T. R.
VAN YUZUNCU YIL UNIVERSITY
INSTITUTE OF NATURAL AND APPLIED SCIENCES
ELECTRICAL AND ELECTRONICS ENGINEERING
DEPARTMENT

IMAGE ENCRYPTION BASED ON HAAR WAVELET TRANSFORMATION AND RC4 ALGORITHM

M.Sc. THESIS

PREPARED BY: Elham Tahsin YASIN
SUPERVISOR: Assoc. Prof. Dr. Rıdvan SARAÇOĞLU

VAN-2017

T. R.
VAN YUZUNCU YIL UNIVERSITY
INSTITUTE OF NATURAL AND APPLIED SCIENCES
ELECTRICAL AND ELECTRONICS ENGINEERING
DEPARTMENT

IMAGE ENCRYPTION BASED ON HAAR WAVELET TRANSFORMATION AND RC4 ALGORITHM

M.Sc. THESIS

PREPARED BY: Elham Tahsin YASIN

VAN-2017

THESIS ACCEPTANCE AND APPROVAL PAGE

This thesis entitled "**Image Encryption Based on Haar Wavelet Transformation and RC4 Algorithm**" presented by Elham Tahsin YASIN under the supervision of Assoc. Prof. Dr. Rıdvan SARAÇOĞLU in the Department of Electrical and Electronics Engineering has been accepted as an M. Sc. thesis according to Guidelines of Graduate Higher Education on 28/07/2017 with unanimity of vote's members of the jury.

Chair: Assoc. Prof. Dr. Mustafa TÜRK Signature:

Member: Assoc. Prof. Dr. Rıdvan SARAÇOĞLU Signature:

Member: Assist. Prof. Dr. Özkan ATAN Signature:

This thesis has been approved by the committee of The Institute of Natural and Applied Science on 02/08/2017 with decision number 2017/35-1

Signature

Prof. Dr. Ersun SENSOY

Director of the Institute

THESIS STATEMENT

All information presented in the thesis obtained in the frame of ethical behavior and academic rules, In addition, all kinds of information that does not belong to have been cited appropriately in the thesis prepared by the thesis writing rules.

.....

Elham Tahsin YASIN

ABSTRACT

IMAGE ENCRYPTION BASED ON HAAR WAVELET TRANSFORMATION AND RC4 ALGORITHM

YASIN, Elham Tahsin
M. Sc. Thesis, Electrical-Electronics Engineering
Supervisor: Assoc. Prof. Dr. Rıdvan SARAÇOĞLU
July 2017, 59 Pages

Security and privacy of information or data nowadays have turned into a critical concern; progressed techniques for secure transmission and recovery of digital images are progressively required for various military, restorative, country security, and different applications. Different sorts of strategies for increment security information or data as of now is created, one basic path is by cryptographic systems. Keep up the security of the message by changing information or data into an alternate frame, so the message can't be perceived. The basic idea behind the thesis is to optimize security by combining the two algorithms namely Haar wavelet transformation and RC4 encryption algorithm. Haar wavelet transformation is used to compress the image for simplicity and estimate high-speed performance we can send it over the network quickly. RC4 encryption is utilized to encrypt the image for image security and transform image safely and securely over any network.

Keywords: Cryptography, Haar transformation, Image compression, Image encryption, Information security, RC4 stream cipher.

ÖZET

HAAR DALGACIK DÖNÜŞÜMÜ VE RC4 ALGORİTMASINA DAYALI GÖRÜNTÜ ŞİFRELEME

YASIN, Elham Tahsin
Yüksek Lisans Tezi, Elektrik-Elektronik Mühendisliği Anabilim Dalı
Tez Danışmanı: Doç. Dr. Rıdvan SARAÇOĞLU
Temmuz 2017, 59 Sayfa

Günümüzde bilgi ve verilerin güvenliği, gizliliği kritik bir meseleye dönüşmüştür. Güvenli iletim için ilerlemiş teknikler, ileri düzeydeki resimlerin düzeltilmesi, çeşitli askeri ve onarmaya yönelik uygulamalar, ülke güvenliği ve farklı uygulamalar için devamlı olarak gereklidir. Günümüzde bilgi güvenliğinin güçlendirilmesi için kulanılan farklı yollardan en temeli şifreleme sistemleridir. Bilgileri veya verileri anlaşılmayacak şekilde başka bir yapıya dönüştürerek mesajın güvenliği sağlanır. Bu tezdeki temel fikir, Haar dalgacık dönüşümü ve RC4 şifreleme algoritması olmak üzere iki algoritmayı birleştirerek güvenliği optimize etmektir. Haar dalgacık dönüşümü, görüntüyü sıkıştırmak, sadeliği sağlamak ve yüksek hızlı performans elde etmek için kullanılır. Ayrıca ağ üzerinden hızlı gönderilebilir. RC4 şifreleme ise görüntüyü herhangi bir ağ üzerinden güvenli ve sağlam bir şekilde şifrelemek ve göndermek için kullanılır.

Anahtar Kelimeler: Bilgi güvenliği, Görüntü sıkıştırma, Görüntü şifreleme, Haar dönüşümü, Kriptografi, RC4 akış şifresi.

ACKNOWLEDGMENTS

This study was intended to determine RC4 encryption algorithm combined with Haar wavelet transformation method to encrypt and compress images so that it can be easily and safely send over the network.

Before sending thanks to anybody I need to express gratitude toward Allah for blessing me and gift me with all these resources, favors and empowering me to finish this thesis.

I would like to appreciate my supervisor Assoc. Prof. Dr. Rıdvan SARAÇOĞLU for encouraging and guiding me during the experimental methods and executing of my study and all of his supports and information that gave me.

My endless appreciation would be for my parents who have supported through all aspects of my life and raised me with their love and encouragement, without them I would never have enjoyed so many opportunities.

Also, I appreciate my sisters and brother for their supports and encouragements during my study. Finally, my regards and respect would be to my friends and mates for their help and supports.

July 2017

Elham Tahsin YASIN

CONTENTS

Page

Page

LIST OF TABLES

Table **Page**

LIST OF FIGURES

Figure **Page**

Figure **Page**

SYMBOLS AND ABBREVIATIONS

Some abbreviations used in this study are presented below.

Symbols	Description
ψ	Psi – Waveform symbol

Abbreviations	Clarification
3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
ATM	Automate Teller Machine
DCST	Discrete Cosine Stock-well Transform
DES	Data Encryption Standard
DH	Diffie-Heliman
DNA	Deoxyribonucleic Acid
DRBG	Deterministic Random Bit Generator
DSA	Digital Subtraction Angiography
DWT	Discrete Wavelet Transforms
ECC	Elliptic Curve Cryptography
FPGA	Field-Programmable Gate Array
HDWT	Haar Discrete Wavelet Transforms
HWT	Haar Wavelet Transforms
IDEA	International Data Encryption Algorithm
JPEG	Joint Photographic Experts Group
KSA	Key Scheduling Algorithm
MSE	Mean Square Error
MSVD	Multi-resolution Singular Value Decomposition

PC	Personal Computer
PNG	Portable Network Graphics
PRGA	Pseudo-Random Generation Algorithm
PRNG	Pseudo-Random Number Generator
PSNR	Peak Signal to Noise Ratio
RAM	Random-Access Memory
RC4	Rivest Cipher 4
RC6	Rivest Cipher 6
RSA	Rivest, Adi Shamir, and Leonard Adleman
S/MIME	Secure/Multipurpose Internet Mail Extensions
SIM	Subscriber Identification Module
SSH	Secure Shell Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security

LIST OF APPENDIX

APPENDIX **Page**

1. INTRODUCTION

The fast development of PC networks permitted extensive files, for example, advanced pictures, to be effortlessly transmitted over the web. Information security is a vital issue and encryption is one of the guaranteed securities in communication and image repository. However, the majority of the accessible encryption calculations are utilized for content information. Because of huge information size and continuous limitations, calculations that are important for textual information may not be appropriate for sight and sound information (Dixit et al., 2012). Encryption will be the procedure of transforming the data with protected its security. With the immense development of PC networks and the most recent advances in computerized innovations, an enormous amount of computerized information is being traded over different sorts of networks. It is frequently true that a considerable some portion of this data is either classified or private. Subsequently, extraordinary security methods have been utilized to give the required assurance. In the computerized world today the security of digital images has turned out to be increasingly critical considering of the quick development of the Internet. Starting late The security of computerized pictures has advanced in more idea, and to upgrade the security of these pictures an extensive variety of image encryption techniques have been prepared (Dixit et al., 2012).

Image encryption assumes a basic part in the section of data masking. Image encryption method arranged information unreadable. Hence, no hacker or meddler, among other server overseers and others, approach the main message or any other sorts of transmitted data through open systems, for example, the web (Aashish, 2014). The essential aim of keeping pictures ensured is to look after confidentiality, integrity, and authenticity. Different techniques are available for making images secure and one technique is encryption.

Image encryption strategies attempt to change over an image using an algorithm to an unreadable form that is difficult to get it. Then again, image decoding recovers the original image from the encoded one. There are different image encryption frameworks to

encode and decode information, and there will be no absolute encryption calculations fulfill the different image sorts. Image encryption has utilization in multimedia systems, medical imaging, soldierly communication, Internet communication, etc. In order to transmit images securely, a number of encryption strategies have been proposed. One of the schemes is RC4 encryption algorithm (Patel and Belani, 2011).

With the techniques of image encryption, image compression is used with algorithms to maintain security and safety for image and decrement size of it. Image compression is removing the redundant data. There are several methods used for compression images among them Haar wavelet transformation is one of the most used mathematical methods for compressing the images.

1.1. Aim of Thesis

The basic idea behind the thesis is to first compress the image so that we can send it over the network quickly and encrypt it so that we can transmit it over any network securely and safely. Security was optimized by combining the two algorithms namely Haar wavelet transformation for the compression and RC4 encryption algorithm into one application. The Haar wavelet is used for the best performance in terms of computational time, high-speed computation, its memory efficient and simplicity. Furthermore, RC4 is the developed form of the RSA. Since RC4 is a symmetric stream cipher, very quick and used for secure communications we prefer it as the encryption algorithm for images.

1.2. Outline of Thesis

The rest of the thesis is organized into 5 sections: Section one contains the problem and objectives of the study, the main aim of doing the study with a brief introduction about the encryption and compression methods. While section two; explains the works and activities that have linked with this review. Lots of studies and works are done with different-different algorithms. In section three the background to encryption and methodology was described within the materials and methods with explanations of all

materials that used in this research including compression method, encryption algorithm, and statistical analyses done for the study. Implementation of the study is given in section four, that all results and executions are included in this section, also with the result of the practical works. Finally, section five concludes this research and mentions the future works also.

2. LITERATURE SURVEY

This section describes the works and projects which are related to this study. Throughout the years a wide range of strategies has been presented for image encryption for secure transmission of images over networks. Some related works are clarified below:

Kumar et al. (2014), proposed an image encryption algorithm based on Haar wavelet transformation and DNA technique, which the first image is compressed using Haar transformation and then the image is encrypted by DNA algorithm. Wavelets are mathematical functions; a wavelet transformation changes over information from the spatial into the frequency space and afterward stores every segment with the comparing coordinating determination scale. DNA algorithm used for further encrypting the image, this method changes the data into an unreadable form. For compressing the image GUI was designed. In DNA technique initials a mystery key produced utilizing DNA succession and particular arithmetic operations. At that point, every pixel value of the image experiences the encryption procedure utilizing the key and DNA calculation strategies.

Zhang et al. (2012), worked on a cryptosystem based on DNA subsequence. Here only DNA sub-sequence operation is used hence it does not have any match with traditional DNA approach for encryption. Location and the value of the pixel of the image are scrambles using logistic chaotic map. Encryption process based on this approach has good security and efficiency. DNA subsequence operation is based on horizontal, or the length of the subsequences selected is longer. The horizontal correlation was improved by changing the lengths of DNA subsequences from each bit-plane.

in this paper Zeghid et al. (2007), worked on The Advanced Encryption Standard (AES), the encryption study was analyzed and added a key stream generator (A5/1, W7) to AES for guarantee enhancing the encryption execution. The key stream creator has an essential impact on the encoding.

Dixit et al. (2012), worked around the binary code of the pixel values for a color image, it was separated and changed concurring to the indexed 8-bit key which takes place by the permutation of all 8 continuous pixels. The image is further isolated into pieces

which are shifted accordingly. To further authorize the encryption another strategy is annexed to it which requires a 43 digit key. The encryption takes an average of 10 rounds in which two keys are utilized, both of which were gotten from the 43 digits indexed key. The proposed encryption process takes place in two stages and utilizes two keys: which outcome in a total of (8!*256^43) combinations. This large key size makes a brute force attack repetitious as it is wanted that half the keys are attempted before a person can split the key.

In this paper, Sasidharan and Philip (2011), prepared a quick partial image encoding framework used Discrete Wavelet Transform with RC4 Stream Cipher. The approximation matrix (lowest frequency band) was encoded in this study, utilizing the stream cipher as it purchases a majority of the picture's data. The encoding time is decreased by encoding just the section of the image and by shuffling the remain of the image preserved a great level of security. The current way to deal with lessening the computational pre requisites for huge volumes of images is the current encryption. The algorithm is expressed as a quick image encryption calculation, according to the chosen encryption of certain part of the image (lowest frequency band). PSNR values of the encrypted images are less and are incomplete able to statistical attacks.

Mousa and Hamad (2006), worked on breaking down the RC4 parameters have shown that the speed of encoding or disentangling time is particularly related to the encryption key length and to the data record measure if the data is sufficiently huge. Information sort is additionally vital since picture information needs more opportunity to be prepared than content or sound information primarily as indicated by the bigger record estimate. This relationship had been changed into conditions to show these connections thus might be used to anticipate the execution of the RC4 under various conditions.

Rathee and Vij (2014), proposed a study that presents discrete Haar wavelet transform (DWT) for image compression. The image compression methods are extensively characterized into two classes depending on if or not a correct reproduction of the original image could be remade using the compacted image. Haar discrete wavelet transform (HDWT) was utilized to compress the signal. The prepared compression techniques

significantly upgrade the time execution of the framework. Also, the proposed Compression technique is understandable and computationally less difficult.

A paper proposed by Tamboli and Udupi (2013), namely an efficient calculation scheme for 2D-Haar wavelet transformation in image compression. The prepared study objected at growing computationally productive and compelling calculations for lossy picture compression using wavelet techniques. The study is especially focused towards wavelet image compression utilizing Haar Transformation with an idea to decrease the computational needs by implementing various compressions beginning for the wavelet coefficients and these results obtained in a fraction of seconds and in this way to enhance the nature of the reconstructed picture. The promising outcomes got concerning reconstructed images quality and in addition the safeguarding of significant picture detail.

A chronological review demonstrating the cryptanalysis of RC4 stream cipher was presented in the study. Different weaknesses of the RC4 algorithm summarized. To build up a safe RC4 algorithm it was set up that imaginative research endeavors are required, which can take the weaknesses of RC4, such as biased bytes, key collisions, and key recovery attacks on WPA (Jindal and Singh, 2015).

In another paper Jolfaei (2011), proposed Image Encryption Using Chaos and Block Cipher, a picture encryption plot in view of a merge of chaotic baker's map and modified version of S-AES was prepared. Baker's map utilized to create a permutation matrix. The paper contains a pixel shuffler unit and a block cipher unit. Pixel shuffling widens the diffusion property and expands vertical, horizontal and diagonal difference of two adjacent pixels.

A new image encryption scheme was presented by Guan et al. (2005). Shuffling the places and altering the gray values of image pixels are mixed all the while to guarantee the security of the strategy. The encryption algorithm contains two stages: Firstly, the pixels of the original image are shuffled using Arnold cat map. After the pixel values of the shuffled image are encoded by Chen's chaotic framework. Shuffled image is encoded by the pre-handled signal pixel by pixel. The calculation has three benefits: (1) the method has a good key space against all types of brute- force attacks; (2) the cipher-image has a decent measurable property; (3) the encoding method is exceptionally delicate to the secret keys.

Ahadpour et al. (2016), acquainted another technique to image encryption. The proposed method used the flexibility of the gradient Haar wavelet transform and chaotic property of the rational order chaotic maps to produce the encrypted images. Haar wavelet is one of the best scientific apparatuses in image cryptography and examination. This strategy utilizes linearity properties of the scaling capacity of the gradient Haar wavelet and deterministic behaviors of rational order chaotic maps in order to create encrypted images with the high-security factor.

In this paper, Hashim and Neamaa (2014), exhibited a specific public key cryptosystem expressed with the assistance MATLAB Program to be utilized over images called the ElGamal Cryptosystem. Hence the ElGamal cryptosystem is utilized over a primitive foundation, the free GNU Privacy Guard software of a huge prime in messages encoding, late forms of Pretty Good Privacy (PGP), and other cryptosystems. This study presents a modification of this cryptosystem by using it over gray and color images. That would be by transforming an image into its matching matrix using MATLAB Program after that applying the encryption and decoding algorithms on it.

Gao and Chen (2008), presented another picture encoding framework, which utilizes a picture add up to rearranging network to rearrange the places of picture pixels and after that uses a hyper chaotic framework to befuddle the connection between the plain picture and the encoded picture. The exploratory outcomes exhibit that the recommended encryption calculation of the picture has the upsides of vast key space and high security.

In this research, Tedmori and Al-Najdawi (2014), proposed a novel lossless symmetric key encoding/decoding system. In the prepared algorithm, the image is changed into the frequency area utilizing the Haar wavelet transform, after that the picture sub-bands are encoded in such way that certifications a safe, dependable, and an unbreakable shape. The encryption includes dispersing the recognizable recurrence information in the picture utilizing a reversible weighting factor among whatever remains of the frequencies. The calculation is intended to rearrange and switch the indication of every recurrence in the changed picture before the picture frequencies are changed back to the pixel space. The outcomes demonstrate an aggregate deviation in pixel esteems between the first and encoded picture. The decoding calculation turns around the encryption procedure and

reestablishes the picture to its unique shape. The proposed calculation is assessed utilizing standard security and factual techniques; results present that the prepared work is impervious to most known assaults and more secure than different calculations in the cryptography area.

Kumar and Vaish (2017), taken a shot at another image encoding and decoding algorithm in light of Multi-resolution Singular Value Decomposition (MSVD) and Discrete Cosine Stock-well Transform (DCST) prepared. Firstly an original image is changed in DCST domain and after that decomposed into four sub bands utilizing MSVD; every four sub-bands are later decomposed into four sub-images concurring to their inputs and hide by the parameters created by MSVD. A number of bands of DCST were utilized, Course of action of MSVD sub-bands, the arrangement of different sub-images got from MSVD sub-bands, qualities, and course of action of a 4×4 matrix created by MSVD and the arrangement of hidden sub-images as encoding and decoding keys.

Taqieddin et al. (2015), dealt with another equipment execution of the RC4 calculation utilizing FPGA. RC4 is a known stream cipher, which is generally utilized as a part of numerous security conventions and models because of its speed and adaptability. The primary thought of this outline is the utilization of a dual-port block RAM in the FPGA keeping in mind the end goal to better use the accessible rationale and memory assets. Merged with a new pipelined equipment execution, the new plan accomplishes better execution. The plan is portrayed utilizing Verilog HDL and synthesized and executed utilizing Xilinx ISE good for various FPGA devices. Synthesis comes about demonstrate that the proposed configuration accomplishes higher proficiency than past usage by lessening the region while maintaining a suite throughput/LUT ratio. The proposed configuration is likewise more effective as far as power utilization.

3. MATERIALS AND METHODS

3.1. Information Security

Nowadays, information security is becoming more important in data storage and transmission. Images are widely used in different-different processes. Therefore, the security of image data from unauthorized users is important. The essential expectation of keeping images protected is to maintain confidentiality, integrity, and authenticity (Kumar et al., 2014). Different techniques are available for making images secure and one technique is cryptography (encryption). Cryptography is science to look after the security of the message by changing data or information (Irfan et al., 2015). Image encryption plays an important role in the field of information hiding. Image encryption method prepared information unreadable. Therefore, no hacker or eavesdropper, including server administrators and others, have access to an original message or any other type of transmitted information through public networks such as the internet (Aashish, 2014).

Generally, Encryption is a procedure that transforms an image into a cryptic image by using a key. Furthermore, a user can retrieve the initial image by applying a decryption method on the cipher image, which is usually a reverse execution of the encryption process (Kumar et al., 2014). The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted via the Internet or other computer networks. Modern encryption algorithms play a vital role in the security assurance of IT systems and communications as they can provide not only confidentiality but also the following key elements of security: Authentication, the origin of a message can be verified. Integrity, proof that the contents of a message have not been changed since it was sent. Non-repudiation, the sender of a message cannot deny sending the message.

3.2. Image

Nowadays Digital Images find a lot of applications almost in all the fields, for e.g. Information Hiding, Communication etc. Security of these images is very important. Image encryption is one method of providing security to digital images. An image is nothing more than a two dimensional signal of numbers ranging between 0 and 255. It is defined by the mathematical function f(x, y) where x and y are the two coordinates horizontally and vertically. The value of f(x, y) at any point gives the pixel value at that point of an image (Anonymous, 2017).

Pixels are the fundamental components of an image, so keeping in mind the end goal to encrypt an image; we need to encode the data covered up in every pixel. Pixel's position esteems can likewise be utilized for encryption reason (Kumar et al., 2014). Pixel is the littlest component of a picture. Every pixel relates to any one value. In an 8-bit gray-scale picture, the value of the pixel is in the range of 0 and 255. The value of a pixel at any point corresponds to the force of the light photons striking by then. Every pixel stores a value corresponding to the light power at that specific area (Anonymous, 2017).

The very first image that has been sent over the wire was from London to New York by using a submarine cable (Figure 3.1). The image took three hours to reach.

Figure 3.1. First sent image (Anonymous, 2017).

We have characterized an image as a two-dimensional signal or matrix. At that point, all things considered, the quantity of PEL would be equivalent to the number of lines increase with the number of columns. It's mathematically expressed as in "Equ. 3.1":

Entire Number of Pixels= Number of Rows i × Number of Columns (j) (3.1)

For image dimensions, we can determine it as represented in "Equ. 3.2" image dimensions depend upon three points; the number of rows, the number of columns, and the number of bits per pixel (Anonymous, 2017).

Dimension of an image= rows × columns × bit per pixels (3.2)

3.3. Image Compression

Image compression is a technique used for representing the image using data which are repeated in the image several times (data redundancy). For example in a black and white image, 0000011111 can be represented as (0, 5) (1, 5). 0 is repeated five times and so on. This technique is called run length coding. Similarly, there are several techniques available to represent an image with a minimum number of bits. Image compression aims to remove the redundancies and generates an image with less number of bits per pixel (Wei, 1997). Image compression techniques fall into two categories, namely, lossless and lossy. In lossless techniques, the image can be reconstructed after compression, without any loss of data in the entire process. Lossy techniques, on the other hand, are irreversible, which results in loss of data (Sethi et al., 2011). In image compression, a small loss in quality is usually not noticeable. Discrete cosine and wavelet transform based methods (jpeg, jpeg2000) are mainly used for lossy image compression. There are other methods for lossless compression based on entropy coding as an example PNG is lossless image compression file format.

In image compression, the size in bytes of a graphics file is minimizing without lowering the quality of the image to an unacceptable level. More images stored in a given

amount of disk or memory space when the file size reduced. Likewise, it increases the time needed for images to be sent over the internet or downloaded from pages. If we ask why is image compression important? It's because it goes to save space (storage, bandwidth) and time. When trying to see an image from the Internet on a cell phone you may need to hold up 5 seconds to download a crude one or 1 second while downloading a compressed one. This adds to client experience and makes your information arrangement less expensive. When you hire a virtual server where you have your site with images you commonly pay for a repository and the measure of information the server sends and gets over a detailed period. So you can serve more compressed images to your watchers without paying more for the used transmission capacity (Suliga, 2015).

As an answer to the question, why an image can be compressed? The reason is that the correlation between one pixel and its neighbor pixels is very high, or we can say that the values of one pixel and its adjacent pixels are very similar. Once the correlation between the pixels is reduced, we can take advantage of the statistical characteristics and the variable length coding theory to reduce the storage quantity. There are a lot of relevant processing methods being proposed. The best-known methods are (predictive coding, orthogonal transform, and subband coding) (Wei, 1997).

Image data compression is concerned with minimizing the number of bits required to represent an image. Minimizing the number of bits can be simplified as this example repetition of messages to reduce the probability of errors in transmission, in data in a way which makes image reconstruction possible. Image compression algorithms calculate which data needs to be kept in order to reconstruct the original image and therefore which data can be "thrown away". By removing the redundant data, the image can be represented in a smaller number of bits, and hence can be compressed (Gaur, 2014).

3.4. Image Encryption

Cryptography got its name from a Greek word called "Kryptos" which implies "Hidden Secrets". Cryptography is the practice and study of concealing information. It is the Art or Science of changing over a plain knowable data into an unknowable data and

once more retransforming that message into its original structure using a number of different mathematical algorithms or techniques (Arur, 2013). This technique is utilized when secret statements are sent from one person to another in excess of the communication line. It gives Confidentiality, Integrity, and Accuracy. The learning of securing the protection of data throughout communication under opposed situations is cryptography. Presently, cryptography assumes an essential part in the growing information technologies and quickly increasing computer network transmissions. Current cryptographic techniques are based theoretic or logarithmic ideas (Jolfaei, 2011).

3.4.1. History of encryption

The use of encryption is nearly as old as the art of communication itself. As early as 1900 BC, an Egyptian scribe used non-standard hieroglyphs to hide the meaning of an inscription. In a time when most people couldn't read, simply writing a message was often enough, but encryption schemes soon developed to convert messages into unreadable groups of figures to protect the message's secrecy while it was carried from one place to another. The contents of a message were reordered (transposition) or replaced (substitution) with other characters, symbols, numbers or pictures in order to conceal its meaning (Gaur, 2014).

In 700 BC, the Spartans wrote sensitive messages on strips of leather wrapped around sticks. When the tape was unwound the characters became meaningless, but with a stick of exactly the same diameter, the recipient could recreate (decipher) the message. Later, the Romans used what's known as the Caesar Shift Cipher, a monoalphabetic cipher in which each letter is shifted by an agreed number. So, for example, if the agreed number is three, then the message, "Be at the gates at six" would become "eh dw wkh jdwhv dw vla". Possibly the most famous implementation of a polyalphabetic substitution cipher is the Enigma electro-mechanical rotor cipher machine used by the Germans during World War Two (Gaur, 2014).

It was not until the mid-1970s that encryption took a major leap forward. Till now, all encryption schemes used the same secret for encrypting and decrypting a message: a

symmetric key. In 1976, B. Whitfield Diffie and Martin Hellman's paper *New Directions in Cryptography* solved one of the fundamental problems of cryptography, namely how to securely distribute the encryption key to those who need it. This breakthrough was followed shortly afterward by RSA, an implementation of public-key cryptography using asymmetric algorithms, which ushered in a new era of encryption (Gaur, 2014).

3.4.2. How we use encryption today

Until the arrival of the Diffie-Hellman key exchange and RSA algorithms, governments and their armies were the only real users of encryption. Encryption is generally utilized in numerous computer applications to protect data in transit and at rest. Client inclusion in the encryption process may change for every application. However, Diffie-Hellman and RSA led to the broad use of encryption in the commercial and consumer realms to protect data both while it is being sent across a network (data in transit) and stored, such as on a hard drive, smartphone or flash drive (data at rest). Devices like modems, set-top boxes, smart cards and SIM cards all use encryption or rely on protocols like SSH, S/MIME, and SSL/TLS to encrypt sensitive data. In some applications of secure Web browsing using Secure Socket Layer (SSL) or Transport Layer Security (TLS) protocols, the use of encryption may be transparent to users. In other implementations, users may be required to enter a password to encrypt or decrypt the protected data if the cryptographic key is derived from the password (Stine and Dang, 2011).

Email can be encrypted by the sender and then decrypted by the intended recipient using Secure/Multipurpose Internet Mail Extensions (S/MIME). E-mail can be read only by the sender and the intended recipient. Internet Protocol Security (IPsec) is a suite of network layer security protocols frequently used to establish virtual private networks. They enable only the two ends of a communication in a computer network to understand the encrypted messages exchanged between them. The SSL protocol and its successor, TLS, are the primary end-to-end security protocols used to protect information traversing the Internet. The most common usage scenario for these protocols is a Web browser, acting as a client for the human user, interacting with a Web server. Using SSL and TLS, encrypted

messages between a Web browser and a Web server cannot be decrypted by any unauthorized party (Stine and Dang, 2011).

Encryption is used to protect data in transit sent from all sorts of devices across all sorts of networks, not just the Internet; every time someone uses an ATM or buys something online with a smartphone, makes a mobile phone call or presses a key fob to unlock a car; encryption is used to protect the information being relayed. Digital rights management systems, which prevent unauthorized use or reproduction of copyrighted material, are yet another example of encryption protecting data (Rouse, 2014).

3.4.3. How encryption works

Data often referred to as plaintext, is encrypted using an encryption algorithm and an encryption key. This process generates cipher-text that can only be viewed in its original form if decrypted with the correct key. Decryption is simply the inverse of encryption, following the same steps but reversing the order in which the keys are applied. Today's encryption algorithms are divided into two categories: symmetric and asymmetric. Some classified into three groups: symmetric encryption, asymmetric encryption, and those used in cryptographic hash functions (Rouse, 2014).

Symmetric key cryptography (secret key cryptography) uses the same key, or secret, for encrypting and decrypting a message or file (Figure 3.2). The most widely used symmetric-key cipher is AES, which was created to protect government classified information. Symmetric-key encryption is much faster than asymmetric encryption, but the sender must exchange the key used to encrypt the data with the recipient before he or she can decrypt it. This requirement to securely distribute and manage large numbers of keys means most cryptographic processes use a symmetric algorithm to efficiently encrypt data but use an asymmetric algorithm to exchange the secret key (Rouse, 2014). The advantage is simpler and faster. The disadvantage is less secured. Some of the encryption algorithms that use symmetric keys include AES (Advanced Encryption Standard), Blowfish, DES (Data Encryption Standard), 3DES, IDEA, Serpent, RC6, and Twofish.

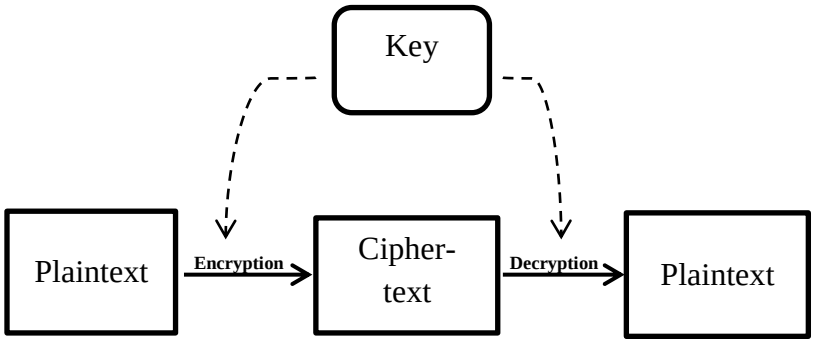


Figure 3.2. Symmetric key cryptography.

Asymmetric key cryptography, also known as public-key cryptography, uses two different but mathematically linked keys, one public and one private (Figure 3.3). The public key can be shared with everyone, whereas the private key must be kept secret. RSA is the most widely used asymmetric algorithm, partly because both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute provides a method of assuring not only confidentiality but also the integrity, authenticity, and non-reputability of electronic communications and data at rest through the use of digital signatures. Two of the most widely used asymmetric key algorithms are RSA, DH, ElGamal, ECC, and DSA (Rouse, 2014).

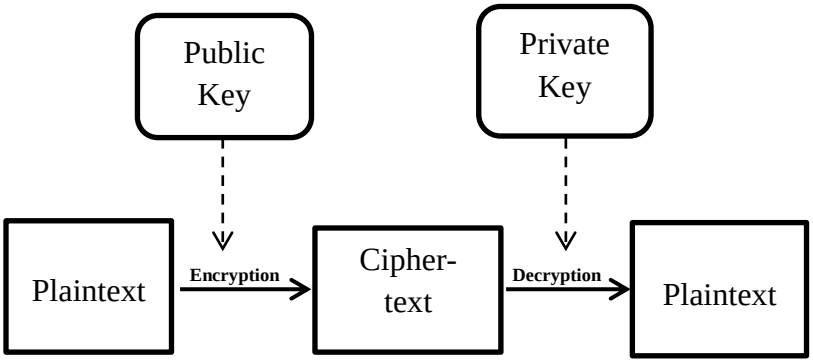


Figure 3.3. Asymmetric key cryptography.

Image encryption techniques try to convert an image to another one that is hard to understand. On the other hand, image decryption retrieves the original image from the

encrypted one. There are various image encryption systems to encrypt and decrypt and to transmit images securely (Patel and Belani, 2011). Image encryption has applications in multimedia systems, medical imaging, military communication, Internet communication, etc.

Encryption or Enciphering is the process of converting plain text into an unintelligible format (cipher text) is called Encryption, which cannot be easily understood by anyone except authorized parties. The encryption function requires two inputs, plain-text, and a cryptographic key in order to output cipher-text (Arur, 2013), as shown in (Figure 3.4).

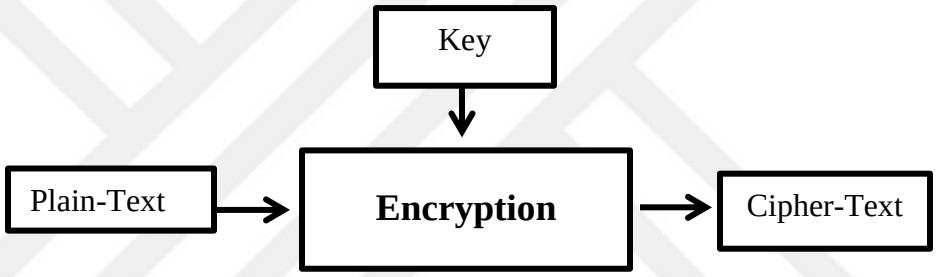


Figure 3.4. Encryption diagram.

Decryption or Deciphering is the process of converting cipher text into a plain text is called Decryption. Decryption is the process of converting Cipher-text again into its original form. The decryption function requires two inputs, cipher-text and a cryptographic key in order to output original form (Arur, 2013), as shown in (Figure 3.5).

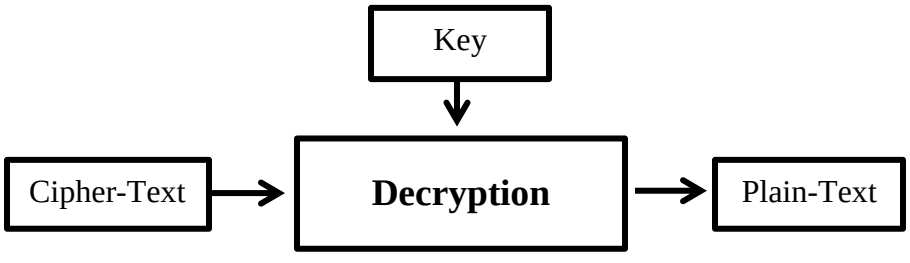


Figure 3.5. Decryption diagram.

The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted via the Internet or other computer networks. Modern encryption algorithms play a vital role in the security assurance of IT systems and communications as they can provide not only confidentiality (Rouse, 2014) but also (authentication, integrity, and non-repudiation). Short explanations for the security key elements are presented as the following:

- Authentication: the origin of a message can be verified.
- Integrity: proof that the contents of a message have not been changed since it was sent.
- Non-repudiation: the sender of a message cannot deny sending the message.

Image encryption is different from text encryption because of the larger scale of data, higher redundancy and stronger correlation of pixels in images. The secret part of encryption algorithm is the key used for encryption and decryption process. The key is made of random bits and it can be any value. Each algorithm makes use of key space. The key is constructed using random values within the key space of algorithm. The larger the key space, larger the values of keys we can use to show differ keys (Abhinandan and KN, 2011).

The strength of an encryption largely depends on two components: 1) the cipher and 2) the length of the key. A cipher is simply a method for encrypting (and decrypting) messages(Villanueva, 2015).

A cipher is simply a method for encrypting (and decrypting) messages. These ciphers can be classified into two groups: stream ciphers and block ciphers. A block cipher is an encryption algorithm that encrypts a fixed size of n-bits of data - known as a block - at one time. The usual sizes of each block are 64 bits, 128 bits, and 256 bits. A stream cipher is a method of encrypting text (to produce cipher-text) in which a cryptographic key and algorithm are applied to each binary digit in a data stream, one bit at a time. A stream cipher is one of the simplest methods of encrypting data where each bit of the data is sequentially encrypted using one bit of the key (Figure 3.6). It’s the generalization of the one-time pad and initialized with short key (Bradford, 2016). The key is stretched into long key-stream. Key-stream is used like a one-time pad. The main advantage of the stream cipher is that it is faster and more suitable for streaming application but its main

disadvantage is that it is not suitable for some architecture. One example of the stream cipher method is the RC4 technique.

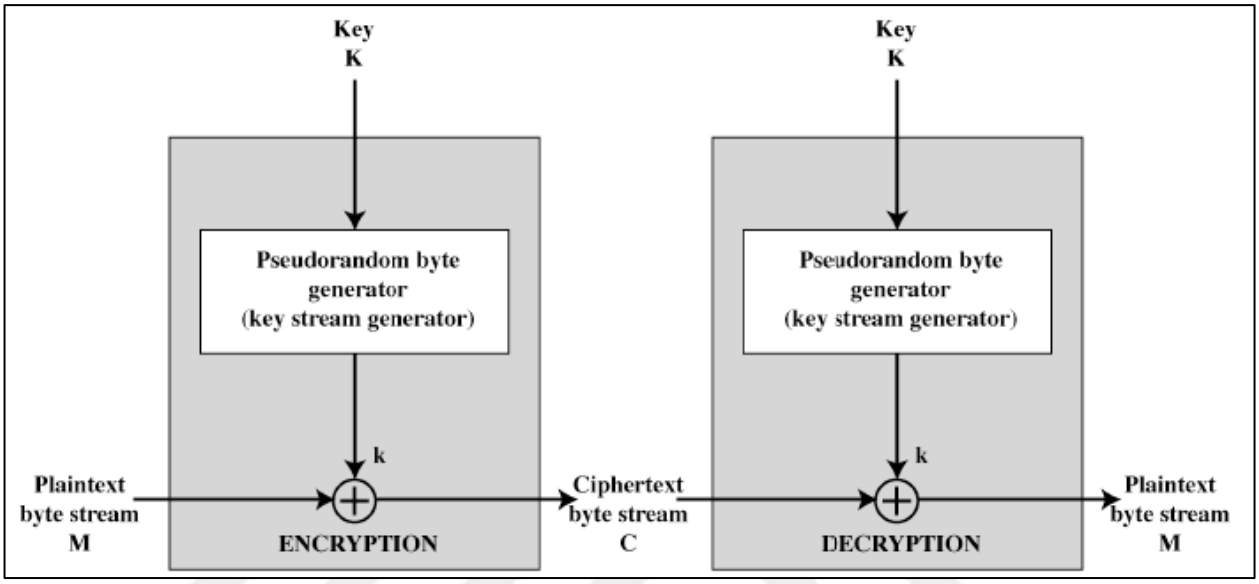


Figure 3.6. Stream Cipher Diagram (Stallings, 2005).

In cryptography, key size or key length is the number of bits in a key. Used by a cryptographic algorithm (such as a cipher). Keys are the number of binary digits, or bits, in an encryption algorithm. Key length is sometimes used to measure the relative strength of the encryption algorithm (i.e., the longer the key length, the more difficult the key is to decode).

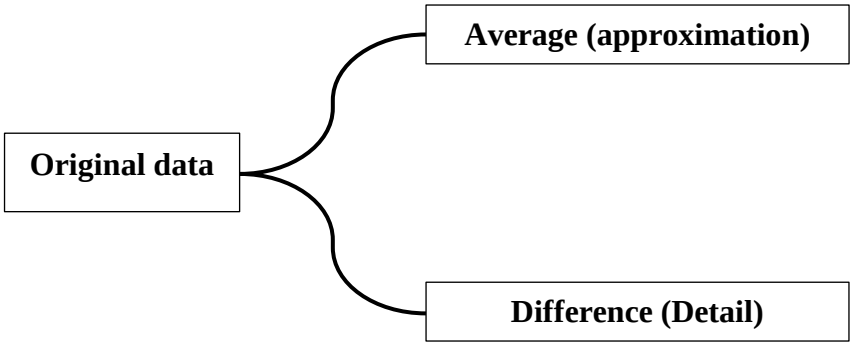
3.5. Haar Wavelet Transformation

The computer is becoming more and more powerful day by day. As a result, the use of digital images is increasing rapidly. Data requires considerable storage capacity and transmission bandwidth, compression is one of the ways. First, we compress the image using Haar wavelet transformation. Wavelets are a set of mathematical basis function. When approximating a function in terms of wavelets, the wavelet basis functions are selected according to the function being approximated. Wavelets employ a dynamic set of

basic functions that represents the input function in the most efficient way. Thus wavelets are able to provide a great deal of compression and are therefore very popular in the fields of image and signal processing. A Wavelet transformation converts data from the spatial into the frequency domain and then stores each component with a corresponding matching resolution scale. By applying the Haar wavelet transform we can represent this image in terms of a low-resolution image and a set of detail coefficients. Haar Transform is nothing but averaging and differencing.

Haar wavelet transformation proposed in 1909 by Hungarian mathematician Alfred Haar. Wavelets are mathematical functions that were developed for sorting the data by frequencies. The wavelets have been applied in many fields such as image compression, data compression, encrypted data and a lot more. The word "wavelet" stands for an orthogonal basis of a certain vector space. Orthogonality means the original signal is split into a low and a high-frequency part and filters enabling the splitting without duplicating information (Raviraj and Sanavullah, 2007). The main advantage of wavelet basis is that they despite having irregular shape are able to perfectly reconstruct functions with linear and higher order polynomial shapes, such as rectangle, triangle, second order polynomials, etc.

Haar wavelet transformation may be considered to simply pair up input values, storing the difference and passing the sum. This process is repeated recursively, pairing up the sums to provide the next scale. Finally resulting in differences and one final sum. With Haar, high compression ratio and high PSNR values are provided. It makes the basic transformation from the space domain to a local frequency domain. HT decomposes a discrete signal into two sub-signals of half its length (Average and Difference).



The Haar function is “Equ. 3.3”

$$\psi(t) = \begin{cases} 1 & t \in [0, \frac{1}{2}) \\ -1 & t \in [\frac{1}{2}, 1) \\ 0 & t \notin [0,1) \end{cases} \quad (3.3)$$

Haar Transform is nothing but averaging and differencing. This can be explained with a simple 1D image with eight pixels

[3 2 -1 -2 3 0 4 1]

By applying the Haar wavelet transform we can represent this image in terms of a low-resolution image and a set of detail coefficients. So the image after one Haar Wavelet Transform is:

Transformed coefficient = [2.5 -1.5 1.5 2.5]

Detail Coefficients = [0.5 0.5 1.5 1.5]

The detail coefficients are used in the reconstruction of the image. Recursive iterations will reduce the image by a factor of two for every cycle. In 2D wavelet transformation, structures are defined in 2-D and the transformation algorithm is applied for row first, and then for the column.

The array sizes are expressed in powers of two. Mathematically, the original resolution of the images is converted into the next larger power of two, and the array sizes are initialized accordingly. The Haar transform separates the image into high frequency and low-frequency components (Sethi et al., 2011). For the first cycle, the transformation algorithm is first run along the row (Figure 3.7).

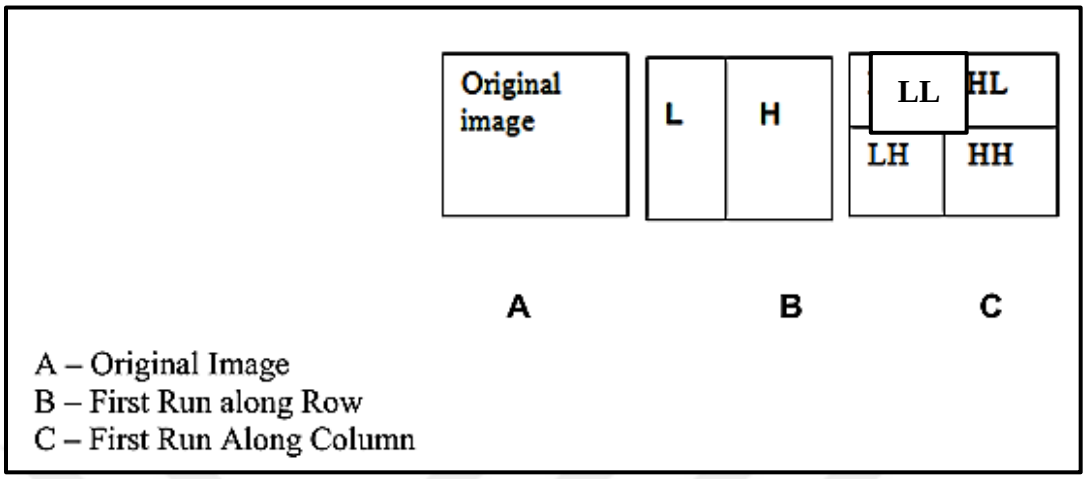


Figure 3.7. Haar wavelet diagram (Sethi et al., 2011).

The image array is split into two halves containing the transformed data and the detail coefficients. The transformed data coefficients are the results of the low-pass filter while the detail coefficients are the results of the high-pass filter. After transforming the image in the row, the image is then transformed along the column (Sethi et al., 2011). This process repeats till two iterations. A program was written in MATLAB and the output is given in the implementation and results section. The reason wavelets are being used more and more is that they are capable of deconstructing complex signals into basis signals of finite bandwidth and then reconstructing them again with the very little loss of information. The structure of Haar will be shown as (Figure 3.8).

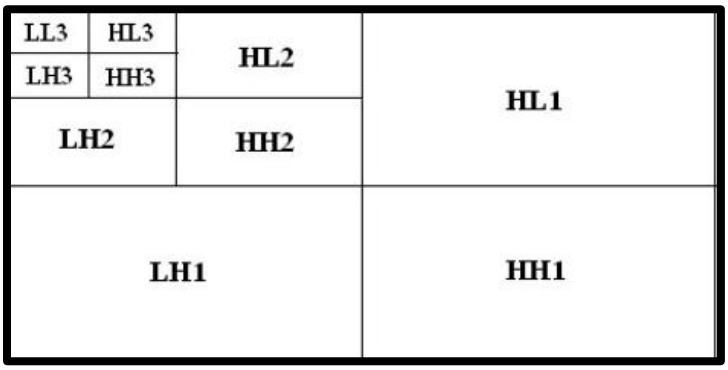


Figure 3.8. The structure of wavelet decomposition (Raviraj and Sanavullah, 2007).

We can summarize the advantages of Haar Wavelet transform as follows:

1. Best performance in terms of computation time.
2. Computation speed is high.
3. Simplicity.
4. HWT is efficient compression method.
5. It is memory efficient since it can be calculated in place without a temporary array (Raviraj and Sanavullah, 2007).

3.6. RC4

RC4 (Rivest Cipher 4 also known as ARC4 or ARCFOUR meaning Alleged RC4) is a stream cipher, symmetric key algorithm (Figure 3.9), designed in 1987 by Ronald Rivest of RSA Security and is one of the most widely software stream cipher and used in popular protocols, such as Secure Sockets Layer/Transport Layer Security (SSL/TLS) (protect Internet traffic), The RC4 encryption algorithm is used by standards such as IEEE 802.11 within WEP (Wireless Encryption Protocol) secure wireless network and PDF using 40 and 128-bit keys. Also, it's used in many commercial software packages such as Lotus Notes and Oracle Secure SQL. It's considered to be fast and simple in terms of software (Anonymous, 2013).

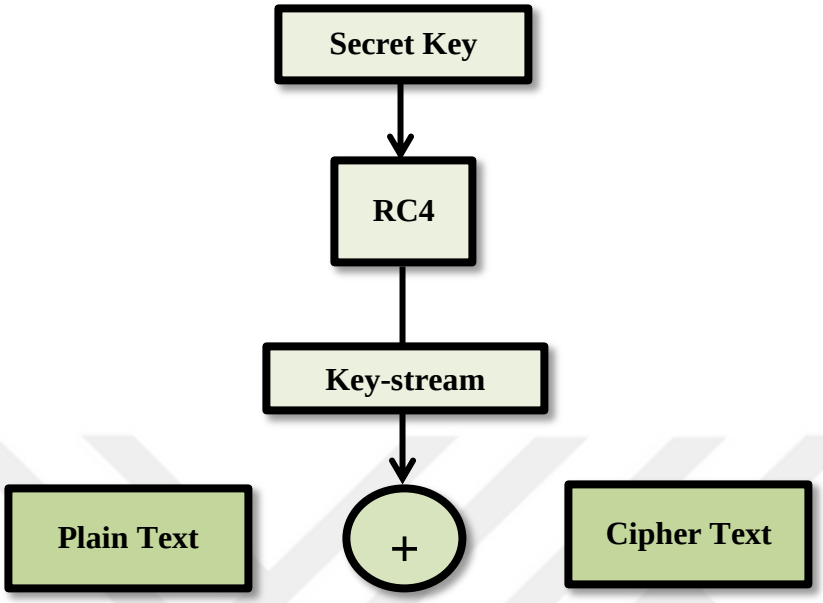


Figure 3.9. RC4 block diagram.

Rivers Shamir Adleman (RSA) is the most popular cryptography algorithm. Virtually all standard cryptographic protocols using the RSA algorithm, including SSL / TLS (for securing HTTP) and SSH (secure shell). Security algorithms RSA lies in the difficulty of factoring large numbers into a number of factors - the prime factor which is used as a private key to unlock cipher text. Due to the excess of the RSA algorithm is a standard for cryptography algorithms both on text encryption or other data types, the authors try to implement these algorithms on digital image (Irfan et al., 2015).

A pseudo-random number generator (PRNG), also known as a deterministic random bit generator (DRBG), is an algorithm for generating a sequence of numbers whose properties approximate the properties of sequences of random numbers. The PRNG-generated sequence is not truly random because it is completely determined by a relatively small set of initial values, called the PRNG's seed. PRNGs are central in applications such as simulations, electronic games, and cryptography. Cryptographic applications require the output not to be predictable from earlier outputs, and more complicated algorithms (Jindal and Singh, 2015).

Strengths of RC4 are mentioned as the following points:

- The difficulty of knowing where any value is in the table.
- The difficulty of knowing which location in the table is used to select each value in the sequence.
- A particular RC4 Algorithm key can be used only once.
- Encryption is about 10 times faster than DES.

The same algorithm is used for both encryption and decryption as the data stream is simply XORed with the generated key sequence. The key stream is completely independent of the plaintext used. The operation is initialized with a variable length key, typically between 40 and 256 bits, using the key-scheduling algorithm (KSA). Then the stream of bits is generated by a pseudo-random generation algorithm. It uses a variable length key from 1 to 256 bit to initialize a 256-bit state table (Anonymous, 2013).

The key-scheduling algorithm is used to initialize the permutation in the array "S". "key-length" is defined as the number of bytes in the key and can be in the range $1 \leq$ key-length ≤ 256, typically between 5 and 16, corresponding to a key length of 40 – 128 bits. First, the array "S" is initialized to the identity permutation. S is then processed for 256 iterations in a similar way to the main PRGA but also mixes in bytes of the key at the same time.

The state table is used for subsequent generation of pseudo-random bits (a pseudo-random number generator uses a function that produces a deterministic stream of bits that eventually repeats) and then to generate a pseudo-random stream which is XORed with the plaintext to give the cipher-image. The algorithm can be broken into two stages: initialization, and operation. In the initialization stage the 256-bit state table, S is populated, elements S [0], S [1] … S [255], using the key, K as a seed. Once the state table is setup, it continues to be modified in a regular pattern as data is encrypted. The initialization process can be summarized by the pseudo-code.

This algorithm produces a stream of pseudo-random values. The input stream is XORed with these values, bit by bit. The encryption and decryption process is the same as the data stream is simply XORed with the generated key sequence. The output byte is selected by looking up the values of S(i) and S(j), adding them together modulo 256,

(Figure 3.10) and then looking up the sum in S; S(S(i) + S(j)) is used as a byte of the key-stream, K.

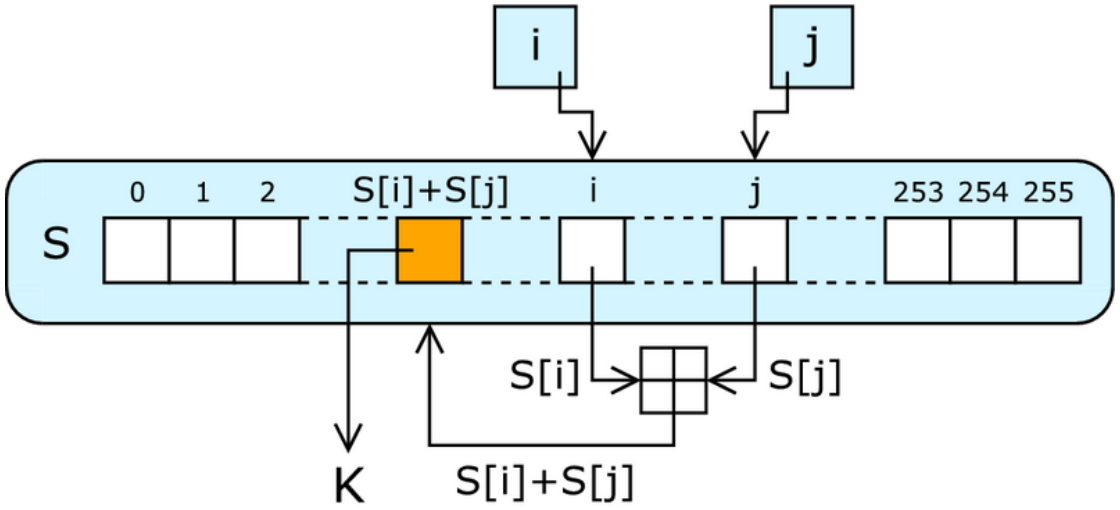


Figure 3.10. The structure of PRNG (Goncalves, 2009).

Some of the RC4 algorithm features can be summarized as (Mousa and Hamad, 2006):

1- Symmetric stream cipher
2- Variable key length.
3- Very quick in software
4- Used for secured communications as in the encryption of traffic to and from secure web sites using the SSL protocol.

So RC4 consists of two parts KSA and PEGA, in KSA state array is generated, in PRGA key-stream is generated then the key-stream is XORed with the data to produces encrypted data. The same key is used for the decryption. The encrypted data is XORed with key-stream to get the plain data. The encryption and decryption in the RC4 algorithm are shown in (Figure 3.11, Figure 3.12).

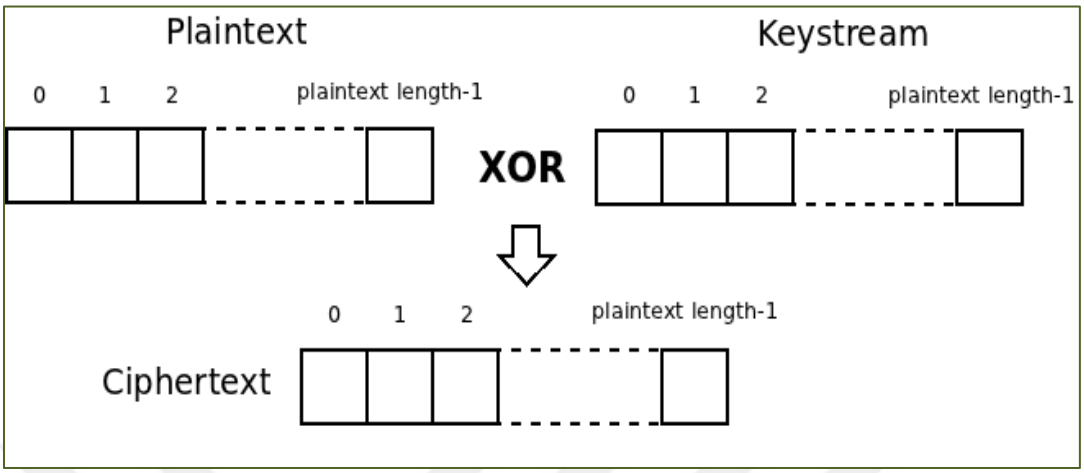


Figure 3.11. Encryption structure.

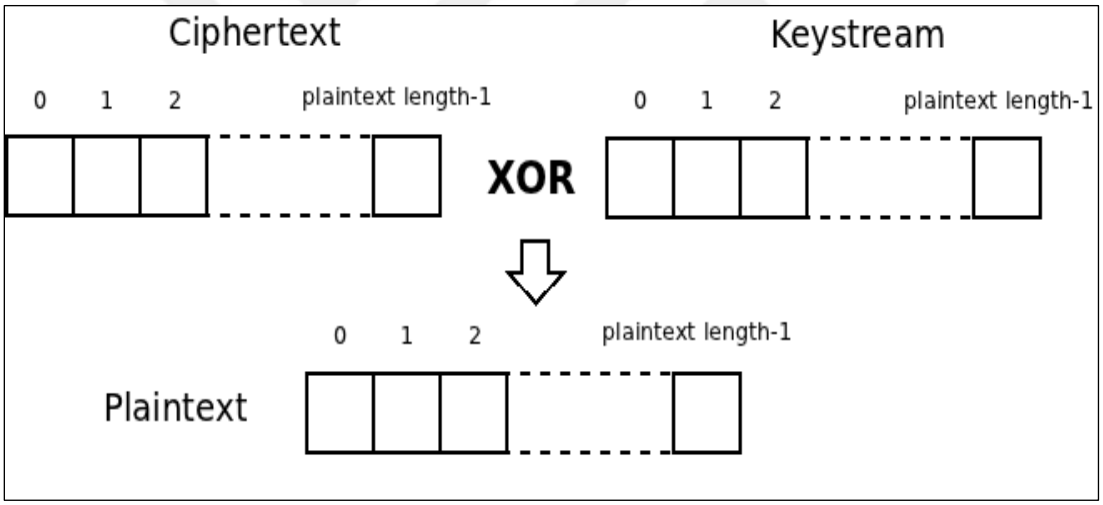


Figure 3.12. Decryption structure.

The steps for RC4 algorithm is summarized as follows (Mousa and Hamad, 2006):

1- Get the data to be encrypted and the selected key.
2- Create two string arrays.
3- Initiate one array with numbers from 0 to 255.
4- Fill the other array with the selected key.
5- Randomize the first array depending on the array of the key.
6- Randomize the first array within itself to generate the final key stream.
7- XOR the final key stream with the data to be encrypted to give cipher text.

3.7. Security Analysis by Statistical Approach

Nowadays, security is most important part of an image encryption. For the most part, a great encryption method qualifies different security criteria to assess the efficiency and security of the image encryption algorithm and some of them are following as:

3.7.1. PSNR for compressed image

In order to evaluate the performance of the image compression coding, it is necessary to define a measurement that can estimate the difference between the original image and the decoded image. Two commonly used measurements are the Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR). PSNR is used to measure the quality of reconstruction of lossy and lossless compression (e.g., for image compression). The signal, in this case, is the original data, and the noise is the error introduced by compression. When comparing compression codecs, PSNR is an approximation to human perception of reconstruction quality. There is an inverse relationship between PSNR and MSE. So a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not. PSNR is most easily defined via the mean squared error (Pantech, 2013).

Which is defined “Equ. 3.4” and “Equ. 3.5” respectively. f(x, y) is the pixel value of the original image, and f’(x, y) is the pixel value of the decoded image. Most image compression systems are designed to minimize the MSE and maximize the PSNR (Wei, 1997).

$$MSE = \frac{\sum_{x=0}^{W-1}\sum_{y=0}^{H-1}\left[f(x,y) - f'(x,y)\right]^2}{WH} \tag{3.4}$$

$$PSNR = 20\log_{10}\frac{255}{MSE} \tag{3.5}$$

3.7.2. Histogram

A histogram is a graph, a graph that shows frequency. Usually, histograms have bars that represent the frequency of occurring of data in the whole data set. A Histogram has two axes the x axis and the y axis. The x axis contains event whose frequency you have to count. The y axis contains frequency. The different heights of the bar show different frequency of occurrence of data. A cipher image should have a uniform histogram to be secure from the known plaintext attack (Kumar et al., 2014)

Histogram of an image, like other histograms, also shows frequency. The x axis shows the gray level intensities and the y axis shows the frequency of these intensities. The x axis of the histogram shows the range of pixel values. Whereas on the y-axis, is the count of these intensities (Anonymous, 2017).

3.7.3. Information entropy

Information theory is the mathematical theory of data communication and storage founded in 1949 by Shannon (Stinson, 1995). It is well known that information entropy can measure the distribution of gray value in the image. It identifies the degree of uncertainty and uniform distribution in the system. We can make sure that the bigger information entropy the more uniform for the distribution of gray value. The calculation of information entropy is as following formula "Equ. 3.5":

$$H\ m\ =\ \sum_{i=0}^{2N-1} P\ m_i\ \log_2 \frac{1}{P(m_i)} \tag{3.5}$$

Where P (*mi*) states probability *mi* in a message P (*mi*) = n/N, n is the number of gray levels that repeat themselves. The information entropy of an idea random image is 8 (Zhang et al., 2012). In the gray scale image there are 256 gray values (m0 = 0, m1 = 1, ..., m255 = 255) and probability of each grey value is calculated from its histogram. Without loss of generalization, we calculate entropy for gray scale image only (Munir, 2012).

3.7.4. Differential attack analyses

In general, a desirable property for an encrypted image is being sensitive to the small changes in plain-image (e.g., modifying only one pixel). The opponent can create a small change in the input image to observe changes in the result. By this method, the meaningful relationship between original image and encrypted image can be found. If one small change in the plain-image can cause a significant change in the cipher-image, with respect to diffusion and confusion, then the differential attack actually loses its efficiency and becomes practically useless. To test the influence of one-pixel change on the whole image encrypted by the proposed algorithm, three common measures were used: MAE, NPCR, and UACI (Jolfaei, 2011). NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) measures the invulnerability of an algorithm against the differential attacks on the image. NPCR evaluates the pixels change rate in the coded image after modification in one pixel of a prime image. consequently, high NPCR value is effective (Xu et al., 2010). Furthermore, UACI computes the variation in the intensity of the corresponding pixel of the plain image and the encrypted image (Zhang et al., 2005). MAE, NPCR, and UACI can be calculated by following formula:

$$MAE = \frac{1}{W \times H} \sum_{i=0}^{H-1} \sum_{j=0}^{W-1} C\ i,j\ - P\ i,j \tag{3.6}$$

Let *C(i, j)* and *P(i, j)* be the gray level of the pixels at the *i*th row and *j*th column of a H×W cipher and plain-image. The large the MAE value, the better the encryption security.

$$NPCR = \frac{1}{W \times H} \sum_{i=1}^{M} \sum_{j=1}^{N} D\ i,j\ \times 100\% \tag{3.6}$$

Where

$$D\ i,j\ = \begin{matrix} 1\ C1\ i,j\ \neq C2\ i,j \\ 0 \qquad otherwise \end{matrix} \tag{3.7}$$

$$UACI = \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{C1\ i,j\ - C2\ i,j}{255} \times \frac{100\%}{W \times H} \quad (3.8)$$

Where W and H are the dimensions and (*i*, *j*) is the coordinates of the image. H and W are the width and height of C_1 or C_2. The C_1 and C_2 are two encrypted images whose corresponding plain images have the size only and also have a one-pixel difference. The $C_1(i, j)$ and $C_2(i, j)$ are gray scale values of the pixels at grid (*i*, *j*). The D(*i*, *j*) determined by $C_1(i, j)$ and $C_2(i, j)$. If $C_1(i, j) = C_2(i, j)$, in result, D(*i*, *j*) = 1; otherwise, D(*i*, *j*) = 0. (Ahadpour et al., 2016).

4. RESULTS AND DISCUSSION

For designing a secure and simple transformation of information over the Internet we should use one of the methods of security which is cryptography. So in this segment, the scheme utilized for image compression and image encryption alongside the calculation of Haar wavelet transformation and RC4 method was introduced. A model was loaded out using four steps, the first stage analyzing the requirements. The second step is the general design while the third step is execution and the last part is running the result of the designed prototype.

4.1. Analyzing the Requirement

The needs for the study was introduced as before in material and methods section, for encrypting an image an encryption algorithm utilized for better result of security and safety a compression method was combined with the used encryption algorithm which is Haar wavelet transformation. As it's known that HWT is one of the simplest and fast methods among the compression methods. This method is combined with RC4 encryption algorithm for a better result of encryption.

Each of the requirements deeply introduced and explained in chapter three. The essential thought behind the study is to first compress the image with the goal that we can send it over the network rapidly and encode it so we can transmit it over any networks safely and securely. Matlab software was used to perform all of the calculations and generate and display all of the pictures.

4.2. General Design

Initially, we compress the image utilizing Haar wavelet transformation. Wavelets are an arrangement of numerical basis functions. While approximating a function as far as wavelets, the wavelet basis functions are chosen to concur to the purpose being approximated. Wavelets utilize a dynamic arrangement of basic functions that stand for the

input function in the most effective way. In this way, wavelets can give a great deal of compression and are thus extremely well known in the sector of image and signal processing. A wavelet transformation changes over information from the spatial into the frequency domain and afterward stores every segment with a relating coordinating determination scale.

By applying the Haar wavelet transformation we can stand for this image as far as a low-determination image and an arrangement of detail coefficients. Haar Transform is only averaging and differencing. In HWT form, firstly the image experiences the single-level wavelet resulting four coefficient scheme; the approximation (ca), horizontal (ch), vertical (cv), and diagonal (cd) frameworks. The minimum frequency sub-band is indicated in the (ca) framework. The (ca) framework will be encoded as it contains the vast majority of the image's information utilizing the RC4 Stream Cipher.

For encryption, the RC4 key-stream will be merged with the (ca) coefficients utilizing the XOR operation. The proposed study is summarized in a diagram (Figure 4.1).

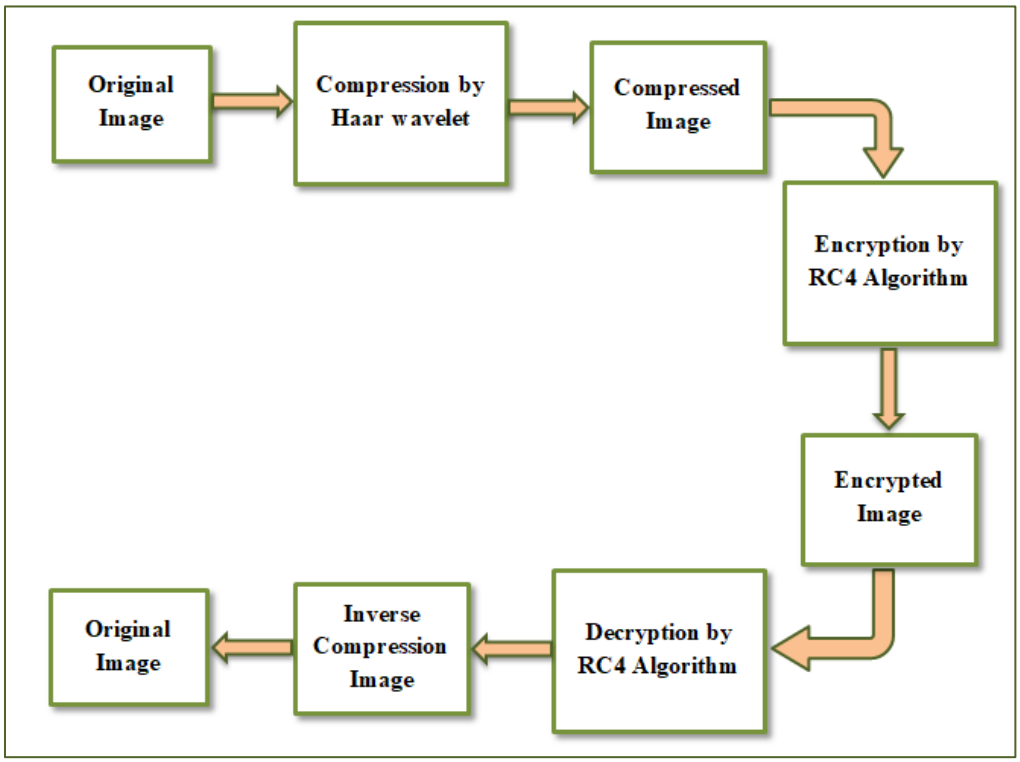


Figure 4.1. Diagram of the prototype.

4.3. Execution

For writing the source codes Matlab software was used. A GUI was prepared while running the program user should upload an image and a key so far compression and encryption done. A part of the designed interface shown in (Figure 4.2) and (Figure 4.3). The running code was previewed in (Figure 4.4) that process done for a standard image (Lena).

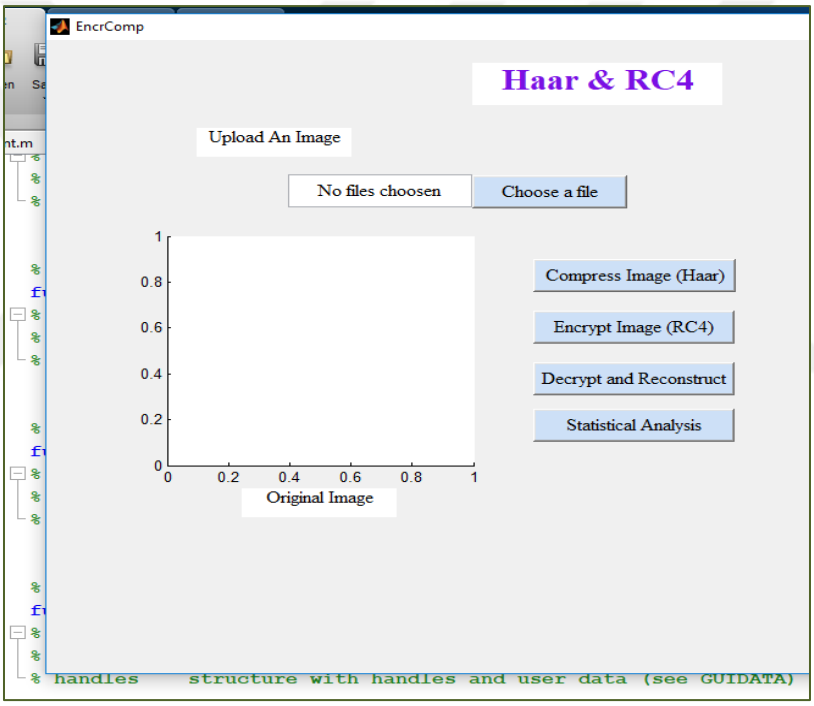


Figure 4.2. Structure of design

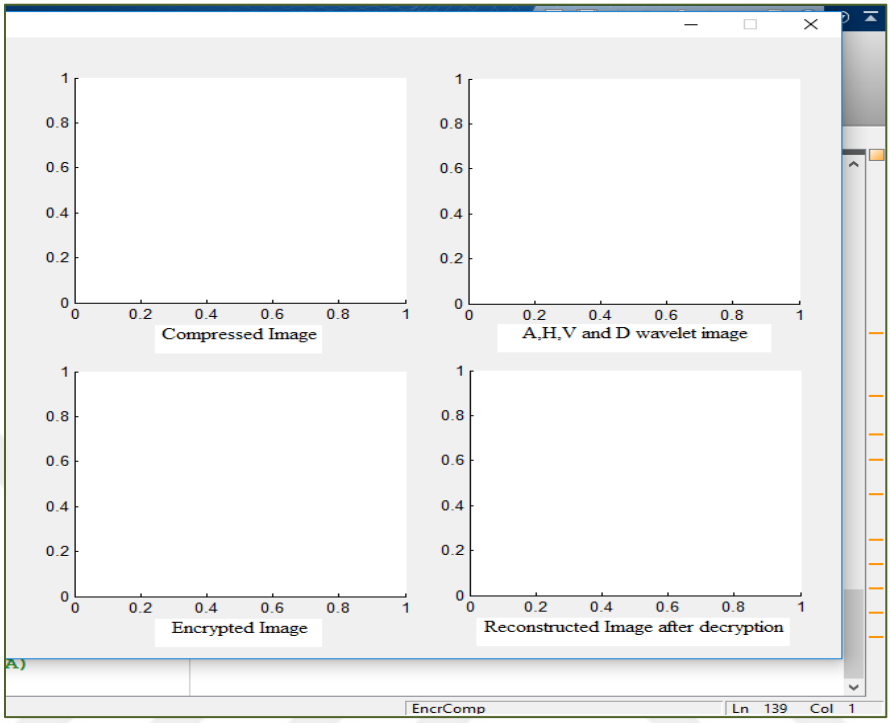


Figure 4.3. Axes of Images

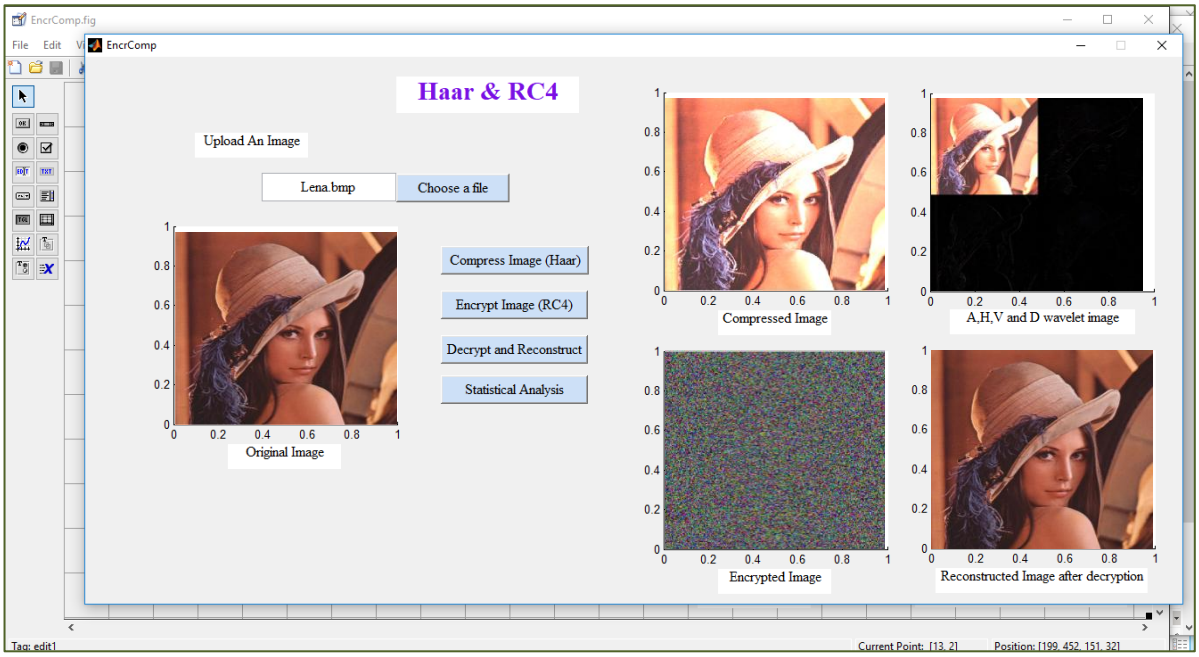


Figure 4.4. Execution of project.

4.4. Study Result and Discussion

At the end of the study, the completions were successful and fulfill requirements. An image was chosen to be compressed after the compression, the compressed image was encoded by RC4, the encoded image was decoded by RC4 again to the compressed image and by using inverse wavelet the image returns to its original form. Five different images from the standard images were used. Images are of size (512x512x3) with different type (.bmp, .jpg, .png). For each images Haar, encryption, decryption, and inverse of Haar was applied. For more clarification result of the encrypted images are presented.

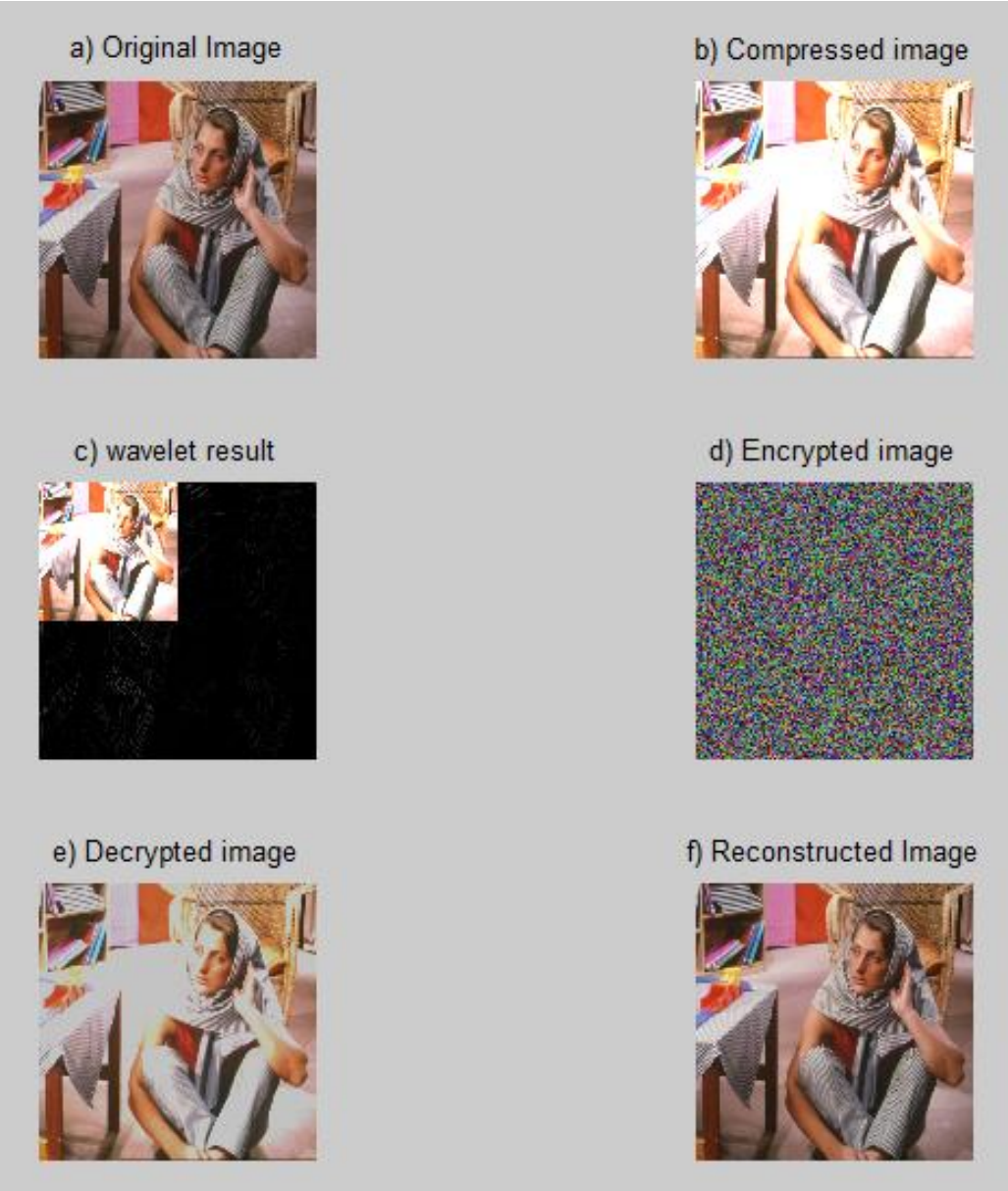


Figure 4.5. Result for Barbara image.

In (Figure 4.5) the standard image Barbara was used and a) is the original image form. b) Shows the compressed image. c) Presents the HWT illustration. d) The result of the encrypted image. e) The decoded image after decryption by RC4. f) Displayed the inverse transform HW.

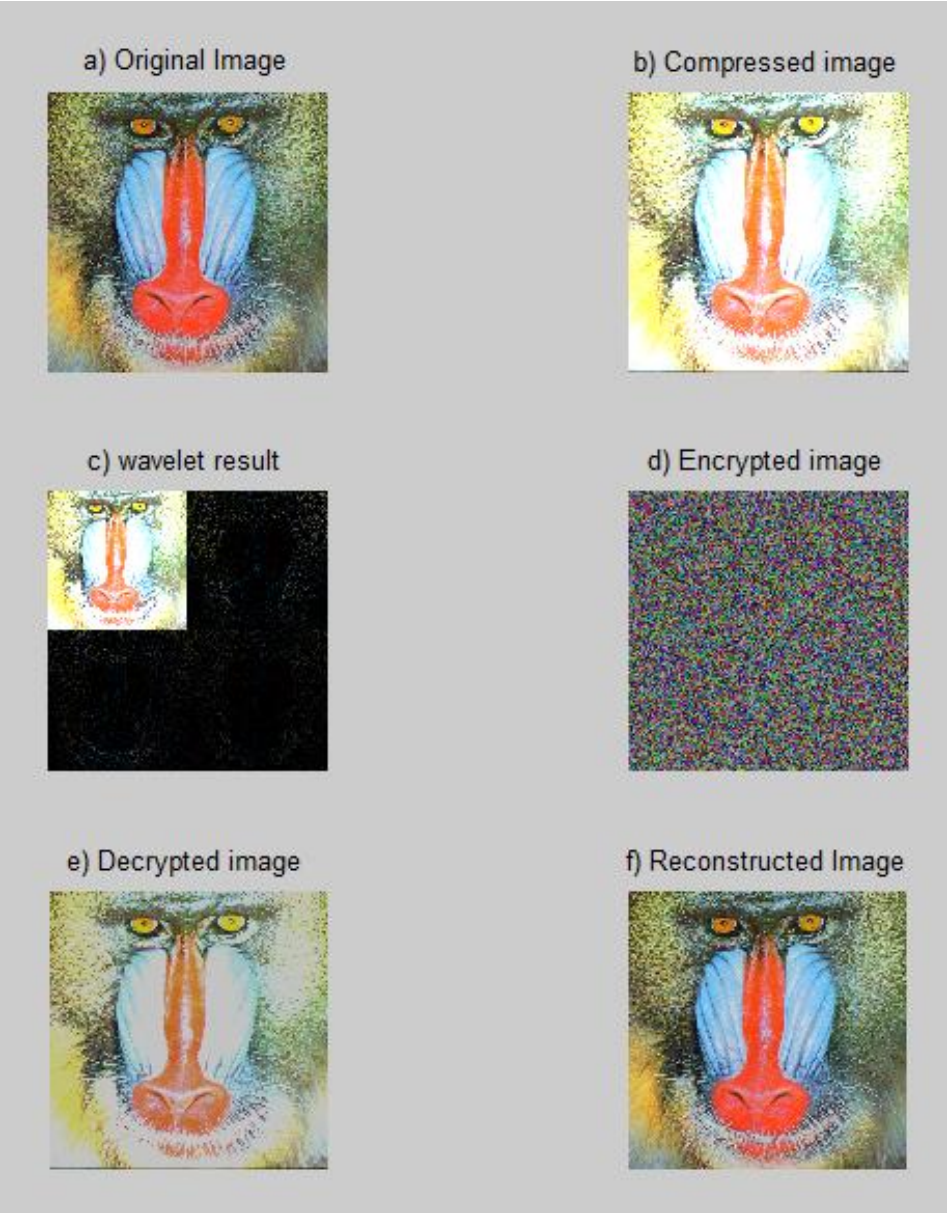


Figure 4.6. Result for Baboon image.

In (Figure 4.6) the standard image Baboon was used and a) is the original image form. b) Shows the compressed image. c) Presents the HWT illustration. d) The result of the encrypted image. e) The decoded image after decryption by RC4. f) Displayed the inverse transform HW.

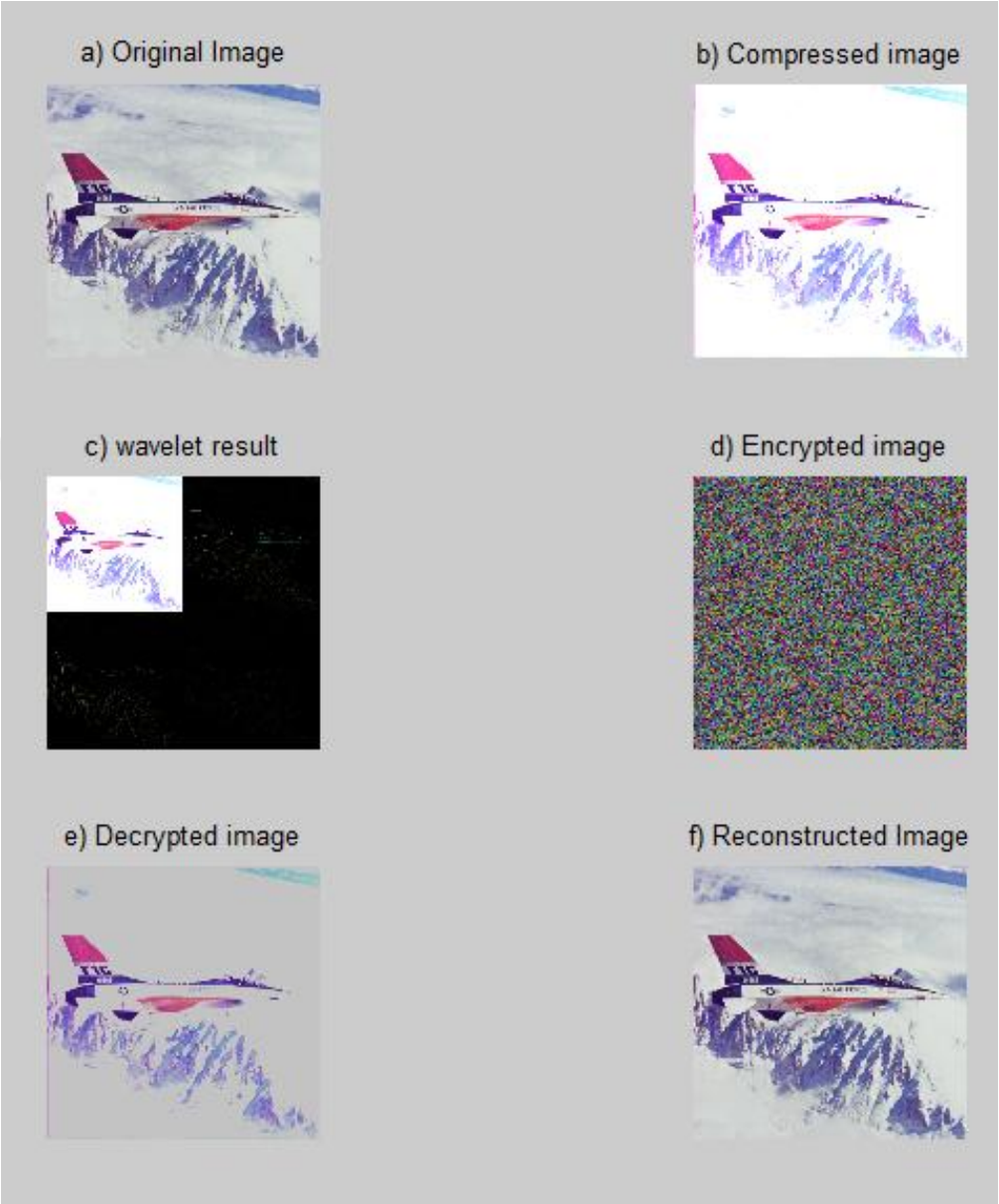


Figure 4.7. Result for Airplane image.

In (Figure 4.7) the standard image Airplane was used and a) is the original image form. b) Shows the compressed image. c) Presents the HWT illustration. d) The result of the encrypted image. e) The decoded image after decryption by RC4. f) Displayed the inverse transform HW.

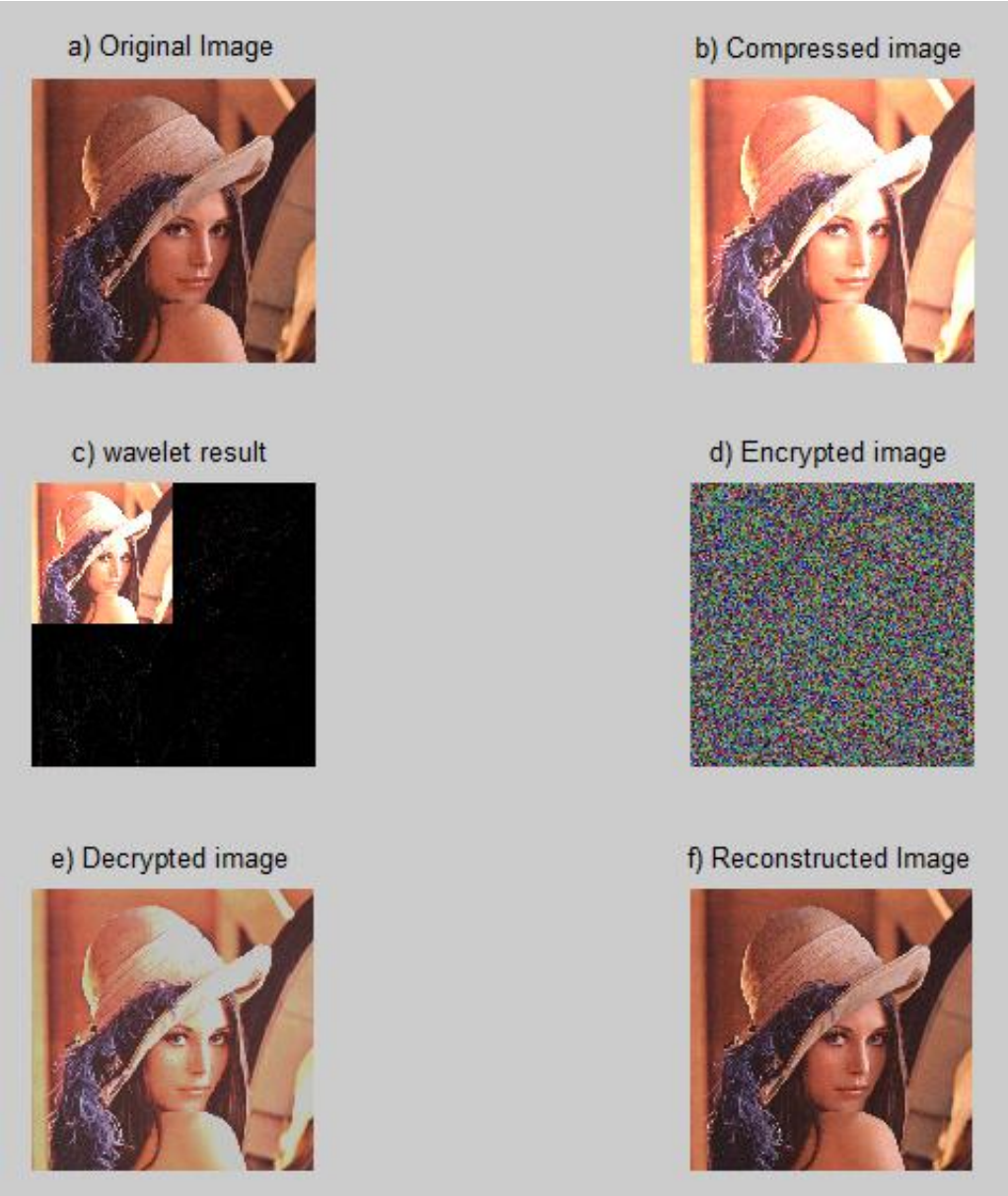


Figure 4.8. Result for Lena image.

In (Figure 4.8) the standard image Lena was used and a) is the original image form. b) Shows the compressed image. c) Presents the HWT illustration. d) The result of the encrypted image. e) The decoded image after decryption by RC4. f) Displayed the inverse transform HW.

Figure 4.9. Result for Pepper image.

In (Figure 4.9) the standard image Pepper was used and a) is the original image form. b) Shows the compressed image. c) Presents the HWT illustration. d) The result of the encrypted image. e) The decoded image after decryption by RC4. f) Displayed the inverse transform HW.

4.4.1. Histogram analysis

Several grey-scale images having different contents were preferred, and their histograms were calculated. Typical examples are presented in (Figure 4.10, Figure 4.11, Figure 4.12, Figure 4.13, and Figure 4.14), each image shows the histogram of each (original image, compressed image, encrypted image, and reconstructed image). The histogram of the ciphered image is genuinely uniform and is fundamentally unique in relation to that of the plain image can be seen. Subsequently, it doesn't give any sign to utilize any measurable assault on the image under thought. Additionally, there is no loss of picture quality subsequent to playing out the encryption/decryption steps. From the shown images histogram was presented for 5 standard images.

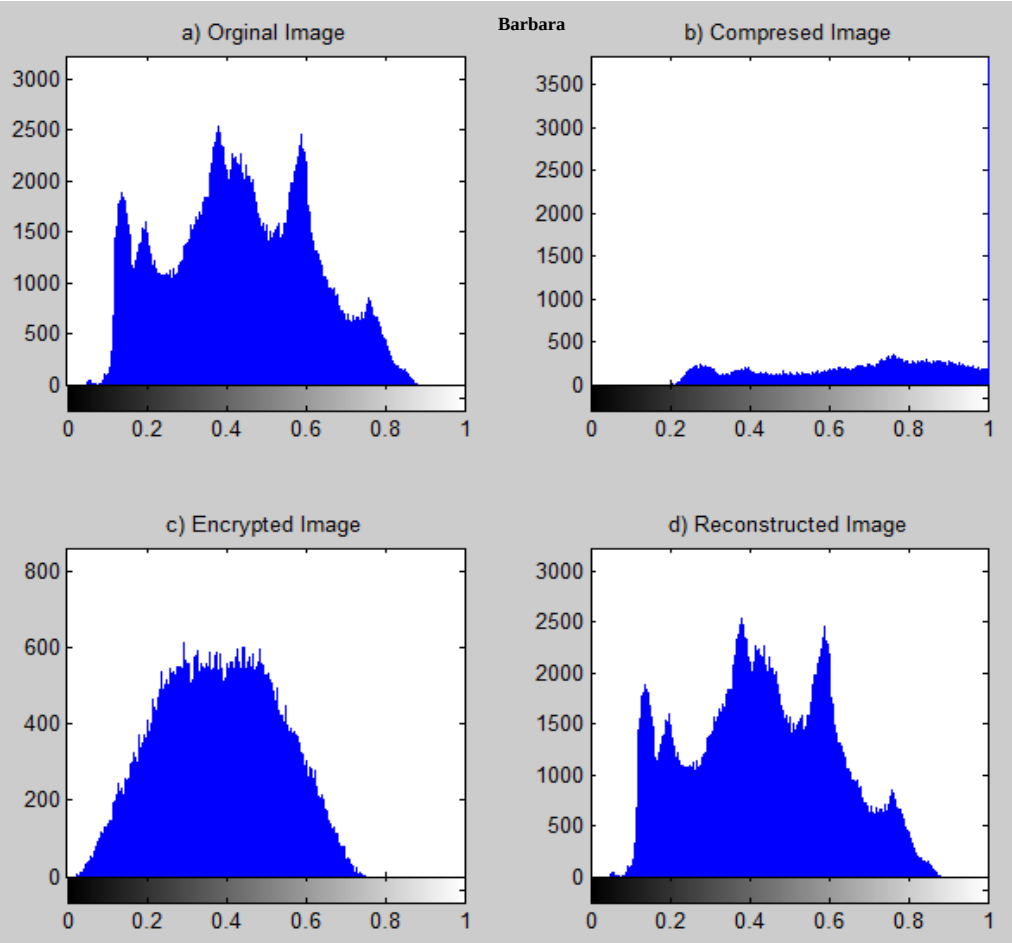


Figure 4.10. Histogram of Barbara image.

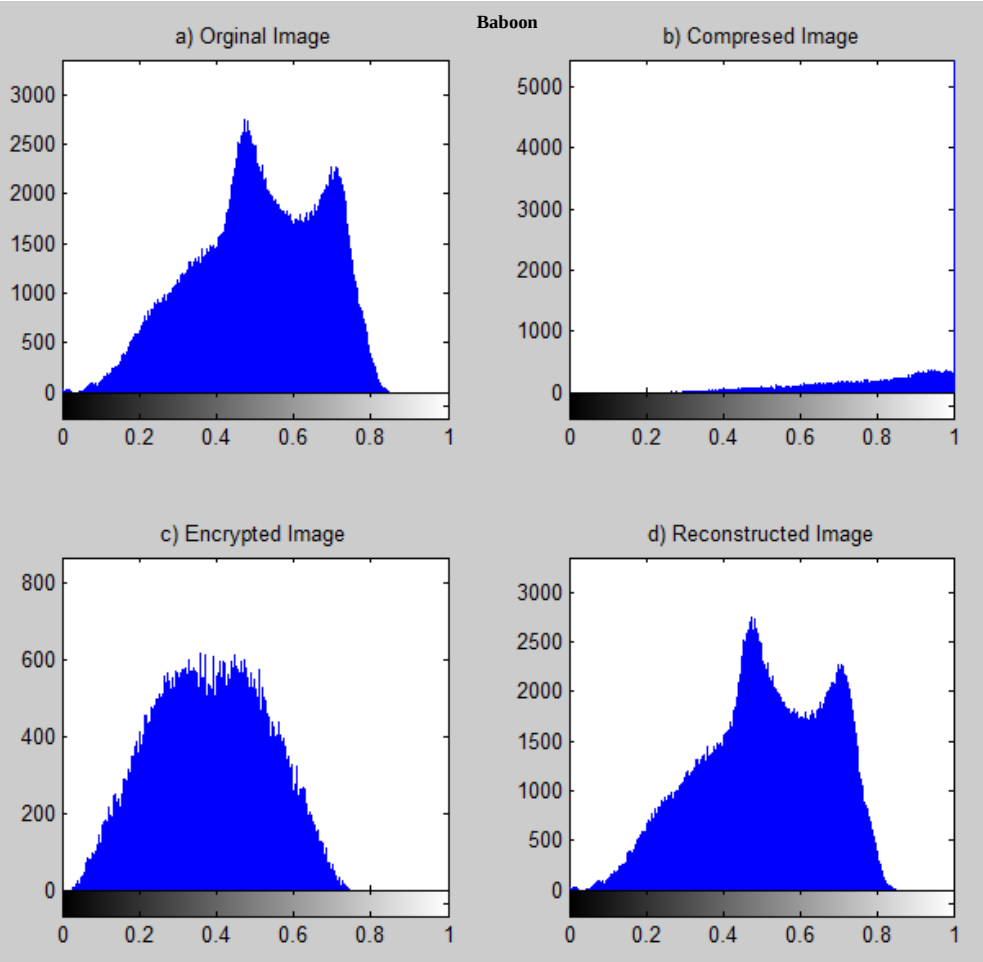


Figure 4.11. Histogram of Baboon image.

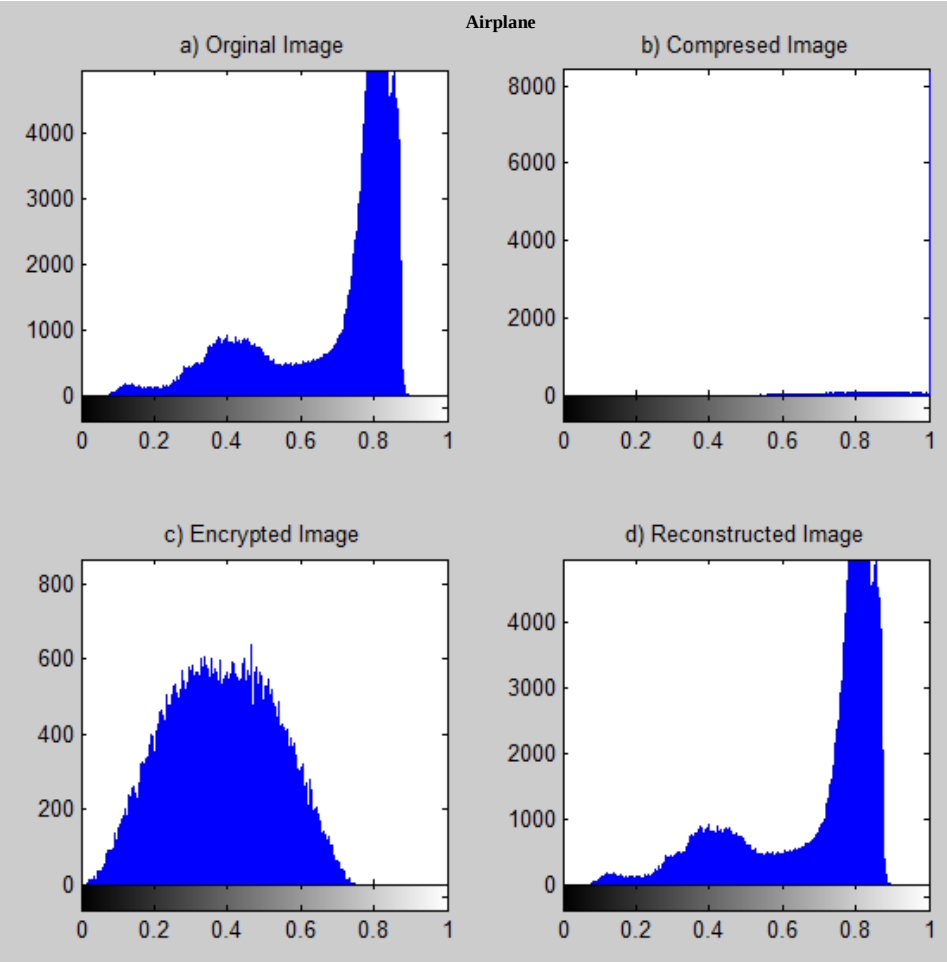


Figure 4.12. Histogram of Airplane image.

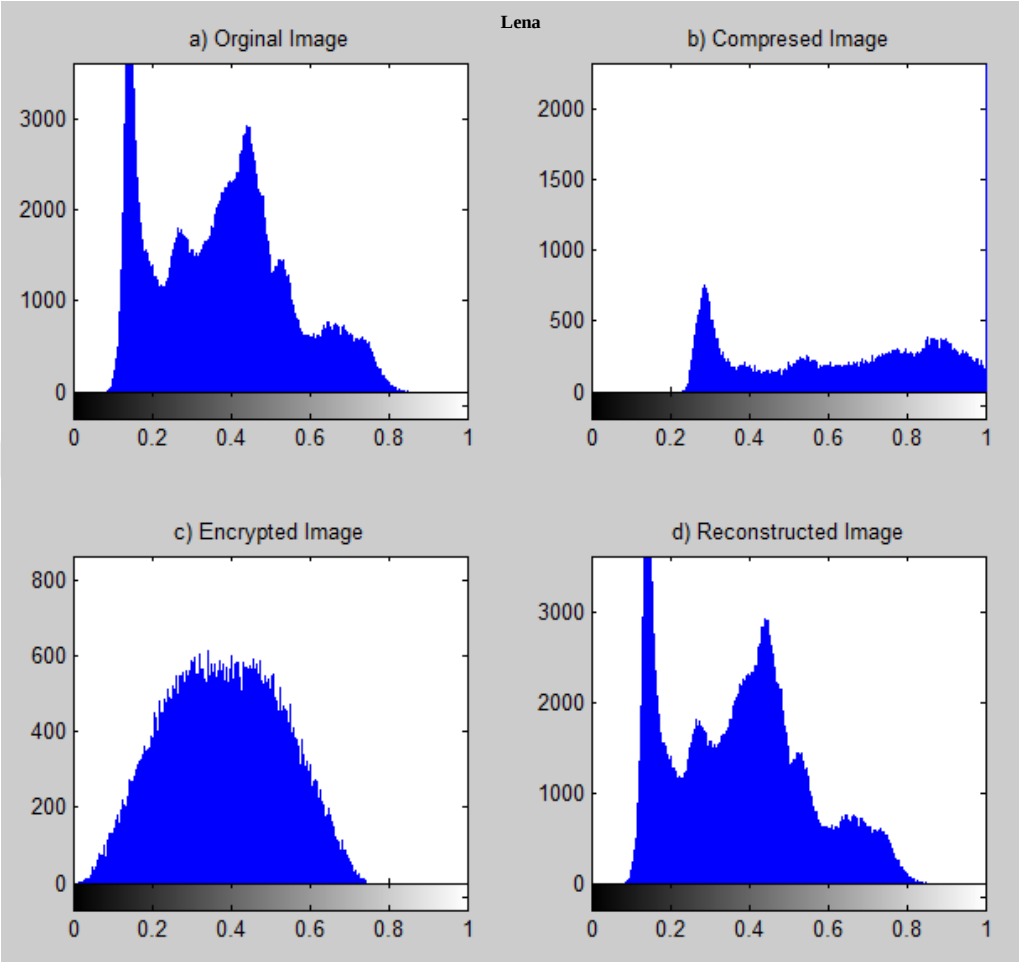


Figure 4.13. Histogram of Lena image.

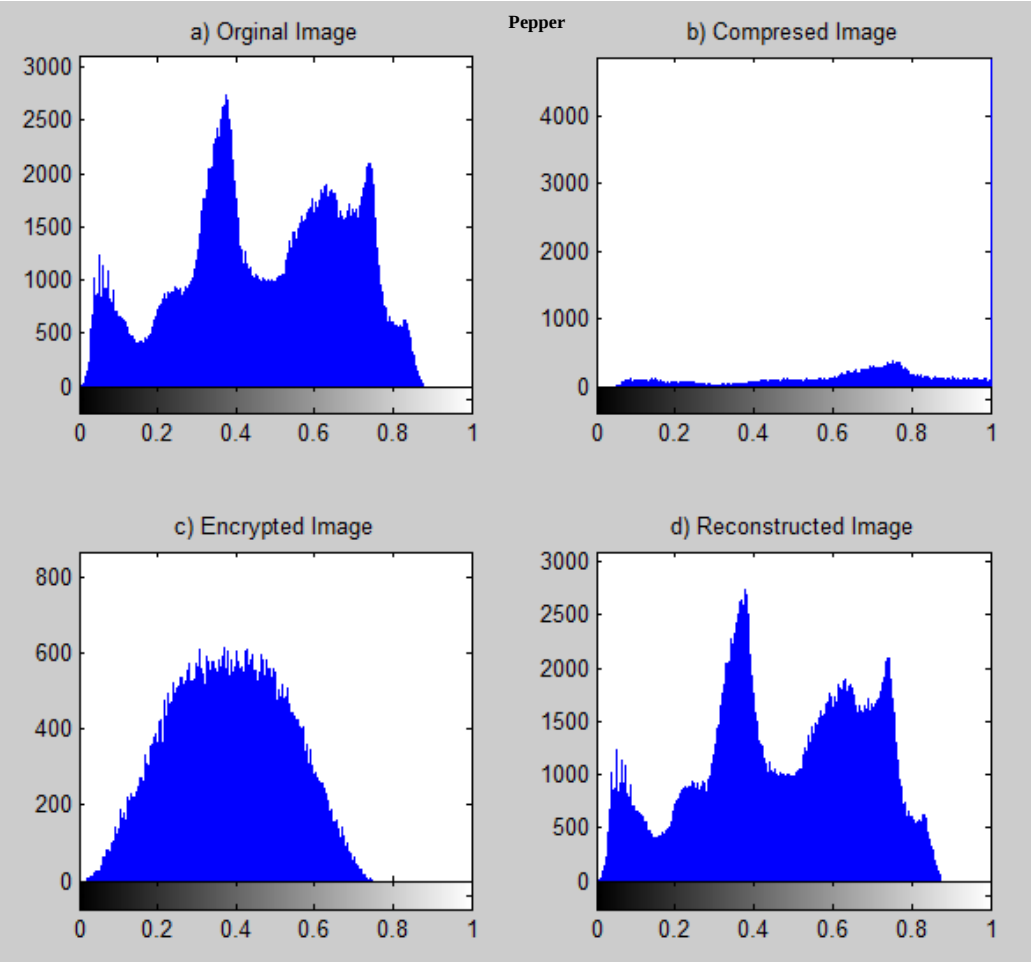


Figure 4.14. Histogram of Pepper image.

For testing histogram of an image, there is another way which is quantity analyzed by the variance of the histogram, its examined to test the uniformity of the encrypted image. The variance values are shown in the table (Table 4.1), which they are in the range of 50000-50000 since these results are for the encrypted image which firstly it's compressed then encoded.

Table 4.1. The obtained variance by proposed method

Image	Variance
Airplane	54125.6313
Baboon	54203.3176
Barbara	54475.1058
Lena	54668.8078
Pepper	54196.5176

The variance was measured in another study namely "Image encryption using a synchronous permutation-diffusion technique" which results are shown in (Table 4.2) since the proposed study's variance values are in the range of 5000-5000 (Enayatifar et al., 2016).

Table 4.2. The obtained variance using method (Enayatifar et al., 2016)

Image	Variance
Airplane	5264.710
Baboon	5119.29
Lena	5118.094
Pepper	5403.283

4.4.2. Speed test

In another side elapsed time for the encryption steps was calculated by Matlab "tic-toc" function, tic starts a stopwatch timer to measure performance. The function records the internal time at the execution of the tic command. Display the elapsed time with the toc function. Tic returns the value of the internal timer at the execution of the tic command so that you can record time for simultaneous time spans. Presented results in (Table 4.3) are for (512x512x3) sized images, with PC of Pentium (R) Dual-core, 2.00 GHz with RAM of 4.00 GB, 64-bit operating system type and Windows 10 Pro, of Matlab R2013a version.

Table 4.3. Time elapsed for encryption

Images	Elapsed Time in (sec.)
Airplane	0.2346
Baboon	0.2335
Barbara	0.2320
Lena	0.2355
Pepper	0.2342

4.4.3. Key space analysis

The number of keys that can be generated known as key space and secret key space must be sufficiently large to oppose brute-force attacks. The key length and the array size of an internal state are variable. Typical parameters are key length= 16 (128-bit key) and array size = 256. RC4 consists of two methods: Key Scheduling Algorithm (KSA) and Pseudo-Random Generation Algorithm (PRGA). Each single input key can be of 256 which is 2^8. Which is $2^8 \times 2^8 \times 2^8 \times \ldots = 2^{8+16} = 2^{128}$.

4.4.4. Error metrics for image compression quality

The most important section of an image encryption is security. Then, a complete analysis should apply to ensure the security of the encrypted image of the proposed method. Statistical analysis was tried to explain that encrypted images are sufficiently secure facing different cryptographic attacks. The execution examination of specific image encryption HWT with RC4 stream cipher is calculated utilizing Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Histogram Analysis, correlation coefficient and Entropy. To show the variation between encoded image and interrelated plain-image, three calculations were used: NPCR and UACI.

Encryption was done for five standard images and the results of PSNR with MSE were successfully obtained since there is an inverse relationship between PSNR and MSE. So a higher PSNR generally indicates that the reconstruction is of higher quality (Table 4.4) presents the obtained results. The different key length was used to see the difference in the

result. There were a few point differences which were so little. Here 16-key length was used for image size (512x512x3).

Table 4.4. Results of PSNR and MSE for plain and decoded image

Images	PSNR			MSE		
	Red	Green	Blue	Red	Green	Blue
Baboon	367.5278	368.0185	368.8293	0.0000	0.0000	0.0000
Barbara	367.6645	369.8337	370.2642	0.0000	0.0000	0.0000
Lena	367.5845	371.6509	373.1584	0.0000	0.0000	0.0000
Pepper	366.9396	368.0659	372.7907	0.0000	0.0000	0.0000

4.4.5. Entropy analysis

Moreover, entropy analysis was done for the same five images, the results are shown in (Table 4.5). The entropy results between the original image and the single level compressed-encrypted image, from those entropy values we note that entropy value of the encrypted images is very close to the ideal value of 8 sh. This means that the proposed study is highly robust towards entropy attacks.

Table 4.5. Entropy results of encrypted image

Images	Original image			Encrypted image		
	Red	Green	Blue	Red	Green	Blue
Airplane	6.7177	6.7989	6.2137	7.5297	7.5327	7.5273
Baboon	7.7066	7.4744	7.7522	7.5283	7.5277	7.5302
Barbara	7.5770	7.4189	7.5149	7.5288	7.5274	7.5308
Lena	7.5889	7.1059	6.8147	7.5285	7.5294	7.5274
Pepper	7.3388	7.4962	7.0583	7.5288	7.5289	7.5322

Entropy was calculated for the same images but without compression, the encryption by RC4, the results shown in (Table 4.6).

Table 4.6. Results for entropy of encrypted image (RC4)

Images	Original Image			Encrypted Image		
	Red	Green	Blue	Red	Green	Blue
Airplane	6.7177	6.7989	6.2137	7.5300	7.5316	7.5304
Baboon	7.7066	7.4744	7.7522	7.5294	7.5300	7.5290
Barbara	7.5770	7.4189	7.5149	7.5313	7.5297	7.5305
Lena	7.5889	7.1059	6.8147	7.5292	7.5324	7.5324
Pepper	7.3388	7.4962	7.0583	7.5310	7.5305	7.316

Through the results obtained the proposed study is successfully fulfilled and for more assurance, the results were compared to the previous researches. In a proposed study "Image Encryption Using Block Based Transformation With Fractional Fourier Transform" the entropy value was calculated and the results are in range of 5.0-6.0 which is less than the ideal value of entropy the proposed study used different encryption algorithms like Kamlesh Gupta's scheme, Blowfish, and Twofish (Cui et al., 2013).

From another proposed study the entropy value shown like (Table 4.7), the results are so near to 8. This shows good entropy.

Table 4.7. Entropy value presentation (Loukhaoukha et al., 2012)

Image	Original	Encrypted
Lena	7.4318	7.9968
Baboon	7.2279	7.9979

4.4.6. Differential attack

Moreover, high NPCR value (near 100%) and suitable UACI rate were gotten. The calculation was done for a number of images. Results of NPCR and UACI between two encrypted images are presented in (Table 4.8). These encrypted images are firstly compressed.

Table 4.8. NPCR and UACI of various images

Images	NPCR %	UACI %
Lena- Barbara	99.611	35.859
Baboon- Pepper	99.609	36.679
Barbara-Pepper	99.621	36.620
Airplane-Lena	99.605	34.952
Pepper- Airplane	99.632	39.313

Likewise in another proposed image encryption study namely “A Secure Image Encryption Algorithm Based on Rubik's Cube Principle” the NPCR and UACI values were obtained for images of size (256×256) by using Rubik’s Cube algorithm, (Loukhaoukha et al., 2012) as shown in (Table 4.9).

Table 4.9. Difference measures between original and encrypted images

Image	NPCR (in %)	UACI (in %)
Lena	99.5850	28.6210
Black	99.6078	50.1931
Baboon	99.6094	27.4092
Checkerboard	99.62.01	50.0233

For more assurance, the same calculations done for the original image and the encrypted image as the results can be seen in (Table 4.10), which there is no compression for the image. The results were obtained from images of size (512x512).

Table 4.10. Difference measures between original and encrypted image of RC4

Image	NPCR (in %)	UACI (in %)
Airplane	99.9983	40.3892
Baboon	99.9986	26.9736
Barbara	99.9975	25.0005
Lena	99.9978	24.9490
Pepper	99.9835	30.4124

Same calculations of NPCR and UACI made between compressed image and the encrypted image, the reason of using compressed image here is the original image is instead of our compressed image, because for calculating the NPCR and UACI the size of two

images should be in the same size, for that reason measurement is done between the compressed image and the encrypted image, the results are presented in the table below (Table 4.11):

Table 4.11. Measures for NPCR and UACI of compressed and encrypted image

Images	NPCR %	UACI %
Airplane	99.9994	49.3946
Baboon	99.9989	49.5132
Barbara	99.9994	49.5952
Lena	100	49.6516
Pepper	99.9877	49.6221

More methods and encryption algorithms were used since the past till nowadays, from all of the prepared studies it has been mentioned that for a good result the entropy value should be near to the ideal entropy value 8 sh. And for the NPCR and UACI they have confirmed that the value of NPCR should be high across the UACI, while UACI should be lower. The value of PSNR and MSE they are in an inverse relation also the scientists substantiated that the rate of PSNR is high.

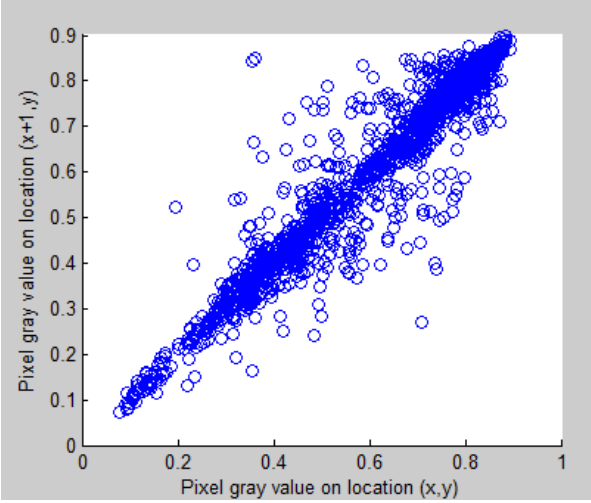
4.4.7. Correlation coefficient analysis

The values of the coefficients can range from -1 to 1 with -1 representing a direct, negative correlation, 0 representing no correlation, and 1 representing a direct, positive correlation. The correlation in plain-image is more than in cipher-image. The correlation was calculated for the original and encrypted images and they are presented in (Figure 4.15). The below table (Table 4.12), presents the value of the correlation coefficient.

Table 4.12. Obtained correlation coefficient value

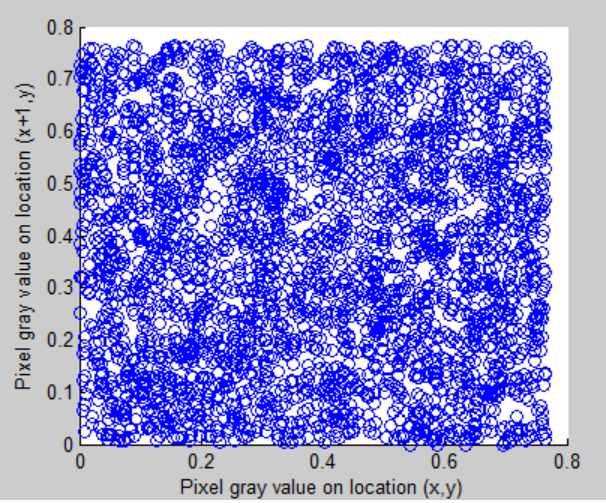
Image	Correlation Coefficient (Horizontal)	
	Original Image	Encrypted Image
Airplane	0.9663	0.0001
Baboon	0.8665	-0.0002
Barbara	0.9297	0.0018
Lena	0.9679	0.0003
Pepper	0.9767	0.0013

Correlation coefficient = 0.9663



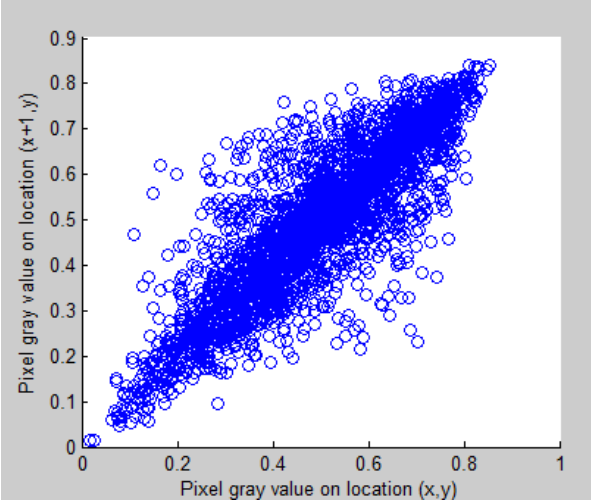
(a) Original Airplane

Correlation coefficient = 0.00012



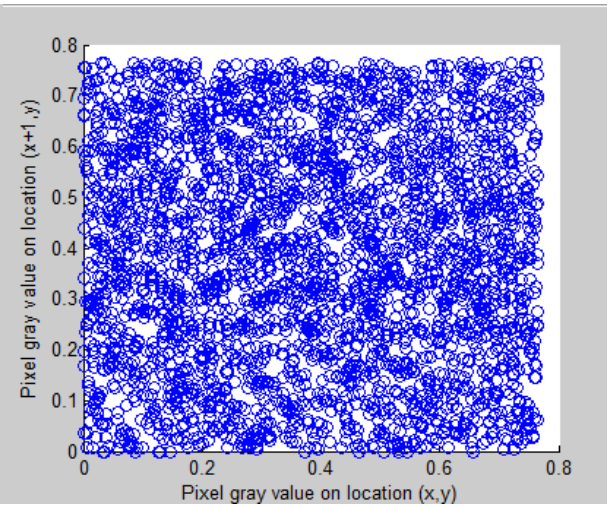
(b) Encrypted Airplane

Correlation coefficient = 0.8665



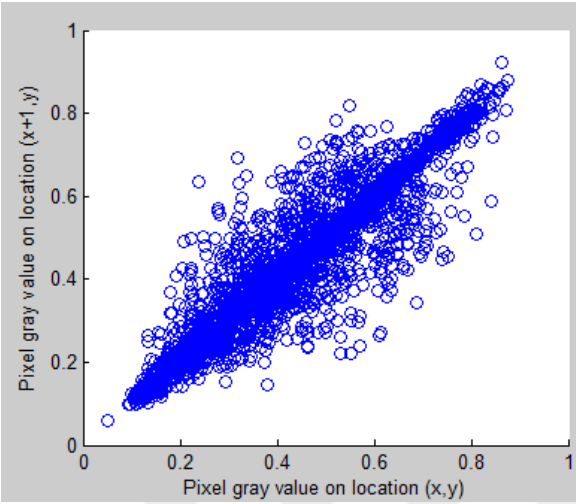
(c) Original Baboon

Correlation coefficient = -0.00026



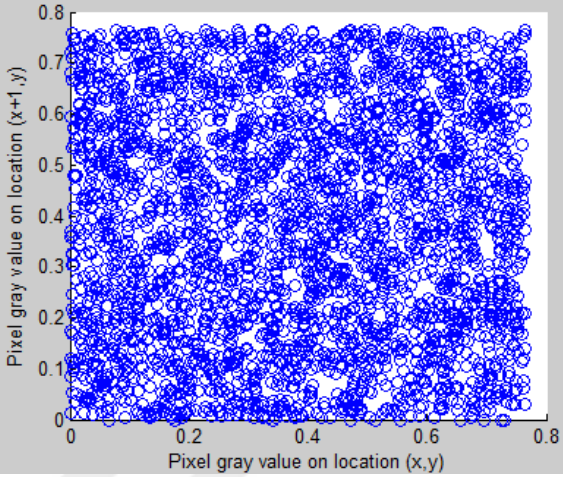
(d) Encrypted Baboon

Correlation coefficient = 0.9297



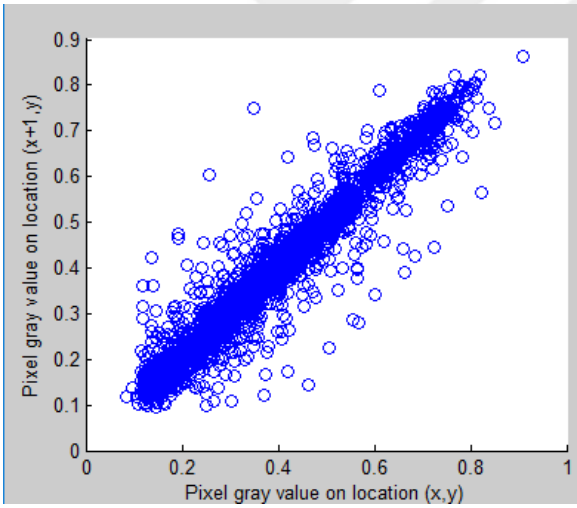
(e) Original Barbara

Correlation coefficient = 0.0018



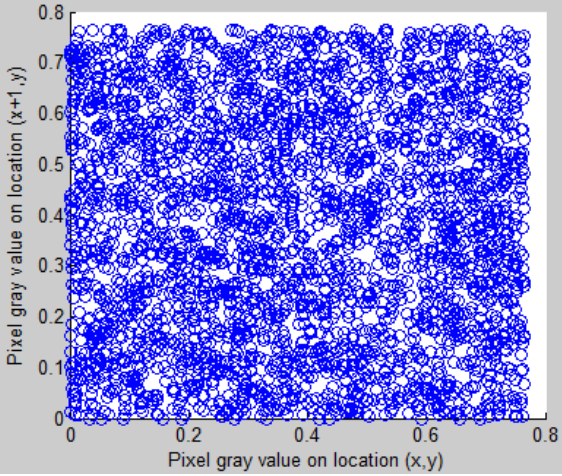
(f) Encrypted Barbara

Correlation coefficient = 0.9679



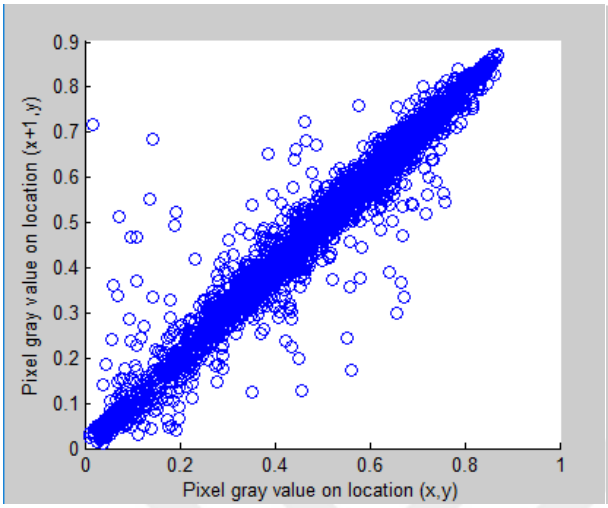
(g) Original Lena

Correlation coefficient = 0.00032



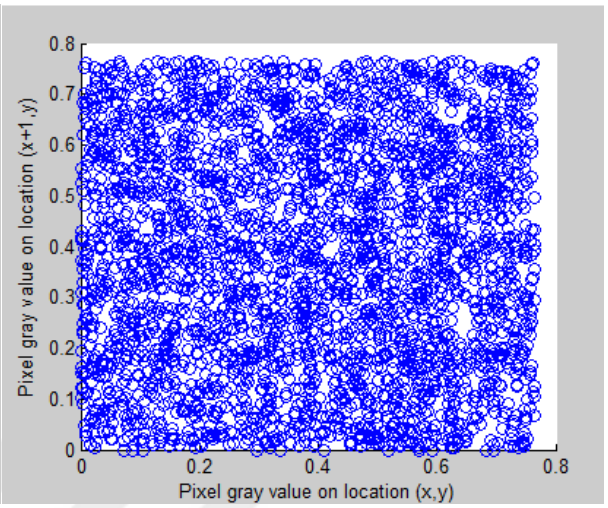
(h) Encrypted Lena

Correlation coefficient = 0.9767



(i) Original Pepper

Correlation coefficient = 0.0013



(j) Encrypted Pepper

Figure 4.15. Correlation distribution of the pair's horizontal to adjacent pixels.

5. CONCLUSIONS

An image encryption framework for images using HWT with RC4 Stream Cipher has been presented in this letter. The system compresses the image at first with single level compression and then encrypts it; furthermore the image is decoded and reconstructed to the original image.

Some of the applications need a fast image compression technique but most of the available technique requires impressive time. So this proposed algorithm (Haar wavelet transformation) used to compress the image rapidly. Examining the RC4 parameters have demonstrated that the speed of encoding or decoding time is straightforwardly identified with the encryption key length and to the information record estimate if the information is sufficiently extensive.

As a conclusion from the results that have been submitted after the execution of the codes and statistical analysis, we can say that the methods are successfully done and the values that have been submitted are significant. The time tested for the process was quick and the entropy for the original and encrypted image is near to 8 ideal values. In image processing field cryptography takes an important part because of information that is sensitive must keep their security safe. Therefore encryption algorithms have the main role in this segment. Developers and programmers can take benefit from such studies and researches.

This design can be used for transformation of information and digital data over the network securely, Till now it’s impossible to make sure that the Internet networks are secure completely but at list, these encryption algorithms work against the hackers.

The obtained results for the statistical analysis shows good results, according to other proposed methods in some analysis proposed method’s results are more significant and good, while in others there was little difference.

For the future works, this research can be used as an application for encryption and add other various algorithms and collect all in one design.

REFERENCES

Aashish, R., 2014 Image Encryption and Decryption, Jul 15, 2014. Available at: **https://www.slideshare.net/ramamurthyaashish/image-encryption-and-decryption**. Accessed 1 July 2017.

Abhinandan, V. and KN, S. 2011. ***Image Encryption Techniques***. Bengaluru.

Ahadpour, S., Sadra, Y., Sadeghi, M. 2016. ***Image Encryption Based On Gradient Haar Wavelet and Rational Order Chaotic Maps***, University of Mohaghegh Ardabili.

Anonymous, 2013. RC4 Encryption Algorithm. ***https://www.vocal.com/cryptography/rc4-encryption-algoritm/***. Accessed 30 June 2017.

Anonymous, 2017. Digital Image Processing. ***https://www.tutorialspoint.com/dip/index.htm***. Accessed 30 June 2017.

Arur, S., 2013. Cryptography. ***https://www.slideshare.net/shivanandarur/cryptography-ppt-slideshare***. Accessed 1 July 2017.

Bradford, C., 2016. 5 Common Encryption Algorithms and the Unbreakables of the Future. ***https://www.storagecraft.com/blog/5-common-encryption-algorithms/***. Accessed 30 June 2017.

Cui, D., Shu, L., Chen, Y. and Wu, X. 2013. Image encryption using block based transformation with fractional Fourier transform. ***Communications and Networking in China (CHINACOM)***, ***2013 8th International Conference on*** (pp. 552–556).

Dixit, A., Dhurve, P. and Bhagwan, D. 2012. ***Image Encryption Using Permutation and Rotation XOR Technique,*** Mumbai University.

Gao, T. and Chen, Z. 2008. A new image encryption algorithm based on hyper-chaos. ***Physics Letter A***, **372**, 394–300.

Gaur, D., 2014. What is The Definition of Image Compression? ***https://www.researchgate.net/post/What_is_the_definition_of_image_compression*** Accessed 2 July 2017.

Goncalves, B. 2009. Etude de WEP et Rivest Cipher 4. ***http://paginas.fe.up.pt/~ei10109/ca/rc4.html*** Accessed 15 July 2017.

Guan, Z.-H., Huang, F. and Guan, W. 2005. Chaos-based image encryption algorithm. ***Physics Letters A***, **346**(1–3), 153–157.

Hashim, H. R. and Neamaa, I. A. 2014. Image Encryption and Decryption in A Modification of ElGamal Cryptosystem in MATLAB. ***Journal of Basic and Applied Research***, **4531**, 141–147.

Irfan, P., Prayudi, Y. and Riadi, I. 2015. Image Encryption using Combination of Chaotic System and Rivers Shamir Adleman (RSA). ***International Journal of Computer Applications***, **123**(6), 11–16.

Jindal, P. and Singh, B. 2015. RC4 Encryption-A Literature Survey. ***Procedia Computer Science Elsevier Masson SAS Icict***, **46**, 697–705.

Jolfaei, A. 2011. Image Encryption Using Chaos and Block Cipher. ***Computer and Information Science***, **4**(1), 172–185.

Kumar, M., Aggarwal, A. and Garg, A. 2014. A Review on Various Digital Image Encryption Techniques and Security Criteria. ***International Journal of Computer Applications***, **96**(13), 19–26.

Kumar, M. and Vaish, A. 2017. Encryption of Color Images Using MSVD in DCST Domain. ***Optics and Lasers in Engineering***, **88**, 51–59.

Kumar, R., Pratap, B. and Singh, V. 2014. Image Encryption Using a Combination of Haar and DNA Algorithm. ***International Journal of Advanced Trends in Computer Science and Engineering***, **3**(5), 82–87.

Loukhaoukha, K., Chouinard, J., Berdai, A. 2012. A Secure Image Encryption Algorithm Based on Rubik's Cube Principle. ***Journal of Electrical and Computer Engineering***, 2012, 1-13.

Mousa, A. and Hamad, A. 2006. Evaluation of the RC4 Algorithm for Data Encryption. ***International Journal of Computer Science & Applications***, **3**(1), 44–56.

Munir, R. 2012. Security analysis of selective image encryption algorithm based on chaos and CBC-like mode. ***Telecommunication Systems, Services, and Applications (TSSA), 2012 7th International Conference on*** (pp. 142–146). IEEE.

Pantech, 2013. Matlab Code For PSNR And MSE. ***https://www.pantechsolutions.net/blog/matlab-code-for-psnr-and-mse/*** Accessed 3 July 2017.

Patel, K. D. and Belani, S. 2011. Image encryption using different techniques: A review. ***International Journal of Emerging Technology and Advanced Engineering***, **1**(1), 30–34.

Rathee, M. and Vij, A. 2014. Image Compression Using Discrete HAAR Wavelet Transforms. ***International Journal of Engineering and Innovative Technology***, **3**(12), 47–51.

Raviraj, P. and Sanavullah, M. Y. 2007. The Modified 2D-Haar Wavelet Transformation in Image Compression. ***Middle-East Journal of Scientific Research***, **2**(2), 73–78.

Rouse, M., 2014. Encryption. ***http://searchsecurity.techtarget.com/definition/encryption*** Accessed 2 July 2017.

Sasidharan, S. and Philip, D. S. 2011. A Fast Partial Image Encryption Scheme with Wavelet Transform and RC4. ***International Journal of Advances in Engineering & Technology(IJAET)***, **1**(4), 322–331.

Sethi, N., Krishna, R. and Arora, R. P. 2011. Image Compression Using HAAR Wavelet Transform. ***International Journal of Advanced Research in Computer and Communication Engineering***, **2**(3), 1–6.

Stallings, W. 2005 The RC4 Stream Encryption Algorithm.1-7.

Stine, K. and Dang, Q. 2011. Encryption Basics. ***Journal of AHIMA***, **5**(82), 44–46.

Stinson, D. R. 1995. Cryptography: Theory and Practice. ***CRC Press LLC***.

Suliga, M., 2015. Why is image compression important? ***https://www.quora.com/Why-is-image-compression-important*** Accessed 1 July 2017.

Tamboli, S. . and Udupi, V. 2013. Image Compression Using HAAR Wavelet Transform. ***International Journal of Advanced Research in Computer and Communication Engineering***, **2**(8), 3166–3170.

Tedmori, S. and Al-Najdawi, N. 2014. Image cryptographic algorithm based on the Haar wavelet transform. ***Information Sciences***, **269** (March), 21–34.

Villanueva, J. C., 2015. What Is A Cipher? ***http://www.jscape.com/blog/what-is-a-cipher.*** Accessed 1 Feb 2017.

Wei, W.-Y. 1997. An Introduction to Image Compression. ***Institute of Communication Engineering***, 1-20.

Xu, S., Wang, Y., Wang, J. and Guo, Y. 2010. A Fast Image Encryption Scheme Based on a Nonlinear Chaotic Map. ***Signal Processing Systems (ICSPS) 2nd International Conference on*** 326–330.

Zeghid, M., Machhout, M., Khriji, L., Baganne, A. and Tourki, R. 2007. A Modified AES Based Algorithm for Image Encryption. ***International Journal of Computer, Electrical, Automation, Control and Information Engineering***, **1**(1), 745–750.

Zhang, L., Liao, X. and Wang, X. 2005. An Image Encryption Approach Based on Chaotic Maps. ***Chaos, Solitons & Fractals***, **24**(3), 759–765.

Zhang, Q., Xue, X. and Wei, X. 2012 'A Novel Image Encryption Algorithm Based On DNA Subsequence Operation. ***The Scientific World Journal***, **2012**.

APPENDIXES

APPENDIX 1. Genişletilmiş Türkçe Özet (Extended Turkish Abstract)

HAAR DALGACIK DÖNÜŞÜMÜ VE RC4 ALGORİTMASINA DAYALI GÖRÜNTÜ ŞİFRELEME

YASIN, Elham Tahsin
Yüksek Lisans Tezi, Elektrik-Elektronik Mühendisliği Anabilim Dalı
Tez Danışmanı: Doç. Dr. Rıdvan SARAÇOĞLU
Temmuz 2017, 59 Sayfa

Günümüzde bilgi ve verilerin güvenliği, gizliliği kritik bir meseleye dönüşmüştür. Güvenli iletim için ilerlemiş teknikler, ileri düzeydeki resimlerin düzeltilmesi, çeşitli askeri ve onarmaya yönelik uygulamalar, ülke güvenliği ve farklı uygulamalar için devamlı olarak gereklidir. Günümüzde bilgi güvenliğinin güçlendirilmesi için kulanılan farklı yollardan en temeli şifreleme sistemleridir. Bilgileri veya verileri anlaşılmayacak şekilde başka bir yapıya dönüştürerek mesajın güvenliği sağlanır. Bu tezdeki temel fikir, Haar dalgacık dönüşümü ve RC4 şifreleme algoritması olmak üzere iki algoritmayı birleştirerek güvenliği optimize etmektir. Haar dalgacık dönüşümü, görüntüyü sıkıştırmak, sadeliği sağlamak ve yüksek hızlı performans elde etmek için kullanılır. Ayrıca ağ üzerinden hızlı gönderilebilir. RC4 şifreleme ise görüntüyü herhangi bir ağ üzerinden güvenli ve sağlam bir şekilde şifrelemek ve çözmek için kullanılır.

Anahtar kelimeler: Bilgi güvenliği, Görüntü sıkıştırma, Görüntü şifreleme, Haar dönüşümü, Kriptografi, RC4 akış şifresi.

1. GİRİŞ

Dijital görüntü işleme ve ağ iletişimi, elektronik yayıncılık ve dijital multimedya verisinin internet üzerinden yaygın olarak yayınlanmasıyla birlikte, yasadışı kopyalama ve dağıtıma karşı dijital bilgilerin korunması, saklaması ve iletimi son derece önem kazanmıştır. Görüntüler, farklı işlemlerde yaygın olarak kullanılmaya başlamıştır. Bu nedenle, görüntü verilerinin yetkisiz kullanımlara karşı güvenliği önemli bir durum olmaya başlamıştır.

Görüntü şifreleme bilgi gizleme alanında önemli bir rol oynamaktadır. Resim şifreleme yöntemi bilgiyi okunamaz hale getirmektir. Bu nedenle, sunucu yöneticileri de dahil olmak üzere herhangi biri, orjinal mesaja ya da iletilen bilgilere herhangi bir internet ağı üzerinden erişemez. Görüntüleri korumalı tutmanın ana amacı, gizlilik, bütünlük ve orijinalliği korumaktır. Görüntüleri güvenli hale getirmek için farklı teknikler mevcuttur ve bunlardan biri de şifreleme yöntemidir.

Ayrıca kablo TV, çevrimiçi kişisel fotoğraf albümü, tıbbi görüntüleme sistemleri, askeri görüntü iletişimi ve gizli video konferansları gibi birçok uygulamada dijital görüntülerin saklaması ve aktarılmasında özel ve güvenilir sistemler gereklidir. Böyle bir gereksinimi gidermek için birçok görüntü şifreleme yöntemleri önerilmiştir.

Şifreleme, elektronik verileri şifreli hale getiren ve yetkili taraflar haricindeki kimseler tarafından kolaylıkla anlaşılamayan başka bir biçime dönüştürülmesidir.

Şifrelemenin birinci amacı, bilgisayar sistemlerinde saklanan veya internet ve diğer bilgisayar ağları vasıtasıyla iletilen dijital verilerin gizliliğini korumaktır. Modern Şifreleme Algoritmaları, yalnızca gizliliği sağlamakla kalmaz. Aynı zamanda aşağıdaki güvenlik unsurlarını da sağlayabileceğinden Bilgi Teknolojileri sistemlerinin ve iletişim güvenliğinin sağlanmasında hayati bir rol oynarlar:

- Kimlik doğrulama: bir mesajın orijinini doğrulayabilir.
- Bütünlük: bir mesajın içeriğinin gönderildikten sonra değiştirilmediğini kanıtlar.
- Reddedememe: bir mesajı gönderen gönderilen mesajı yalanlayamaz.

Bu tezin temel amacı, önce görüntüyü sıkıştırmak ve sonra şifrelemek, böylece onu ağ üzerinden hızlı, güvenli ve korumalı bir şekilde iletebilmektir

2. MATERYAL ve YÖNTEM

2.1. Resim

Günümüzde Dijital görüntü, neredeyse tüm alanlardaki birçok uygulamada yer almaktadır; Bilgi Gizleme, Haberleşme vb. Bu görüntülerin güvenliği çok önemlidir. Resim şifreleme, dijital görüntülere güvenlik sağlama yöntemlerinden biridir.

Pikseller bir görüntünün temel öğeleridir, bu nedenle bir görüntüyü şifrelemek için her pikselde gizli bilgiler şifrelenir. Pikselin konum değerleri şifreleme amacı için de kullanılabilir.

2.2. Resim Şifreleme

Şifreleme, düz metinleri şifreli metin haline dönüştürme işlemidir. Şifreleme, şifreleme metodunu kullanarak, şifrelenecek metin denilen ya da düz metin olarak adlandırılan orijinal veriyi ya da bilgiyi, yetkisiz bir kişi tarafından okunamayan bir biçime dönüştürme yöntemidir. Görüntü şifreleme teknikleri bir görüntüyü anlaşılması zor olan başka bir görüntüye dönüştürmeye çalışır. Öte yandan resim şifre çözmesi; orijinal resmi; şifrelenmiş halinden oluşturur. Verileri şifrelemek ve şifre çözmek için çeşitli görüntü şifreleme sistemleri vardır.

Resim şifreleme, multimedya sistemleri, tıbbi görüntüleme, askeri iletişim, İnternet iletişimi vb. uygulama alanlarına sahiptir. Görüntüleri güvenli bir şekilde iletmek için bir dizi şifreleme şeması önerilmiştir. Analiz ettiğimiz şemalar üç farklı biçimde sınıflandırılabilir: konum değiştirme, değer dönüşümü ve görsel dönüşüm.

Görüntü şifreleme, daha büyük veri kaybı, daha yüksek yedeklilik ve görüntülerdeki piksellerin daha güçlü korelasyonu nedeniyle metin şifrelemesinden farklıdır.

Şifreleme algoritmasının gizli kısmı, şifreleme ve şifre çözme işlemi için kullanılan anahtardır. Anahtar rasgele bitlerden oluşur ve herhangi bir değer olabilir. Her algoritma anahtar alanı kullanır. Anahtar, algoritmanın anahtar alanında rastgele değerler kullanılarak

oluşturulmuştur. Anahtar alanı ne kadar büyük olursa, farklı anahtarları göstermek için kullanabileceğimiz anahtarların değerleri de o kadar yüksek olur.

2.3. Haar Dalgacık Dönüşümü

Görüntü sıkıştırma yöntemlerinden biri olan bu yöntem, 1908'de Macar matematikçisi Alfred Haar tarafından önerilen HDD üzerine kuruludur. Dalgacıklar, verilerin frekanslara göre sıralanması için geliştirilen matematiksel fonksiyonlardır. Dalgacıklar görüntü sıkıştırma, veri sıkıştırma, şifrelenmiş veriler ve çok daha fazlası gibi birçok alanda uygulanmıştır.

Önce, Haar dalgacık dönüşümü kullanılarak görüntü sıkıştırılır. Dalgacıklar, matematiksel temel işlev kümesidir. Dalgacık terimleri cinsinden bir fonksiyona yaklaşırken, dalgacık temel fonksiyonları yaklaşık fonksiyona göre seçilir. Dalgacıklar, girdi işlevini en etkili biçimde temsil eden dinamik bir temel işlev dizisi kullanır. Dolayısıyla dalgacıklar çok fazla sıkıştırma sağlayabilir ve bu nedenle görüntü ve sinyal işleme alanlarında çok popülerdirler.

Bir dalgacık dönüşümü verileri uzaysal frekans alanına dönüştürür ve her bileşeni karşılık gelen bir özünürlük skalasıyla saklar. Haar dalgacık dönüşümü uygulandığında, bu görüntüyü düşük çözünürlüklü bir görüntü ve bir detay katsayıları terimleri ile temsil edebiliriz. Haar Transform, ortalama ve fark almadan başka bir şey değildir.

Haar dalgacık dönüşümünün avantajları olan hesaplama süresi açısından en iyi performansı vermesi, hesaplama hızının yüksek olması, basit olması sebebiyle HDD verimli bir sıkıştırma yöntemidir ve mevcut bir geçici dizin olmaksızın hesaplanabildiğinden dolayı hafızayı verimli kullanır.

2.4. RC4 Algoritması

RC4, RSA Güvenlik'ten Ronald Rivest tarafından 1987'de tasarlanmış ve en yaygın yazılım akış şifrelemelerinden biri olarak bilinmektedir. Güvenli Yuva Katmanı / Aktarım Katmanı Güvenliği (SSL / TLS) (İnternet trafiğini korumak için), WEP (güvenli kablosuz

ağlar) ve PDF gibi popüler protokollerde kullanılan bir akış şifresi olup bir simetrik anahtar algoritmasıdır. Yazılım açısından hızlı ve basit olarak kabul edilir.

RC4 şifreleme algoritması, 40 ve 128 bitlik anahtarlar kullanarak WEP (Kablosuz Şifreleme Protokolü) içinde IEEE 802.11 gibi standartlarda kullanılır. Ayrıca, Lotus Notes ve Oracle Secure SQL gibi birçok ticari yazılım paketinde de kullanılır.

RC4 şifreleme algoritması için adımlar:

- Şifrelenecek verileri ve seçili anahtarı alın.
- İki string dizisi oluşturun.
- 0'dan 255'e kadar olan sayıları içeren bir diziyi başlatın.
- Seçili anahtar ile diğer diziyi doldurun.
- Anahtar dizisine bağlı olarak ilk diziyi rastgele oluşturun.
- Son anahtar akışını oluşturmak için kendi içindeki ilk diziyi rastgele oluşturun.
- Kesin metin akışı sağlamak için şifrelenecek verilerle son anahtar akışını XOR'layın.

Aynı algoritma hem şifreleme hem de şifre çözme için kullanılır çünkü veri akışı, üretilen anahtar dizisiyle XOR yapılır. Anahtar akış, kullanılan düz metinden tamamen bağımsızdır. 256 bitlik bir durum tablosunu başlatmak için 1 ila 256 bit arasında değişken uzunlukta bir anahtar kullanılır.

Durum tablosu daha sonra sahte rastgele bitlerin üretilmesi ve daha sonra şifreli metin vermek üzere düz metinle XOR yapılan bir sahte rastgele akış üretmek için kullanılır. Algoritma iki aşamaya ayrılabilir: başlatma ve işlem. Başlangıç aşamasında 256 bitlik durum tablosu S, bir kaynak olarak K tuşu kullanılarak doldurulur. Durum tablosu kurulduktan sonra, veri şifrelendiği için düzenli bir şekilde değiştirilmeye devam eder. Başlatma işlemi sahte kodla özetlenebilir.

Bu algoritma, sahte rastgele değerler akışı üretir. Giriş akışı, bu değerlerle, bit-bit eşleştirilerek XOR yapılır. Şifreleme ve şifre çözme işlemi; veri akışı, üretilen anahtar diziyle sadece XOR yapılırken aynıdır. Çıktı baytı, S (i) ve S (j) değerlerine bakılarak, bunları modulo 256'ya ekleyerek ve sonra S'deki toplamı aramakla seçilir; S (S (i) + S (j)), anahtar akışının bir K baytı olarak kullanılır.

Görüntü şifrelemesinin en önemli kısmı güvenliktir. Önerilen yöntemin, şifreli görüntünün güvenliğini sağlamak için eksiksiz bir analizi yapılmalıdır.

Tüm hesaplamaları gerçekleştirmek ve tüm resimleri oluşturmak ve görüntülemek için Matlab sayısal ve görselleştirme yazılımı kullanılmaktadır.

3. SONUÇ

Görüntüler için RC4 şifreleme akışı ile Haar dalgacık dönüşümü kullanılan bir resim şifrelendirme sistemi bu tezde sunulmuştur. Sistem ilk önce görüntüyü sıkıştırır ve şifreler, daha sonra sistem resmin şifresini çözer ve orijinal resme tekrardan dönüştürür.

Bazı uygulamalarda hızlı görüntü sıkıştırma tekniğine ihtiyaç duyulur ancak mevcut tekniklerde görüntü sıkıştırma uzun zaman alır. Dolayısıyla bu önerilen algoritma (Haar) görüntüyü hızlıca sıkıştırır. RC4 parametrelerinin incelenmesi, kodlama veya kod çözme süresi, şifreleme anahtarı uzunluğu ve bilgilerin yeterince kapsamlı olup olmadığı bilgisi, kayıt tahminiyle açık bir şekilde tanımlandığını göstermiştir.

Kodların ve istatistiksel analizlerin uygulanmasından sonra elde edilen sonuçların yola çıkarak, yöntemlerin başarıyla yapıldığını ve elde edilen sonuçların önemli olduğunu söyleyebiliriz. Görüntü işleme alanındaki şifreleme, hassas bilgileri güvende tutması nedeniyle önemli bir rol oynamaktadır. Bu nedenle, bu bölümde şifreleme algoritmaları ana rolü oynamaktadır. Geliştiriciler ve programcılar, bu tür çalışmalar ve araştırmalardan faydalanabilir.

Bu tasarım, bilgi ve dijital verilerin ağ üzerinde güvenle dönüştürülmesi için kullanılabilir, ancak İnternet ağlarının tamamen güvende olmasını sağlamak imkansız olsa bile bu şifreleme algoritmaları en azından bilgisayar korsanlarına karşı koymaya çalışmaktadır.

Gelecekteki çalışmalar için bu araştırma, şifreleme ve diğer çeşitli algoritmaların eklenmesi için bir temel uygulama olarak kullanılabilir ve hepsini tek bir tasarımda toplanabilir.

CURRICULUM VITAE

Elham Tahsin YASIN was born in 1993- Erbil / Iraq, finished her secondary and high school education from Private Nilüfer Girls' College in 2011. The same year got accepted in Computer Science (IT) Department of Science College at Salahaddin University – Erbil. In 2015 got graduated from Computer Department. In September 2015, started her postgraduate study in the department of Electrical-Electronics Engineering Department, Institute of Natural and Applied Sciences at Van Yüzüncü Yıl University – VAN.

UNIVERSITY OF YUZUNCU YIL
THE ISTITUTE OF NATURAL AND APPLIED SCIENCES
THESIS ORIGINALITY REPORT

Date:04/08/2017

Thesis Title: IMAGE ENCRYPTION BASED ON HAAR WAVELET TRANSFORMATION AND RC4 ALGORITHM

The title of the mentioned thesis above having total 36 pages with cover page, introduction, main parts and conclusion,has been checked for originality by Turnitin computer program on the date of 04/08/2017 and its detected similar rate was 13% according to the following specified filtering originality report rules:

- Excluding the Cover page,
- Excluding the Thanks,
- Excluding the Contents,
- Excluding the Symbols and Abbreviations,
- Excluding the Materials and Methods
- Excluding the Bibliography,
- Excluding the Citations,
- Excluding the publications obtained from the thesis,
- Excluding the text parts less than 7 words (Limit match size to 7 words)

I read the Thesis Originality Report Guidelines of Yuzuncu Yil University for Obtaining and Using Similarity Rate for the thesis, and I declarethe accuracy of the information I have given above and my thesisdoes not contain any plagiarism; otherwise I accept legal responsibility for any dispute arising in situations which are likely to be detected.

Sincerely yours,

04/08/2017
Date and Signature

Name and Surname: Elham Tahsin YASIN

Student ID# :159101110

Science : Department of Electrical and Electronics Engineering

Program: .....

Statute:M. Sc.☐ Ph.D.☐

APPROVAL OF SUPERVISOR
SUITABLE
Assoc. Prof. Dr. Rıdvan SARAÇOĞLU

(Title, Name-Surname, Signature)

APPROVAL OF THE INSTITUTE
SUITABLE
Prof.Dr.Suat ŞENSOY
Enstitü Müdürü

(Title, Name-Surname, Signature)