T.C.

AKSARAY UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCE

DEPARTMENT OF ELECTRICAL ELECTRONIC AND COMPUTER ENGINEERING

A CRYPTOGRAPHIC SCHEME FOR COLOR IMAGES

MASTER OF SCIENCE THESIS

Nada Mohammed Murad MURAD

SUPERVISOR

Assoc. Prof. Dr. Yunus UZUN

AKSARAY, 2019

Aksaray University, Institute of Science and Technology Approval **NADA MOHAMMED MURAD MURAD**, M.Sc. with thesis student No. **162335816** successfully presented the M.Sc. thesis titled "**A CRYPTOGRAPHIC SCHEME FOR COLOR IMAGES**", prepared after satisfying all the requirements identified in the concerned bylaws, before the jury whose signatures are affixed below.

Thesis Advisor: Assoc. Prof. Dr. Yunus Uzun
Aksaray University
I approve that this thesis is a Master Thesis in scope and quality .....

Asst. Prof. Dr. Filiz SARI
Aksaray University
I approve that this thesis is a Master Thesis in scope and quality .....

Asst. Prof. Dr. Murat IŞIK
Ahi Evran University
I approve that this thesis is a Master Thesis in scope and quality .....

Date of Defence: 25/07/2019

I agree that this thesis, which is accepted by the jury, has fulfilled the requirements for being a Master Thesis.

.....
Assoc. Prof. Dr. M.Ali HINIS

DECLARATION

I declare that I write this work as a master thesis without any help and a way that would be contrary to academic rules and scientific ethics, morals, and traditions.

I declare that I will endure all moral and legal consequences that will arise if this situation is found to be contrary to my statement, regardless of a certain time period by the Institute.

N.A

Nada Mohammed Murad MURA

ACKNOWLEDGEMENT

Foremost, I am very thankful to the almighty Allah for giving me the strength, and the ability to accomplish this work. I would like to express my sincere gratitude to Assoc.Prof.Dr. Yunus Uzun for being the supervisor of my work. He offered me all the essential information necessary to make my thesis solid and useful. Similarly, I seize the opportunity to extend my thanks to all my friend as well as all my other colleagues for kindly helping and supporting. Finally, a special thanks to my family, brothers, sisters, and their families for their continuous encouragement.

Nada Mohammed Murad MURAD

AKSARAY, 2019

TABLE OF CONTENTS

YÜKSEK LİSANS TEZİ

RENKLİ GÖRÜNTÜLER İÇİN BİR KRİPTOGRAFİK ŞEMA

NADA MOHAMMED MURAD MURAD

Aksaray Üniversitesi
Fen Bilimleri Enstitüsü
Elektrik Elektronik ve Bilgisayar Mühendisliği Anabilim Dalı

Tez Danışmanı: Doç. Dr. Yunus Uzun

ÖZET

Multimedya uygulamalarının geniş kullanımı nedeniyle, görüntü kodlama standartları, multimedya yayılımını destekleyen yollardan biriydi.İnternet saniye binlerce kişi tarafından sosyal medya veya reklam veya iş amaçlı web siteleri aracılığıyla yüklenen dijital belgelerle doludur.Dijital multimedya yayılımı için şifreleme ve şifre çözme teknikleri gerekir. Günümüzde, İnternet üzerinden veri yayılımında gizlilik ve kimlik doğrulama hizmetleri çok önemlidir.Bu çalışma, çoklu ortam sıkıştırma sistemleri ile şifrelemeyi bütünleştiren görüntü güvenliğine odaklanmaktadır. Ayrıca JPEG şifrelemeyle birleştirilmiş görüntü şifreleme algoritmaları da önerilmiştir. Görüntü sıkıştırma sistemiyle şifrelemenin entegrasyonu için üç yaklaşım önerilmiştir. Bunlar; Renk Düzlemi Geçirgenliği, Ayrık Kosinüs Dönüşüm (DCT) katsayıları ve DCT katsayılarının şifrelenmesi işaretidir.Önerilen yaklaşımlar katsayıların bazıları bir sıkıştırma sisteminin nihai sonuçlarından veya ara aşamalarından elde edilen seçici şifreleme ile desteklenmiştir.Önerilen yaklaşımların güvenlikleri de analiz edilmiştir. Simülasyon sonuçları önerilen sistemin güvenli, düşük maliyetli ve doğrudan bit hızı kontrolünü desteklediğini göstermiştir. Bu özellikler çalışmanın gerçek zamanlı işletim ve görüntü aktarımı içeren multimedya uygulamaları için uygun olmasını sağlar.

Anahtar Kelimeler: Kriptografi, Multimedya, Görüntü, Ayrık kosinüs dönüşümü.

Temmuz, 2019; 62 sayfa

M.Sc. THESIS

A CRYPTOGRAPHIC SCHEME FOR COLOR IMAGES

NADA MOHAMMED MURAD MURAD

Aksaray University
Graduate School of Natural and Applied Sciences
Department of Electrical Electronic and Computer Engineering

Supervisor: Assoc. Prof. Dr. Yunus Uzun

ABSTRACT

Due to the extensive use of multimedia applications, image coding standards are one of theways that supported multimedia spreading. Internet is full of digital documents that are uploaded by thousands every second through social media or any websites for commercials or business. Encryption and decryption techniques are required for digital multimedia distribution. Today, privacy and authentication services are crucial for data dissemination through the Internet. This work focuses on image security integrating encryption with multimedia compression systems. Also, image encryption algorithms combining with JPEG encoding are also proposed. Three approaches for integrating encryption with image compression system are proposed. These are Color Plane Permutation, Discrete Cosine Transform (DCT) coefficients, and sign encryption of DCT coefficients. The proposed approaches are supported by selective encryption, are a portion of the coefficients from either the final results or intermediate steps of a compression system. The securities of the proposed approaches are also analyzed. Simulations results show that the proposed system is secure, low cost, and compatible with direct bit-rate control. These properties make the study suitable for multimedia applications with the real-time operation and image transmission.

Keywords: Cryptography, Multimedia, Image, Discrete cosine transform.

July, 2019; 62 page

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
BRIE	Bit Recirculation Image Encryption
CBC	Cipher Block Chaining
CKBA	Chaotic Key - based Algorithm
CNNSE	Chaotic Neural NetworkSignal Encryption
DCT	Discrete Cosine Transform
DES	Data Encryption Standard
DLP	Data Loss Prevention
ELB	Electronic Library Code
FDCT	Forward Discrete Cosine Transform
HCIE	Hierarchical Chaotic Image Encryption
IDCT	Inverse Discrete Cosine Transform
ISO	International Organization for Standardization
JPEG	Join Photographic Experts Group
MPEG	Moving Picture Experts Group
PSNR	Peak Signal-to-Noise Ratio
RCES	Random Control Encryption Subsystem
RGB	Red Green and Blue
RLE	Run Length Encoding
RMS	Root Mean Square
RSA	Rivest-Shamir-Adleman
RSES	Random Seed Encryption Subsystem
SFC	Space Fill Curve
SNR	Signal-to-Noise
SPIHT	Set Partitioning in Hierarchical Trees

1. INTRODUCTION

Technology has now made a potentially big market for the distribution of digital multimedia content over the Internet, in particular in the computer and telecoms industries. The copyright of such contents is required because of its sensitivity and its importance (Raid et al.,2014)The application of encryption techniques on images and videos, enabled the attainment of the necessary privacy and security due to the worldwide Web availability, which makes it the perfect location for multimedia content. Multimedia encryption is the technology used when distributing digital content across a variety of distribution systems for comprehensive security.

The fundamental concept of an encryption system is to hide confidential data from unauthorized access and use. The methods commonly used are the storage and transmission of data on a computer, or via the Internet (usually regarded as an insecure network).

Cryptographic information is secured in the transmission channel so that the sender and the authorized recipient can easily access it. The encrypted text is known as encrypted plaintext or encryption, based on a set of rules known as encryption algorithms (Ambritha et al., 2016). This algorithm usually works according to the encryption key. The main core for the recipient to receive a specific message containing key encryption and message decryption is encryption algorithms.

1.1 Relationship Between Multimedia and Cryptography

Security of communication is one of the social necessities with the advancements in technology. The primary question that needs attention in this context:

- How can a file (image, video, audio) be transmitted secretly in a multimedia file without access from an unauthorized person?

Cryptography is the art or science of keeping secret secrets, an effective scientific approach to resolving this problem is via secure connection encryption in insecure channels(Chitra and Venkatesan, 2016).

Today, multimedia security becomes ever more important as multimedia data move through more and more open networks with the speedy development of digital networking technology. Reliable security in numerous true applications, such as pay television, medical systems, military image databases, and video conferencing, is usually required to store and transmit digital images and videos(Guanghui et al., 2014). Image encryption includes applications for

communications on the Internet, telemedicine, medical imaging, multimedia, telemedicine, military communication, and so on.

Although pictures encoding system varies significantly from the text, the traditional encryption practice has been to encode images directly, for two sources, which has been detrimental to the security of the file during transmission(Ao, 2012). The above technique is limited by two factors; first, the image size is usually significantly larger than the text; therefore, it takes long to directly encrypt image data by traditional cryptosystems like Data Encryption Standard (DES), Rivest–Shamir–Adleman (RSA), etc. Secondly, the encoding of images is different from the conventional practice where the original text is encoded in its original form (Ao, 2012).

1.2 A Brief Introduction to Cryptography

Cryptography describes ways to transmit messages otherwise so that the masquerade cannot be removed easily; thus, the message can be read only by the intended recipients(Fu et al ., 2018). The message that we want to send is the plain text and the masked message is referred to as the encrypted text. Enciphering or encryption is a process by which plain text is converted into encrypted text, and the reverse process is called decrypting. Sending data between transmitter and recipient ensures the protection of content by encryption(Fu et al., 2018). The data, however, are no longer snug and clear when subsequently received and decrypted.

Cryptography is an expertise in designing cipher systems, whereas code analysis is called the process of extracting plaintext information from a cipher without providing the relevant key. For both encryption and cryptanalysis, cryptology can be defined as the collective expression(AL-Laham, 2015). The techniques of encryption usually come in three basic types. Two for a key, two for text, graphics and other multimedia types, and the third for authentication and schemes. Figure (1.1) shows the encryption system.

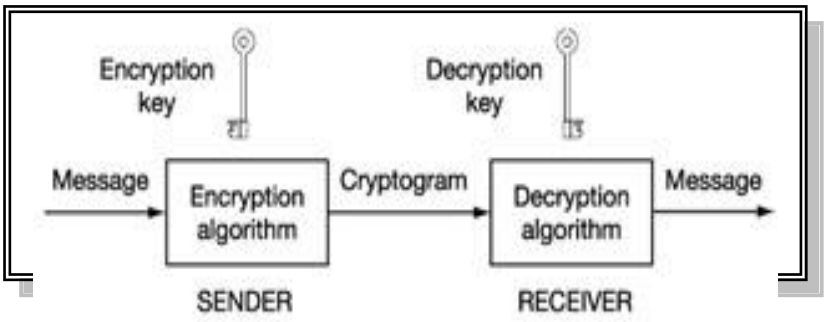


Figure 1.1. Cipher system.

• Secret key encryption technique uses one key to encrypt and decrypt the data. The approach employs a symmetric key encryption(AL-Laham, 2015). The encrypted data may be transmitted or stored on disks on insecure channels.

• Cryptography of the public key uses two keys, these keys are not symmetrical. One private key is used for encryptions, and another private key for decryption. All the keys are available to the public.

• Hash functions uses "fingerprint" as the only key to keep the message from being changed. The output of this algorithm is called the digest message. This algorithm also lists the recipient to reach the same digest after executing the message algorithm.

1.3 The Needfor Image/Video EncryptionSchemes

In this section we will evaluate the possibility of encrypting images and videos and outline the reasons for the existence of the various multimedia encryption schemes.

1. The tradeoff between voluminous data and slow-speed: Images and video clips are often large, large, even with a highly efficient compression process (AL-Laham, 2015). Since encryption of certain conventional nulls is not fast enough, particularly for software applications, it is difficult to simultaneously secure and fast encryption of large-scale data in real time.

2. Tradeoff between encryption and compression: If encryption is used in the past, a significant reduction of the effective pressure will be achieved by random encrypted script(Younes, 2019). You must therefore apply encryption after compressing, but it is difficult to incorporate the encryption algorithm into your integrated system due to the special and different image/video structures.

3. Compression dependency: the widely-used compression image/video technology reduces data size for encryption significantly and it is normal to expect fast encryption systems design and implementation to be easier. The encryption of such data reduction cannot however be

taken advantage of, since the compressor's encryption algorithm usually takes longer than the time. The efficiency of encryption is therefore largely dependent upon the compression algorithm.

4. Unwanted compression of pictures/videos in some applications is unacceptable because of legal considerations. Compression is not compressible to reduce data. Examples are well known in medical imaging systems. The loss model should store diagnostic pictures and visual videos of all patients. In this case, compression without loss is the only option, or images/videos will be left uncompressed.

5. Highly redundant, uncompressed images and videos are repeated extensively, which can cause the ECB (electronic library code) to switch on ciphers to fail to hide all visual information in certain normal images/videos. In order for you to encode high frequency uncompressed images and videos, you have to use cluster encoding that works with CBC (Cipher Block Chaining).

6. Loss of the avalanche property: The image and video breakdown cannot be achieved directly by using traditional zeros.

7. New security and usability concepts: different multimedia services require various levels of security and requirements for use. Typical examples are so-called cryptographic codes that encode only partial visual information and that provide an approximate view of high-quality services with an image from the code/video.

1.4 The Objective of Cryptography

For multimedia information security, the four key coding targets include:

1. Confidentiality.

Security of data from a prohibited incoming entry indicates confidentiality. The unwanted contact party, the opposing party, should not have access to the material for communication.

2. Data integrity.

Ensures licensed manipulation of the information.

3. Authentication.

The authentication includes a proof of information integrity because the sender cannot be the originator of the message if it is adjusted by transmission. The authentication of the entity confirms receipt of an identity message as well as the active share of the sender(Nisha, 2017).

4. Non-repudiation

The system assures the users access to data provided they are party to the communication thus

they can always authenticate their signature on a document.

1.5 Aim of This Thesis

The purpose of this message is:

1) Suggested image encryption is a suitable way to protect image data.

2) Combine JPEG encoding with image encryption algorithms.

3) Encryption system that is safe enough to stop attack by brute force and keeps the pressures unaltered.

4) Propose cryptographic algorithms based on localized interference.

5) Offer 3 image encryption algorithms:

- The first algorithm is mixed by semi - random SFCs (space fill curves) with the level of lighting and coloring.
- The second algorithm is mixed with DCTs in the various frequency bands in each DCT block.
- DCT tags are encrypted with the DES encryption algorithm for the third algorithm.

1.6 Literature Review

The search for multimedia encryption, like images, sound and video, becomes a hot topic with the development of multimedia technology. It is difficult to encrypt multimedia data directly by traditional encryption for large-scale properties and real-time requirements. Some new algorithms based on confusion or replacement can increase encryption, but the statistical properties of the data that affect the pressure can be changed, like(Younes, 2019; Agarwal, 2017; Geetha et al., 2018). In practice, before transmission or storage, the multimedia data is often compressed and therefore the conventional text-based algorithms are not adequate. Some cryptographic algorithms are preferred based on the problem of the increased need for multimedia encryption and compression, which combine the encryption process and the compression process.(Agrahari et al., 2017) suggested an image encryption algorithm based on router encoding. At the same time, the algorithm encrypts and secures both the sum table and the code stream during the encoding process.(Ochoa et al. , 2015) suggested the Set Partitioning in Hierarchical Trees (SPIHT) encoding-based image encryption algorithm.

JPEG compression is commonly used, and the requirements for JPEG image compression are vital. JPEG image encryption may be encrypted by encrypting Huffman tables, Hμ tables, and DCT parameters, according to the JPEG encryption process(Setyaningsih and Wardoyo,

2017). However, Huffman tables or tables are known to all users, making them vulnerable to attackers, produced through various tests and tests. Moreover, the tables or tables in Huffman are not secure against familiar attackers, as encrypted text and text can be recovered by comparison. The algorithm for the encryption of traditional DCT encryption changes the compression ratio substantially, in order to largely alter the statistical properties of DCTs(Shah and Haryan, 2018). Since the compression ratio is achieved in JPEG by adjust the quantization steps, DCT transaction ranges should not be altered to facilitate the direct bit rate control in the encryption process. In this thesis, we propose a JPEG image encryption algorithm, which blocks DCT blocks in the lighting and coloring levels through semi-random sfcs, blends DCTs by the different parts of each DCT block and encodes DCT parameters through the coding of an oscillatory current(Shah and Haryan, 2018). The algorithm is safe and affordable. It also affects the compression ratio somewhat and keeps the data format unchanged so that it can be controlled with direct bitrate.

1.7 Thesis Layout

The reminder of this thesis will be structured as follows:

Chapter two: discuss the various encryption techniques on image and video in addition on other related objects.

Chapter three: contains the design and the implementation of the proposed system with its encryption techniques.

Chapter four: contains the tests of the system, which include security analysis of the proposed encryption methods, experimental results, direct bit-rate control, and the encryption speed test.

Chapter five: presents the conclusions and the future works

2. MULTIMEDIA CRYPTOGRAPHY

Multimedia security, supplied by methods for video, sound and picture protection based on the cryptography and multimedia content. These methods are capable of communication safety or safety from content piracy (digital rights management and watermarking) or both(Shah and Pancholi, 2014).Developing effective encryption techniques for a wide range of multimedia issues, including streaming applications and the multi-media trade. For example, only those who use the service can have access to the content and achieve the purpose by appropriate encryption techniques(Kendhe., 2013). Two cryptosystems are available as described by (Iyer et al, 2016)

2.1 Symmetric Key Cryptosystems (private)

Every symmetrical key cryptosystem has a common property based on a secret shared by connected parties that are used to encrypt and decrypt. Nonetheless, the disadvantage of the symmetric key cryptography is the handling of an extensive communication network. For instance, n nodes with all other nodes n-1 shared secrets are required in the communication network. The large value of n is very unworkable and uncomfortable. Symmetrical cryptosystems are of benefit, for which the key sizes of public-key cryptosystems are considerably smaller for the same level of safety (Kendhe , 2013).

2.2 Asymmetric Key Cryptosystems (public)

This is a types of public-key cryptosystems where the secrete key is generated by a publicly known owner. The system is considered to be "asymmetric," because there is provision of different keys used for encryption and decryption. Only when publicly encrypted can the data be encrypted by a private key. Public key encryption systems today rely on computationally unwieldy issues. The RSA (Rivest–Shamir–Adleman) cryptosystem, for example, depends on the factoring integer difficulty, whereas the El-Gamal cryptosystem depends upon the DLP (Data Loss Prevention), which identifies a group element logarithm based on a generators in a final Abelian group(Nisha and Farik, 2017). The public - key cryptosystem does not need a common secret between communicators in order to solve the problem of a large, confidential communication network. Public cryptography therefore ensured all cryptographic objectives(Iyer et al., 2016).

2.3 Cryptanalysis

Encrypting a whole message or part of it is known as cryptanalysis while the deciphering key is not known. The cryptosystem's objective is to resist this attack and to give the opponent only one or more encrypted messages.The types that are based on both knowledge and system controlare cryptanalytic attack types(Tiwari et al., 2013).

-Brute force attack: exhaustive search and cryptosystem against brute force attacks should be ineffective. 128-bit key for brute force attacks is secure.

-Attack with known plaintext: it may be helpful to identify part of the whole key with little knowledge in plaintext matches for Cipher-text.

-Attack with the plaintext: by filling the plaintext selected in a black box which contains both the coded and keys algorithm, the black box sends the ciphertext that is matched to help you discover a secret key, or even a small part of it with a certain level of information.

-Attack chosen: Feed decryption algorithm and blackbox key to produce the corresponding plaintext containing a secret part or entire key.

2.4 Cryptography Techniques

Cryptography is a crucial technology in securing transmission of data via insecure channel. Different techniques can be utilized for the encryption of multimedia data. This section introduces the different multimedia cryptographic techniques such as video and image encryption.

2.4.1 Video encryption techniques

The popularity of multimedia application in the recent decade has made confidentiality of video communication a primary concern of the technology world. A variety of video encryption techniques exist that can be utilized in research and commercially(Tiwari et al., 2013). The video encryption technique is usually categorized based on the relations with the compression approach used. From this classification the following video encryption techniques can be used.

2.4.1.1 Video scrambling

The most popular way was to scratch video. This was used to make it more difficult to view paid cable channels freely than to do nothing about video. With the simplest possible safety in view of the simple substitution or transposition cipher, the video screw is very easy to use for

the permutation of signal or distortion of signal. These schemes lack serious security because they are easy to crack using modern computers.

2.4.1.2 Selective video encryption

Selective encryption techniques are the idea to encrypt part of the compressed bit stream for multimedia video playback and to meet the real-time constraint. Integrate encryption compression is regarded as a selective encryption approach (Goyal and Hemrajani, 2014). The selective video encryption can further classified based on technique used:

2.4.1.2.1Aegis

MPEG-1 and MPEG-2 video standard which unencrypts the B- and P-frames that Aegis has designed for I-frames(Hamidouche, Farajallah, Raulet, and Déforges, 2015). By holding all the parameters for decoding initialization, the MPEG encryption video sequence header is. This method also codes the ISO end code (Hamidouche et al., 2015).

2.4.1.2.2Block shuffling

Each sub-band of the MPEG/Audio is divided into blocks of identical size. The block size may differ depending on the sub-band and blocks of coefficients will be shuffled within each sub-band in accordance with a shuffling table generated by means of the key. For different sub-bands, the shuffling table varies and varies according to the frames. Scrambling contains most of the 2-D local sub-band signal statistics (Nisha et al., 2017). The negative effect on future statistical coding is therefore very small, while the visual impact is dramatic on a decompressed encrypted picture. Thus, the local transformation has less safety than the global transformation of the same image block. The high - level spatial structure is changed with the worldwide block transformation, which makes it more difficult to analyze the frequencies of local coefficients transmission. Block sizes can be selected for security trading using large blocks and less blocks with less safety (Nisha et al., 2017).

2.4.1.2.3Block rotation

For further safety improvement, every coefficient block can be rotated into an encrypted block. A set of eight blocks will select an encrypted block, taking into account rotating versions of the original block, as illustrated in Figure (2.1). Controlled key selection process(Madani et al., 2017).

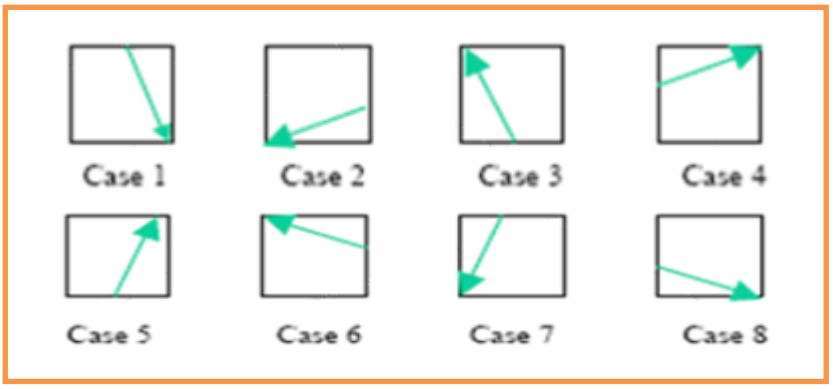


Figure2.1. Rotated versions of a block.

2.4.1.2.4Motion vector scrambling

In some situations, the motion of the scene is visible even if there are few or no intra-coded blocks in the P/B frame and I frame. That means that information on motion vector information scrambling may be essential for specific applications. Motion vectors are likely to encrypt the sign of movement vector in the same manner as encrypted signs of DCT coefficients and are also likely to change movement vector (Madani et al., 2017) in the same manner which coefficients can be changed.

2.4.2 Image encryption techniques

For fixed images the security of the complete image encryption can be achieved by using a naive approach. However, for certain applications, bottleneck problems remain a problem in communication and processing. Some kinds of encryption of images:

2.4.2.1 Selective Encryption

The first method that has the highest bitplane closest to the original (gray) color, with the least significant bitplane being random (Goyal and Hemrajani, 2014), is the uncompressed gray level frame defining 8-bits plans.

To generate the 8-bits frames and effectively encode them can be accomplished using the Huffman entropy. The Huffman entropy can be utilized in the generation of symbols that are the zero coefficients of zeroes. The symbols may be encoded to the categories of magnitude where non-zero coefficients end(Goyal and Hemrajani, 2014). Furthermore, the symbols will be encoded with 8-bit Huffman coefficients, followed by the attached signs and magnitude bits for the non-zero coefficients. For instance, the in encrypting using the Huffman entropy

the AC coefficients are encrypted while the DC coefficients are not encrypted. Therefore, the codes in both instances will not be encrypted as they are utilized for synchronization(Goyal and Hemrajani, 2014).

2.4.2.2 Selective bitplane encryption

Advanced Encryption Standard (AES) was the proposed cryptosystem method, but it can be selected for any fast conventional cryptosystem. The most important bitplane in the AES is not encrypted with good security(Banu, Tabassum, Fatima, 2013). The reconstruction of the MSB plane can be done using the remaining unencrypted bitplanes to form at least two or four bitplanes. As long as severe image data isolation is acceptable, only two bitplanes are encrypted, while the level of security is higher when encrypting four bitplanes. The user is responsible for determining whether the 2-bitplane degradation method, is considered to be adequate for the particular application or more reliable with four bitplanes(Banu, Tabassum, Fatima, 2013).

2.4.2.3 Image encryption schemes based on 1-D chaotic maps

The logistic map expressed as a function $f(x) = \mu x(1-x)$ is the chaotic map used to realize the control parameter μ within the secret kernel, in the precise computing of the computers, and the initial condition x(0).

In this encryption technique for every chaotic state the generation of pseudo - random binary sequence depends on the same thing as illustrated in the expression 2.1 (AL-Laham, 2015):

$$x(k) = 0.b(n.k)b(n.k+1)b(n.k+n-1) \quad (2.1)$$

Where the*n* is total number of pixels in an image and *k* represents the key, for each finite computing precision is higher than n by running the logistic map.

Further use chaotic binary sequence and/or value substitutions for pseudo - randomly control permutations requires the definition of the following terms.

- BRIE: Bit Recirculation Image Encryption is used for all pixel shift operations and replacing value.
- CKBA – For each pixel with key1 or key2, the chaotic key - based algorithm uses XOR or NXOR.
- HCIE: The division SM − Sn blocks depend on the plan M − N, where¨ Alternatively SM¨ TODAY M, SN¯ Alternatively N is used for control of no - round 4(SM + SN) − 2

transactions in the 4 different direction of block permutation. − 2 transactions in a single - image manner depending on the plane.

- CNNSE: The Chaotic Neural Signal Encryption Network uses weight control of the neural network for bit encryption of each pixel. The neutral function of chaotic network is given in equation 2.2(Ao, 2012):

$$d_i'(n) = d_i(n)pb(8xn + i) \tag{2.2}$$

Where

$d_i(n)$ and $d_i'(n)$represent the ith plain-bit and the ith cipher-bit.

- RSES and RCES: CKBA improved versions include the Random Seed Encryption Subsystem and the Random Control Encryption Subsystem. In CKBA, the two masking keys (key 1 and key2) used to control the exchange operations of adjacent pixels.

2.4.2.4 Image encryption scheme based on Space Filling Curve

Space-Filling Curves (SFC) are multi-dimensional one-dimensional space mappings. There is also a way to produce these curves geometrically for a distinct space in recurrent ways. For the reduction of bandwidth and dynamically unstructured partitioning in parallel systems, SFCs have been used in various application domains to multidimensional index data in image compression.

The d-dimensional space will first be separated into (n) equal sub-space (cells), depending on the recurrent construction of the SFCs. Approximation of the SFC is obtained by joining the centers of those cells, which these cells are joined to the line segments to join each cell within two adjacent cells.

Each cell can be equally filled with the same algorithm. The rotation and reflection for the curves passing through the cells may be carried out according to their link, in the form of a single curve that only crosses each of the n2d regions once and is called an approximation of each of these curve refinements (Suresh and Madhavan, 2012).

The main property of SFCs, dependent on recursive nature, are digital causality. The Kth approximation SFC construction contains the same portion of its length as each cell (nk x d). The number of points on the cells and belonging to the line segment is the same in its first (k-1) x d digits (Suresh and Madhavan, 2012), as long as the line distances are expressed as the base number.

The preservation of the location is considered SFCs. The 1-dimensional (curved) points of space that are closely connected are mapped from points of d-dimensional space. The otherwise not true, i.e., not all cells adjacent to d-dimensional space or even close to the curve. The other way around The contiguous cells of D dimensional space are usually mapped to an SFC segment collection (Suresh and Madhavan, 2012).

2.5 JPEG (Join Photographic Experts Group)

JPEG is a still image compression technique supporting the grayscale or color of black and white images that is not very easy to use. It works in continuous-tone pictures, depending on pixels with similar color adjustments. JPEG uses a large number of parameters to allow data lost to be adjusted. Even at the compression speed (10:1 or 20:1), image degradation often cannot be seen through the naked eye. JPEG designed for continuous-tone images. A variety of reasons of using JPEG are:

- Has a high compression rate and with high-quality pictures, it's excellent.
- Uses many parameters that allow compression or quality to be necessary.
- The chances of getting a good result are high with any continuous tone images.
- An advanced but simple method of compression that can work with many platforms(Nisha , 2017).

2.5.1 Luminance

The term light refers to the brightness of the image by light source power, but the sensitive brightness of human vision depends on the luminance's spectral composition.

Color spaces can be helpful if Y color is utilized in according to the sensitivity of the eye of man to small changes of luminance, which can be seen from the RGB subtraction in Y from the Blue and Red and Yellow- Blue, and Red-Yellow for new colors. Chroma is the presence or absence of blue (Cb) and red (Cr) color in a given luminance intensity.

For different applications, different number ranges Blue - Yellow and Red - Yellow are used. The YPbPr (designation for analog component video signals) range can be used to optimize the analog video component (Gonzalez et al., 2001).

Conversions from 16 - 235 to YCbCr between RGB are linear. The transformation of Red - Green - Blue to Yellow - Cb - Cr is(Rathod, Sisodia, & Sharma, 2011). The luminance can be transformed in accordance to equation 2.3:

$$R = Y + 1.371(Cr - 128)$$

$$G = Y - 0.698(Cr - 128) - 0.336(Cb - 128) \quad (2.3)$$

$$B = Y + 1.732(Cb - 128)$$(Rathod et al., 2011)

2.5.2 Discrete Cosine Transform (DCT)

The DCT is an orthogonal transformation that is based on a set of certain functions. The DCT techniques is used in the mapping of images into a frequency space. The DCT is desired in image processing as it packs energy in the lower frequencies of the image data.

Therefore, the JPEG standard can apply DCT to the data blocks of 8×8 pixels. The main reasons are:

1. The use of DCT on all image pixels results with better compression but slow, because many arithmetic operations are involved.
2. The use of DCT on data units reduces the compression ratio, making it faster.
3. Connections between pixels are within short range in continuous - ton images.

A pixel in an image has a particular value close to its neighbors. The DCT can be described using equation 2.4:

$$G_{ij} = \frac{1}{4} C_i C_j \sum_{x=0}^{7} \sum_{y=0}^{7} \cos\left(\frac{(2x+1)i\pi}{16}\right) \cos\left(\frac{(2y+1)i\pi}{16}\right) \quad (2.4)$$

Where

$$C_f = \begin{cases} \frac{1}{\sqrt{2}} & f = 0, \\ 1 & f = 0, and\ 0 \leq i, j \leq 7 \end{cases} \quad (2.5)$$

where C_f is C_i, C_j and P_{xy} are the values of image component

The JPEG decoder operates with the following equation by calculating the reverse DCT (2.6):

$$P_{xy} = \frac{1}{4}\sum_{x=0}^{7}\sum_{y=0}^{7} C_i C_j C_{ij} \cos\left(\frac{(2x+1)i\pi}{16}\right)\cos\left(\frac{(2y+1)i\pi}{16}\right) \quad (2.6)$$

where

$$C_f = \begin{cases} \frac{1}{\sqrt{2}} & f = 0, \\ 1 & f > 0 \end{cases}$$

2.5.3 Quantization

Quantization is the process of converting a continuous degree of terms into a finite range of discontinuous values. In cases, where loss occurs (exclusively some inevitable loss due to the calculation of finite accuracy of other steps), then the conversion of the discontinuous values will occur when each 8 to 8 matrix DCT coefficient is determined Gij. Each matrix number of the DCT coefficients is divided into "quantization table" by the corresponding number and the results are rounded to the nearest integer(de la Hucha Arce, Moonen, Verhelst, & Bertrand, 2017). The total number of JPEG parameters for each quantizing table is 64. The user can usually specify them all and fine-tune them to maximum compression. The following approaches normally apply to JPEG software:

1. Default table for quantizing. In accordance with the JPEG Committee for luminance (gray scale) and chiromancy components, two tables were the results of many experiments. Table (2.1) as demonstrated.

Table 2.1. Recommended Quantization tables(de la Hucha Arce et al., 2017).

16	11	10	16	24	40	51	61	17	18	24	47	99	99	99	99
12	12	14	19	26	58	60	55	18	21	26	66	99	99	99	99
14	13	16	24	40	57	69	56	24	26	56	99	99	99	99	99
14	17	22	29	51	87	80	62	47	66	99	99	99	99	99	99
18	22	37	56	68	109	103	77	99	99	99	99	99	99	99	99
24	35	55	64	81	104	113	92	99	99	99	99	99	99	99	99
49	64	78	87	103	121	120	101	99	99	99	99	99	99	99	99
72	92	95	98	112	100	103	99	99	99	99	99	99	99	99	99

Luminance Chrominance

2. A simple Q calculation table is based on the user supplied parameter R. The Qi j= 1+(i+j) lemon R simply means that QCs start small at the upper right corner and grow bigger to the lower right corner. Select, for example, R= 2 that produced the table quantization coefficients (2.2) as shown in Table (2.2).

Table 2.2: The Quantization table 1- (i + j) × 2

1	3	5	7	9	11	13	15
3	5	7	9	11	13	15	17
5	7	9	11	13	15	17	19
7	9	11	13	15	17	19	21
9	11	13	15	17	19	21	23
11	13	15	17	19	21	23	25
13	15	17	19	21	23	25	27
15	17	19	21	23	25	27	29

2.5.4 Zig-Zag scanning

Only the small-frequency block contains after the quantization non-zero coefficients. For reducing the number of bits, storage and communication are required. Instead of dealing with every single null, representation is many zeros are put together. It is done by zig-zag scan accomplished as demonstrated as (Figure (2.2).

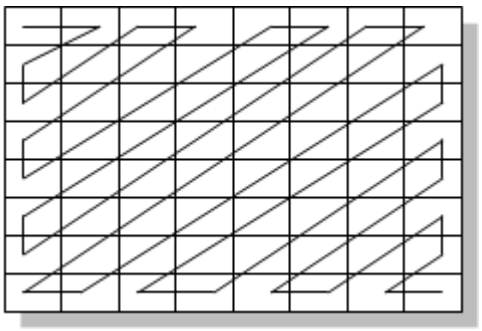


Figure2.2. Zig-Zag scanning(Candra et al., 2017).

2.5.5 Coding

Each of the 8 / 8 matrix quantized DCT coefficients has one [top left (0, 0))] DC coefficient and 63 AC coefficients. The DCT is quantified according to the Run-length encoding (RLE)and Huffman coding combinations. Furthermore, Run–Length encoding (RLE) is a compression process that counts adjacent pixels by gray level value, which is referred to as

the Run length count. The fundamental RLC execution is in different ways, so the first step is to define the necessary parameters(de la Hucha Arce et al., 2017).We can use either the horizontal RLC, or the vertical RLC, which can count along the rows. The next step is to define for the first RLC number a convention in a row, to set the convention to represent the first RLC number of 0(de la Hucha Arce et al., 2017).

The Huffman coding another form of coding that can be used in the coding of data. The minimum code for the length is Huffman, which means that the statistical distribution of the gray levels is provided. The result of this procedure is to produce a variable code length according to unparalleled code words(Mourad and Bouhlel, 2017).

The Huffman algorithm can be described in five steps:

1. Find the histogram to find the probabilities of gray-level of the image.
2. According to the size, order the input probabilities (histogram magnitudes).
3. Add the smallest two to each other.
4. Back to step 2, till only 2 probabilities left.
5. Generate code by alternating assignment of 0 and 1 and working backward along the tree.

2.6 Fidelity Criteria

For unbiased results, fidelity assessment measures are useful in comparing various versions of the same image for relative measurements. The measures used are the generally used RMS, the signal-to-noise (SNR) ratio and the maximum signal-to-noise ratio(Mourad & Bouhlel, 2017). The measurement method is usually used. The error between the original pixel value and the pixel value encryption can be defined using the expression in equation 2.7.

$$error(r,c) = \hat{I}(r,c) - I(r,c) \tag{2.7}$$

Where

$I(r,c)$ is the original image

$\hat{I}(r,c)$ is the decipher image.

The total error in an N × N deciphered imageas defined in equation 2.8:

$$Total\ error = \sum_{r=0}^{N-1}\sum_{c=0}^{N-1}[\hat{I}(r,c) - I(r,c)] \tag{2.8}$$

The root mean square can be computed as

$$RMS = \sqrt{\frac{1}{N^2}\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}[\hat{I}(r,c) - I(r,c)]^2} \quad (2.9)$$

Where N is the total number of pixels in the image.

The smaller the metric value, the better the encrypted image of the original image(Mourad and Bouhlel, 2017). Signal to Noise Ratio (SNR) is another measure, and a larger number involves a better image. In the SNR, the deciphered image is considered to be the signal and the noise error(Rathod, Sisodia, and Sharma, 2011).

$$SNR_{rms} = \sqrt{\frac{\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}[\hat{I}(r,c)]^2}{\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}[\hat{I}(r,c)-I(r,c)]^2}} \quad (2.10)$$

Another measure is the Peak Signal-to-Noise Ratio, defined as(Rathod, Sisodia, and Sharma, 2011):

$$PSNR = 10\log_{10}\frac{(L-1)^2}{\frac{1}{N^2}\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}[\hat{I}(r,c)-I(r,c)]^2} \quad (2.11)$$

Where

L is the number of gray levels.

3. THE PROPOSED CRYPTOSYSTEM

3.1 Introduction

In the usual cryptographies it is difficult to encrypt data image directly for the properties of large volumes and the requirement for real time. Bearing in mind that compression is an important factor in transmitting or saving, the new algorithm based on confusion or substitution may not be useful. Thus 3 techniques of image encryption are provided in the proposed system. These algorithms generally are based on DCT encryption so that the compression ratio does not change. The proposed system thus combines encryption with Jpeg encoding which allows DCT blocks to be permuted.

3.2 Selective Image Encryption

In selective encryption which is used to encrypt part of the bit stream, integration compression is common. That means that some schemes are still lightly encrypted by leaving fewer coefficients unencrypted (Figure 3.1.). The term light coding means low security with a high-speed simple coding system(Fu et al., 2018). The application of variable encryption is therefore a good solution, as this technique is able to apply various encryption systems with various safety features.

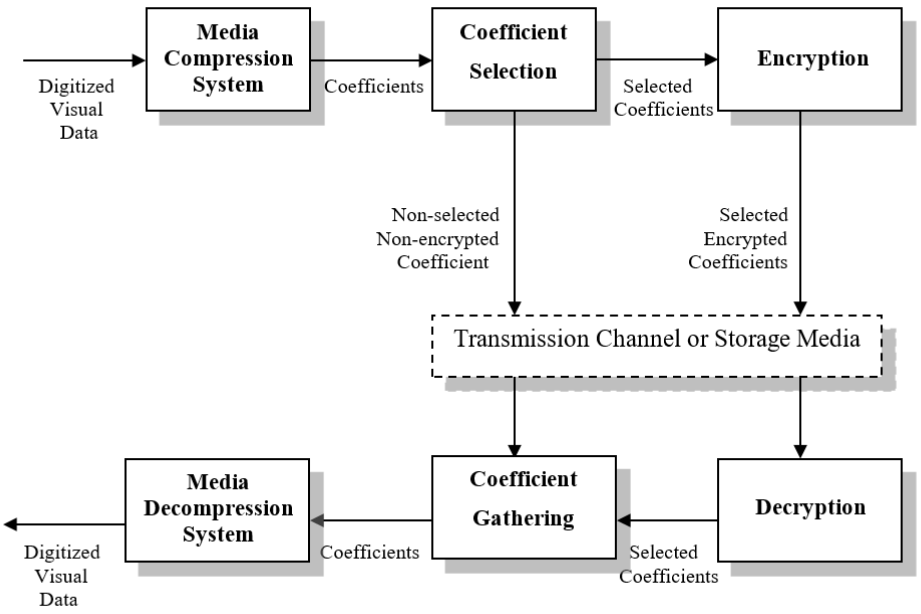


Figure 3.1.A common image selective encryption scheme(Goyal and Hemrajani, 2014).

3.3 The Proposed Image Encryption Scheme

In combination with the compression operation the proposed encryption procedure. The encryption operation consists of 3 algorithms: permutation of color planes, sign encoding and confusion of the DCT coefficients.

3.3.1 Color plane permutation

The confusion method used to determine the position of DCT blocks under the clue controls is used with pseudo-random Space Filling (SFC) supported to decrease the changes in compression ratio(Patro and Acharya, 2018). The previous JPEG adjustment can be referenced by encoding DC coefficients and having the same size in pseudo-random SFC between blocks as seen in (Figure 3.2.).

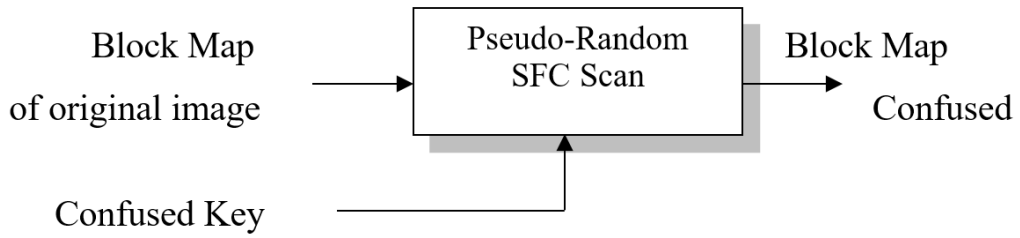
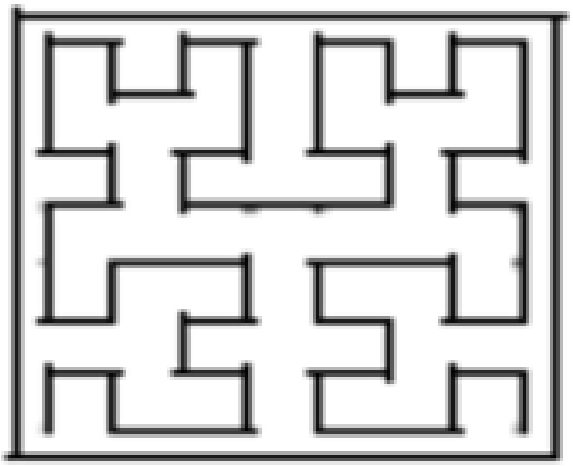


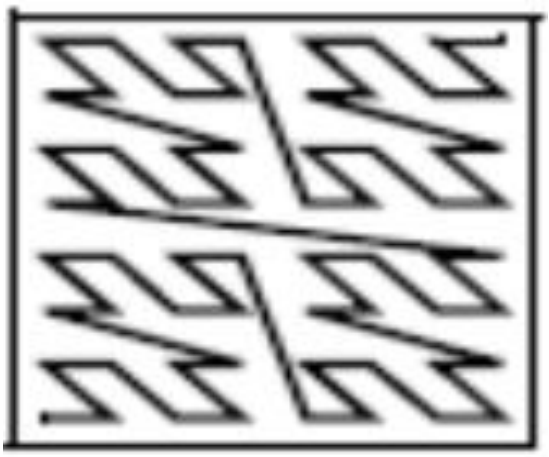
Figure 3.2. Color plane confusion method.

3.3.1.1 Alternative space filling curve techniques

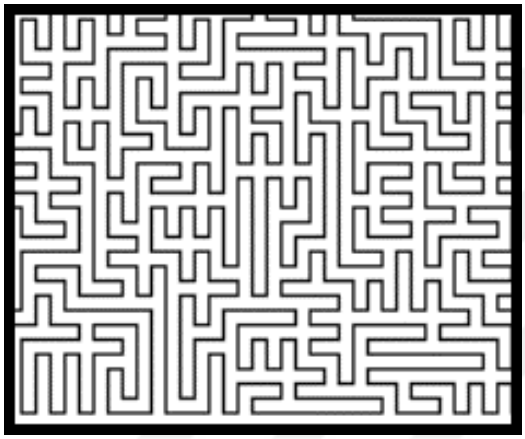
Space fill curve is a form of continuous mapping with an interval, area or volume in one, two or three-dimensional form. There are different types of SFCs, each with different local characteristics (also known as clustering properties). Several types of SFCs are shown in Figure (3.3).



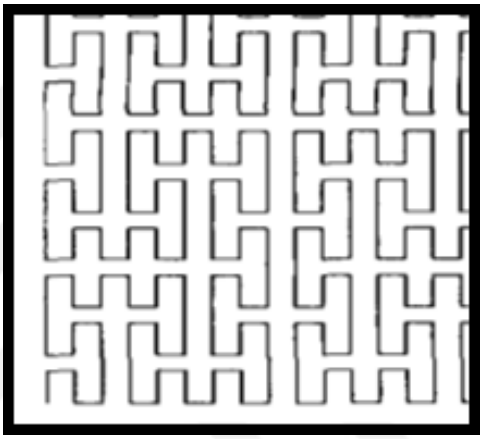
a) Hilbert



b) Z-order



c) Pseudo - Random



d) Peano scan

Figure 3.3. Various space-filling curves.

3.3.1.2 Peano scan

The Peano scan can be seen in the Figure (3.4) divides a block into a sub block and ordering process for each block.

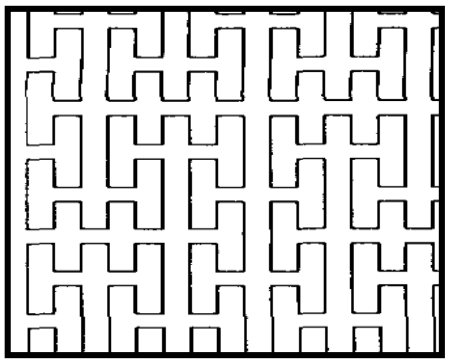


Figure3.4. Peano scan.

Considering *B (M, N)* as rectangular block of *M* columns and *N* rows:

(a) *B(M, N),* as long as M > N and M>3 are split into 3 vertical sub - blocks. B1, B2 and B3arethe M1, M2 and M3 sub-blocks which are computed by (Ambritha et al ., 2016):

$$M_1 = INT(\frac{M}{3})$$

$$M_2 = \begin{cases} 1 + INT\left(\frac{M}{3}\right) & REM\left[INT\left(\frac{M}{3}\right)\right] = 1 \\ INT\left(\frac{M}{3}\right) & Otherwise \end{cases} \quad (3.1)$$

$$M_3 = \begin{cases} INT\left(\frac{M}{3}\right) & REM\left[INT\left(\frac{M}{3}\right)\right] = 0 \\ 1 + INT\left(\frac{M}{3}\right) & Otherwise \end{cases}$$

The whole division values are INT (p / q) from p to q, and REM [INT (p / q)] depend on the remainder of the division operation.

(b) The same is true if N > M and N > 3 are divided by the same calculation, B (M, N) by 3 horizontal sub blocks, B1 blocks, B2 and B3 by N1, N2 and N3 blocks, respectively.

(c) Sub blocks are not divided if (M, N) is divided (2, 2).

The above procedure applies to every sub - block until it is divisible. The above procedure applies. The rearrangement of the sub - blocks begins with Sp and ends with E_p for each sub – block (Figure 3.5.).

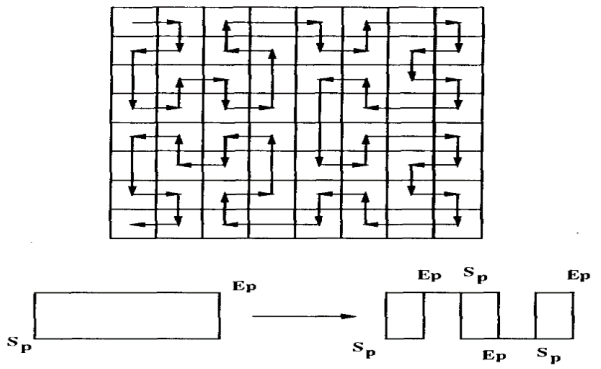


Figure3.5. Peano scan of block of size 8×8.

3.3.1.3 Z-Ordering

The space-filling curve provides a recursive decomposition for a Z-order data space that is supposed to be two-dimensional unit square[0... 1]. The unit square is divided into four

quadrants, equally large from 0 to 3, as shown in Figure 3.6, with the algorithm.

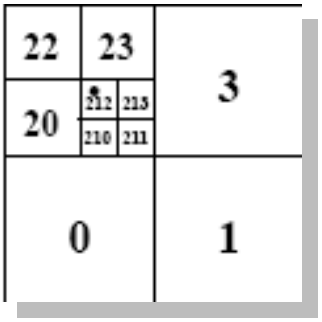


Figure3.6. Z-ordering**.**

This technique is repeated as long as there is no fundamental resolution. The results are all quadrant sequences that can be interpreted to number within the quaternary system without changing the order of points. The quadrant sequences are equal length.

3.3.1.4 Hilbert curve

By having a square grid with the sizes 2×2, 4×4, 8×8, 16×16 or others of power 2, Hilbert curve visits every point in this grid. Figure (3.7) shows how Hilbert Curve works shows the first 3 steps for an infinite operation in the case of a 2 dimensional case(Panda et al., 2016). A square is divided into 4 sub-squares and is ordered through a central-spot line by drawing a line (this line called the first-order curve). The next step is shown in Figure (3.7), which divides each sub-square into four sub-squares, which are ordered for adjacent property insurance in a different order. Figure (3.7) According to the ordering set, the 4 sub-squares can produce different first order orientations.

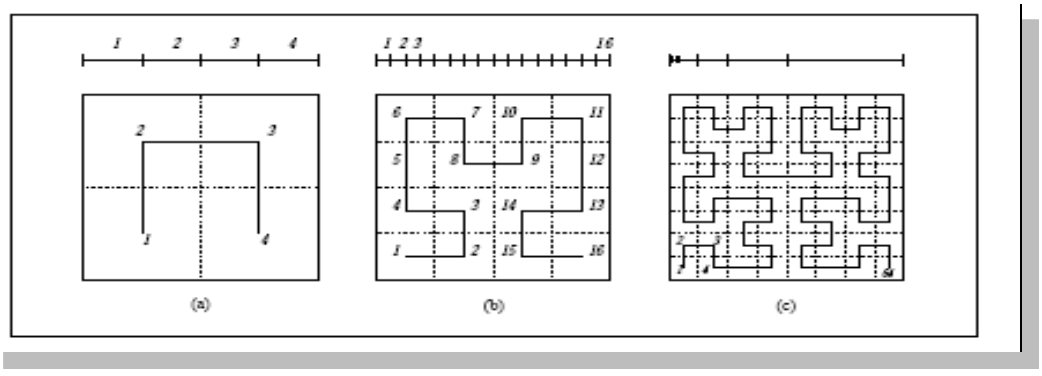


Figure3.7. Approximations of the Hilbert curve in 2 dimensions.

In some applications the operation is terminated after k-steps in order to produce an

approximation of the order k of a space curve passing through the 2 kn sub-square. The center points in a space are finite granularity(Nair, Sinha, & Vachhani, 2017). The transformation is the replacement of every point on the first order curve. Hilbert Curve offers a useful and interesting property in higher dimensions, both 2 and 3 dimensional, adjoining the ordered points.

3.3.1.5 Random space filling curve pseudo

Pseudo Random scan is a continuous scan that traverses every pixel of an image exactly once as shown in Figure (3.8).

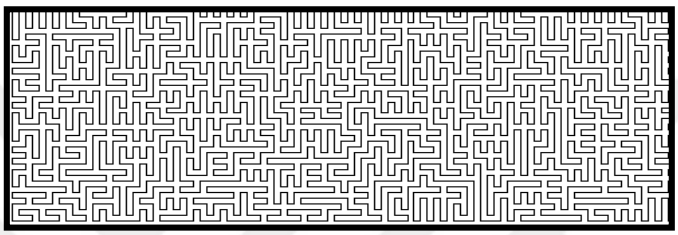


Figure3.8. Pseudo random SFC.

The image is randomly read with the use of a specific application and in order that the pixel sequence works as necessary. For sequence compression or encoding, usually lossless or loss compression is used.

This is because it randomly scans the image and previous methods are used to scan the image by fixed order, and it is therefore difficult for any attacker to get the plain image from the encoder.

3.3.1.6 The proposed colour plane permutation stages

The steps of method implementation are stated below:

3.3.1.6.1 Convert Image

First, the color picture from RGB becomes a color space for luminance/chromedness. Three matrices will be produced for this operation: luminance and chrominance.

3.3.1.6.2 Apply SFC Confusion

This approach is to perform a block permutation, without changing the value, by changing the position of the DCT blocks. Thus, blocks are confused with a SFC; this method randomly confuses blocks. The Blocks are confused with the SFC(Nair, Sinha, & Vachhani, 2017).

Confusion needs a file containing block positions where positions are randomly generated (e.g., block 2 is in position 16). It is used to confuse the image following the generated file.

3.3.1.6.3 Apply DCT

To perform DCT, it must first divide the image to a block (8 × 8 pixels), and then apply DCT equationaccording to the following algorithm.

Algorithm (3.1) Space Filling Curve (SFC)

Input: Image matrix IN×N

Output: Confused matrix

1. Divide I to a set of blocks bi = [b1, b2, …, bm].
2. Generate position array POS[1…m] with random sequence without repeated any number, where m is the number of blocks in image and the block size (8×8) pixels.
3. Set i ← 1

   While (i ≤ m)

   a. Get a block number i from I

      bi = I(block POS[i])

   b. Insert bi into new matrix I'

      I' (block i) = bi

   c. i = i + 1

This process will be vital in the transformation of the image pixels during processing. The first step in the above algorithm will be to create a pixel matrix for the image that will be divided in into the characteristic8 x8 block. Secondly, the FDCT (Forward Discrete Cosine Transform) will be applied on each 8 x 8 block of pixel matrix which will be equivalent to the 8 x 8 DCT matrix. The original image will be obtained using the Inverse Discrete Cosine Transform (IDCT) on the 8 x 8 blocks.

3.3.1.6.4Quantize each block

Once the quantization matrix is proposed, the corresponding input of the quantization matrix divides each input of the DCT coefficients, producing the quantized DCT coefficients rounded to the nearest integer.

3.3.1.6.5Application of the Zig-zag scan

After the quantization exercise the JPEG operation for the DCT coefficients in zig - zag pattern will be utilized to reduce the number of bits required for storage.

3.7.1.6.6 Apply Run Length Encoding

Upon completion of the scanning operation, RLE is used for optimal bits.
The stages of color plane permutation method are illustrate in Figure (3.9).

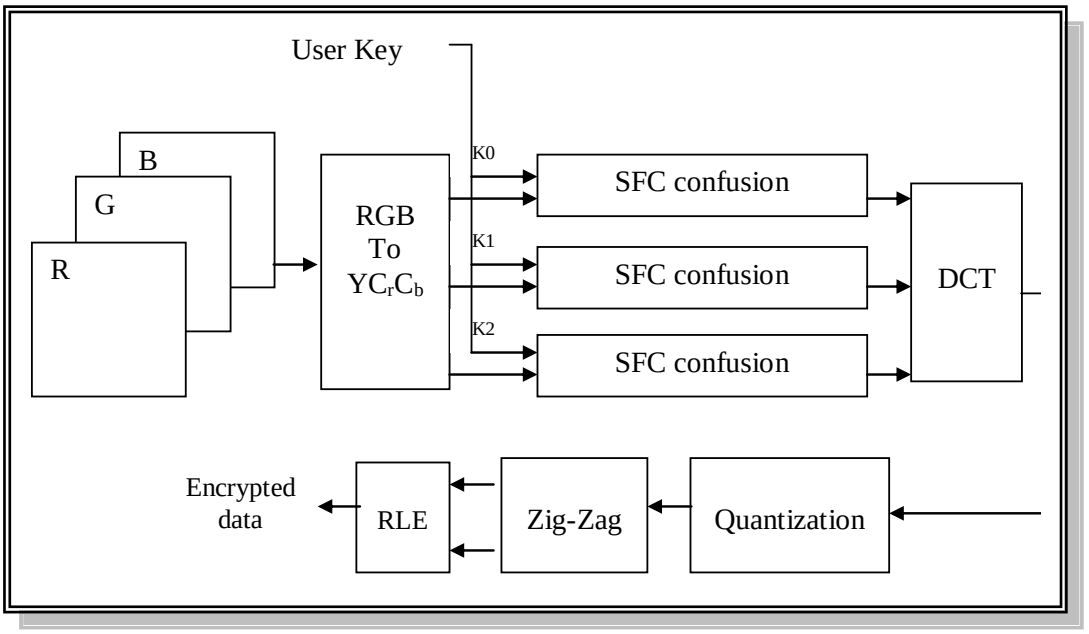


Figure3.9. The proposed color plan permutation based on JPEG encoding.

The proposed color technique will be based on the color plan permutation which is reliant on the JPEG encoding. The image will be encrypted by combining the encryption key with the space filled curve (SFC). Further, the DCT algorithm was used to maintain the pixels of the images. The quantization technique will be used to divide the result of the confusion algorithm to the relevant output blocks (Chen, Zhu, Fu, and Yu, 2014). The zig-zag matrix in the proposed system will be used to reduce the bits for each image to the appropriate value for storage. The RLE will form the final steps for the optimization of the bits after encryption leading to encrypted data.

3.3.2 DCT coefficient confusion matrix

DCT usually concentrates energy at a lower frequency to perform data compression. The distribution coefficient changed with confusing coefficients that distort the decoded images. This makes subsection confusion suitable for JPEG encryption, since it can reduce the compression ratio effect(Goyal and Hemrajani, 2014). Dividing the DCT coefficients can be used in several subsections, which are all confused, preventing the exchange of big-small coefficients. This eventually reduces the compression ratio change.

The Proposed DCT Coefficient Confusion

The DCT coefficient confusion stages are illustrated in Figure (3.10)

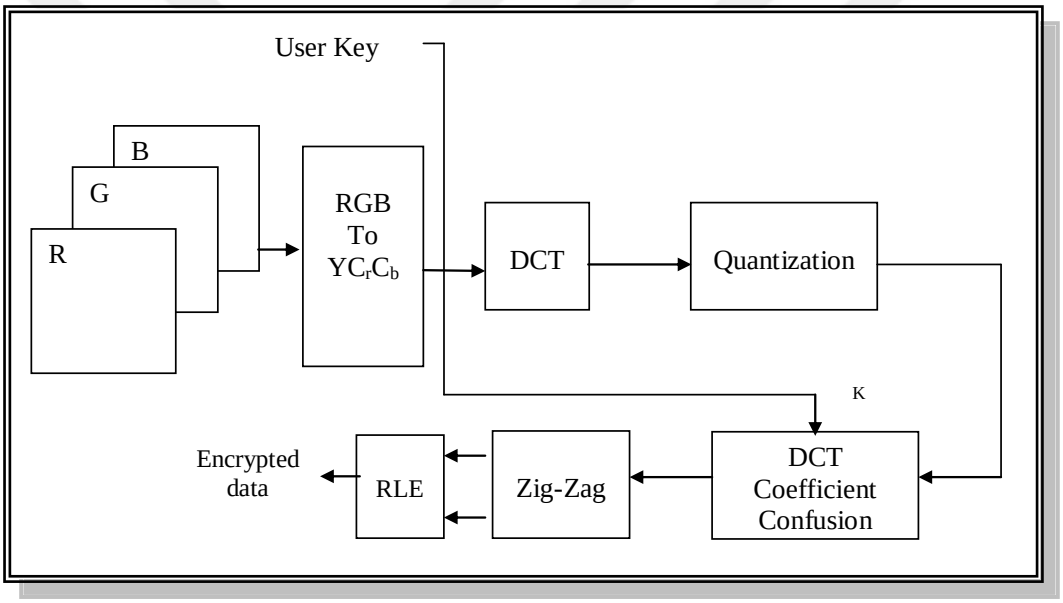


Figure 3.10. The proposed DCT coefficient confusion (Chen et al., 2014).

The steps of this method are the same with the Color Plane Permutation but with some differences, as shown in Figure above:

DCT Coefficient Confusion

Turn each block into a single - dimensional (one row) matrix. This line of coefficients consists of four regions ([1,5] region 1 [6,20] region 2 [21,40] region 3 ; [41,63] area 4), respectively, and confuses these regions, as shown in Figure (3.11), respectively.

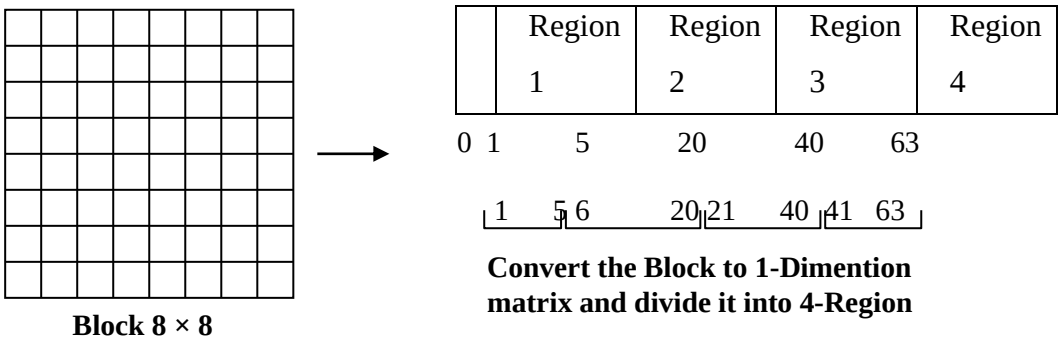


Figure 3.11. Confuse the 4-regions.

To confuse the above regions (1, 2, 3, 4) the 4 areas must be randomized, as in Figure. (3.12) in order to obtain a confused matrix, by producing a matrix in a two - dimensional format: the number of rows equal to the image number and the number of columns equal to the number of the four regions.

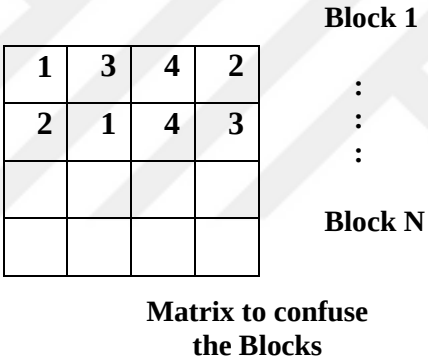


Figure 3.12. The confusion matrix.

3.3.3 Sign encryption of DCT coefficient

The main reasons for the change in the DCT Coefficient Sign are the possibility to reduce the understandability of images and the encryption of a single signal bit for each of these coefficients (Nisha , 2017). The sign is displayed as' 1' if the coefficient is greater than 0, otherwise' 0' that encodes a highly safe block cipher or chaotic stream cipheraccording to the following algorithm.

Algorithm (3.2) DCT Coefficient Confusion

Input: Image blocks after apply Quantization, the blocks bi to bm are of size (8×8) where m is the number of blocks.

Output: Confused image matrix.

1. Generate position file

   a. Let Pixel Pa = [P0, P1, …. ,P63].

      Let Region R1 = P1, P2, ….,P5

      Let Region R2 = P6, P7, ….,P20

      Let Region R3 = P21, P22, ….,P40

      Let Region R4 = P41, P42, ….,P63

   b. Pa = [P1, R1, R2, R3, R4]

      Represent R1 → 0

      R2 → 1

      R3 → 2

      R4 → 3

   c. Read blocks number m.

   d. Set counter i = 1

      begin

      While (i ≤ m)

      POS(i) = Random Sequence (0,1,2,3)

      i =i + 1

      end

2. Get the block i from quantization matrix Q(i,j)

   bi = Q(block i).

3. Convert bi from (8×8) block to vector Vi

   Vi = vector 1 to 64 pixel.

4. Change the position of the pixels in Vi according to the position file POS(i).

Each bit of coefficient viewed in three types is to encrypt the image using this method: bits of significance contain 1 to the most significant coefficient and 0 to process bits which limit the size of the coefficient. Refining bits are the bits of magnitude to refine the factor. Sign bit checks whether the known range is positive or negative(Agrawal and Pal, 2017).

The majority of transformations are created by a large number of small and grouped coefficients, which are eventually relatively low entropy and highly compressible. These transformations produce coefficients almost equal to 1 or 0 in the form of sign bits. Refining bits also have an area of 1 and 0. This is because of the high entropy with limited

predictability, sign bits and compression.

The refining bits can be scrambled without the same degradation. But even if the refining bits are scrambling correctly, the image and complexity for better security are further degraded.

The proposed sign encryption of DCT coefficient

The proposed method encrypts the sign bit of every DCT coefficients in JPEG as shown in Figure (3.13).

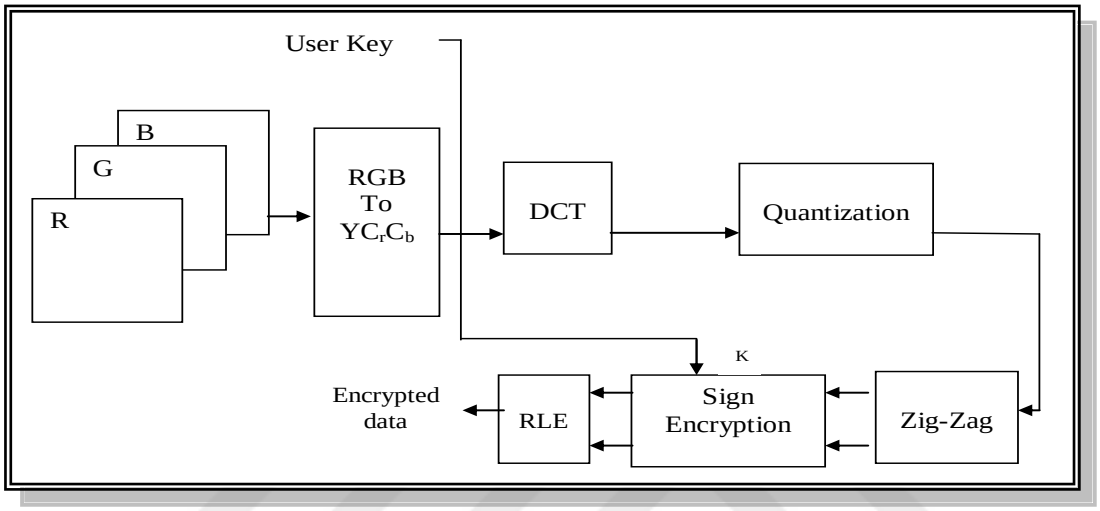


Figure3.13. The proposed sign encryption of DCT Coefficient.

The main steps of this method are the same in the two previous methods but with some differences as shown in Figure above. The Sign bits convert the DCT matrix sign x, meaning that if the coefficient is higher than 0 (positive) the DCT matrix is 1. If the factor is 0 or less, then the sign is 0. This creates a matrix for the signsaccording to the following algorithm.

A. Encrypt sign matrix

To encrypt these coefficients apply DES encryption algorithm onto the sign matrix.

B. DES encryption algorithm

The encryption operation consists of two parts, one dealing with the text, and dealing with the key, Figure (3.14) shows the DES computations and general algorithm:

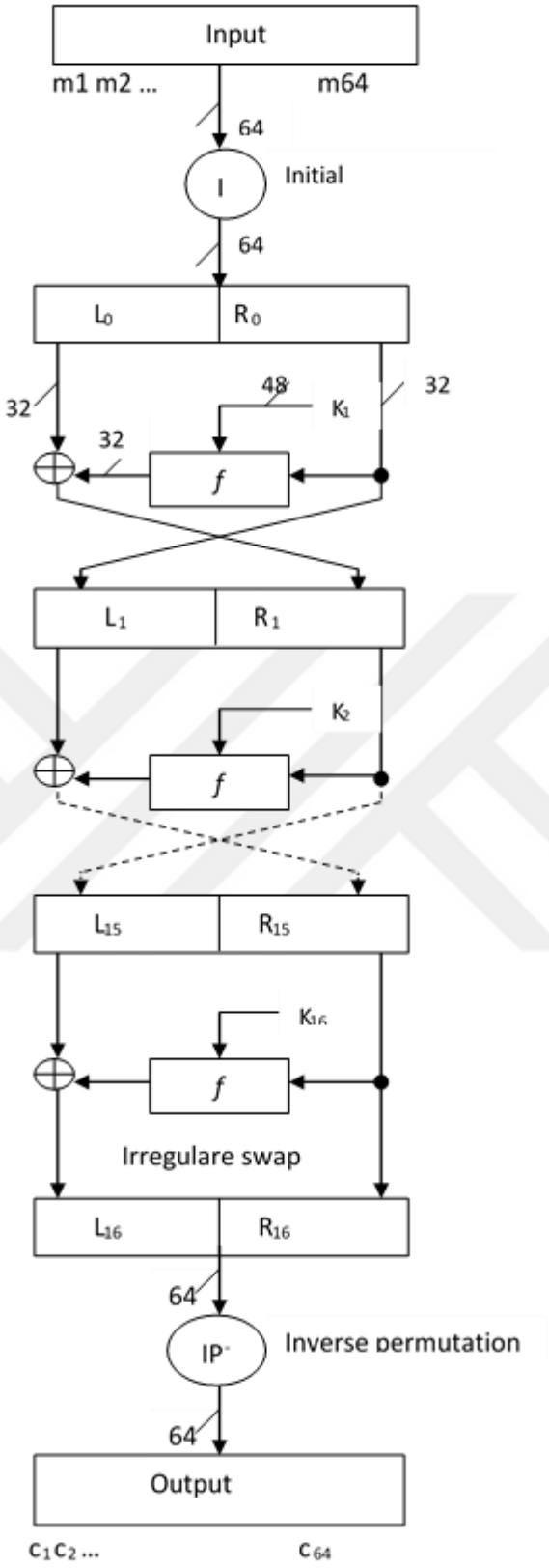


Figure 3.14. DES computations path.

3.4 System Development and Interface

3.4.1 Main window

This section shows how the cryptosystem operates, how the user can use the cryptosystem, and the buttons it contains.

3.4.1.1 Encoding

As shown in Figure 3.15, the first screen in the system proposed is the chip screen. The image is encrypted with this screen.

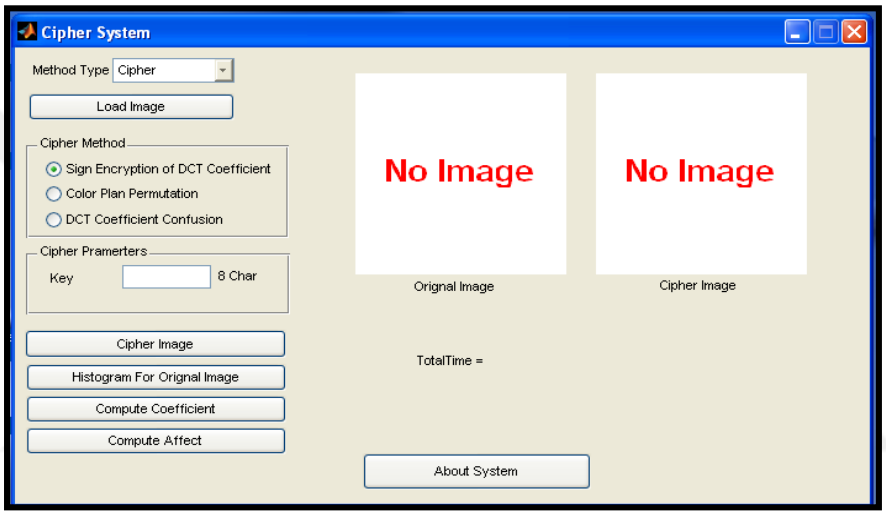


Figure 3.15. Cipher system screen.

A. Method Type Pop-Up Menu Figure (3.16) :

1. Cipher.
2. Decipher.

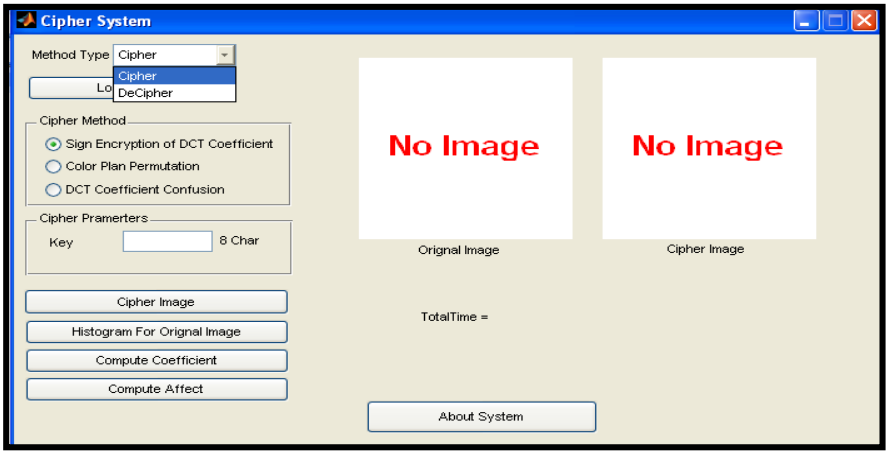


Figure 3.16. Selecting the method type.

3.4.1.2 Load image button

This button displays a standard window browse box that a user could select an image from the computer, Figure (3.17).

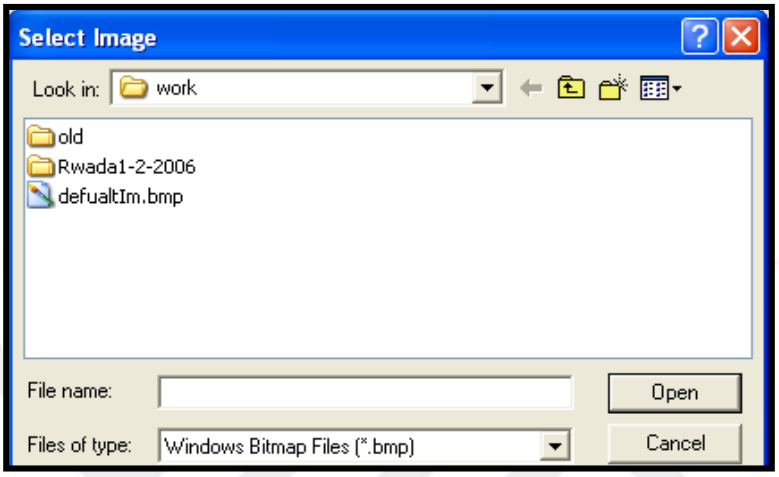


Figure 3.17. System load image.

3.4.1.3 Cipher method

There are three Radio buttons:

1. First approach. First method. This button enables the DCT Coefficient Method Sign Encryption. After the method has been selected and the photo loaded, an edit text box (Ciffer parameter) appears in the main window. It should be 8, Figure (3.18) for entering the key.

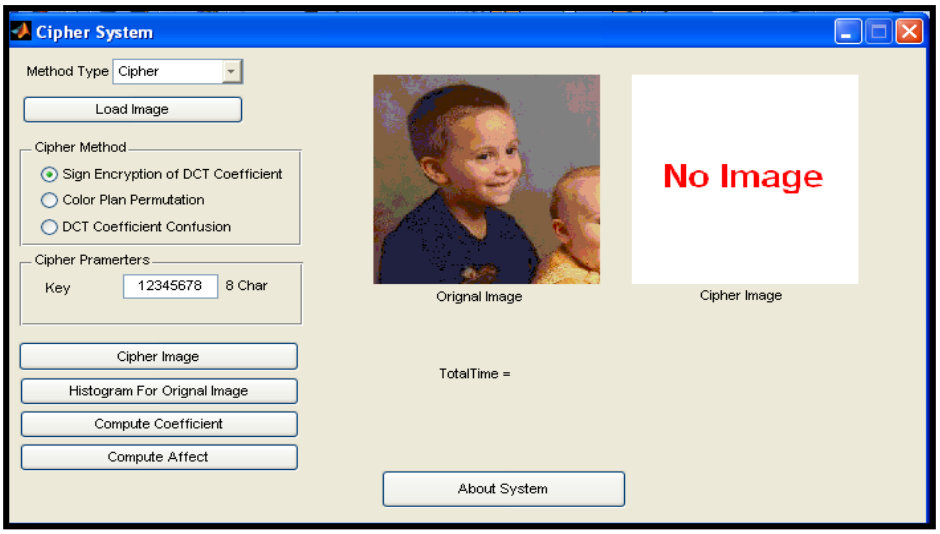


Figure 3.18. The first method.

1. Second method, the Color Plane Permitting Method is performed. When this method is selected and the image is loaded by the user, the main window (cypher parameter) shows the edit text box. It should be the same as 2Figure (3.19) when entering the Schlüssel.

Figure 3.19. The second method.

2. Third method. This button performs the confusion method of the DCT coefficient. If the user chooses this procedure and charges the image, the main window (Cipher parameter) contains an edit text box. This must be equal to 1 Figure (3.20) for entering the key.

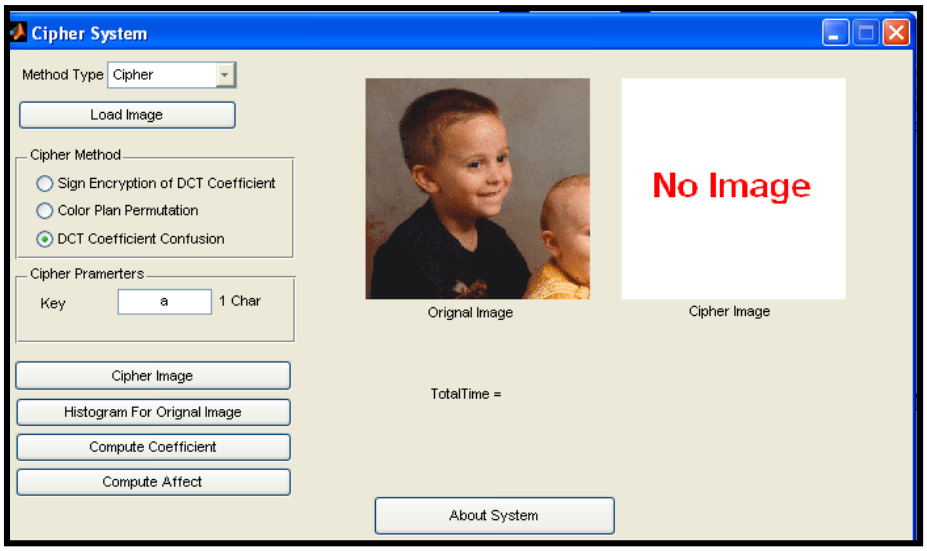


Figure 3.20. The third method**.**

3.4.1.4 Cipher image button

This button will encrypt the image by any of the three methods above; when the user selects this button a loading bar will appear Figure (3.21).

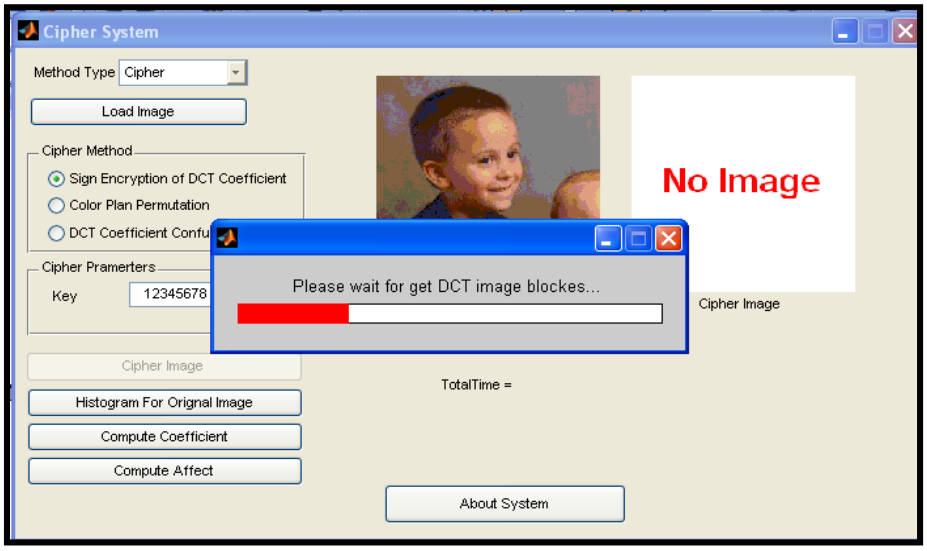


Figure 3.21. The loading bar.

After the load has been completed, the image Figure is saved by a new window (saving image) (3.22). The program tells the user that the image is not saved as shown in Figure

(3.23) when the image is not saved. In the window, you see Figures (3.24) (3.25) and (3.26). The image is ciphered.

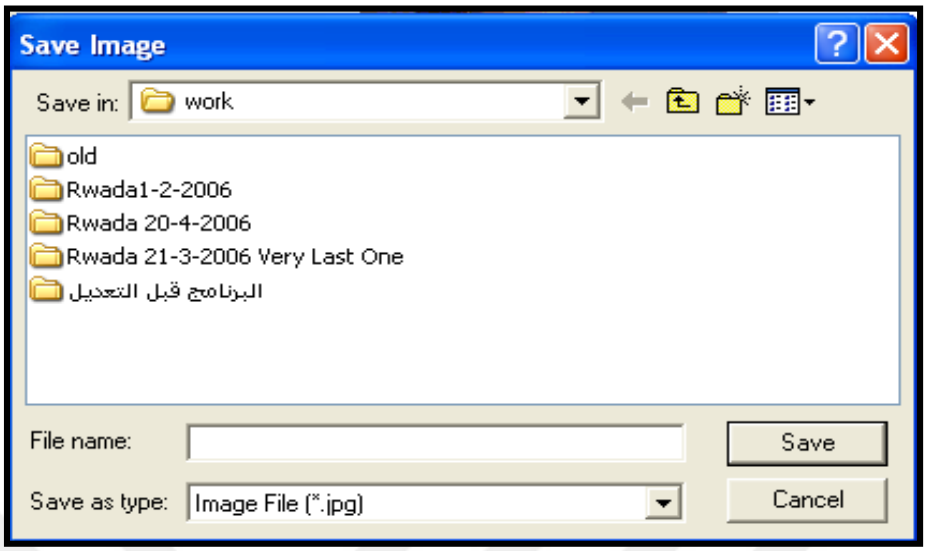


Figure 3.22. Save image window.

Figure 3.23. Warning window image not saved.

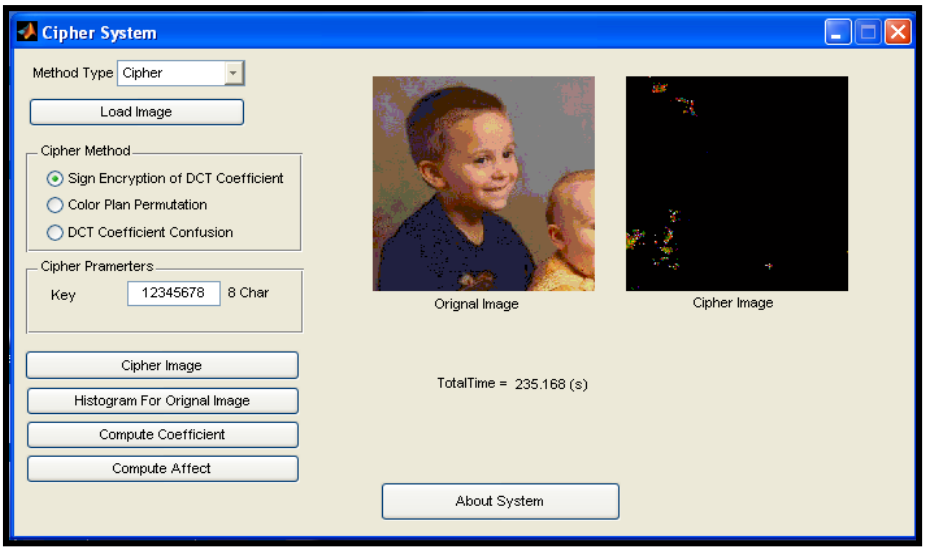


Figure 3.24. The ciphered image in first method.

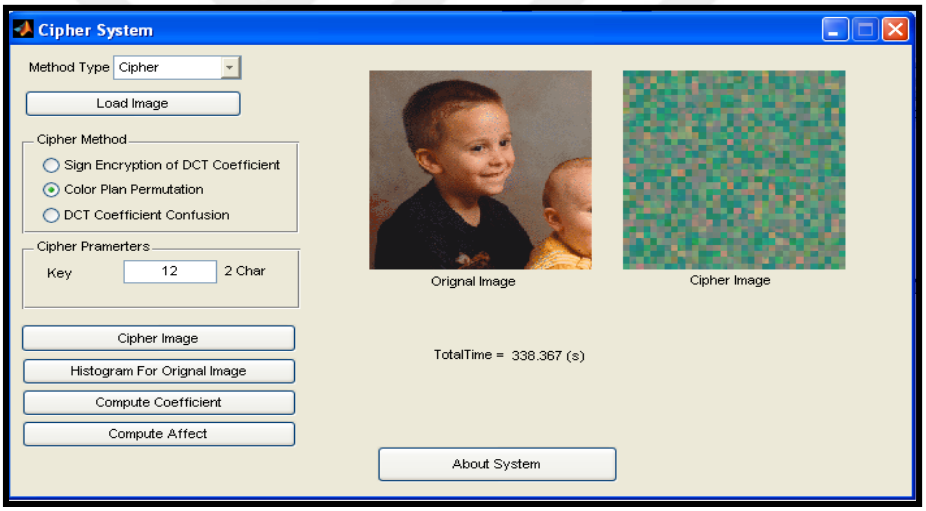


Figure 3.25. The ciphered image in second method.

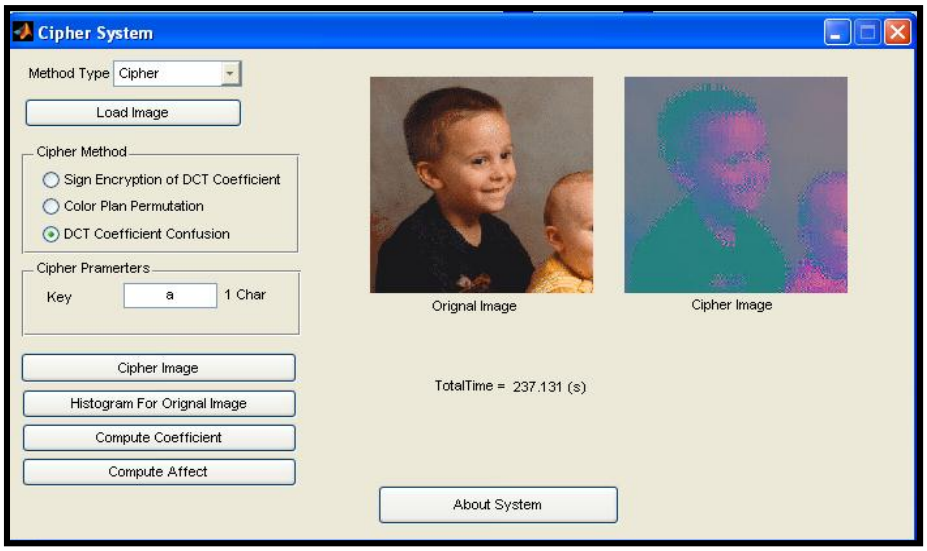


Figure 3.26. The ciphered image in third method.

3.4.1.5 Compute coefficient button

It calculates the time required to crypt and decrypt between the image and the chip image and the chip - coded image as shown in Figure (3.31). This button calculates SNR, RMS, and PSNR.

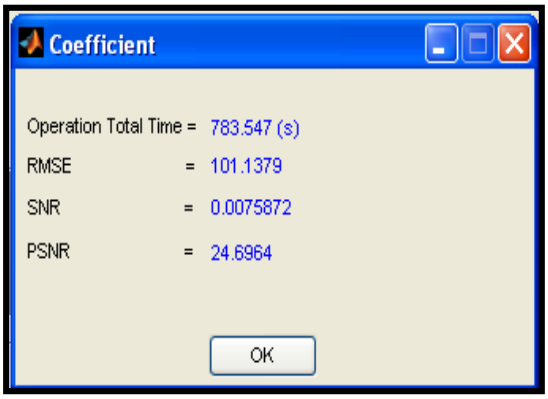
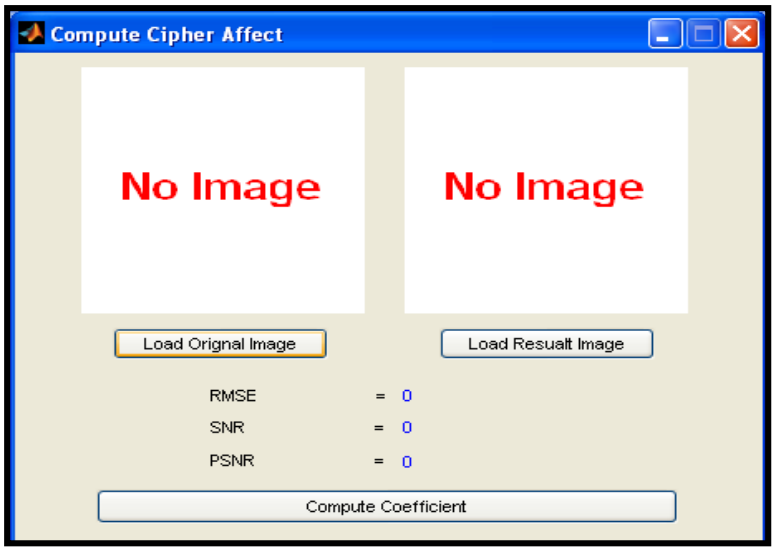


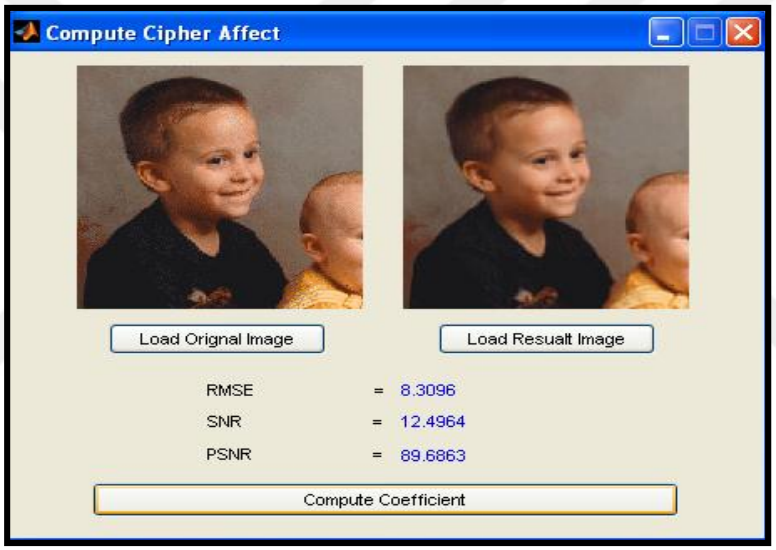
Figure 3.27. Coefficients computation window.

3.4.1.6 Compute effects button

This button will show up once again in another Window that calculates RMS, SNR, PSNR and time between the pictures loaded (e.g. between the original pictures and the decoded ones) See Figure(3.28).



a) Before loading images



b) After loading images and compute the coefficients

Figure 3.28. Compute cipher effect window.

3.4.1.7 Decoding

A new window (Decipher) will be displayed when the user wants to decrypt the image. As shown in Figure (3.29), the name of the button will be different.

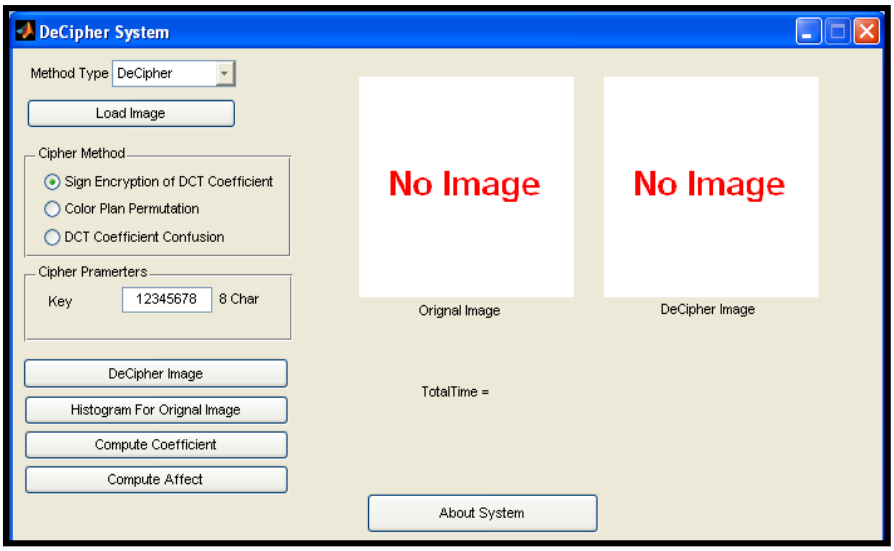


Figure 3.29. The decipher window.

A. Load Image Button

The user first chooses any method and load images as in the chipboard procedure for deciphering the image. In the ciphering process, the user must enter the same key.

B. Decipher Image Button

The loading will be shown as well when the user selects Decipher image, and the decrypted image as above is saved. The deciphered images are shown in Figures (3.30), (3.31) and (3.32).

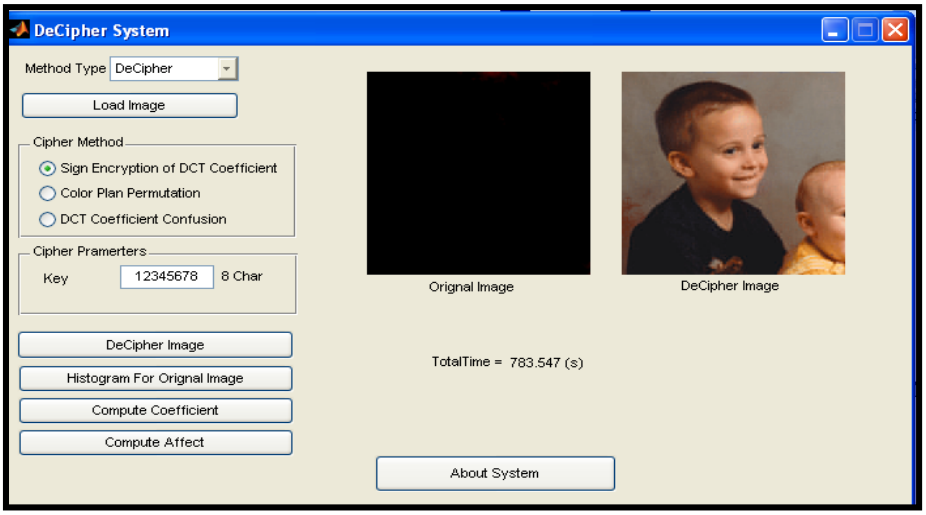


Figure 3.30. The deciphering image of the first method.

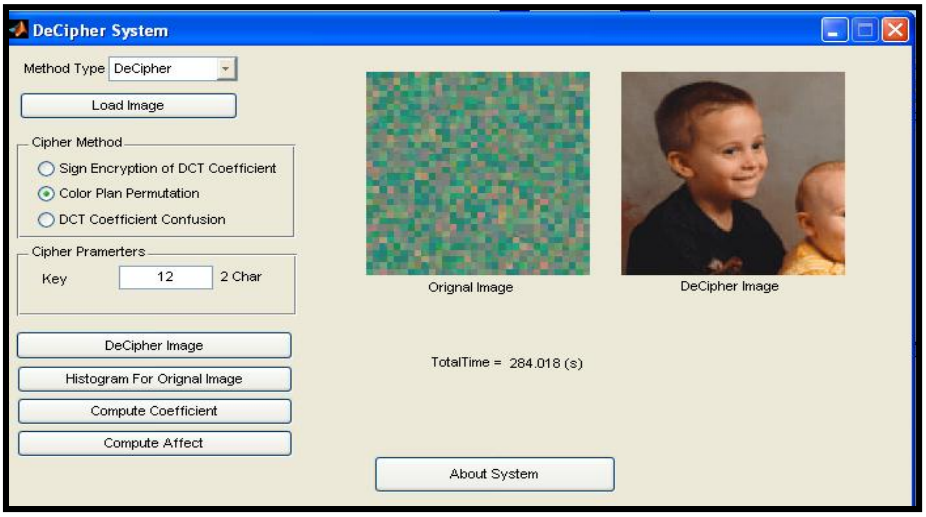


Figure 3.31. The deciphering image of the second method.

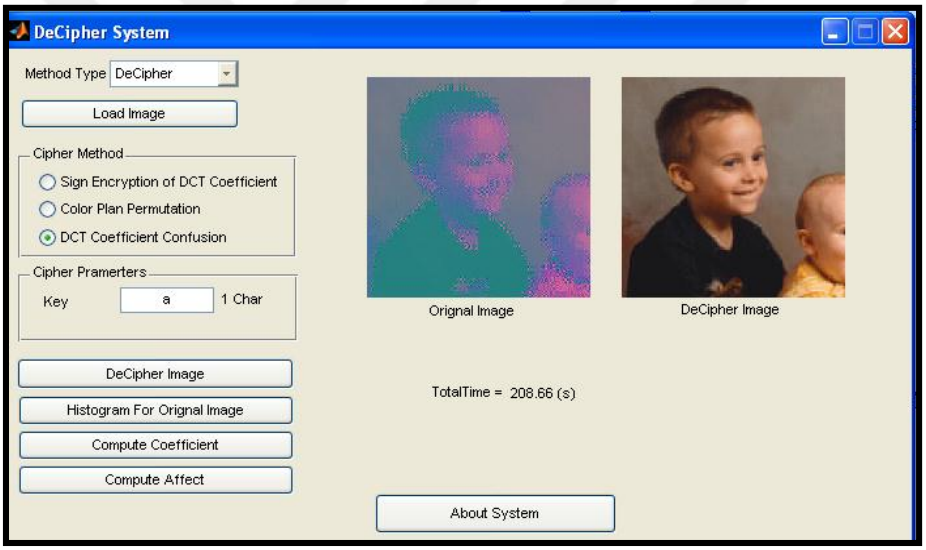


Figure 3.32. The deciphering image of the third method.

4. SYSTEM RESULTS AND TESTS

4.1 Security Tests

A. Color Plane Permutation

The Security of Color Plane Permutation will render an unintelligible image which in theory very hard to recover the image without the confusion method which is based on Space Filling Curve (SFC) use Pseudo Random Space Filling Curve confusion method. For 64 blocks image, the blocks are confused to one of 64. It's possible for large homogeneous regions type of images to have a similar block within the image. Keeping in mind that *n* amount of zero blocks and all other blocks different from each other. Considering that the number of permutations is$\frac{64!}{n}$, the number of permutations is about 1028, which makes that attacker perform inverse transforms for all blocks with each permutation specifically for all blocks that affected by the sub band permutation. Looking of the best estimation directly in the transformed domain is one of the most priorities that the attacker would try to do in general which can be done by exploiting some structure of the coefficient image such as edge continuity which considered as a difficult to be constructed due to the diversity of high-level object structure also uncorrelated nature of the coefficient image.

B. DCT Coefficient Confusion

In DCT Coefficient Confusion, each block is divided to four regions, and these regions confused randomly. In this case, we will assume 4! possible ways of confusion for the sake of the experiment, there are 256 (64x4) potential candidate blocks to fill 64 locations. For the second time, keeping in mind *n* amount ofzero blocks in decompressed sub band and all other blocks are different from each other, then the number of different configurations is 256!/(4*n*)!.

C. Sign Encryption of DCT Coefficient

The security of the encryption of the sign bits can be analyzed as follows, for *M* amount of the number of non-zero coefficients in the image code-breaker used to recover a single block completely with exhaustive search of 2^M. 256 non-zero coefficient exist in 512x512 frame for 10^{77} of required trials. To look for the best estimated of the original sign bits, it's possible to use smoothness constraint in the spatial domain which includes an inverse transformation that makes the attack expensive.

4.2. Direct Bit – Rate Control

Compression ratio effected lightly by the encryption schemes where sign encryption of DCT coefficients holds compression ratio unchanged according to JPEG encoding. Because of the adjacent relationship among blocks usually kept and on DC coefficient in each block is encoded, pseudo random SFC method affects compression ratio slightly. To avoid having the permutation between bigger ones and smaller ones, Subsection confusion of DCT coefficients has a slightly lower effect on compression ratio than complete confusion method does. Usually bit-rate conversion realized by JPEG encoding by changing quantization steps while in the proposed encryption scheme relative position of DCT blocks, the signs and the relative positions of DCT coefficients, also leaves the range of DCT coefficients unchanged. Bit-rate control is supported by the encryption scheme which permits to recompress the encoded and encrypted data before decrypting it. While this scheme avoids the processes of decryption and encryption comparing it with decryption recompression-encryption process.

4.3. Experimental Results

Applying these encryption methods to various images, the encrypted images are all too chaotic to be understood. The results of images (car, cats, sport) are shown in Figure (4.1).Where, images (a), (b) and (c) are original ones, images (a1, a2, a3), (b1, b2, b3) and (c1, c2, c3) are encrypted ones, and (a4, b4, c4) are the decrypted images. It is obvious that, the encrypted ones cannot be understood at all unless DCT Coefficient Confusion, which shows that the encryption methods are of high security.

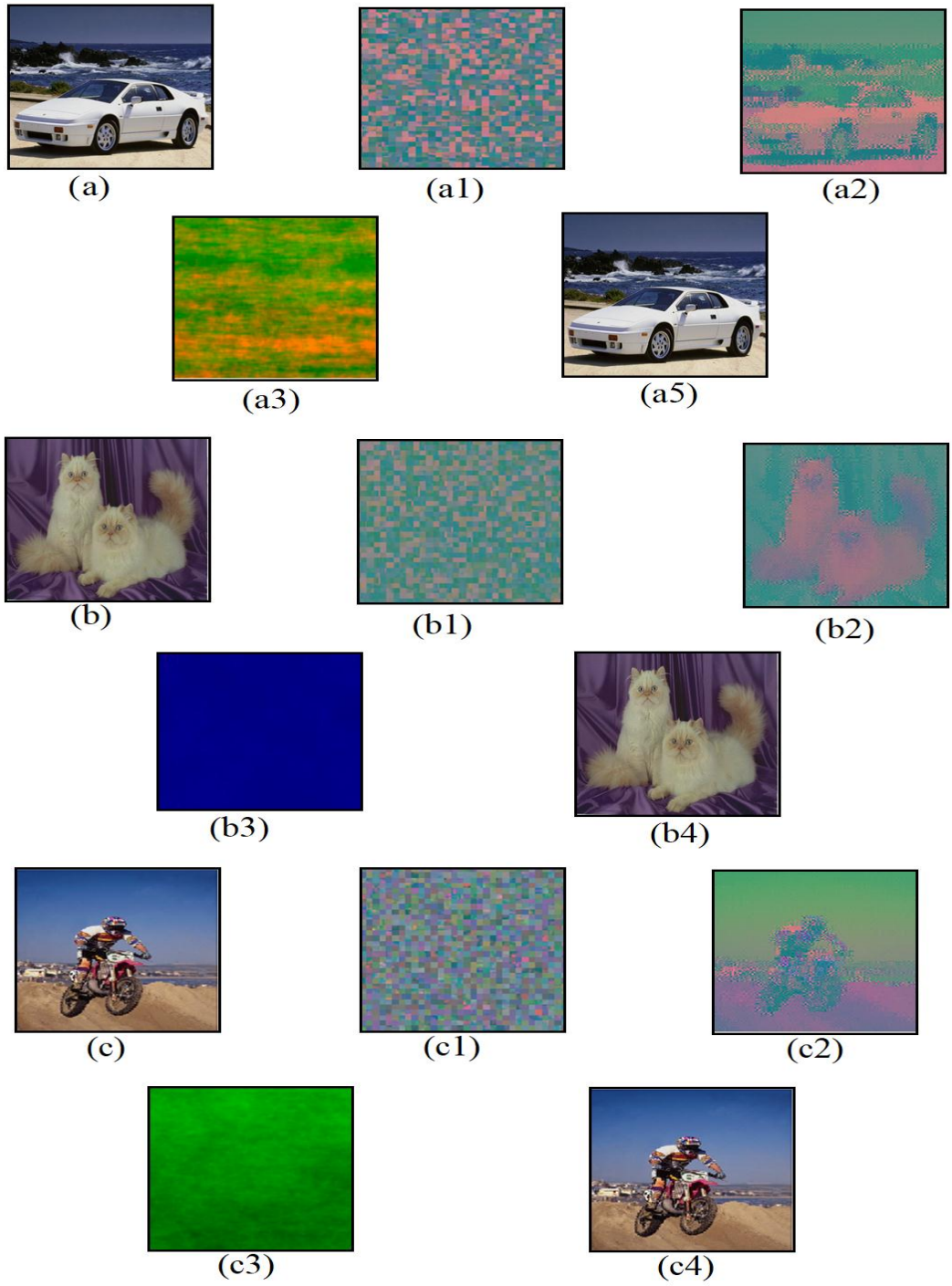


Figure4.1. Encryption results.

4.4. Encryption Speed Test

From the various images that we experimented with, the results showed as that the proposed encryption schemes are of high speed. Here, taking various images for example, the times required for encryption are shown in Table (4.1). Where, the computer is of 3GB CPU/256MB RAM. From the comparison it can be seen that the DCT Coefficient Confusion is fast than the other as seen in Table (4.1).

Table 4.1. Encryption speed test for 20 images of size 256 × 256.

image	Encryption time (Sec.)		
	Color Plan Permutation	**DCT Coefficient Confusion**	**Sign Encryption of DCT Coefficient**
Car	52.135	36.452	143.346
Cats	51.363	36.302	154.212
Sport	51.784	36.033	153.981
Garden	51.654	36.222	154.702
Child	52.054	36.172	150.336
Roses	51.864	36.342	149.034
Man	51.544	36.142	150.416
Couple	52.335	36.312	147.883
Chinese girl	52.405	36.162	148.634
Clown	51.834	36.342	154.252
Average	51.897	36.248	150.680

The above table captures the results for the three proposed system of encrypting images during transmission or storage. Considering that all the techniques were applied to the same images in the same computers. The DCT coefficient Confusion was the fastest technique as the encryption time was lower than that for the color plan permutation and sign encryption of DCT coefficient. The DCT coefficient confusion is recommended based on the encryption time for the 20 images.

4.5. Quality of Decrypted Image

We used RMS, SNR, PSNR measures to show the quality of images as shown in Table (4.2), Table (4.3),and Table(4.4).

Table 4.2. Comparison of PSNR.

Image	PSNR (d b)		
	Color Plan	**DCT Coefficient**	**Sign Encryption of**
Car	77.072	71.457	77.098
Cats	94.447	91.747	94.492
Sport	78.370	76.594	78.387
Garden	71.473	68.908	71.491
Child	79.746	76.846	79.748
Roses	71.512	69.815	71.511
Man	86.848	83.475	86.870
Couple	91.121	84.825	91.148
Chinese girl	77.625	73.339	77.658
Clown	73.494	69.861	73.527

The peak-signal-to-noise ratiowas used to characterize the sensitivity of each technique applied for the encryption of the 20 images. The PSNR test for the images demonstrated that the sign encryption DCT coefficients was higher than the two other algorithms. The DCT coefficient performed poorly in this section as it was the less sensitive algorithm for image encryption.

Table 4.3. Comparison of SNR.

Image	SNR		
	Color Plan	**DCT Coefficient**	**Sign Encryption of**
Car	9.807	7.907	9.817
Cats	15.233	13.732	15.259
Sport	9.532	8.918	9.539
Garden	7.258	6.593	7.262
Child	7.839	6.994	7.840
Roses	5.621	5.227	5.521
Man	15.098	13.257	15.111
Couple	25.983	20.405	26.010
Chinese girl	8.143	6.872	8.153

Clown	8.662	7.536	8.673

The signal-to-noise ratio (SNR) test was used to characterize the level of distortion encountered when encrypting the images. The DCT coefficient algorithm had a lower SNR meaning that it introduces a lot of noise during the encryption compared to the other techniques. The increased noise means it will be difficult to decrypt the image during transmission therefore meaning that DCT coefficient is better at encrypting image data.

Table 4.4. Comparison of RMS.

image	**RMS**		
	Color Plan	**DCT Coefficient**	**Sign Encryption of**
Car	13.296	16.492	13.283
Cats	6.826	7.570	6.814
Sport	12.650	13.548	12.642
Garden	16.486	18.237	16.475
Child	12.001	13.416	12.000
Roses	16.460	17.585	16.461
Man	9.14	10.401	9.132
Couple	7.757	9.875	7.749
Chinese girl	13.021	15.376	13.005
Clown	15.253	17.539	15.233

The RMS describe the fitness of the data i.e., the imperfection in the encryption of the three algorithms. The greater the value of the RMS illustrate that the method had more deviations compared to the other estimators. The DCT coefficients had a higher value compared to the Color plan and the sign encryption demonstrating a greater source of errors. The DCT coefficient technique had more errors due to the introduction of more noise in the encryption process.

4.6. Comparative Analysis

The results shown above have effectively shown that the DCT techniques can be

recommended for the encryption of the images both in storage and transmission. The DCT techniques can be compared to the conventionalvigenere and the DES algorithm for image processing and encryption. According to (Mohammad et al., 2017). the Vigenere performed better that the DCT and Data Encryption Standard (DES) in the performance analysis(Mohammad et al., 2017). The Vigenere had better performance in both correlation and time analysis than the DCT with the DES performing poorly in this two cases. The DCT algorithms were superior in the pixel sensitivity using PSNR and quality of decrypted images using SNR. The vigenere performed poorly in the preserving the quality of the images. The DES performed moderatein analytical comparison in for the cryptographic techniques(Mohammad et al., 2017).Thus, based on the analytical comparison the DCT is a superior technique compared to the vigenere and DES in image quality preservation and encryption time. The vigenere performed better in correlation analysis.

4.7. Security Measurement Values

The best security measure value technique for this research was the security and statistical analysis method (Mohammad et al., 2017).The security analysis was completed using the PSNR analysis, where both the image and the encrypted image are evaluated based on the noise addition. In table 4.2, the values represent the proportional relation between the Mean Square Error and the error in the encrypted image. Further, the statistical analysis approach describes the confusion and diffusion properties of the encrypted images (Mohammad et al., 2017). In the statistical technique, the RMS in table 4.4 was used to evaluate the correlation coefficients that demonstrated the pixel relation with the frequency. Ultimately, the PSNR techniques were the best approach to determine the security value of the three methods developed.

5. CONCLUSIONS AND FUTURE WORKS

5.1 Conclusions

The study was used effective in investigating the various types of image encryption using DCT techniques. Three techniques were proposed for the image encryption for both transmission and storage. The research has shown that the chaotic techniques are vital in image encryption as the pixels can extremely uncorrelated pixels. The research has shown that the DCT improves the time for encryption of the images. Further, the results show that the DCT-based algorithm performs better than the traditional image process techniques of DES and vigenere.From the study and the implementation of the proposed system we were able toinfer the following conclusions;

- Sign encryption of DCT Coefficient, DCT Coefficient Confusion, and Color Plan Permutation encryptions method may be used to strengthen the security of cryptosystem by enhancing the encryption time and preserving the image quality.
- The original image is decrypted correctly with little degradation in the quality.
- The DCT algorithm incorporates a JPEG image encryption scheme is proposed, which supports direct bit-rate control, and its security, computing complexity, compression ratio and bit-rate control are analyzed respectively.
- The encryption schemes in this proposed algorithm have a high security which these results show according to theoretical analyses and experimental results.
- The encryption schemes are low cost and high speed based on encryption only certain parts of the image.
- Due to similarity between MPEG videos and JPEG images, most JPEG encryption methods can be used to encrypt MPEG videos.

5.2 Color Plane Permutation

Color Plane Security permutation will make an unintelligible image which is in theory very difficult to retrieve the image without the Space Filling Curve (SFC)-based confusion-based method. The blocks are confused with one of 64 for 64 blocks of image. It is possible to have similar blocks in the image for large homogenous regions of pictures. Keep in mind that n numbers of zero blocks differ from each other and all other blocks. Considering that the number of permutations is$\frac{64!}{n}$, the number of permutations is about 1028, which makes that attacker perform inverse transforms for all blocks with each permutation specifically for all blocks that affected by the sub band permutation. Looking of the best estimation directly in the transformed domain is one of the most priorities that the attacker would try to do in general which can be done by exploiting some structure of the coefficient image such as edge continuity which considered as a difficult to be constructed due to the diversity of high-level object structure also uncorrelated nature of the coefficient image.

5.3 DCT Coefficient Confusion

In DCT Coefficient Confusion, each block is divided to four regions, and these regions confused randomly. Assuming 4! Possible ways of confusion, there are 256 (64x4) potential candidate blocks to fill 64 locations. For the second time, keeping in mind *n* amount ofzero blocks in decompressed sub band and all other blocks are different from each other, then the number of different configurations is 256! /(4*n*)!.

5.4 Sign Encryption of DCT Coefficient

The security of the encryption of the sign bits can be analyzed as follows, for *M* amount of the number of non-zero coefficients in the image code-breaker used to recover a single block completely with exhaustive search of 2^{M}. 256 non-zero coefficient exist in 512x512 frame for 10^{77} of required trials. To look for the best estimated of the original sign bits, it's possible to use smoothness constraint in the spatial domain which includes an inverse transformation that makes the attack expensive.

5.5 Future Works

1. Adding more scrambling techniques to increase the security level.
2. In the Sign Encryption method, instead of using DES encryption algorithm we can use

another algorithm, which is much more secured than the DES.

3. These encryption schemes may be extended to JPEG2000 and MPEG codec's.

4. Encryption of only some of DCT coefficients should be attempted so that the computational speed could be further increased.

5. The three-encryption schemes can be combined in one scheme to increase the security level.

6. Since encryption only DC coefficients could be not enough to destroy intelligibility, it would be helpful if a few low frequency AC coefficients are also encrypted.

REFERENCES

Agarwal, S., 2017. Image Encryption Techniques Using Fractal Function: A Review. *International Journal of Computer Science & Information Technology*, 9(2), 53-68.

Agrahari, A. K., Sheth, M., and Praveen, N. 2017. Comprehensive Survey on Image Steganography Using LSB With AES. *International Journal of Applied Engineering Research*, 13(8), 5841-5844.

Agrawal, E., and Pal, P. R. 2017. A Secure and Fast Approach for Encryption and Decryption of Message Communication. *International Journal of Engineering Science and Computing*, 7(5), 11481-11485.

AL-Laham, M. M., 2015. Encryption-Decryption RGB Color Image using Matrix Multiplication. *International Journal of Computer Science & Information Technology*, 7(5), 109-119.

Ambritha, T., Sri, P. J., Jebarani, J. J., and Selvarani, P. 2016. Visual Cryptography Scheme for Colored Image using XOR with Random Key Generation. *International Journal of Advanced Trends in Computer Science and Engineering*, 5(4), 16282-16287.

Ao, A., 2012. Visual Cryptography for Color Image. *International Journal of Electrical and Electronics Engineering*, 2(1), 31-33.

Banu, N. S., Tabassum, Z., Fatima, K., and S, A. S. 2013. Selective Bitplane Encryption for Secure Transmission of Image Data in Mobile Environment. *International Journal of Scientific & Technology Research*, 2(6), 92-96.

Chen, J.-x., Zhu, Z.-l., Fu, C., and Yu, H. 2014. A fast image encryption scheme with a novel pixel swapping-based confusion approach. *Nonlinear Dynamics*, 77(4), 1191-1207.

Chitra, K., and Venkatesan, P. V., 2016. Visual Cryptographic Scheme for Color Images using Threshold Level Determination. *International Journal for Innovative Research in Science & Technology*, 406-409.

De la Hucha Arce, F., Moonen, M., Verhelst, M., and Bertrand, A. 2017. Adaptive Quantization for Multichannel Wiener Filter-Based Speech Enhancement in Wireless Acoustic Sensor Networks. *Wireless Communications and Mobile Computing*, 1-15.

Fu, C., Zhang, G.-y., Zhu, M., Chen, Z., and Lei, W.-m. 2018. A New Chaos-Based Color Image Encryption Scheme with an Efficient Substitution Keystream Generation Strategy. *Security and Communication Networks*, 2018, 1-13.

Geetha, S., Punithavathi, P., Infanteena, A. M., and Sindhu, S. S. 2018. A Literature Review on Image Encryption Techniques. *International Journal of Information Security and Privacy*, 12(3), 42-83.

Goyal, D., andHemrajani, N., 2014. Novel Selective Video Encryption for H.264 Video. *International Journal of Information Security Science*, 3(4), 216-226.

Guanghui, C., Kai, H., Yizhi, Z., Jun, Z., and Xing, Z. 2014. Chaotic Image Encryption Based on Running-Key Related to Plaintext. *The Scientific World Journal*, 2014, 1-9.

Hamidouche, W., Farajallah, M., Raulet, M., and Déforges, O. 2015. Selective Video Encryption Using Chaotic System in the SHVC Extension. *Conference: IEEE, 40th International Conference on Acoustics, Speech and Signal Processing*, ICASSP-2015 (pp. 1762-1766). Brisbane, Australia: IEEE.

Iyer, S. C., Sedamkar, R. R., and Gupta, S. 2016. A Novel Idea on Multimedia Encryption Using Hybrid Crypto Approach. *Procedia Computer Science*, 79, 293-298.

Iyer, S. C., Sedamkar, R. R., and Gupta, S. 2016. Multimedia Encryption using Hybrid Cryptographic Approach. *IJCA Proceedings on International Conference on Communication, Computing and Virtualization*, 1, 1-5.

Kendhe, A. K., and Agrawal, H., 2013. A Survey Report on Various Cryptanalysis Techniques. *International Journal of Soft Computing and Engineering*, 3(2), 287-293.

Madani, M., Bentoutou, Y., and Taleb, N. 2017. An improved image encryption algorithm based on cyclic rotations and multiple chaotic sequences: Application to satellite images. *Journal of Electrical and Electronics Engineering*, 10(2), 29-34.

Mohammad, O. F., Mohd Rahim, M., Zeebaree, S. R., and Ahmed, F. Y. 2017. A Survey and Analysis of the Image Encryption Methods. *International Journal of Applied Engineering Research*, 12(23), 13265-13280.

Mourad, T., and Bouhlel, S., 2017. Application of a Lightweight Encryption Algorithm to a Quantized Speech Image for Secure IoT. *Proceedings of the Sixth International Conference on Advances in Computing, Electronics and Communication*. Rome, Italy: Institute of Research Engineers and Doctors.

Nair, S. H., Sinha, A., and Vachhani, L. 2017. Hilbert's space-filling curve for regions with holes. *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*. 313-319. Melbourne, Australia: IEEE.

Nisha, S., and Farik, M., 2017. RSA Public Key Cryptography Algorithm – A Review. *International Journal of Scientific & Technology Research*, 6(7), 187-191.

Ochoa, H., Vergara, O., and Sánchez, V. G., 2015. Modified set partitioning in hierarchical trees algorithm based on hierarchical subbands Modified set partitioning in hierarchical trees algorithm based on hierarchical subbands — *Journal of Electronic Imaging*, 24(3).

Panda, S., Mishra, S., and Mishra, S. 2016. Study and Analysis of Multi-Dimensional Hilbert Space-Filling Curve and Its Application-A survey. *International Journal of Computer Science, Engineering and Information Technology*, 6(2), 1-9.

Patro, K. A., and Acharya, B., 2018. Secure multi-level permutation operation based multiple colour image encryption. *Journal of Information Security and Applications*, 111-113.

Raid, A. M., Khedr, W. M., El-dosuky, A. M., and Ahmed, W. 2014. Jpeg Image Compression Using Discrete Cosine Transform - A Survey. *International Journal of Computer Science & Engineering Survey*, 39-47.

Rathod, H., Sisodia, M. S., and Sharma, S. K. 2011. Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm). *International Journal of Computer Technology and Electronics Engineering*, 1(3), 7-13.

Setyaningsih, E., and Wardoyo, R., 2017. Review of Image Compression and Encryption. *International Journal of Advanced Computer Science and Applications*, 8(2), 83-94.

Shah, R. J., & Haryan, Y. S., 2018. Analysis of Image Compression & Encryption. *International Journal of Innovative Research in Computer and Communication Engineering*, 6(1), 136-143.

Shah, R. J., and Pancholi, B. K. 2014. Multimedia Security Techniques. *International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering*, 2(5), 1477-1481.

Suresh, V., and Madhavan, V. C., 2012. Image Encryption with Space-filling Curves (Short Communication). *Defence science Journal*, 62(1), 46-50.

Tiwari, G., Nandi, D., and Mishra, M. 2013. Cryptography and Cryptanalysis: A Review. *International Journal of Engineering Research & Technology*, 2(10), 1898-1902.

Younes, M. A., 2019. A Survey of the Most Current Image Encryption and Decryption Techniques. *International Journal of Advanced Research in Computer Science*, 10(1).

APPENDIX LIST

APPENDIX A: In selective encryption which is used to encrypt part of the bit stream, integration compression is common. That means that some schemes are still lightly encrypted by leaving fewer coefficients unencrypted (Figure 3.1.). The term light coding means low security with a high-speed simple coding system(Fu et al., 2018). The application of variable encryption is therefore a good solution, as this technique is able to apply various encryption systems with various safety features.

APPENDIX B: In combination with the compression operation the proposed encryption procedure. The encryption operation consists of 3 algorithms: permutation of color planes, sign encoding and confusion of the DCT coefficients.

APPENDIX C: This section shows how the cryptosystem operates, how the user can use the cryptosystem, and the buttons it contains.

APPENDIX A

In selective encryption which is used to encrypt part of the bit stream, integration compression is common. That means that some schemes are still lightly encrypted by leaving fewer coefficients unencrypted (Figure 3.1.). The term light coding means low security with a high-speed simple coding system (Fu et al., 2018). The application of variable encryption is therefore a good solution, as this technique is able to apply various encryption systems with various safety features.

```
function varargout = CipherSystemGUI(varargin)
gui_Singleton = 1;
gui_State = struct('gui_Name',       mfilename, ...
'gui_Singleton',  gui_Singleton, ...
'gui_OpeningFcn', @CipherSystemGUI_OpeningFcn, ...
'gui_OutputFcn',  @CipherSystemGUI_OutputFcn, ...
'gui_LayoutFcn',  [] , ...
'gui_Callback',   []);
if nargin && ischar(varargin{1})
   gui_State.gui_Callback = str2func(varargin{1});
end

if nargout
   [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
else
   gui_mainfcn(gui_State, varargin{:});
end
function CipherSystemGUI_OpeningFcn(hObject, eventdata, handles, varargin)
handles.output = hObject;
guidata(hObject, handles);
global IFS;
global OFS;
global BlockSize;
global keyLength;
global methodFlag;
methodFlag=true;
keyLength=8;
BlockSize=8;
IFS.flag=false;
OFS.flag=false;
banner= imread('defualtIm.bmp');
axes(handles.axesImDisplay1);
imshow(banner)
set(handles.axesImDisplay1,'Visible', 'off','Units', 'pixels');
axes(handles.axesImDisplay2);
imshow(banner)
```

```
set(handles.axesImDisplay2,'Visible', 'off','Units', 'pixels');
function varargout = CipherSystemGUI_OutputFcn(hObject, eventdata, handles)
varargout{1} = handles.output;
function cmdLoadImag_Callback(hObject, eventdata, handles)
global IFS
global BlockSize;
hf1=@ReadImageFromFile;
x=get(handles.comBoxMethodType,'Value');
if x==1
   isCipher=true;
else
   isCipher=false;
end
OFS=feval(hf1,BlockSize,true,isCipher);
banner= imread('defualtIm.bmp');
axes(handles.axesImDisplay1);
imshow(banner)
set(handles.axesImDisplay1,'Visible', 'off','Units', 'pixels');
set(handles.labTime2,'String','');
axes(handles.axesImDisplay2);
imshow(banner)
set(handles.axesImDisplay2,'Visible', 'off','Units', 'pixels');
if ~OFS.flag
   msgbox(OFS.str,'Error in image select','error');
else
   IFS=OFS;
   axes(handles.axesImDisplay1);
if OFS.imDim==2
      imshow(uint8(OFS.imMat),OFS.map)
else
      im(1:OFS.high,1:OFS.width,1)=OFS.imMatR;
      im(1:OFS.high,1:OFS.width,2)=OFS.imMatG;
      im(1:OFS.high,1:OFS.width,3)=OFS.imMatB;
      imshow(uint8(im))
end
   set(handles.axesImDisplay1,'Visible', 'off','Units', 'pixels');
end
clc
```

APPENDIX B

In combination with the compression operation the proposed encryption procedure. The encryption operation consists of 3 algorithms: permutation of color planes, sign encoding and confusion of the DCT coefficients.

```
function radioM1_Callback(hObject, eventdata, handles)

global BlockSize;
global keyLength;
OFS.flag=false;
banner= imread('defualtIm.bmp');
axes(handles.axesImDisplay2);
imshow(banner)
set(handles.axesImDisplay2,'Visible', 'off','Units', 'pixels');
BlockSize=8;
keyLength=8;
set(handles.labChar,'String','8 Char');
set(handles.labTime2,'String','');
function radioM2_Callback(hObject, eventdata, handles)
global BlockSize;
global keyLength;
OFS.flag=false;
banner= imread('defualtIm.bmp');
axes(handles.axesImDisplay2);
imshow(banner)
set(handles.axesImDisplay2,'Visible', 'off','Units', 'pixels');
BlockSize=8;
keyLength=2;
set(handles.labChar,'String','2 Char');
set(handles.labTime2,'String','');
function radioM3_Callback(hObject, eventdata, handles)
global BlockSize;
global keyLength;
OFS.flag=false;
banner= imread('defualtIm.bmp');
axes(handles.axesImDisplay2);
imshow(banner)
set(handles.axesImDisplay2,'Visible', 'off','Units', 'pixels');
BlockSize=8;
keyLength=1;
set(handles.labChar,'String','1 Char');
set(handles.labTime2,'String','');
function txtKey_Callback(hObject, eventdata, handles)
global keyLength;
```

```
x=get(handles.txtKey,'String');
if length(x)~=keyLength
   set(handles.txtKey,'String','');
   msgbox(sprintf('Length of Key must be = %g',keyLength),'Error in Key length','error');
end
 function txtKey_CreateFcn(hObject, eventdata, handles)
if ispc
   set(hObject,'BackgroundColor','white');
else
   set(hObject,'BackgroundColor',get(0,'defaultUicontrolBackgroundColor'));
end
function cmdWork_Callback(hObject, eventdata, handles)
global IFS
global keyLength;
global BlockSize;
global methodFlag;
global OFS
tFlag=methodFlag;
set(handles.labTime2,'String','');
set(handles.cmdWork,'Enable','off');
banner= imread('defualtIm.bmp');
axes(handles.axesImDisplay2);
imshow(banner)
set(handles.axesImDisplay2,'Visible', 'off','Units', 'pixels');
if IFS.flag
   index=0;
   key=get(handles.txtKey,'String');
   lk=length(key);
if get(handles.radioM1,'Value')==1;
if lk==keyLength
        index=1;
end
elseif get(handles.radioM2,'Value')==1;
if lk==keyLength
        index=2;
end
else
if lk==keyLength
        index=3;
end
end
if index>0
if index==1
try,
          hf1=@m6test;
if tFlag
             OFS=feval(hf1,IFS,key,1);
else
             OFS=feval(hf1,IFS,key,-1);
end
```

```
catch,
            OFS.flag=false;
end
elseif index==2
if tFlag
                hf2=@m2test;
else
                hf2=@m3test;
end
            OFS=feval(hf2,IFS,BlockSize,key);
catch,
            OFS.flag=false;
end
elseif index==3
try,
if tFlag
                hf3=@m4test;
else
                hf3=@m5test;
end
OFS=feval(hf3,IFS,key);
catch,
            OFS.flag=false;
end
end
if OFS.flag
        banner= imread('defualtIm.bmp');
        axes(handles.axesImDisplay2);
        imshow(banner)
        set(handles.axesImDisplay2,'Visible', 'off','Units', 'pixels');
        axes(handles.axesImDisplay2);
if OFS.imDim==2
            im=uint8(OFS.imMat);
            imshow(im,OFS.map)
else
            im(1:OFS.high,1:OFS.width,1)=uint8(OFS.imMatR);
            im(1:OFS.high,1:OFS.width,2)=uint8(OFS.imMatG);
            im(1:OFS.high,1:OFS.width,3)=uint8(OFS.imMatB);
            imshow(im)
end
        set(handles.axesImDisplay2,'Visible', 'off','Units', 'pixels');
        set(handles.labTime2,'String',sprintf('%g (s)',OFS.Time));
else
        msgbox('Cannot continue work !!!Check pramerters or change method','Error in
Operation','error');
end
else
      msgbox('Check your key Please','Error in the Key','error');
end
else
```

```
    msgbox('Please Load Image first','Loading Error','error');
end
set(handles.cmdWork,'Enable','on');
clc
function comBoxMethodType_Callback(hObject, eventdata, handles)
global methodFlag;
global IFS;
IFS.flag=false;
OFS.flag=false;
banner= imread('defualtIm.bmp');
axes(handles.axesImDisplay1);
imshow(banner)
set(handles.axesImDisplay1,'Visible', 'off','Units', 'pixels');
axes(handles.axesImDisplay2);
imshow(banner)
set(handles.axesImDisplay2,'Visible', 'off','Units', 'pixels');
set(handles.labTime2,'String','');
if get(handles.comBoxMethodType,'Value')==1
    methodFlag=true;
    set(handles.cmdWork,'String','Cipher Image');
    set(handles.CipherSystemGUI,'Name','Cipher System');
    set(handles.labCipherImage,'String','Cipher Image');
    set(handles.labCipherImage,'String','DeCipher Image');
end
```

APPENDIX C

This section shows how the cryptosystem operates, how the user can use the cryptosystem, and the buttons it contains.

```
function comBoxMethodType_CreateFcn(hObject, eventdata, handles)
if ispc
   set(hObject,'BackgroundColor','white');
else
   set(hObject,'BackgroundColor',get(0,'defaultUicontrolBackgroundColor'));
end
function cmdHisto_Callback(hObject, eventdata, handles)
global IFS;
if IFS.flag
if IFS.imDim==2
      im=uint8(IFS.imMat);
      Figure, imhist(im),title 'Image Layer',xlabel 'Gray Level',ylabel 'Pixels No'
else
      im(1:IFS.high,1:IFS.width,1)=uint8(IFS.imMatR);
      im(1:IFS.high,1:IFS.width,2)=uint8(IFS.imMatG);
      im(1:IFS.high,1:IFS.width,3)=uint8(IFS.imMatB);
      Figure, imhist(im(:,:,1)),title 'Red Layer',xlabel 'Gray Level',ylabel 'Pixels No'
      Figure, imhist(im(:,:,2)),title 'Green Layer',xlabel 'Gray Level',ylabel 'Pixels No'
      Figure, imhist(im(:,:,3)),title 'Blue Layer',xlabel 'Gray Level',ylabel 'Pixels No'
end
else
   msgbox('Please Load Image first','Loading Error','error');
end
function cmdCompute_Callback(hObject, eventdata, handles)
global IFS;
global OFS;
if IFS.flag && OFS.flag
   AFS.IFS=IFS;
   AFS.OFS=OFS;
   save('tempafs.$$$','-struct','AFS');
   CofiGUI;
else
   msgbox('Please Complete your operatrion Image first','Compute Error','error');
end
function cmdAbout_Callback(hObject, eventdata, handles)
AboutGUI;
function cmdAffect_Callback(hObject, eventdata, handles)
ComputeCipherAffectGUI;
```

CURRICULUM VITAE

Name and surname **:** Nada Mohammed Murad ALJAFF

Address **:**Iraq / Baghdad

E-mail address **:** aven.jaff00@yahooo.com

EDUCATION INFORMATION (Institution and Year):

Bachelor's Degree: Computer Science (Baghdad Collage of Economic Science University ,2005)

Master degree: Aksaray University**,** Department of Electrical Electronic And Computer Engineering, 2019

PROFESSIONAL EXPERIENCE AND AWARDS:

1. Website manager (IT department) Ministry of sporting (2007-2009).
2. Internet and mail manager (IT department) Ministry of sporting (2010-2012).
3. Manager of management unit, Ministry of higher education (2012-2013).
4. Manager of electronic official letter unit, Ministry of higher education (2014-2018).
5. Manager office of consultation board, Ministry of higher education (2018-2019).

PUBLICATIONS, PRESENTATIONS AND PATENTS

1. A cryptographic scheme for color images, journal of advance research in dynamical and control system, (ISSN 1943-023x) www.Jardcs.org/backissues/abstract.php?archive=6419