three digit number into byte form to be XORed with input image.

Figure 3.1 presents the main steps of the embedding secret image encryption operations with the following initial values of Lorenz Attarctor are:

$$a = 10 \quad , \quad b = 28 \quad , \quad r = 2.66666666676.$$

Also the standard parameters of Lorenz are public but the input values of x , y and z are secret values, these values are converted into integer values according the above equations, to generate secret chaotic sequence according the following equation:

$$x_{i+1} = x_{i+1} * 10000000 - [x_{i+1} * 10000000] \dots\dots (3.11)$$

$$y_{i+1} = y_{i+1} * 10000000 - [y_{i+1} * 10000000] \dots\dots (3.12)$$

$$z_{i+1} = z_{i+1} * 10000000 - [z_{i+1} * 10000000] \dots\dots (3.13)$$

The proposed chaotic image encryption algorithm is listed in figure 3.3.

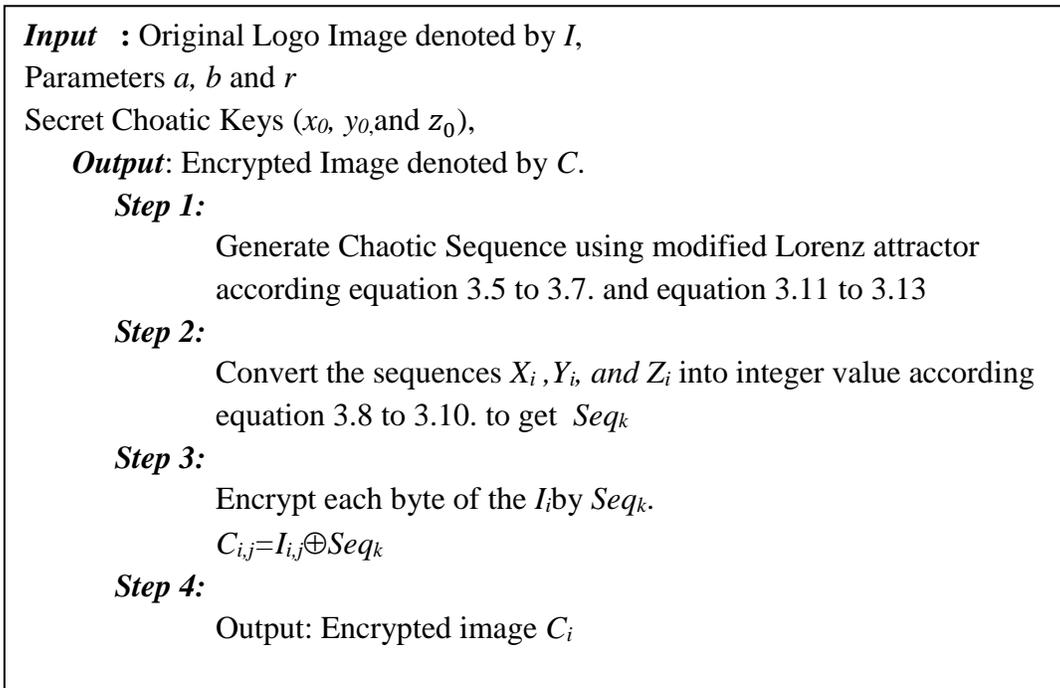


Figure 3.3 The Proposed Chaotic Image Encryption

3.3.1 Initial Secret key for modified Lorenz PRNG

To compute the initial values of Lorenz x_0 , y_0 and z_0 , the input key string is divided into three substrings, and then the first substring is taken to compute them as follows.

$$x_0 = \frac{\sum_{i=0}^n ASCII(KeySubStr_{1i}) \text{ Mod } 256}{256} \dots\dots\dots (3.14)$$

$$y_0 = \frac{\sum_{i=0}^n ASCII(KeySubStr_{2i}) \text{ Mod } 256}{256} \dots\dots\dots (3.15)$$

$$z_0 = \frac{\sum_{i=0}^n ASCII(KeySubStr_{3i}) \text{ Mod } 256}{256} \dots\dots\dots (3.16)$$

For example the input seed key is “AYSSERSHAMIL”, then

$$x_0=0.25.$$

$$y_0=0.1953125.$$

$$z_0=0.13671875.$$

3.4 The Modified Trivium PRNG:

The second PRNG is a modified version of Trivium (Paar, I. C, &Pelzl, 2010).Pseudo-random number generator. It is accomplished by using Linear Feedback Shift Registers (LFSR) based Pseudo Random Generator of the fashion shown in the block diagram of figure 3.4. The introduced modifications in this research work include, bit lengths, XOR selected sections and some other bits for initialization. This proposed PRNG will be initialized by two vectors; first, the secret key of length 12 characters (for example AYSSERSHAMIL), which will be converted into 84 bits using ASCII codes, and second, the Initial Vector which is 87 bits long, also. It is fixed for each user in the algorithm.

3.4.1 PRNG Structure

The core of this PRNG is three shift registers, A, B and C. Each with a length of 87bits. The XOR-sum of all three registers outputs form the output pseudo random stream. The PRNG structure as shown in figure 3.4 is selected to be the main PRNG of the proposed method for embedding. But it is modified according to the study needs. The selected secret key length fits the proposed algorithm. The secret key seed is selected first which is of 12 characters length (84bits). It is chosen in the experimental part of the thesis as “AYSSER SHAMIL”, however, any other seed related to the owner of the proposed system can be used. The length of shift registers is chosen as the nearest prime number to 84, i.e. 87 bits (which is equals the length of the seed key+3other bits added to it).

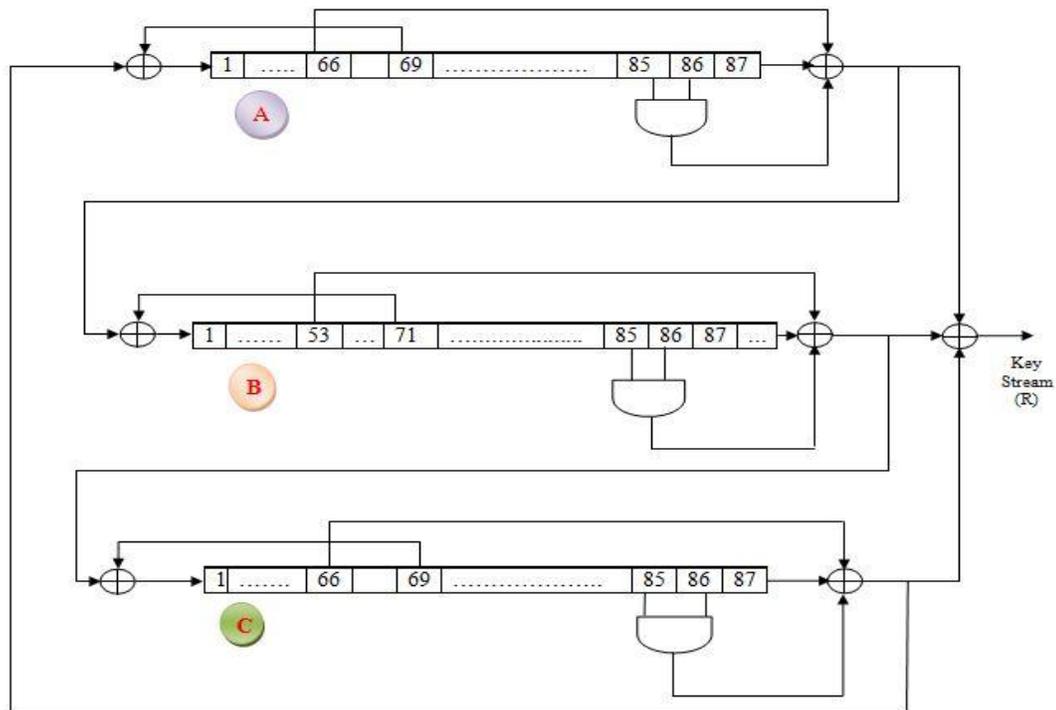


Figure 3.4 Structure of Modified Trivium PRNG.

3.4.2 Initialize generation Phase

Initially, an 87-bit, Initial Vector (IV) is loaded into the 87 locations of register A, and an 84-bit key which will be “**AYSSERSHAMIL**” is loaded in the 84 leftmost locations of register B, while the last three bits will be set to 1. All other register bits are set to zero with the exception of the three rightmost bits of register C, i.e., bits c_{85} , c_{86} and c_{87} , which are set to 1.

Table 3.1 Trivium PRNG Parameters

Parameter	Length
Secret Seed Key	87 bit
Initial Vector (IV)	87 bit
Internal State	261 bit

3.4.3 Warm-up stage

Trivium PRNG requires a warm-up stage, which lasts clocking period of $4 \times 261 = 1044$ times. Clock cycles, during this warming up stage of the PRNG output no cipher output is generated. This operation gives more guarantees for randomness.

3.4.4 Generation of the Modified Trivium PRNG

The PRNG generates a sets of bits, the length of each set is $(\text{Log}_2 K)$, which is used to evaluate the random number R in the interval (0 to K-1), first step is to generate R between 0 and K-1 to locate the first byte location to be modified i.e., the LSB of this byte in the carrier image will be replaced by the logo bit.

The output of each register is connected as input to another register. The three registers are arranged in circle. The generation can be viewed as consisting of one circular register with a total length of $87+87+87 = 261$. Each of the three registers has similar structures.

Registers inputs are computed as the XOR-sum of two bits:

- The output bit of any register is part of input of another register as shown in Figure3.4. For instance, the output of register A is part of the input to register B.
- One register bit at a selected location is fed back to the input. The positions are given in Figure3.4. For instance, bit 69 of register A is fed back to its input.

The output of each register is computed as the XOR-sum of three bits, namely rightmost register bit.

- One register bit at a selected location is forward to the output. The positions will be change in every round by the second PRNG. For instance, bit 66 of register A is fed to its output, in next round it might be fed to bit 16 etc.
- The output of a logical AND function whose input is two specific register bits. The positions of all AND gates, registers lengths, feedback bit and feed forward bit inputs are given in Table 3.2.
- Finally all registers output are computed by XOR to generate the Key Stream (R).

Table 3.2 PRNG workflow

	Register length bits	Feedback bit	Feed forward bit	AND inputs Bit locations
A	87	66	69	85,86
B	87	53	71	85,86
C	87	66	69	85,86

The generated key from this PRNG refers to the candidate pixel location in the carrier image for each segment by using LSB method to hide the information, the encrypted logo image bits will be embedded one by one until the last bit. A simple example of how the embedding process of the bits of a logo is embedded into the segments of a cover image is illustrated in figure 3.5 using output of the second PRNG.

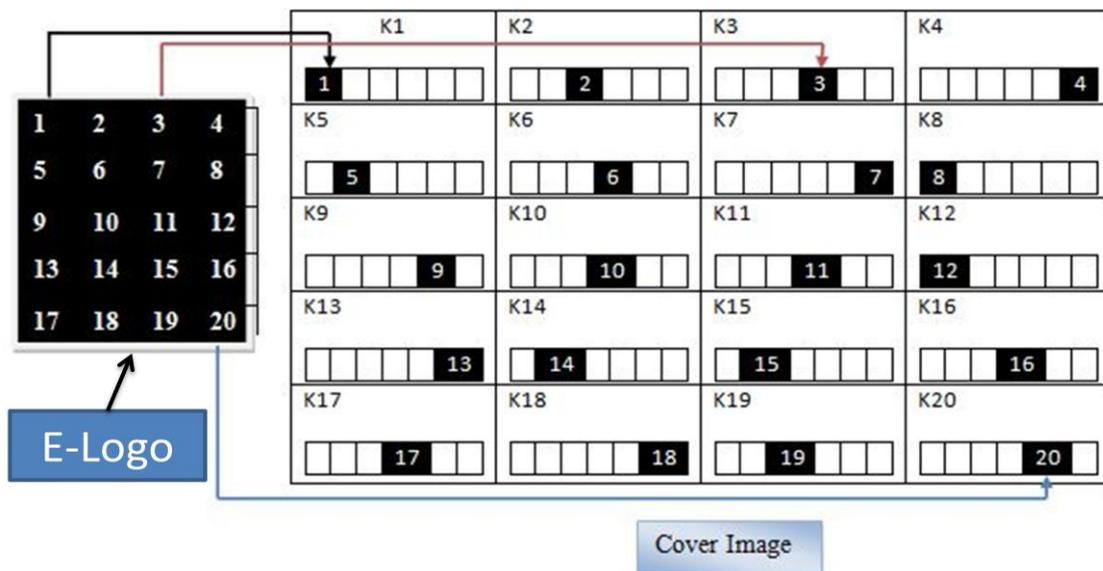


Figure 3.5 Trivium PRNG implementation

3.5 Secret Key Strength:

The strength of the secret keys used in this study technique causes a major effect on the performance of the system, as the PRNGs depend on the input secret seed keys. The change of the secret key length has a strong impact on the watermark security, if the key space become much large, then the number of possible keys becomes very large too. The security is really achieved and enhanced if 256 bit of key length is chosen. It may be considered unbreakable because the possible key space would be 2^{256} possible keys. Therefore, the key strength is depending on the input key size. Such that if the input key for first PRNG is n and the second PRNG is m the possible key space is 2^{n+m} possible keys, which becomes very hard to guess even if the brute force attacked is adopted.

Chapter Four

Implementation and Results

Chapter Four

Implementation and Results

4.1 Introduction

This chapter investigates and evaluates the implementation of the proposed algorithms (Multiple Pseudo Random Generator implementations for robust watermark technique) of chapter three under wide range of attacks. These attacks include the effect of adding various noises, rotating, cropping and image resizing and will summarize the types of attacks considered while the rest of the chapter contains the results tables, charts and discussion. The considered noises are, Gaussian, salt and pepper, Poisson, localvar and speckle noise, then the encryption and watermarking results will be compared with number of previews works on many tests, depending on a common robustness tests, such as PSNR. The test results are compared with algorithms Singh, A. K., Sharma, N., Dave, M., & Mohan, A. (2012, December) and Varkale, A, & Sharma, (2014, October),. MSE results also compared with the algorithms Anees, A., &Siddiqui, A. M. (2013, December), Yang, X., &Guo, C. (2016, December). Entropy test with algorithms Seyedzadeh, S. M., &Mirzakuchaki, S. (2012) and Celik, K., & Kurt, E. (2016, June). NPCR test with algorithms Varkale, A, & Sharma, (2014, October), Wu, Y. Noonan, J. P., &Agaian, S. (2011). HCR, VCR, DCR with algorithms, Behnia, S., et.al. (2008), Sakthidasan, K., & Krishna, B. S. (2011, June). In addition to UACI test, the proposed algorithm is coded using Microsoft visual studio 2010 C# program language. Noise tests implemented by using Matlab R2013a, because it is a suitable environment for noise image testing, which is

used in many researches and produced adequate results. The GUI of the program is included in appendix(B).

4.2 Evaluation Metrics

The performance evaluation of the proposed watermarking scheme is obtained by measuring imperceptibility, robustness and encryption of the resulting watermarked images. The error metrics used to test the proposed algorithm are Peak Signal to Noise Ratio (PSNR), Correlation (RC) and Mean Square Error (MSE), Number Pixel Change Ratio (NPCR), Unified Average Change Intensity (UACI) and entropy tests, which modulated the equations will describe later in this chapter.

The Peak signal to noise ratio value is computed to evaluate the differences between the original image and watermarked image it indicates the image resistance to the presence of noise.

As an example, a logo of dimension 160*149 pixels is embedded in a carrier image of dimension 3818*2540 pixels using the proposed algorithm is shown in figure 4.1.

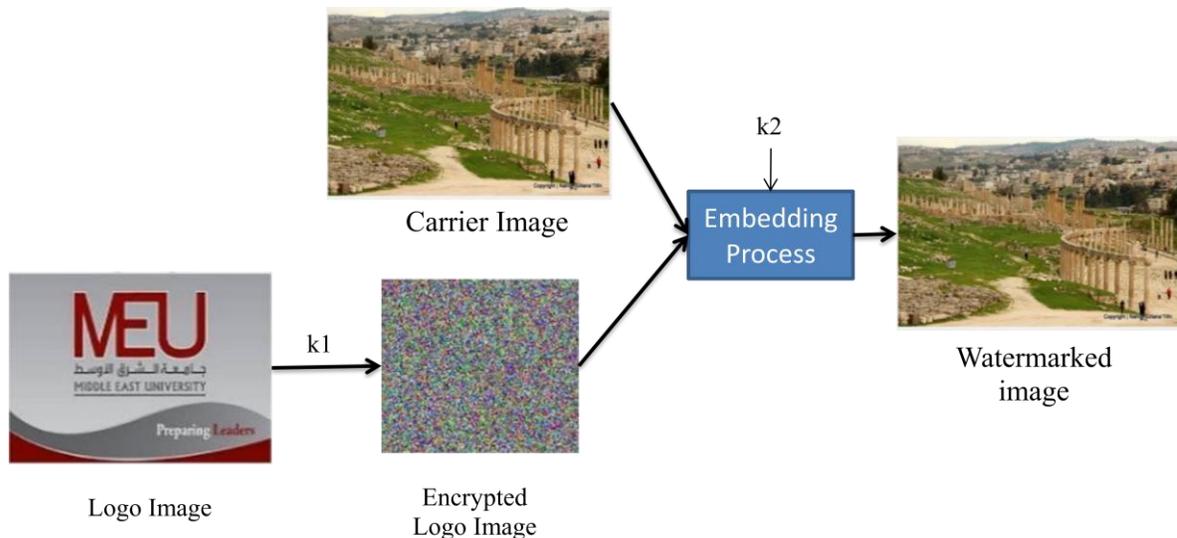


Figure 4.1 an example of Watermarking steps

4.3 Embedding algorithm tests

The embedding algorithm of the proposed method are tested with many watermarking tests such as PSNR, MSE, NPCR, H-CR, V-CR and D-CR using different logos and various carrier image sizes. An example for the implementation, the carrier images and the logo show in table 4.1 are used for this test and the obtained results are listed in table 4.2.

Table 4.1 Used Images for the tests

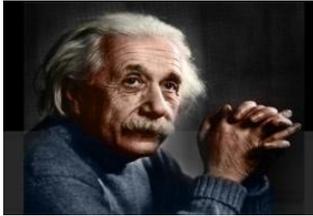
<p>Lena 255*255</p>		<p>MEU 640*360</p>	
<p>Baboon 256*256</p>		<p>Camera 820*532</p>	
<p>Einstein 337*268</p>		<p>Jerash 800*469</p>	
<p>Taj-Mahal 1203*941</p>		<p>LOGO 271*186</p>	

Table 4.2 Embedding Tests

Image	Size	PSNR	MSE	H-CR	V-CR	D-CR	NPCR
Lena	255*255	60.471db	0.05	0.989	0.997	0.979	19.624%
Baboon	256*256	61.537db	0.04	0.965	0.958	0.948	13.359%
Einstein	337*268	62.619db	0.03	0.973	0.945	0.953	9.713%
MEU	640*360	66.936db	0.002	0.980	0.982	0.949	0.377%
Camera	820*532	68.662db	0.006	0.992	0.996	0.931	2.018%
Jerash	800*469	69.161db	0.007	0.932	0.956	0.897	2.33%
Taj-Mahal	1203*941	74.042db	0.003	0.998	0.996	0.989	0.769%

Different sizes of logos are embedded into various types of images with different sizes, and the important parameters are calculated, an example of the results summarized in table 4.2.

It is noticed that as the size of image increases, PSNR increases and MSE decrease. Also cross correlation shows little variations with image size.

More tests are done to investigate the conduct of proposed algorithm for different type of images. Here carrier images of HD (High definition) quality are used and compared

with results when normal quality is used. The same watermark logo with size 160*149 pixels is used for both cases and the results are listed in tables 4.3 and 4.4.

Table 4.3: Example of watermarking using HD carrier image Bmp types and JPG logo image 160*149 pixels.

Table 4.4: Example of watermarking using normal quality carrier image Bmp types and JPG logo image 160*149 pixels.

Table 4.3 HD Images

Image Name	Size	PSNR	MSE	NPCR	Correlation		
					H-CR	V-CR	D-CR
Istanbul	1500*1000	69.88607db	0.0066	2.01%	0.9994	0.9914	0.9952
Sydney	1650*1080	70.8253db	0.0056	1.6%	0.9998	0.9158	0.9304
Paris	1024*768	63.78894db	0.0527	8.16%	0.9698	0.9973	0.9821
Roma	1730*1100	67.45560db	0.0108	3.52%	0.9957	0.8976	0.8992
London	3318*2540	76.8237db	0.0012	0.40%	0.9995	0.9994	0.9943

Table 4.4 Normal Quality Images

Image		Correlation					
Name	Size	PSNR	MSE	NPCR	H-CR	V-CR	D-CR
Istanbul	550*338	56.45711db	0.0125	13.7%	0.9985	0.9693	0.87154
Sydney	300*168	∞	0.030	0.01%	0.9999	0.9518	0.9674
Paris	512*512	58.6859db	0.077	24.4%	0.9912	0.9573	0.8713
Roma	540*359	∞	0	0%	0.9881	0.9918	0.9159
London	337*268	56.1953db	0.1285	0.43%	0.9730	0.9459	0.9529

Table 4.3 and table 4.4 shows that the noise is less in HD images as compared with that in normal quality images, as the PSNR is still over 56dB for normal quality images, which is within acceptable level.

4.4 Short Definition of the Metrics

In the following a short definition of the metrics used and a sample figures one example for each metric which are PSNR, NPCR, MSE, H-CR, V-CR and D-CR for five deferent images with various sizes, with same logo as mentioned before in 4.3 section.

4.4.1 PSNR Test:

The Peak signal-to-noise ratio (PSNR) value was used to evaluate the quality of the watermarked images. In this section, five images with deferent resolutions used to measure

the PSNR test in encryption and embedding phases according to the equation 4.1(Bamatraf, A., Ibrahim, R., &Salleh, M. N. B. M. 2010, December).

$$PSNR = 10 \log_{10} \frac{Max^2}{MSE} \dots\dots\dots (4.1)$$

Where MAX is equal to 255 in grayscale images, and MSE is the mean square error.

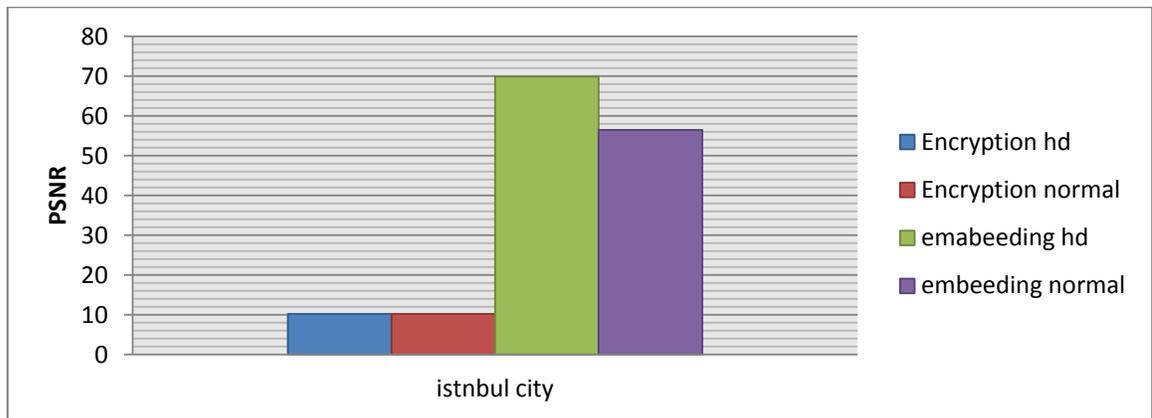


Figure 4.2 PSNR Istanbul City

4.4.2 NPCR Test

Number of change pixel ratio (NPCR),is the evaluation of indicators testing ability to resist differential attack, which refers to changes in the number of pixels of the cipher text after a pixel image changed. NPCR is applied on number if images, examples of them that showing results in figure 4.3 calculated according to the equation 4.2(Varkale, A., & Sharma,(2014, October).

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W*X} * 100\% \dots\dots\dots 4.2$$

When D(i, j) is the bipolar array defend by D= $\begin{cases} 0 & \text{if } C_1 = C_2 \\ 1 & \text{if } C_1 \neq C_2 \end{cases}$ C₁ and C₂ are Pixel value before and after changes.

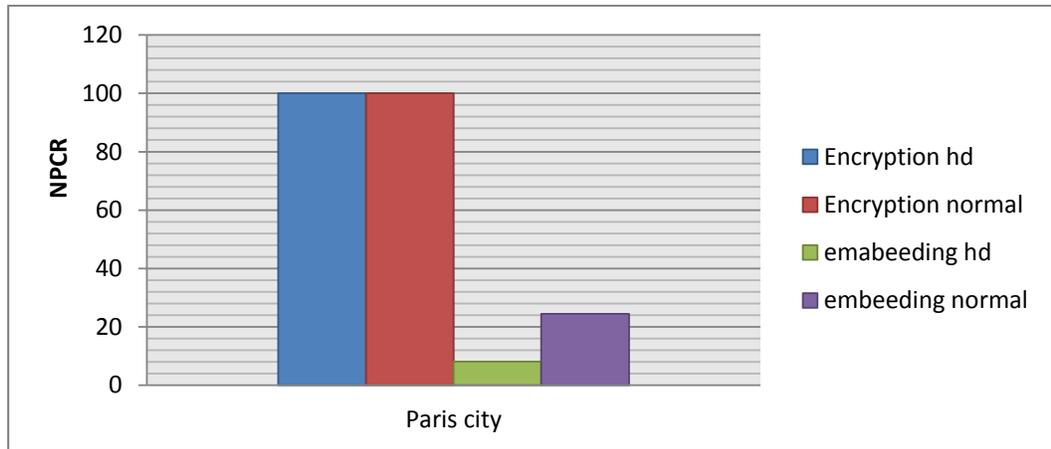


Figure 4.3 NPCR Paris City

4.4.3 MSE Test

Mean Squared Error (MSE) test is used to measure the difference between two digital images by measures the average of the squares of the errors. MSE corresponding to the expected value of the squared error loss or quadratic loss. It is defined in the equation4.4. (Anees, A., &Siddiqui, A. M. (2013, December)):

$$MSE = \frac{1}{n} \sum (X_i - X_i^*)^2 \dots\dots\dots 4.3$$

Where X_i and X_i^* are the original image and the watermarked image, respectively.

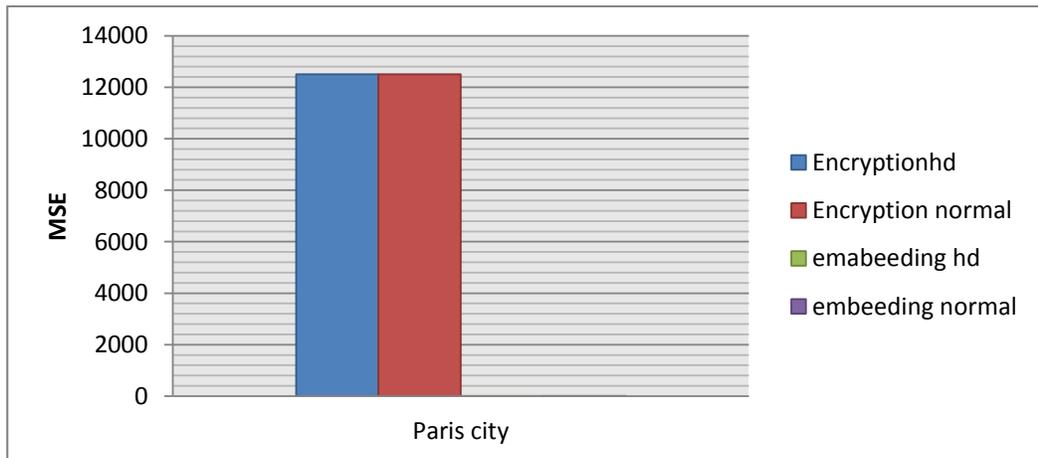


Figure 4.4MSE Paris City

4.4.4. Correlation test

A fundamental method used in determining the similarity between two images is the correlation analysis. Its take the horizontal, vertical and diagonal image pixels. The correlation of an image is given as. (Anees, A., &Siddiqui, A. M. 2013):

$$Corr = \sum \frac{(i-\mu_i)(j-\mu_j)p(i,j)}{\sigma_i\sigma_j} \dots\dots\dots 4.4$$

- i, j correspond to image pixels positions.
- P(i, j) is pixel value at ith row and jth column of digital image.
- π Is the variance. - σ Is the standard deviation.
- μ _ is the variance

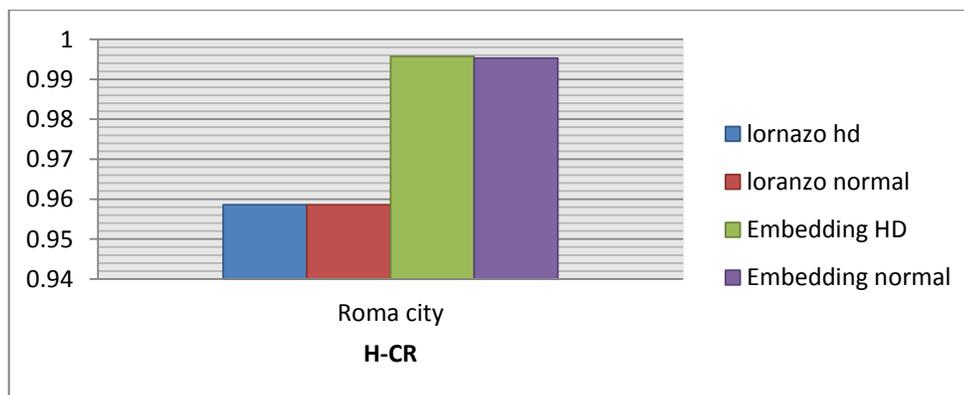


Figure 4.5 H-CR Roma city

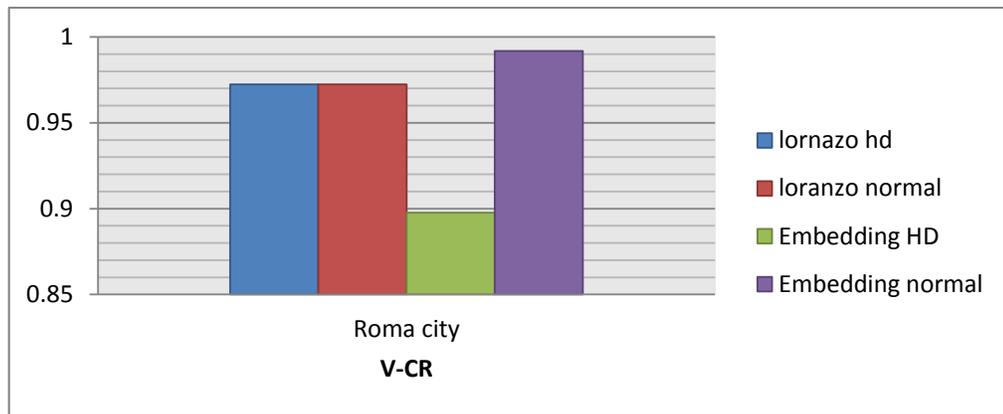


Figure 4.6 V-CR Roma city

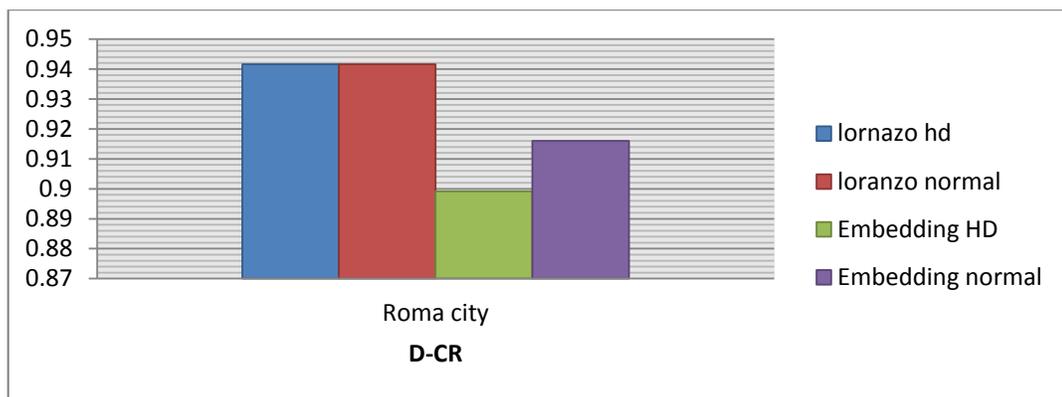


Figure 4.7 D-CR Roma city

4.5 Gray scale

Grayscale mean a collection of monochromic (gray) shades, starting from pure white on the lightest end to pure black. This contains brightness information and no color information. That is why grayscale images contain only shades of gray and no color. In this research some experiments implemented on grayscale images with deferent sizes, Picture (1) Camera with dimensions 820*532 and picture (2) Lion image an HD with dimensions 2560*1600, the PSNR, MSE, NPCR and correlation tests were measured for both pictures

1 and 2 and compared with number of previous related work. Figure 4.8 and 4.9 shows the PSNR and MSE tests:

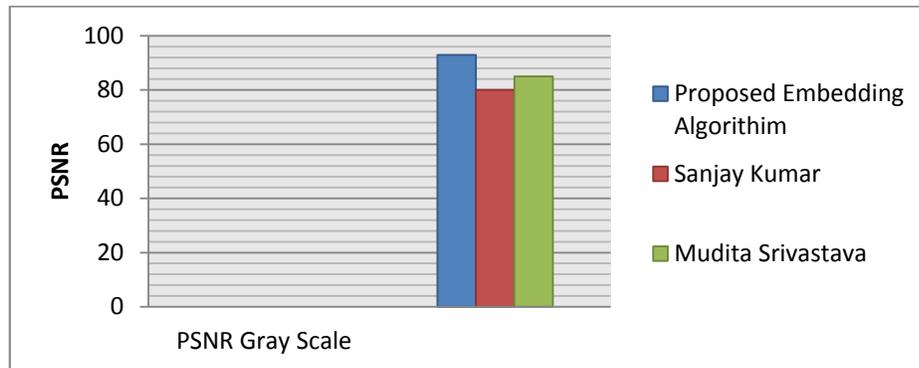


Figure 4.8 Gray Scale PSNR

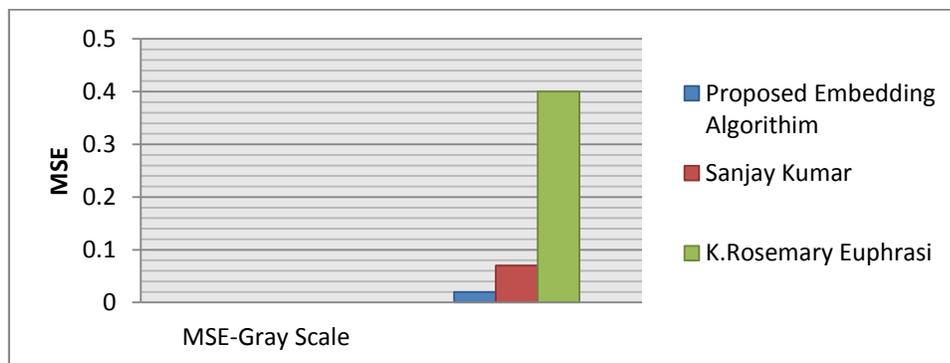


Figure 4.9 Gray Scale MSE

4.6 Summary of watermarking method results

The obtained results of the proposed watermarking technique in this thesis is listed in the table 4.5 together with the available reported result of previous works that implemented the watermark using spatial domain method. The table included calculated values for PSNR, MSE, NPCR, UACI, Entropy and H, V and D correlations for the proposed technique, however the results of some parameters are not available for the other listed works.

Table 4.5 Comparison with similar Techniques**(N/A: Not Available)**

	PSNR	MSE	H-CR	V-CR	D-CR	Entropy	NPCR	UACI
Proposed Technique	69.440dB	0.010	0.995	0.977	0.965	7.996	100%	33.225
(Behnia, S., et.al, 2008)	NA	NA	0.957	0.939	0.981	7.992	99.6%	33.4
(Bamatraf, A. 2010)	61.8427dB	N/A	N/A	N/A	N/A	N/A	N/A	N/A
(Sakthidasan, K., & Krishna, B. S. 2011)	NA	NA	0.997	0.935	0.918	NA	NA	NA
(Seyedzadeh, S. M., & Mirzakuchaki, S. 2012)	NA	NA	0.982	0.989	0.970	NA	NA	NA
(Anees, A., & Siddiqui, A. M. 2013)	66.2247 dB	10.542	0.899	0.893	0.895	7.4677	NA	NA
(Varkale, A & Sharma, 2014)	51.575dB	NA	NA	NA	NA	NA	99.1%	6.129
(Sruthi, N, Sheetal, et.al, 2014)	51.1255dB	0.2310	NA	NA	NA	NA	NA	NA
(Ghosh, Maity, et.al. 2015)	63.016dB	N/A	0.999	0.999	0.999	N/A	N/A	N/A
(Srivastava& Singh et.al. 2016)	63.31dB	N/A	1.000	1.000	1.000	N/A	N/A	N/A
(Mathur,&Murali babu et.al.2016)	51.693dB	N/A	0.665	0.667	0.669	N/A	N/A	N/A
(Dutta& Kumar, 2016)	69.2377dB	0.0078	N/A	N/A	N/A	N/A	N/A	N/A

Looking at the PSNR values obtain in table 4.5, it is found that its calculated value for the proposed technique was 67.44 dB, which is the highest as compared with other techniques listed in the table. This is also supported by having the lowest Mean Square Error, MSE of 0.01. Moreover, the entropy and Number Pixel Change Ratio, NPCR, also have shown slight improvement over other techniques. However, correlation between the original image and watermark image and Unified Average Change Intensity UACI calculation have exhibited some fluctuation, as in some cases, the value for the proposed technique is better , while it comes next to other technique in the cases.

Therefore, these results suggest that the proposed technique would be more suitable for applications that require better to noise ratio and entropy than other techniques.

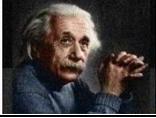
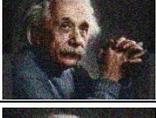
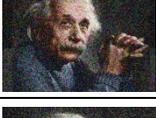
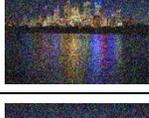
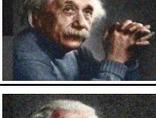
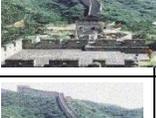
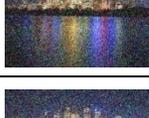
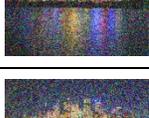
4.7 Performed Attacks

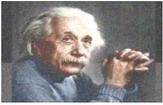
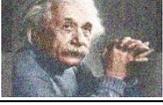
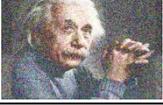
The noise may be considered as any degradation in the image signal caused by external disturbance. If an image is sent from one place to another, via internet, wireless transmission or through networked cable, errors are expected to occur in the image signal. These errors will appear on the image output in different ways depending on the type of disturbance in the signal. Usually one knows what type of errors to expect, and hence the type of noise on the image, therefore one can choose the most appropriate method in order to reduce these effects. In this part, various attacks were applied on different size watermarked images obtained by the proposed method. Although the LSB watermarking is known to be fragile, different types of attacks on the watermarked images were conducted to see if any possibility of watermark survival when different percentages of effects (Noise or Distortion)are used. All experiments have confirmed that the watermarks were lost. These attacks included the following:

4.7.1 Gaussian Noise

Gaussian noise is an idealized form of white noise, which is caused by random fluctuations in the signal. White noise can be observed when watching a television program that is slightly mistuned to a particular channel. This type of noise used in the proposed thesis, with mean value from 0 to 0.5 and variant value (0.01, 0.03, 0.05, 0.07, 0.09, and 0.11) on five images with deferent sizes as illustrated in table 4.6. The image sizes used in this test will be (Great Wall 450*64), (Einstein 337*268), (Fruit 3818*2540), (Sydney300*168), (Penguin 1024*768).

Table 4.6 addition of Gaussian Noise

Mean	Variant	Great Wall	Einstein	Fruit	Sydney	Penguin
0	0.01					
0	0.03					
0	0.05					
0	0.07					
0	0.09					
0	0.11					
0.1	0.01					
0.1	0.03					
0.1	0.05					
0.1	0.07					
0.1	0.09					
0.1	0.011					

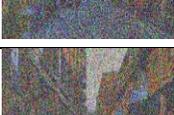
Mean	Variant	Great Wall	Einstein	Fruit	Sydney	Penguin
0.3	0.01					
0.3	0.03					
0.3	0.05					
0.3	0.07					
0.3	0.09					
0.3	0.011					
0.5	0.01					
0.5	0.03					
0.5	0.05					
0.5	0.07					
0.5	0.09					
0.5	0.011					

For all the experiment of table 4.6, no watermark was recovered, this confirms the fragile nature of LSB.

4.7.2 Localvar Noise

It is generated in Matlab as an additive Gaussian noise with mean 0 and variance as a function of image intensity. The localvar noise is implemented with various intensities (1-10, 1-30, 1-50, 1-70, 1-90, 1-110) on number of images with various sizes (Istanbul 55.*338), (London 600*375), (MEU 640*360), (Ishtar Gate 512*512), (Sydney 1650*1080), as shown in table 4.7

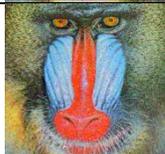
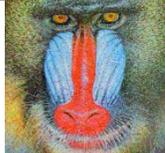
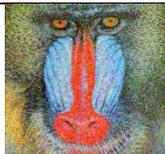
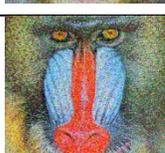
Table 4.7 addition of Localvar Noise

Intensity	Istanbul	London	MEU	Ishtar Gate	Sydney
1-10					
1-30					
1-50					
1-70					
1-90					
1-110					

4.7.3 Salt and Pepper Test

This noise is very common in digital watermarking. Images are corrupted with salt and pepper noise is degraded in only a few random pixel locations. Salt and pepper noise applied on watermarked images with deferent levels (0.01, 0.03, 0.05, 0.07, 0.09, 0.11), as shown in the table4.8 with image sizes (Bridge 256*256), (Cover 1024*768), (Jerash 800*469), (Lena 255*255), (Baboon 256*256).

Table 4.8 addition of Salt and Pepper Noise

Salt & Pepper	Bridge	Cover	Jerash	Lena	Baboon
0.01					
0.03					
0.05					
0.07					
0.09					
0.11					

4.7.4 Speckle Test

This noise is modeled by random values multiplied by pixel values of an image.

With mean 0 and default variance 0.04, the used image sizes were as follow: (Red 720*640), (Istanbul 550*338),(MEU 640*360), (Roma 1730*1100), (Sydney 1650*1080).

Table 4.9 Speckle Test

Speckle	Red	Istanbul	MEU	Roma	Sydney
0.1					
0.2					
0.3					
0.4					
0.5					

4.7.5 Poisson noise Test

It's one of watermark image attack types. It is built into the detector of light particles or the photon counter of any image acquisition devices, this noise is called Poisson or shot noise. A typical context of occurrence of Poisson noise is bio microscopic images where live samples are often observed at very low light levels, due to acquisition-time and photo toxicity constraints (Vonesch et al. 2006), (Luisier et al. 2010).

Table 4.10 Poisson noise Test

Baghdad Tower		 A photograph of the Baghdad Tower, a tall, slender tower with a green top, situated in a park-like setting with palm trees and a green lawn.
London Night		 A photograph of London at night, showing the city lights, the River Thames, and the London Eye Ferris wheel.
Mammon Tower		 A photograph of the Mammon Tower, a tall, slender tower with a blue top, situated in a cityscape.
Meddle East University		 A photograph of a modern university building with a large dome, situated in a landscaped area with palm trees and a paved walkway.
Roma		 A photograph of the city of Roma at night, showing the city lights, the River Tiber, and the St. Peter's Basilica dome.

4.7.6 Cropping:

It's the process of removing certain parts of a picture using an image editing software. Five times cropping are implemented for different image sizes in center crop, down-left, upper- left and down-right and upper right, as shown in the table 4.11.

Table 4.11Cropping

Cropping	Eiffel	Istanbul Masjid	Roma	Sydney	Taj-Mahal
Center					
Down Left					
Upper Left					
Down Right					
Upper Right					

4.7.7 Resizing

This test implemented on watermarked image and all the obtained results lead to damage in the watermark. By using 50%, 60%, 70%, 80% and 90% resizing on the original images (Babylon 900*506, London 1300*760, Petra 1200*630, Roma 1730*1100 and Taj-Mahal 1203*941).

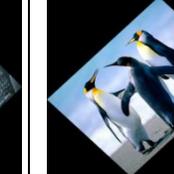
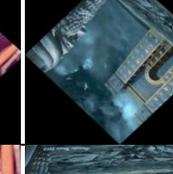
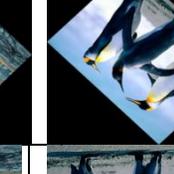
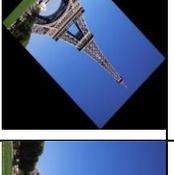
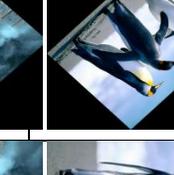
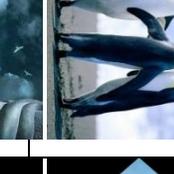
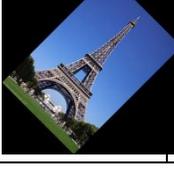
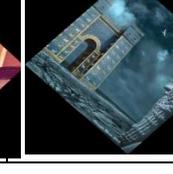
Table 4.12 Resizing

Resize	Babylon	London	Petra	Roma	Taj-Mahal
50%					
60%					
70%					
80%					
90%					

4.7.8 Rotating

Rotating test is applied on number of watermarked images in many anti clock wise (45, 90, 135, 180, 225, 270 and 315 degree), as showing table 4.13.

Table 4.13 Rotating

Rotate	Eiffel	Jarash	Lena	Ishtar Gate	penguin
45 degree					
90 degree					
135 degree					
180 degree					
225 degree					
270 degree					
315 degree					

4.8 PRNG's Tests

This section of the thesis discusses number of aspects for selecting and testing pseudorandom number generators. The outputs of the PRNG generators are used in this research for encryption and embedding of the watermark. Generators suitable for use in cryptographic and watermarking applications may need to meet stronger requirements than for other applications. Particularly, their outputs should be unpredictable in the absence of inputs knowledge. A set of statistical tests for randomness is implemented such as frequency, serial, run, poker and autocorrelation. The National Institute of Standards and Technology (NIST) believe that these procedures are useful in detecting deviations of a binary sequence from randomness.

The secret key length is an important factor of performance of the system, the change of the secret key length has a strong impact on the watermark efficiency.

4.8.1 Used PRNG Test Results

PRNGs are either secure but slow, or fast but insecure, besides they are either not efficient enough, have inherent flaws, or lack formal arguments for their randomness (Neuman and Voegeler, 2009). Many tests were developed to prove the randomness relying on probability as detailed by NIST (Lawrence E. Bassham, 2010). These tests includes the frequency (monobit), frequency within a Block test (series), Runs test, the Longest-Run-of-Ones in a Block test, Poker test, and the autocorrelation test.

A detailed explanation for each of the following randomness tests is available in NIST (Soto, J. 1999). For each table test, there is a pass mark or a value border, the calculated parameter for each test must not be more than it for randomness. The pass marks were fixed by NIST.

The tables below show few examples for the PRNGs test results. Using three different key lengths which are:

K1= “HELLO WORLD”. Sequence Length 552160 bits

K2= “AYSSER SHAMIL”. Sequence Length 59952 bits

K3= “GOD BLESS YOU”. Sequence Length 572160 bits

The K₁, K₂ & K₃, are only examples of the possible key seeds. From each key seed, sequences of random number are generated, and for each generated key, all the tests were done.

Table 4.14 to table 4.18 show only the testing of first key or the key seed they are only included for illustration. All subsequent keys are tested for randomness. If each generated key passes the test, it is accepted and used in the proposed water mark technique, otherwise it is rejected, and the next generated key is tested, and so on.

Frequency test: The main purpose of frequency test is to determine whether the number of 1's and 0's in the key sequence are approximately the same in all entire sequence. All subsequent tests depend on the passing of this test. In this test, if the key consists of n bits sequence and the number of 0's and 1's are represented by n₀ and n₁ respectively, then a chi-function value χ^2 is calculated by equation (1).

$$\chi^2 = \frac{(n_0 - n_1)^2}{n} \dots\dots\dots (1)$$

It is found by the probability theory and set by NIST that good sequence in the generated random number should have χ^2 values in the range $0 < \chi^2 < 3.84$ [J. M. Bahi, and C. Guyeux].

For example for K1 in Table 4.14,

$$\chi^2 = (286202 - 285958)^2 / 572160 = 0.010782381,$$

This value is < 3.84 , therefore this key passes the randomness test.

Any successively generated key will be tested first by this test before proceeding to other tests.

Table 4.14 Samples of frequency test for the PRNG

	K1	K2	K3
No. of 0's in the generated keys	286202	29995	286091
No. of 1's in the generated keys	285958	29957	286069
Pass Mark (Randomness criteria)	< 3.84	< 3.84	< 3.84
Computed Result	0.10782381	0.02408593	0.008459172259
Result	TEST PASSED	TEST PASSED	TEST PASSED

Serial test: The idea of this test is to determine whether the number of occurrences of the $2m$ -bit overlapping patterns is approximately the same as would be expected for a random sequence, where m is the length in bits of each block, and n is the

length in bits of the bit string or key. Therefore if the series test for the frequency of occurrence of sequences of two bits is to be tested, let n_{00} , n_{01} , n_{10} , and n_{11} by the number of 00, 01, 10, and 11 bits series combinations, respectively. Then chi-function χ^2 for this test is given by equation 2.

$$\chi^2 = \frac{4}{n-1}(n_{00}^2 + n_{01}^2 + n_{10}^2 + n_{11}^2) - \frac{2}{n}(n_1^2 + n_0^2) + 1 \quad (2)$$

Where n , n_0 , and n_1 are the same as in equation 1.

The criterion for good randomness sequence is $\chi^2 \leq 5.99$.

For example for K_1 in Table 4.15, where $n=276080$, $n_{00}=71623$, $n_{01}=71276$, $n_{10}=71680$, and $n_{11}=71501$, then substituting in equation 2 gives

$$\chi^2 = 1.34376$$

This value is < 5.99 , therefore this key passes the randomness test.

Table 4.15 Sample of the Serial test for the PRNG

	K1	K2	K3
Total no. of blocks	276080	29976	286080
No. of 00 blocks	71623	7586	71361
No. of 01 blocks	71276	7337	71454
No. of 10 blocks	71680	7486	71915
No. of 11 blocks	71501	7567	71350
Pass Mark (Randomness criteria)	< 5.99	< 5.99	< 5.99
Computed Result	1.34376	5.138243	3.00002
Result	TEST PASSED	TEST PASSED	TEST PASSED

Autocorrelation test: The purpose of this test is to check for correlations between the binary sequences generated. The calculation of the correlation between one random number and the preceding one, the statistical formula used for this test (Pareek, N. K, 2010):

$$Z = 2(A(d) - \frac{n-d}{2})/\sqrt{n-d} \dots\dots\dots (3).$$

Let d be a fixed integer $1 \leq d \leq \lfloor n/2 \rfloor$, where n is the size of binary sequence.

The table below shows the agree bits for correlated random numbers, the test pass mark is 3.498012, the results showed a suitable numbers for randomness.

Table 4.16 Samples of Correlation test for the PRNG

	K1	K2	K3
Agree bits for the random number	285668	30132	285214
Agree bits for the next random number	286492	29820	286946
Pass Mark (Randomness criteria)	< 3.498012	< 3.498012	< 3.498012
Computed Result	1.186691	1.62372	5.242990
Result	TEST PASSED	TEST PASSED	TEST PASSED

Run test: The focus of this test is the total number of runs in the sequence, where a run is an uninterrupted sequence of identical bits. A run of length k consists of exactly k identical bits and is bounded before and after with a bit of the opposite value. The purpose of the runs test is to determine whether the number of runs of ones and zeros of various

lengths is as expected for a random sequence. In particular, this test determines whether the oscillation between such zeros and ones is too fast or too slow. The *P-value* is calculated by

$$P\text{-value} = \operatorname{erfc} \left\{ \frac{|V_n(\text{obs}) - 2n\pi(1-\pi)|}{1\sqrt{2n\pi(1-\pi)}} \right\} \quad \text{equation 4 (Pareek, N. K, 2010):}$$

..... (4)

Where $V_n(\text{obs})$ is the total number of run across n and π is the pre-test proportion in the input sequence given by equation 5 (Pareek, N. K, 2010).

$$\pi = \frac{\sum_j \varepsilon_j}{n} \quad \text{..... (5)}$$

Where n the length of the bit string.

ε The sequence of bits as generated by the PRNG being tested; this exists as a global structure at the time of the function call; $\varepsilon = \varepsilon_1, \varepsilon_2, \dots, \varepsilon_n$.

For example, if $\varepsilon = 1001101011$, then $n=10$.

$$\pi = 6/10 = 3/5.$$

In this test used five different lengths for 0's (1, 2, 3, 4 and 5) and five different length of 1's (1, 2, 3, 4 and 5).

Table 4.17 Samples of the Run test for the PRNG

	K1	K2	K3
Run 0's of length 1	71483	7400	72005
Run 0's of length 2	35653	3701	35808
Run 0's of length 3	17694	1909	17872
Run 0's of length 4	8827	959	9001
Run 0's of length 5	4606	465	4364
Run 1's of length 1	71217	7451	71990
Run 1's of length 2	35829	3648	35830
Run 1's of length 3	17997	1906	17878
Run 1's of length 4	8930	952	8948
Run 1's of length 5	4330	471	4388
0's Pass Mark	< 27.3028	< 27.3028	< 27.3028
1's Pass Mark	< 28.5849	< 28.5849	< 28.5849
0's Computed Result	24.5393	10.31639	26.1400
1's Computed Result	14.06888	13.86042	12.47236
Result	TEST PASSED	TEST PASSED	TEST PASSED

Poker test: this test check certain sequences of five numbers at a time such as aaaaa, aaaab, aaabb, etc., based on hands in the poker game. In this test specified eight

blocks, to account the number of ones for each group, which are (0 1, 1 1, 2 1, 3 1, 4 1, 5 1, 6 1, 7 1 and 8 1).

This value is < 15.22407, therefore this key passes the randomness test, according to equation 5 (Pareek, N. K, 2010):

$$X^2 = \frac{2^m}{k} (\sum_{i=1}^{2^m} n_i^2) - k \dots\dots\dots (6)$$

Where m a positive integer, n is the size of binary sequence, $k = \lfloor n/m \rfloor$.

Table 4.18 Samples of the Poker test PRNG

	K1	K2	K3
Total Blocks	71520	59952	71520
Blocks has 0 1's	276	36	2848
Blocks has 1 1's	2284	227	2210
Blocks has 2 1's	7862	813	7740
Blocks has 3 1's	15502	1648	15597
Blocks has 4 1's	19554	2059	19772
Blocks has 5 1's	15766	1624	15675
Blocks has 6 1's	7790	833	7830
Blocks has 7 1's	2230	226	2151
Blocks has 8 1's	256	28	261
Pass Mark	< 15.22407	< 15.22407	< 15.22407
Computed Result	5.6596	2.61568	8.1840
Result	TEST PASSED	TEST PASSED	TEST PASSED

Chapter Five

Conclusions and Future Work

Chapter Five

Conclusions and Future Work

5.1 Conclusion

The work in this thesis included the development, design, implementation, and testing of an image watermarking technique. It is investigated for embedding logos in both color and grayscale images with different sizes. The proposed method produces watermarks that are imperceptible by visual inspection. The used technique is based on the spatial domain using least significant bit method together with the incorporation of two modified PRNG's for encrypting the logo images and selecting random pixels in the carrier image.

The propose multi pseudo random number watermarking technique has given PSNR values of over 67 dBs as compared with other existing techniques, which means it has given high perceptibility with low image quality degradation.

The used PRNG algorithm in this study is two produce high level contents authentication with less opportunity to be detected, i.e. a steganography stage is added to the embedding technique, which might be required in some special applications.

Measurements of PSNR, MSE, CR and NPCR for the proposed techniques have shown that it is more efficient than other and may replace them for better signal to noise ratio and entropy applications.

The value (∞) that is shown in some the results of the PSNR tests, means that the original image with deferent resolutions has no modifications (i.e. identical) on all image

pixels. These results are giving good impression for security applications because the secret information was embedded in perfect method.

Measurements of mean square error (MSE) show high error detection in the encrypted logo images which is required point, while in the embedding process, the MSE test was near enough to the perfect result. However, for correlation and the unified average change intensity UACI came next to many other techniques.

5.2 future works

Many suggestions can be improved the methods as future work, but the most significant suggestions would increase the watermarking system strength are:

- 1- Design, test and implement online chat system with image watermarking capabilities.
- 2- Develop the method in order to use Arabic text to hiding the data.
- 3- Improve system that can use a watermarking for 3D images.
- 4- 3D videos in watermark system maybe involved too.
- 5- Make the proposed thesis a hybrid system, which mean implement the spatial domain watermarking first, then other technique such as a discrete wavelet transform method with incorporation with PRNG's models.

References

- Abbasfard, M. (2009). *Digital image watermarking robustness: A comparative study* (Doctoral dissertation, TU Delft, Delft University of Technology).
- Al-Qudsy, Z. N. Y. (2011). *An Efficient Digital Image Watermarking System based on Contourlet Transform and Discrete Wavelet Transform* (Doctoral dissertation, Middle East University).
- Amirtharajan, R., Akila, R., & Deepikachowdavarapu, P. (2010). A comparative analysis of image steganography. *International journal of computer applications*, 2(3), 41-47.
- Anees, A., & Siddiqui, A. M. (2013, December). A technique for digital watermarking in combined spatial and transform domains using chaotic maps. In *Information Assurance (NCIA), 2013 2nd National Conference on* (pp. 119-124). IEEE.
- Bamatraf, A., Ibrahim, R., & Salleh, M. N. B. M. (2010). Digital watermarking algorithm using LSB. In *Computer Applications and Industrial Electronics (ICCAIE), 2010 International Conference* (pp. 155-159).
- Bartolini, F., Tefas, A., Barni, M., & Pitas, I. (2001). Image authentication techniques for surveillance applications. *Proceedings of the IEEE*, 89(10), 1403-1418.
- Behnia, S., Akhshani, A., Mahmodi, H., & Akhavan, A. (2008). A novel algorithm for image encryption based on mixture of chaotic maps. *Chaos, Solitons & Fractals*, 35(2), 408-419.
- Boyle, R., & Parvin, B. (2008). *Advances in Visual Computing: 4th International Symposium, ISVC 2008, Las Vegas, NV, USA, December 1-3, 2008, Proceedings* (Vol. 1). Springer Science & Business Media.

Celik, K., & Kurt, E. (2016, June). A new image encryption algorithm based on lorenz system. In *Electronics, Computers and Artificial Intelligence (ECAI), 2016 8th International Conference on* (pp. 1-6). IEEE.

Celik, K., & Kurt, E. (2016, June). A new image encryption algorithm based on lorenz system. In *Electronics, Computers and Artificial Intelligence (ECAI), 2016 8th International Conference on* (pp. 1-6). IEEE.

Chandramouli, R., Memon, N., &Rabbani, M. (2002). Digital watermarking.*Encyclopedia of Imaging Science and Technology*.

Chhibber, N., &Patra, G. (2015, August). Synchronization of chaos in multiple three-dimensional chaotic maps and its application in cryptography. In *Technology Management and Emerging Technologies (ISTMET), 2015 International Symposium on* (pp. 355-359). IEEE.

Chopra, D., Gupta, P., Sanjay, G., & Gupta, A. (2012). LSB based digital image watermarking for gray scale image. *IOSR Journal of Computer Engineering*, 6(1), 36-41.

Cox Ingemar J., Matthew L. Miller and Jeffrey A. Bloom, "*Handbook of Digital Watermarking*", Morgan Kaufmann Publishers, Inc., San Francisco, 2001.

Cox, I. J., Miller, M. L., & Bloom, J. A. (2000). Watermarking applications and their properties. In *Information Technology: Coding and Computing, 2000. Proceedings. International Conference on* (pp. 6-10). IEEE.

Cox, I., Miller, M., Bloom, J., Fridrich, J., &Kalker, T. (2007). *Digital watermarking and steganography*. Morgan Kaufmann.

Coxy, I. J., Kiliany, J., Leightonz, T., &Shamoony, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Trans. on Image Processing*, 6(12), 1673-1687.

Dasgupta, K., Mandal, J. K., &Dutta, P. (2012). Hash based least significant bit technique for video steganography (HLSB). *International Journal of Security, Privacy and Trust Management (IJSPTM)*, 1(2), 1-11.

Delaigle, J. F. (2000). *Protection of intellectual property of images by perceptual watermarking* (Doctoral dissertation, Ph. D Thesis submitted for the degree of Doctor of Applied Sciences, UniversiteCatholique de Louvain, Belgium).

Deshpande, S. S. P. A. *Steganographic Tools for BMP Image Format*. (2011).

Digital Watermarking", Morgan Kaufmann Publishers, Inc., San Francisco, 2001.

Fraćzek, W., Mazurczyk, W., & Szczypiorski, K. (2012). Multi-level steganography: Improving hidden communication in networks. *Journal of Universal Computer Science (J. UCS)*, 18(14), 1967-1986.

Ghosh, S., De, S., Maity, S. P., & Rahaman, H. (2015). A novel dual purpose spatial domain algorithm for digital image watermarking and cryptography using Extended Hamming Code. In *Electrical Information and Communication Technology (EICT), 2015 2nd International Conference on* (pp. 167-172). IEEE.

Goyal, R., & Kumar, N. (2014). LSB Based Digital Watermarking Technique. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, 3(9), 15-18.

Johnson, N. F., Duric, Z., Jajodia, S., & Memon, N. (2001). Information hiding: steganography and watermarking—attacks and countermeasures. *Journal of Electronic Imaging*, 10(3), 825-826.

Khanzode, P., Ladhake, S., & Tank, S. (2011). Digital watermarking for protection of intellectual property. *International Journal of Computational Engineering & Management*, 8-12.

Komatsu, N., & Tominaga, H. (1988). Authentication system using concealed images in telematics. *Memoirs of the school of Science and Engineering, Waseda University*, 52, 45-60.

Kumar, S., & Dutta, A. (2016). A novel spatial domain technique for digital image watermarking using block entropy. In *Recent Trends in Information Technology (ICRTIT), 2016 International Conference on* (pp. 1-4). IEEE.

Langelaar, G. C., Setyawan, I., & Lagendijk, R. L. (2000). Watermarking digital image and video data. A state-of-the-art overview. *IEEE Signal processing magazine*, 17(5), 20-46.

Maaita, A. A., & Al_Sewadi, H. A. (2015). Deterministic Random Number Generator Algorithm for Cryptosystem Keys. World Academy of Science, Engineering and

Technology, *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, 9(4), 943-948.

Maes, M., Kalker, T., Linnartz, J. P., Talstra, J., Depovere, F. G., &Haitsma, J. (2000). Digital watermarking for DVD video copy protection. *IEEE Signal Processing Magazine*, 17(5), 47-57.

Mathur, S., Dhingra, A., Prabukumar, M., Agilandeewari, L., &Muralibabu, K. (2016). An efficient spatial domain based image watermarking using shell based pixel selection. In *Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on*(pp. 2696-2702). IEEE.

Paar, I. C., &Pelzl, I. J. (2010). Stream Ciphers. In *Understanding Cryptography* (pp. 29-54). Springer Berlin Heidelberg.

Pareek, N. K., Patidar, V., & Sud, K. K. (2010). A Random Bit Generator Using Chaotic Maps. *IJ Network Security*, 10(1), 32-38.

Petitcolas, F. A., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding-a survey. *Proceedings of the IEEE*, 87(7), 1062-1078.

Potdar, V., & Chang, E. (2004). Visibly invisible: Ciphertext as a steganographic carrier. In *Proceedings of the 4th International Network Conference (INC2004)* (pp. 385-391).

Provos, N., &Honeyman, P. (2003). Hide and seek: An introduction to steganography. *IEEE security & privacy*, 99(3), 32-44.

Radharani, S., &Valarmathi, M. L. (2010). A study on watermarking schemes for image authentication. *International Journal of Computer Applications*, 2(4), 24-32.

Saini, L. K., &Shrivastava, V. (2014). A survey of digital watermarking techniques and its applications. *arXiv preprint arXiv:1407.4735*.

Sakthidasan, K., & Krishna, B. S. (2011, June). A new chaotic algorithm for image encryption and decryption of digital color images. *International Journal of Information and Education Technology*, 1(2), 137.

Seyedzadeh, S. M., & Mirzakuchaki, S. (2012). A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map. *Signal Processing*, 92(5), 1202-1215.

Sharma, M. K., & Gupta, P. C. (2012). A Comparative Study of Steganography and Watermarking". *International Journal of Research in IT & Management (IJRIM)*, 2(2), 2231-4334

Simpson J. and E. Weiner, editors, 2000. "Oxford English Dictionary", New York:Oxford University Press.

Singh, A. K., Sharma, N., Dave, M., & Mohan, A. (2012, December). A novel technique for digital image watermarking in spatial domain. In *Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on* (pp. 497-501). IEEE.

Singh, P., & Chadha, R. S. (2013). A survey of digital watermarking techniques, applications and attacks. *International Journal of Engineering and Innovative Technology (IJEIT)*, 2(9), 165-175.

Soto, J. (1999). Statistical testing of random number generators. In *Proceedings of the 22nd National Information Systems Security Conference* (Vol. 10, No. 99, p. 12). Gaithersburg, MD: NIST.

Srivastava, M., Singh, H. M., Gupta, M., & Raj, D. (2016). Digital watermarking using spatial domain and triple DES. In *Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on* (pp. 3031-3035). IEEE.

Sruthi, N., Sheetal, A. V., & Elamaran, V. (2014, April). Spatial and spectral digital watermarking with robustness evaluation. In *Computation of Power, Energy, Information and Communication (ICCPEIC), 2014 International Conference on* (pp. 500-505). IEEE.

Sun, Y., Zhan, R., Han, Z., & Lin, Q. (2015, November). A Watermark Algorithm for Image Content Authentication and Correcting Errors in Terms of Pixels. In *P2P*,

Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2015 10th International Conference on (pp. 760-765). IEEE.

Tao, H., Chongmin, L., Zain, J. M., & Abdalla, A. N. (2014). Robust image watermarking theories and techniques: A review. *Journal of applied research and technology*, 12(1), 122-138.

Techniques, S. (2002). Their use in an Open-Systems Environment-Bret Dunbar. *The Information Security Reading Room, SANS Institute*.

Varkale, A., & Sharma,(2014, October) N. Reversible Data Hiding in Encrypted Image using Chaotic Algorithm.*International Journal of Emerging Technology and Advanced Engineering*.

Wong, P. W., & Delp, E. J, (2000). Security and watermarking of multimedia contents II(San Jose CA, 24-26 January 2000). In SPIE proceedings series. SPIE.

Wu, Y., Noonan, J. P., & Aghaian, S. (2011). NPCR and UACI randomness tests for image encryption. *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, 31-38.

Yang, X., & Guo, C. (2016). Parallel spatial-domain liver segmentation of CT abdominal images. In *Intelligent Control and Information Processing (ICICIP), 2016 Seventh International Conference on* (pp. 173-178). IEEE.

Appendices

Appendix A

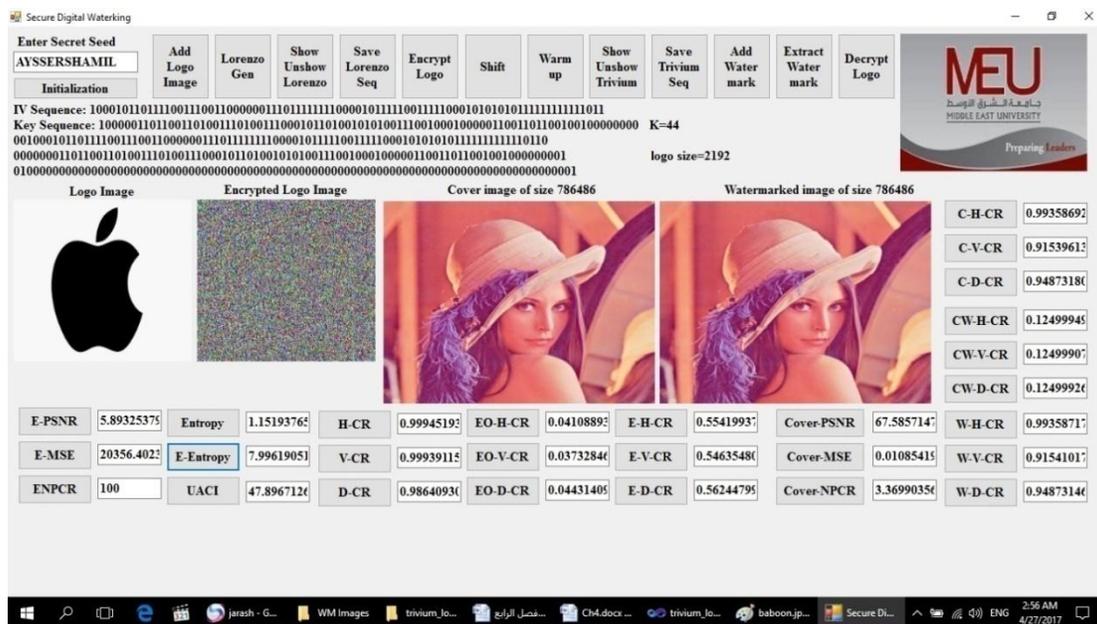
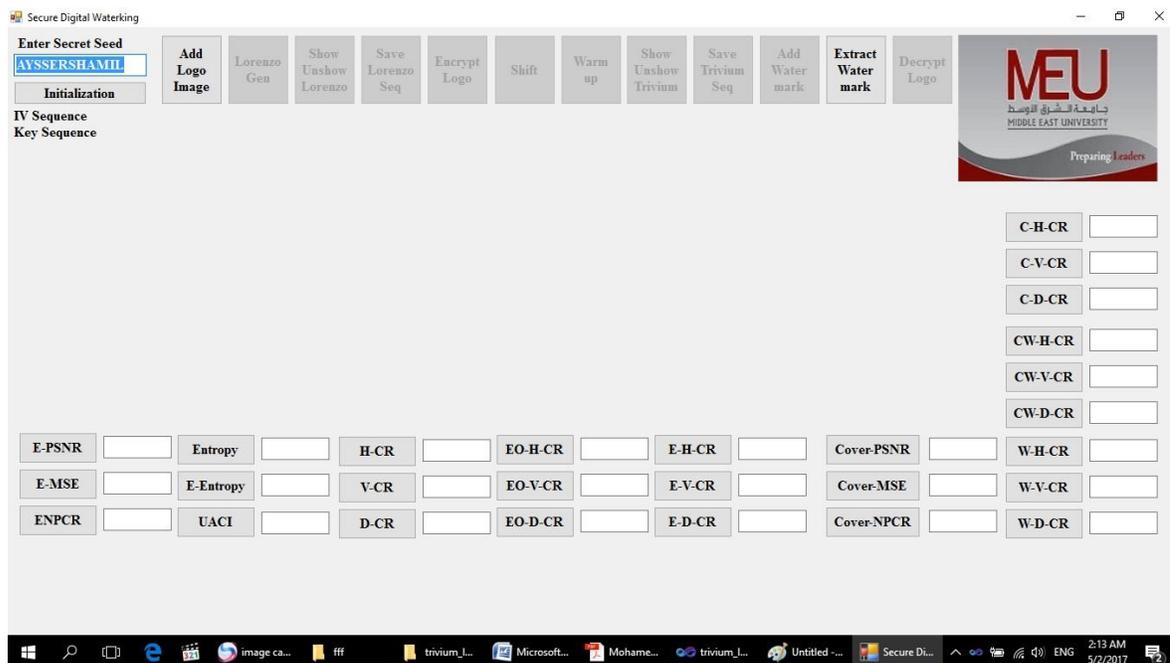
The used images in this research.

Name and Size	Image	Name and Size	Image	Name and Size	Image
Eiffel 400*600		Bridge 256*256		Lena 225*255	
Istanbul 550*338		Red 720*640		Baboon 256*256	
Istanbul 1500*100		Camera 820*532		Lion 1560*1600	
Roma 1730*1100		Roma 540*359		Einstein 337*268	
Sydney 1650*1080		Sydney 300*168		Fruit 3818*2540	
London 1300*760		London 600*375		Petra 1200*630	
Baghdad T 564*702		Jerash 800*469		Penguin 1024*768	

Name and Size	Image	Name and Size	Image	Name and Size	Image
Mammon Tower 736*476		Taj-Mahal 1203*941		Camera Man 256*256	
MEU 640*360		Babylon 900*506		Cover 1024*768	
Ishtar Gate 512*512		Jordan Map 100*865		Great Wall 450*648	
Used Logo's					
Tornado 160*149		A 139*160		Linux 150*180	
MEU 160*10		Baghdad College 160*150			
Apple 271*186		F 626*626			

Appendix B

Graphical User Interface (GUI) for used algorithm and tests implementations.



Appendix C

Test results and compressions Charts.

