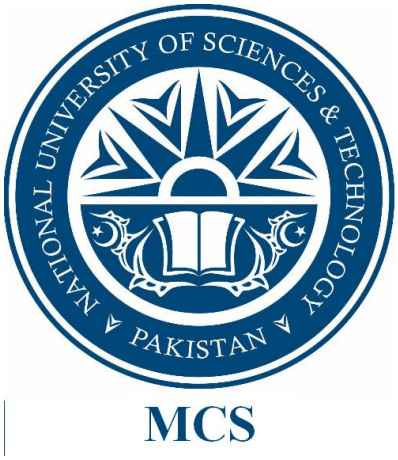
SELECTIVE REGION BASED IMAGE ENCRYPTION



by

Irfan Ullah

A thesis submitted to the faculty of Information Security Department Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of MS in Information Security

May 2014

SUPERVISOR CERTIFICATE

It is to certify that Final Copy of Thesis has been evaluated by me, found as per specified format and error free.

Dated_____

_____
Dr. Mehreen Afzal

ABSTRACT

With the extensive use of the multimedia data over the insecure open natured channels the security of the multimedia data has become very important. There are several encryption techniques for the secure transmission of the images. Encrypting a whole image can make the image information useless for unauthorized access but this whole image encryption of image will increase the computation time of encryption and decryption. To reduce this increase in computation time for encryption/decryption, an approach called selective encryption has been introduced in several new works. With selective encryption considerable reduction in the computation cost can be achieved. This approach however, needs to be explored further for its practical application. We have also found that permutations used in the scheme needs to be revised to obtain better security. The aim of this thesis is to give an efficient image encryption scheme using region based selective encryption.

In this paper a new approach is introduced that will select sensitive area for encryption based on percentage of coefficients and then encrypting the selected area with AES algorithm. To further enhance the security of the image the un-encrypted area is permuted with the encrypted area. The Peak Signal-to-Noise Ratio, PSNR values show a huge difference between the original image and the encrypted image.

DEDICATION

In the name of Allah, the most beneficent, the most merciful
This research work is dedicated to my dear homeland Pakistan, my teachers and my Family.

ACKNOWLEDGMENTS

I would like to thanks my supervisor, Dr. Mehreen Afzal, Temporary Visiting Faculty at the Department of Information Security, Military College of Signals, NUST for her continuous encouragement and able guidance. Without her support and guidance this thesis could not be completed in time.

I am also thankful to my guidance committee members Dr. Asif Masood, Lec Adeela Waqar and Lec. Muhammad Waseem Iqbal of Department of Information Security for their able guidance and support.

I would also like to thank all my family members for the exemplary understanding and support they provided during the entire course of my studies.

TABLE OF CONTENTS

Contents

LIST OF FIGURES

Figure Number *Page*

LIST OF TABLES

Table Number *Page*

Chapter 1

Introduction

1.1 Background

Nowadays image security is of great importance in different applications like for example in Military application, medical imaging etc. In image processing the image encryption is of great importance and has gained lot of attention in encrypting the images to achieve its security and maintain the confidentiality of the images. Trivially all the multimedia data images, audio, video and text data can be encrypted using same algorithms however, multimedia data may require different approaches for encryption. Multimedia data have a bulky size that is why different representation should be considered.

Due to large size of images chaotic maps are considered superior as compared to these conventional encryption algorithms. Chaotic key based algorithm has been presented by Yen and Guo for images encryption [17]. However this technique is costly in terms of storage of image data in the image database.

Improved chaotic baker map was proposed by fingling Han, xinghuo Yu [18], to encrypt bulk size images showing its efficiency and security because of large key space but there are some limitations in using chaotic maps

There exist some invalid keys, Weak keys and some partially equivalent key that reduce size of the key space that may result in a number of attacks [20].

In [19] a Selective image encryption based on hyper-chaos is proposed in which the image is divided into slices and encryption algorithm is applied to each slice ensuring the security of the image. In [21] selective image encryption algorithm, in which the spatiotemporal chaotic system is utilized, is proposed to encrypt gray-level images.

Figure 1.1 Selective Image Encryption

The weaknesses that may be found in image encryption using chaotic maps are listed below because of which a number of attacks may be developed.

First, there exist a number of invalid keys, weak keys and also partially equivalent key which reduce size of the key space and a number of different attacks are developed. When the key space is calculated all the invalid keys are eliminated from the list while in partially equivalent key, one key is considered and the second key is eliminated from the list so it will reduce the key space of the algorithm.

Second, they lack details of, the size of the key and different key generation steps. Because of this it will not be possible to re- implement the algorithm and so the security and performance of the algorithm may not be evaluated in a systematic way thus leaving the doors widely open for the attackers

Third, many chaotic secure communication schemes proposed to date has failed to clearly state the key management scheme. There are some design that does not use any

key in the algorithm and the scheme without a key can be viewed more like a coding system instead of cryptographic.

Selective encryption of human skin in JPEG images by J. Rodrigues, W.Puech and A.G. Bors. This approach detects color spectrum e.g. human skin for encryption. Only certain number of blocks will be selected in this approach. Droogenbroeck and Benedett proposed selective encryption of compressed and uncompressed images by applying XOR functions on some of the bit planes.

Aim of this research is to explore further selective images encryption approach using traditional encryption technique like AES. Our approach selects most sensitive area of the image and is encrypted with AES algorithm. The sensitive area will be selected from the image using maximum information discrete cosine transform (DCT) on the image blocks and after the application of quantization in which the image size is reduced by removing high frequency bits.

The encryption will be applied only to some part of the image and not to the whole image which is the aim of this thesis.

1.2 Objective

The main goal of this research is to selectively encrypt the image in order to achieve the confidentiality of the images and also to increase its efficiency during its transmission on an insecure channel or during its storage in the image Database

Also extend the idea of encryption using different permutation in order to increase security of the image. The permutation will be strong enough between encrypted and

unencrypted regions so that no information is visible if an attacker wants to retrieve the image information.

1.3 Research Scope

Multimedia security is of great importance when it is transmitted over the insecure wireless channel. The images whether medical images, jpeg images or satellite images needs greater security over the internet. This research can be of benefit to different organizations in Pakistan that are storing confidential images or transmitting their images over the internet. This research is applicable to wide range of military organization and healthcare organization when it is required to transmit satellite images among forces or store the confidential medical images.

1.4 Thesis Organization

This research is organized into 4 chapters. Chapter 2 is about the literature review carried out for this research. Chapter 2 discusses selective image encryption and describes its classification, security and performance requirements. Chapter 3 discusses the proposed selective images encryption algorithm and gives different methods for selecting the area for encryption. It also describes the performance of the proposed encryption algorithm compared to full images encryption. Chapters 4 discuss the overall performance of the proposed encryption algorithm and show the different experimental results. This chapter also concludes whole report and describes the directions to extend this work in future.

Chapter 2

Selective Images Encryption

2.1 Introduction

This chapter provides an overview of partial image encryption. This new approach i.e. selective image encryption is suggested that will partially encrypt the image and will maintain the confidentiality of the image as well as reduce the encryption and decryption time of the image.

When we are dealing with encryption of still images then a naïve approach will be good enough to provide high level of security to the images by encrypting the entire image but there are certain things because of which we cannot encrypt the entire image that is limited bandwidth or low processing power. A detail survey study of the images encryption techniques are given in this section.

JPEG (Joint Photographic Experts Group), JPEG is the name of the organization as well that created JPEG [9]. This format is used worldwide over the internet and for extensively storing the photographs [10].

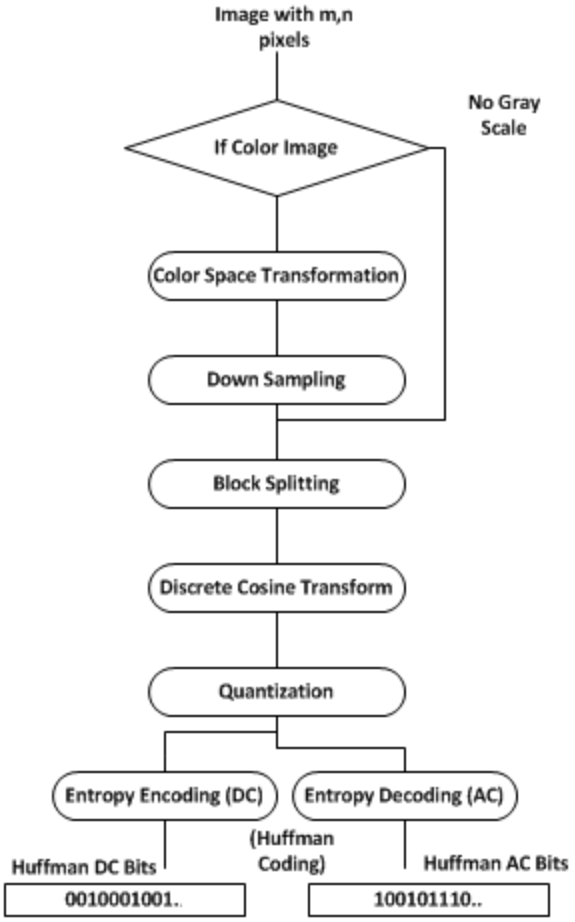


Figure 2.2 Flow Chart of JPEG encoder

JPEG compression technique encodes the pixels that are ranging from 0-255 into binary representation in the form of 0's and 1's. The image after passed through the process of compression will be in reduced size from the original image. As a tradeoff JPEG is lossy algorithm which means that during the process of compression some bits may get lost and those lost bits cannot be recovered after being lost [10, 15]. The aim of JPEG compression is to provide a very good compression ratio and also to preserve the image

quality as well. JPEG compression routine is to encode. A quality factor is available that will allow one that how much of the fine image detail is to be preserved.

2.2 Partial Encryption Algorithms by Cheng and Li

In [2] Cheng and Li proposed a selective/partial image encryption algorithm that will partially encrypt the image that is best suitable for images and that the images are compressed with image compression algorithms. The compression algorithms in this proposed technique are (1) quadtree Compression Algorithm (2) wavelet compression algorithm that is based on zerotress. What kind of encryption and decryption is used it is not specified but the cryptosystem like AES, IDEA, DES etc can be selected by the user.
The compression algorithm quadtree compression for image produces quadtree structure and parameters that describe each block in the tree. For simplicity assume that the only parameter that describes each block will be the average intinsety. The intinsety for each block will never provide too much information about the image but the reconstruction in the original frame of object outlines will be allowed by the quadtree decomposition [2]. Therefore the proposed encryption method quadtree encryption by Cheng and Li's will only encrypts the quadtree structure while at the leaf nodes of quadtree the block intinseties will not be encrypted. The partial quadtree encryption can be applied to lossless image compression as well as lossy compression. That's why Cheng and Li's proposed the encryption of only significance bits and also the threshold parameter n that determine the significant coefficients [2]

2.3 Selective Encryption Methods for Raster and JPEG Images

In 2002, the selective encryption method for compressed images and uncompressed images was proposed by Droogenbroeck and Benedett [3]
In the proposed encryption scheme the author proposed to first select the bitplanes that needs to be encrypted and then the bitplanes that are selected for encryption are xored

with the key. The key size must be equal to the selected bitplanes for encryption. According to the author's, Droogenbroeck and Benedett, to achieve satisfactory visual degradation of the image at least 45 of the LSB should be encrypted. One thing that is important from security point of view is that partial degradation will not provide high security if the requirement is a high security.

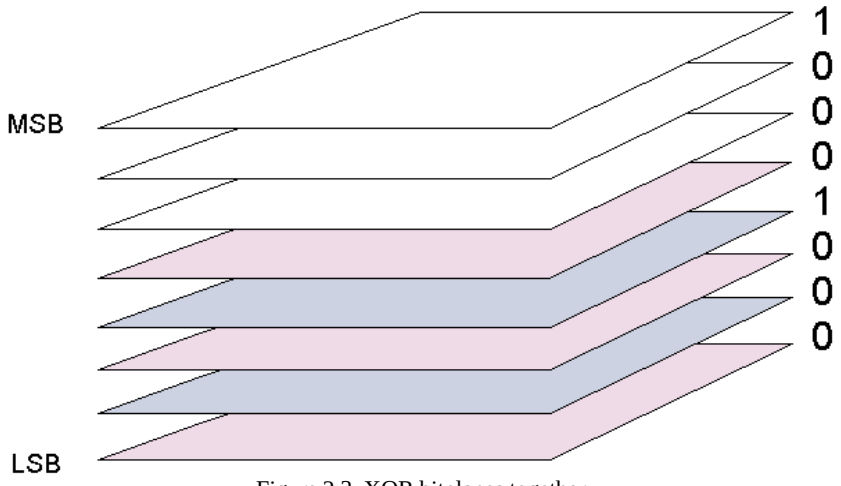


Figure 2.3 XOR bitplanes together.

To selectively encrypt the JPEG compressed images a second method was proposed. In the proposed techniques the author's proposed to encrypt only the AC coefficients while DC coefficient are left unencrypted, after applying quantization a matrix obtain contain one DC coefficient and rest all are AC coefficients. The DC coefficient is highly predictable that's why the DC component is left unencrypted [3]. For the purpose of synchronization the codewords are left unencrypted.

2.4 Selective Bitplane Encryption Algorithm

A new selective image encryption algorithm was proposed by Podesser, Schmidt and Uhl for the uncompressed Image raster images [4]. In the Schmidt and Uhl algorithm the most significant bits (MSB) are encrypted only.

In the proposed cryptosystem [4] Podesser, Schmidt and Uhl proposed the same conclusion that were concluded by Droogenbroeck and Benedett in their algorithm [3] that if you encrypt only the MSB then it is not sufficient to provide greater security because the unencrypted bitplanes will be more enough to reconstruct the MSB from it. Therefore they suggest that encrypting 2 bitplanes or four bitplanes will be good enough. if four bitplanes are encrypted then it will provide a high level of security. It is totally dependent on the user wish whether to encrypt only two bitplanes will be sufficient for degradation of the application or if a user wish for more secure approach then encrypting four bitplanes will be required.

2.5 Selective Image Encryption for Medical and Satellite Images

In this scheme by Panduranga and NaveenKumar [5] the selective image encryption is proposed. This scheme proposed selective image encryption in two different ways. The given Figure 2.4 is showing the first proposed method for selective image encryption.

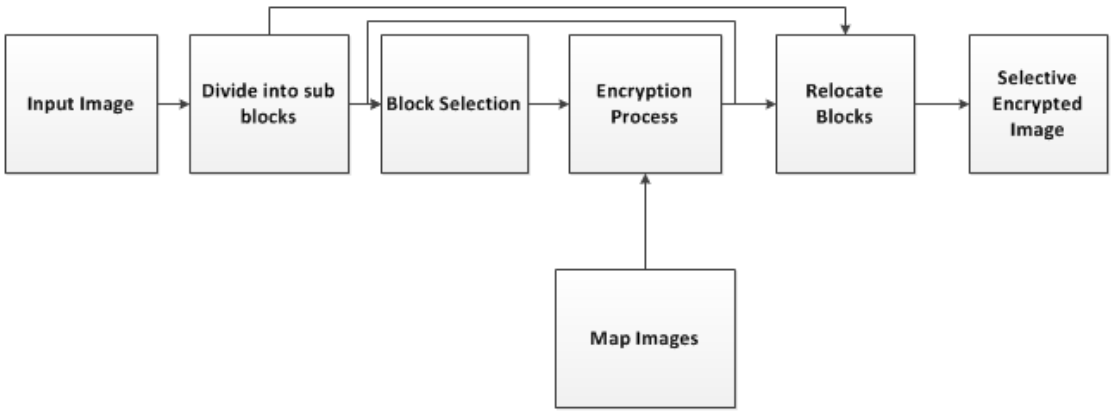


Figure 2.4 Block diagram of selective image encryption using sub blocks.

In this proposed method an image is first input and then it is divided into different sub blocks. This selection of block is done before we apply encryption to the Image. In the encryption process there are two different inputs, one of the input is the selected block that need to be encrypted and the second input is the map image. In the map-based technique for image encryption the blocks that are selected for encryption are encrypted partially. If a complete encryption of the selected block is required then it is also possible and each block selected can use a separate map image for the encryption of the blocks.

The second method that is used for the partial encryption of the image is shown in Figure 2.5, in which an image is input and then performs some morphological operation on the input image that will select the sensitive area of interest for encryption and after the area is selected for encryption, it is encrypted then using map images.

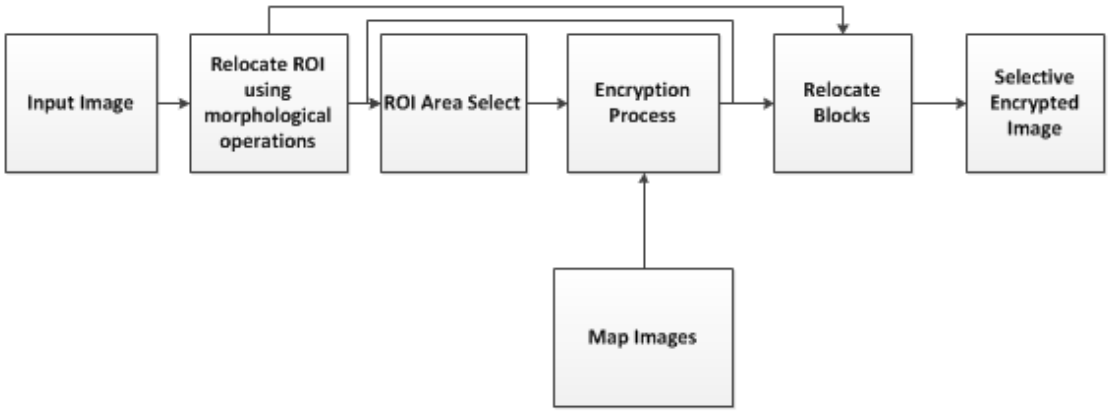


Figure 2.5 Block diagram of selective image encryption using morphological operation

After applying morphological operation on the selected image, different regions can be selected and then a sender can select one or more regions to be encrypted [5, 6]. These

encryption approaches can be used to encrypt different images for encryption. The result of proposed encryption algorithm is shown in the following Figure 2.6.

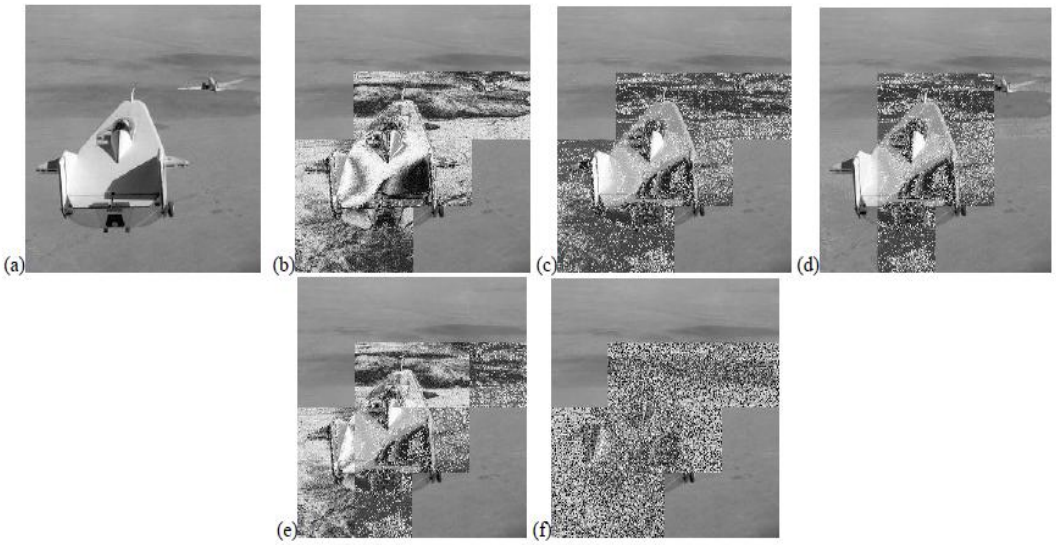


Figure 2.6 Proposed method using different map images.

2.6 Selective Encryption of Human Skin

Selective encryption of human skin in JPEG images it is to detect the human skin in the color images. The reason for this detection is to find certain sub blocks in the images that need to be encrypted in order to secure it from unauthorized access. The basic working of this algorithm is to find those regions in the image that are of the interest which is called as region of interest (ROI) for further processing according to the lumninance level of the pixils. When applying JPEG compression technique, two types of coefficients that are AC coefficient and DC coefficient are produced in this encoding.

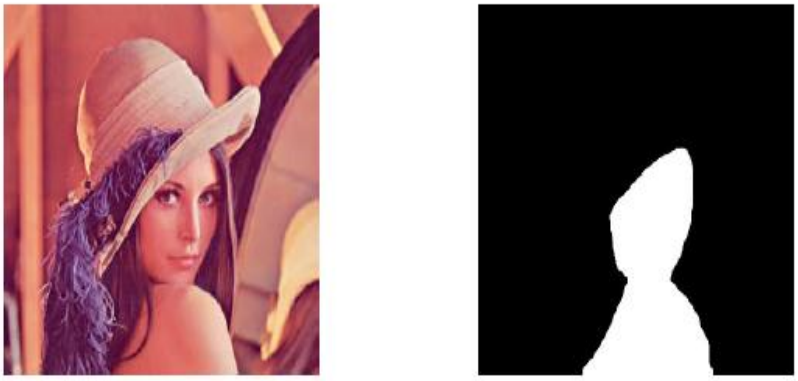


Figure 2.7 Detecting Region Of Interest (ROI) in human skin

The DC coefficient which is at the top left most and contain the mean value of 8 x 8 pixils which are used to detect the color. As a result of this there will be certain blocks that will receive this effect but the whole image will not receive this effect. The AC and DC coefficients are encoded into bits when applying encoding usually the Huffman encoding [8, 7] in the JPEG encoding.

The algorithm proposed in this paper has a lot of advantages; first advantage is that very small amount of data is processed for encryption. Taking an example of CCTV, if a person is walked pass then the CCTV will detect only the human skin for encryption purpose and will not consider the surrounding for processing [7]. Thus it will reduce the computational complexity significantly by processing only some part. The second advantage to this algorithm is that this algorithm will not select all the AC coefficients for encryption purpose but only some of the total AC coefficients are selected and encrypted. In this way 2-4% of the blocks will be encrypted and this will speed up the number of processing. The algorithm will encrypt only the necessary data while leaving the unimportant data unencrypted. There is also a downside of this algorithm that if the background is also of skin color then it will encrypt that portion as well which is not that much important from security point of view.

2.7 Secure and low cost selective encryption for JPEG2000

In [22] a new approach for selectively encrypting the multimedia data was introduced. In this paper a set of evaluation criteria for the selectively encrypting a JPEG 2000 images was introduced that satisfy all the criteria. This proposed algorithm mainly contributed in selecting a very small amount of data for the encryption purpose and provides a given level of security.

JPEG 2000 is comprised of packets and each of the packet is comprised of data from the given Resolution R, Quality Layer L, spatial region that is called precinct P and the Component C. Each of the packets is comprised of the packet header and that packet header is followed by the data Fig. 0.12

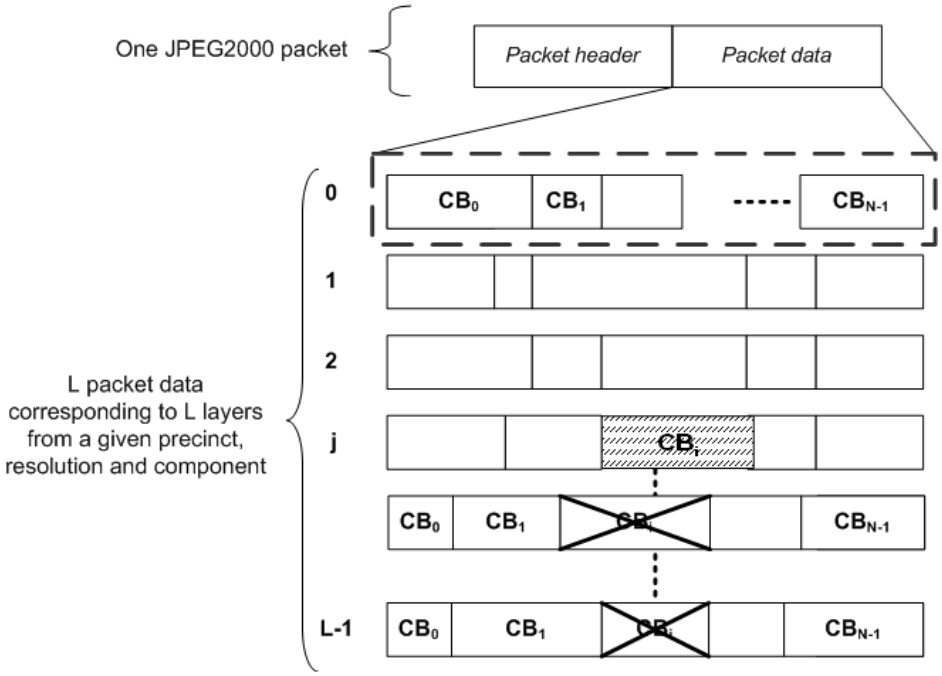


Figure 2.8 JPEG 2000 Packet Structure

Each packet data contains Code Block Contributions (CCP's) as shown in Fig. 0.12. A subset of the packets can be encrypted that depends mainly on the target application Fig. 0.13. .

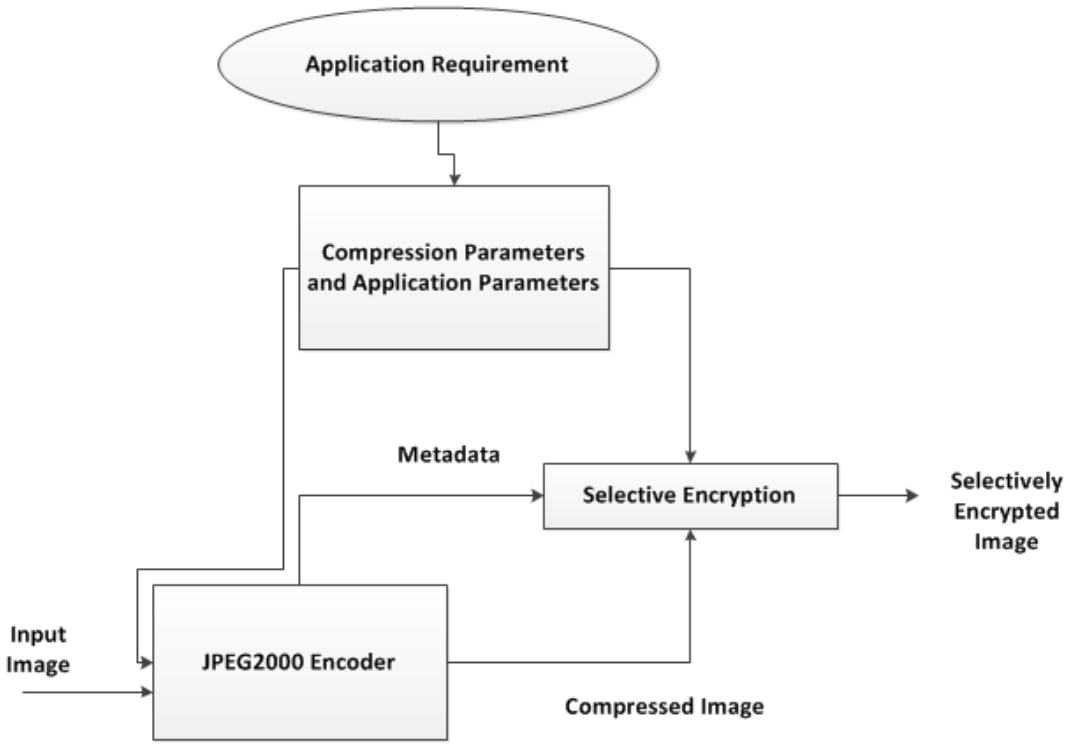


Figure 2.9 Proposed Approach

This proposed algorithm guaranteed to be cryptographically secure and minimum encryption ratio is achieved. The proposed algorithm is compression friendly and save a lot of time as whole image is not processed for encryption purposed.

2.8 Image Encryption Using DCT and Stream Cipher

In [23] the authors of the paper encrypt the image selectively by encrypting some higher frequencies after the DCT transformation is applied on the image and converted to frequency domain and after this the resultant block obtained is shuffled by a pseudorandom sequence of bits. The scheme is illustrated in the Figure.

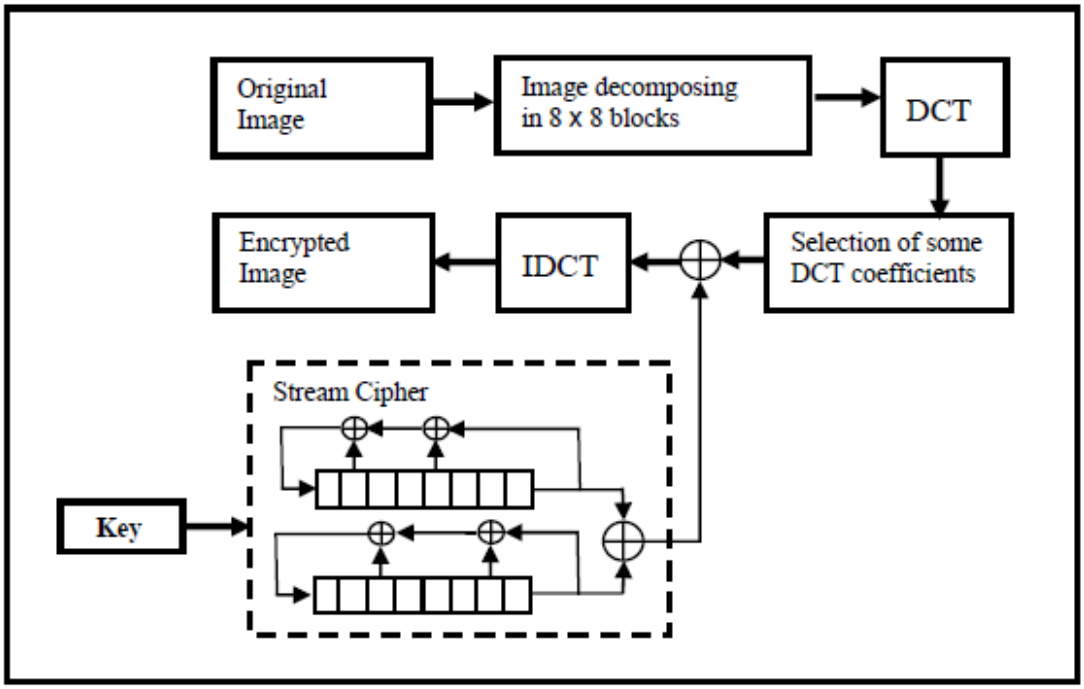


Figure 2.10 Block Diagram of Algorithm

The proposed algorithm is lossless and because of this the images used in this application have very important information and loss of any of the information is not acceptable. Several algorithms are proposed for selectively encrypting DCT Coefficients [2, 3, 4]

In this algorithm an image is taken as input and divides it into different blocks. After which DCT transformation is applied to the image in order to convert the image from

spatial to the frequency domain [10, 12, 26, 27]. After this conversion from spatial domain to the frequency domain, blocks are passed through the DCT transformation and the blocks will contain DC Coefficients and AC Coefficients.

.

Table 2.1 Selective Encryption Scheme Classification

Type of data	Domain	Proposal	Encryption Algorithm	What is encrypted
Image	**Frequency Domain**	Cheng and Li, 2000	No Algorithm is specified	Pixel and set related significance information in the two highest pyramid level of SPIHT
		Droogenbroeck and Benedett, 2002	DES, Triple DES and IDEA	Bits that indicate magnitude & sign of the non-zero DCT coefficients
		Pommer and Uhl, 2003	AES	Subband decomposition structure
	Spatial Domain	Cheng and Li, 2000	No Algorithm is specified	Quadtree Structure
		Droogenbroeck and Benedett, 2002	XoR	LSB
		Podesser, Schmidt & Uhl, 2002	AES	MSB

This algorithm is considered to be a fast algorithm as whole image is not encrypted but only certain portion of the image is encrypted i.e. DC coefficient and some of the AC

Coefficients. Encrypting only DCT coefficient is because human is more sensitive to low frequencies than to the higher frequencies [24, 25] and also the algorithm is considered to be a very secure one because the blocks are encrypted by using block shuffling method that depends mainly on the two prime numbers. These prime numbers are used in the generation of the sequence of rows or columns that further will be used in the shuffling.

2.9 Selective Image Encryption Using Chaotic Maps

A chaotic map is another method that is used for image encryption nowadays. To meet the requirements of providing high level of security to these multimedia data there are different encryption algorithms that are providing some level of security. Considering the bulky size of the images and videos there are different approaches that need to be following to provide better security to it. In 1990's there are different solutions that were presented in order to provide better security to the images [28- 37]. The relation between a chaos theory and cryptography is strong one that's why most the images encryption uses chaos in order to provide better permutation of images [32, 36, 38].

Chaotic maps are very sensitive to their initial conditions and because of this sensitivity to their initial condition they have more application. The two methods confusion and diffusion realize the image encryption and because of sensitivity of chaotic maps to the initial condition and its randomness, these chaotic maps may realize the image encryption. There are several encryption algorithm proposed nowadays based on chaotic maps in order to provide better mixing property [39-45].

In [49, 50, 41, 43, 44, 47] different chaotic maps are used for the efficient transmission of images over the untrusted internet. 1D, 2D and 3D chaotic baker maps are used for the secure transmission of images. First of all standard baker map is extended to 3D baker map and is then used for the encryption process. This will speed up the encryption process because of the light weight nature of the maps and also to provide better security to the images. Similarly image encryption using chaotic logistic map provides efficient

transmission of encrypted images and security as well but because of a number of weaknesses in the using chaotic maps for images encryption, it is vulnerable to different attacks.

2.10 Summary:

This chapter is a summary of different selective image encryption techniques. Different approaches were discussed in this chapter that will selectively encrypt/decrypt the images. Both traditional encryption techniques and chaotic maps are discussed in this chapter, that selectively encrypt/decrypt images.

Chapter 3

Proposed Solution for Selective Region Based Images Encryption

3.1 Introduction:

This chapter proposed a solution to selectively encrypt/decrypt images. In this chapter the whole process is discussed in detail. In section 3.2 proposed encryption algorithm design is shown. Section 3.2 discusses the encryption algorithm. In section 3.4 the process of block division is discussed. In section 3.5 discrete cosine transform is discussed that convert an image from spatial to frequency domain. Section 3.6 discusses quantization. In this section each block is divided using standard quantization matrix to in order to remove high frequency components. Section 3.7 discusses the process of block selection and block encryption using AES algorithm. In section 3.8 permutation is discussed that will permute the encrypted content of the image with the unencrypted content. Section 3.9 discusses the whole decryption process of the proposed encryption technique. Section 3.10 concludes the whole chapter.

3.2 Background Concepts:

3.2.1 Block Splitting:

Blocking splitting is the next stage of the JPEG compression. The pixels are grouped into 8 x 8 blocks and these blocks are passed into the discrete cosine transform (DCT) [11, 15, 16]. We will group these blocks into 8 x 8 and if the image size is such that it cannot be grouped into 8 x 8 then we will add some extra bits so that it can be a multiple of 8. For example if we have an image of size 12x 15 which is not a multiple of

8, add extra bits to make it multiple of 8 or we can repeat the pixels lying at the end to the end of the Image.

	1	2	3	4	5	6
1	<8x8 double>	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...
2	<8x8 double>	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...
3	<8x8 double>	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...
4	<8x8 double>	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...
5	<8x8 double>	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...
6	<8x8 double>	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...
7	<8x8 double>	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...
8	<8x8 double>	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...
9	<8x8 double>	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...
10	<8x8 double>	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...
11	<8x8 double>	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...
12	<8x8 double>	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...
13	<8x8 double>	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...
14	<8x8 double>	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...
15	<8x8 double>	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...
16	<8x8 double>	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...	<8x8 doubl...

Figure 3.11 Shifting Blocks Splitting 8 x 8 Windows

The image is divided into 8x8 different blocks as shown in the Figure. 3.1. Figure 3.1 is showing one layer divided into 8x8, similarly the other two layers can be divided in the same manner. Each layer first block values are shown in the Figure 3.2.

	1	2	3	4	5	6	7	8
1	0.3882	0.3882	0.3882	0.3843	0.3843	0.3843	0.3804	0.3804
2	0.3843	0.3843	0.3843	0.3804	0.3804	0.3804	0.3765	0.3765
3	0.3843	0.3843	0.3843	0.3804	0.3804	0.3804	0.3765	0.3765
4	0.3804	0.3765	0.3765	0.3765	0.3725	0.3725	0.3725	0.3686
5	0.3725	0.3725	0.3725	0.3686	0.3686	0.3686	0.3647	0.3647
6	0.3725	0.3725	0.3686	0.3686	0.3686	0.3647	0.3647	0.3647
7	0.3765	0.3765	0.3725	0.3725	0.3725	0.3686	0.3686	0.3686
8	0.3765	0.3765	0.3765	0.3725	0.3725	0.3686	0.3686	0.3686

Figure 3.2 (a) First Block frequency distribution layer 1

	1	2	3	4	5	6	7	8
1	0.1490	0.1490	0.1490	0.1451	0.1451	0.1451	0.1412	0.1412
2	0.1451	0.1451	0.1451	0.1412	0.1412	0.1412	0.1373	0.1373
3	0.1333	0.1333	0.1333	0.1294	0.1294	0.1294	0.1255	0.1255
4	0.1294	0.1255	0.1255	0.1255	0.1216	0.1216	0.1216	0.1176
5	0.1216	0.1216	0.1216	0.1176	0.1176	0.1176	0.1137	0.1137
6	0.1216	0.1216	0.1176	0.1176	0.1176	0.1137	0.1137	0.1137
7	0.1176	0.1176	0.1137	0.1137	0.1137	0.1098	0.1098	0.1098
8	0.1176	0.1176	0.1176	0.1137	0.1137	0.1098	0.1098	0.1098

Figure 3.2 (b) First Block frequency distribution layer 2

	1	2	3	4	5	6	7	8
1	0.0353	0.0353	0.0353	0.0314	0.0314	0.0314	0.0275	0.0275
2	0.0314	0.0314	0.0314	0.0275	0.0275	0.0275	0.0235	0.0235
3	0.0275	0.0275	0.0275	0.0235	0.0235	0.0235	0.0196	0.0196
4	0.0235	0.0196	0.0196	0.0196	0.0157	0.0157	0.0157	0.0118
5	0.0235	0.0235	0.0235	0.0196	0.0196	0.0196	0.0157	0.0157
6	0.0235	0.0235	0.0196	0.0196	0.0196	0.0157	0.0157	0.0157
7	0.0314	0.0314	0.0275	0.0275	0.0275	0.0235	0.0235	0.0235
8	0.0314	0.0314	0.0314	0.0275	0.0275	0.0235	0.0235	0.0235

Figure 3.2 (c) First Block frequency distribution layer 3

After a block is identified then it will pass through different procedures like DCT transform, Quantization etc. if block is not a multiple of 8 x 8 then it will be made multiple of 8 x 8 by adding extra bits.

3.2.2 Discrete Cosine Transform (DCT):

The next step to perform on an image is DCT that will convert an image from spatial to frequency domain [12]. The DCT is performed on the 8 x 8 block. In DCT image is converted from spatial to frequency domain. Result for each layer after applying DCT is shown in the Figure 3.3.

	1	2	3	4	5	6	7	8
1	3.0029	-5.4468e-04	0.0201	-9.6155e-04	-9.8039e-04	1.9127e-04	0.0023	-8.1517e-04
2	0.0276	0.0062	-0.0212	-0.0015	-5.6269e-04	1.5718e-04	-0.0057	6.8401e-04
3	-7.3592e-04	1.1082e-04	5.3258e-05	-3.0494e-04	-2.2556e-04	8.2854e-04	4.8924e-04	-0.0018
4	0.0052	0.0032	-0.0070	0.0015	-3.9451e-04	0.0026	-0.0022	5.6614e-04
5	-6.0383e-04	5.2803e-04	3.3660e-04	3.7184e-04	-0.0012	4.1015e-04	-5.2006e-05	0.0011
6	8.3500e-04	0.0086	-0.0035	2.2745e-04	0.0025	0.0026	-0.0024	0.0032
7	0.0014	-4.1392e-04	-6.7181e-04	-8.1518e-04	0.0023	-6.3863e-04	-0.0011	-4.1692e-04
8	0.0060	0.0248	-0.0014	0.0016	6.8731e-04	0.0069	0.0014	0.0093

Figure3.3 (a) DCT Result on 8x8 First Block layer 1

	1	2	3	4	5	6	7	8
1	1.0029	-5.4468e-04	0.0273	-9.6155e-04	-9.8039e-04	1.9127e-04	-6.9703e-04	-8.1517e-04
2	0.0328	0.0129	-0.0406	0.0014	-0.0248	-7.6165e-04	-0.0160	-3.5247e-04
3	-7.3592e-04	1.1082e-04	5.3258e-05	-3.0494e-04	-2.2556e-04	8.2854e-04	4.8924e-04	-0.0018
4	0.0105	0.0113	-0.0107	0.0064	-0.0078	0.0028	-0.0059	-1.1925e-04
5	-6.0383e-04	5.2803e-04	3.3660e-04	3.7184e-04	-0.0012	4.1015e-04	-5.2006e-05	0.0011
6	0.0064	0.0197	-0.0039	0.0088	-0.0013	0.0045	-0.0046	0.0028
7	0.0014	-4.1392e-04	-6.7181e-04	-8.1518e-04	0.0023	-6.3863e-04	-0.0011	-4.1692e-04
8	0.0120	0.0514	2.3103e-05	0.0271	-0.0014	0.0155	-1.1425e-04	0.0091

Figure 3.3 (b) DCT Results on 8x8 First Block layer 2

	1	2	3	4	5	6	7	8
1	0.1951	-5.4468e-04	0.0345	-9.6155e-04	-9.8039e-04	1.9127e-04	-0.0037	-8.1517e-04
2	0.0248	0.0023	-0.0039	-5.5122e-04	-6.5697e-04	-8.4266e-04	0.0019	0.0013
3	-7.3592e-04	1.1082e-04	5.3258e-05	-3.0494e-04	-2.2556e-04	8.2854e-04	4.8924e-04	-0.0018
4	0.0023	-0.0016	-0.0019	0.0021	-6.7223e-04	0.0011	2.3081e-04	9.3950e-04
5	-6.0383e-04	5.2803e-04	3.3660e-04	3.7184e-04	-0.0012	4.1015e-04	-5.2006e-05	0.0011
6	-0.0022	0.0013	-8.8084e-04	5.4941e-04	0.0020	5.9008e-05	-0.0011	0.0034
7	0.0014	-4.1392e-04	-6.7181e-04	-8.1518e-04	0.0023	-6.3863e-04	-0.0011	-4.1692e-04
8	0.0027	0.0052	1.5104e-04	0.0017	-8.5574e-06	-7.9699e-04	0.0023	0.0093

Figure 3.3 (c) DCT Results on 8x8 First Block layer 3

After performing DCT operation we obtain only AC and DC coefficients in the blocks. DC coefficient lies on the top left corner of the block that represents the DCT cosine wave. All other coefficients are the AC coefficients that will represent the spatial frequencies [12]. The AC coefficients are 63 in numbers and those AC coefficients that are near to the DC have low frequencies while those lying at the bottom right have very high frequencies [9].

In order to locate the low frequency component on the top left and high frequency corner at the bottom right we apply DCT operation on the block. Human eye are very sensitive to low frequency so most of the low frequency information is preserved [10].

3.2.3 Quantization:

After we apply DCT transformation on the block in order to convert an image from the spatial domain to frequency domain, we then apply another operation called quantization on 8 x 8 blocks in order to further reduce the size of the image. Quantization is done by dividing the block that contains DC and AC coefficients obtained after DCT transformation by a standard quantization matrix [13]. The quantization matrix which is a standard matrix has high values at the bottom right side. It will compress high frequency coefficients [10, 11]. Reason for this is that human eye is very sensitive to low frequency components and less sensitive to high frequency components. So in quantization majority of the high frequency components are rounded to zero and discarded.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
75	92	95	98	112	100	103	99

Figure 3.12 Standard Quantization Matrix

	1	2	3	4	5	6	7	8
1	48	0	1	0	0	0	0	0
2	1	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0

3.5 (a) Quantized Matrix of First Block layer

	1	2	3	4	5	6	7	8
1	16	0	1	0	0	0	0	0
2	1	0	-1	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0

Figure 3.5 (b) Quantized Matrix of First Block layer 2

	1	2	3	4	5	6	7	8
1	3	0	1	0	0	0	0	0
2	1	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0

Figure 3.5 (c) Quantized Matrix of First Block layer 3

As discussed in the previous section that JPEG is a lossy compression algorithm which means that during compression some of the information will get lost. The image size will be reduced but will also degrade a little the quality of the image which is a tradeoff between the image size and the image quality. After quantization majority of the AC coefficients are rounded to zero and discarded which certainly will reduce the image size.

3.2.4 Measuring Image Quality:

When in image processing an image is reconstructed from original image then the difference between them is required to be measured. There are errors between the images and these can be measured numerically by two different methods.

3.2.5 Mean Square Error (MSE):

Mean Square Error (MSE) is the cumulative square error between the original image and the reconstructed image.

Mean Square Error (MSE) can be calculated using the following expression.

$$MSE = \frac{1}{MN} \sum_{y=1}^{M} \sum_{x=1}^{N} \left[I(x, y) - I'(x, y) \right]^2$$

Mean Square Error (MSE) Equation 3.2

Here in this equation the dimensions of the image are M and N that goes through all pixels in an original image and reconstructed image. The total number of pixels will average the result. If the result of the MSE is small then this indicated that there is a very little error and the two images i.e. original image and reconstructed image are very similar [14].

3.2.6 Peak Signal to Noise Ratio (PSNR):

Peak Signal to Noise Ratio (PSNR) is used to measure the peak of error as shown in the equation below.

There exists an inverse relationship between the MSE and the PSNR. Large value for the PSNR between the two images indicates a good result. In Peak Signal to Noise Ratio,

PSNR signal indicates the original image whereas noise indicates the error in the reconstructed image [14].

$$PSNR = 20 \cdot \log_{10}\left(\frac{255}{\sqrt{MSE}} \right)$$

PSNR Equation Equation 3.3

3.3 Proposed Encryption Algorithm:

The proposed Selective Region Based Image encryption is a new approach for selecting the sensitive area in the images for encryption purpose. The main idea in this approach is to selectively encrypt / decrypt the sensitive area followed by permutation. The model for selective region based encryption is shown in the

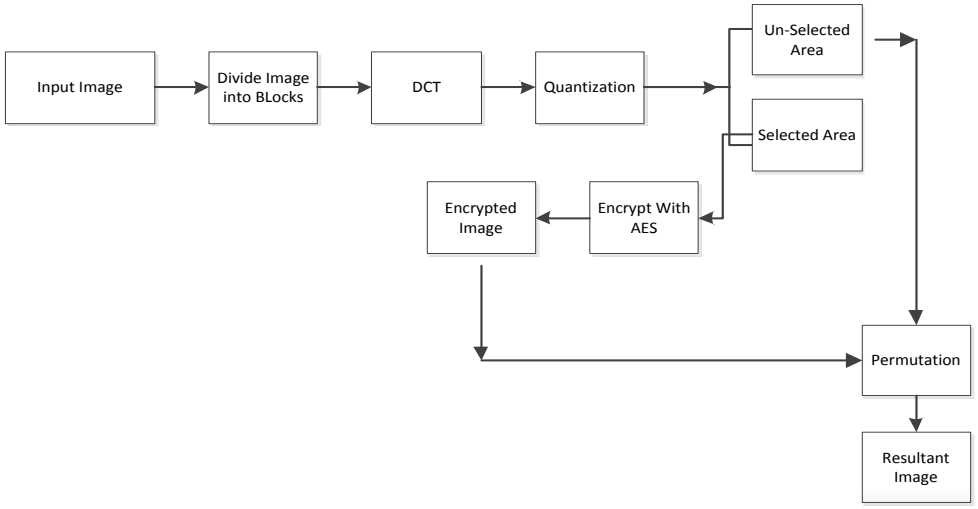


Figure 3.13 Design of proposed encryption scheme

3.4 Encryption Algorithm:

The encryption is shown in the Fig. 2. First input an image and divide the image into different blocks of size 8 x 8. Perform discrete cosine transform (DCT) on the image that will convert image from spatial into frequency domain. The DCT is performed by subtracting $2^7 = 128$.

After performing DCT operation we obtain only AC and DC coefficients in the blocks. DC coefficient lies on the top left corner of the block that represents the DCT cosine wave. All other coefficients are the AC coefficients that will represent the spatial frequencies The AC coefficients are 63 in numbers and those AC coefficients that are near to the DC have low frequencies while those lying at the bottom right have very high frequencies. In order to locate the low frequency component on the top left and high frequency corner at the bottom right we apply DCT operation on the block. Human eye are very sensitive to low frequency so most of the low frequency information is preserved. After we apply DCT transformation on the block in order to convert an image from the spatial domain to frequency domain, we then apply another operation called quantization on 8 x 8 blocks in order to further reduce the size of the image. Quantization is done by dividing the block that contains DC and AC coefficients obtained after DCT transformation by a standard quantization matrix

The quantization matrix which is a standard matrix has high values at the bottom right side. It will compress high frequency coefficients. Reason for this is that human eye is very sensitive to low frequency components and less sensitive to high frequency components. So in quantization majority of the high frequency components are rounded to zero and discarded. The image size will be reduced but will also degrade a little the quality of the image which is a tradeoff between the image size and the image quality. After quantization majority of the AC coefficients are rounded to zero and discarded which certainly will reduce the image size.

After quantization encryption area is selected for encryption and after the area is selected, encryption algorithm AES is used.

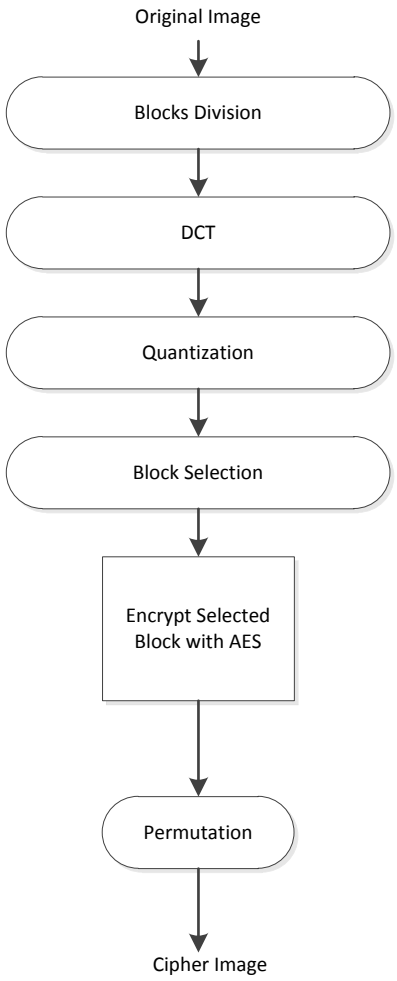


Figure 3.14 Proposed Schematic Algorithm.

3.5 Blocks Division:

The process of encryption starts with division of image into different blocks. In this encryption algorithm the image taken is divides into different blocks of size 8 x 8. The original number of rows and columns are recorded. We are interested in dividing the

image to block of size 8 x 8. Thus the number of total blocks depends on the input image. There is one problem that an Image cannot be directly divided into 8 x 8 if its dimensions are not multiple of 8.

For example if we have a 12 x 15 image then it can be exactly divided into 8 x 8 blocks, so for this purpose dimensions are made multiples of 8 by introducing extra number of rows or columns having zero values. For example in the image of size 12 x 15, four rows and 1 column is introduced in order to divide the image into 4 equal 8 x 8 blocks for further processing. The new dimensions of image are also recorded. For properly indexing the block, a new matrix can be created so that each block can be accessed individually using the new index.

3.6 Discrete Cosine Transform (DCT):

After the image is divided into different blocks, an operation called DCT is apply on the blocks in which the image will be converted from spatial into frequency domain which is discussed in the previous section.

After the image is divided into 8 x 8 blocks and DCT is performed on each block we will be left with 1DC coefficient and 63AC coefficients. In MATLAB the built-in function for DCT transformation is,

```
X = dct (A);
```

Where A is a row matrix. If it is an m x n matrix then DCT will apply on each column individually. Furthermore it works accurately on data type “double”.

As we have 8 x 8 blocks;

They are first converted into double “type”

Each block is converted into row matrix before applying DCT transformation

After applying DCT transformation, the result is reshaped back into 8 x 8 blocks.

Now the block matrix consists of DCT coefficients only. The first element is the DC component and rests are AC coefficients having magnitudes and both positive and negative values.

Further another operation will be performed called quantization on each block in order to further reduce the size of the Image.

3.7 Quantization:

After DCT transformation another operation called quantization is applied on the image that further reduce the size of the image by dividing the image obtained after DCT with a standard quantized matrix. In quantization high frequency coefficients will be discarded because human eye is very sensitive to lower frequency components and are less sensitive to high frequency coefficients. It will compress high frequency coefficients [9]. In this step there is a little degradation in the image quality after converting high frequency coefficients to zero and then discarded and this is a trade-off between the size of the image and the quality of the image.

3.8 Block Selection and Encryption:

In this section a new approach is introduced that will randomly select the area for encryption based on the coefficients percentage of the blocks. The algorithm for determining the percentage coefficient of each block is as,

1. Eliminate negative sign by taking absolute of the whole matrix (keep record of negative sign index)
2. Sum up coefficients of whole matrix which is actually 100% content.
3. Sum up coefficients of individuals blocks and convert it into percentage, this will give the percentage content of each block.
4. Find the block with the maximum percentage content.
5. Select a threshold value as referenced from the block with maximum content.

For example, maximum percentage content for some block is 1%. If threshold value is selected 20%, then block having percentage content from 0.8% - 1% will be selected for further processing and if the threshold value is selected to be 30%, then blocks having percentage content from 0.7% - 1% will be selected.

After selecting the threshold all blocks falling with in the criteria are selected and their index numbers are recorded. These selected blocks will be further processed for the process of encryption using AES algorithm.

Table 3.1 Blocks Division

1 2	9 3	8 6	7 9	6 3	1 2
1 7	7 9	5 9	4 8	6 8	7 6
2 5	1 6	3 7	1 1	2 3	5 4

In Table 5 a toy example is shown that shows block division of an image and the values in each block are the coefficients value of each pixel after converting it from spatial to the frequency domain.

Table 1.2 Number of blocks

Block 1	Block 2	Block 3
Block 4	Block 5	Block 6
Block 7	Block 8	Block 9

A selection criterion is that select block with maximum numbers.

Sum of all matrixes = 1 + 9 + 8 + 7 + 6 + 1 + …….. + 3 + 4 = 174.

174 are the 100% content of the image.

Now find sum of individual's blocks and find its percentage.

Sum block 1 = 1 + 9 + 2 + 3 = 15

Percentage of block 1 = (15/174) *100 = 8.62% content.

After finding percentage content of all blocks, we have

Table 3.3 Percentage Coefficients of Blocks

8.62%	17.24%	6.89%
13.79%	14.94%	15.51%
8.04%	6.89%	8.04%

All these percentage will sum up to 100%

Now find the block with maximum percentage content,

Block 2 having maximum percentage content i.e. 17.24%.

Select a threshold value with respect to the maximum percentage. In this paper 60% of the image is selected. This will give the threshold value.

Threshold value = (60/100) * 17.24 = 10.344

Subtract maximum percentage – threshold value

17.24-10.344 = 6.9%

Now select all blocks that have percentage content ≥ 6.9% and encrypt it with AES algorithm.

The AES function in MATLAB require,

1. An encryption key (16 Bytes)
2. 16 bytes data at a time for encryption
3. Value must be I n the range from 0 – 255
4. Negative values cannot be encrypted

The negative values have already been converted to positive values. The values are in the range from 0 – 255 so the matrix can be encrypted using AES. The data is encrypted using random key (16 Bytes). Each block is encrypted by taking 16 elements for encryption at a time.

Figure 3.15 Original Lena Image (MSE = 45.5038)

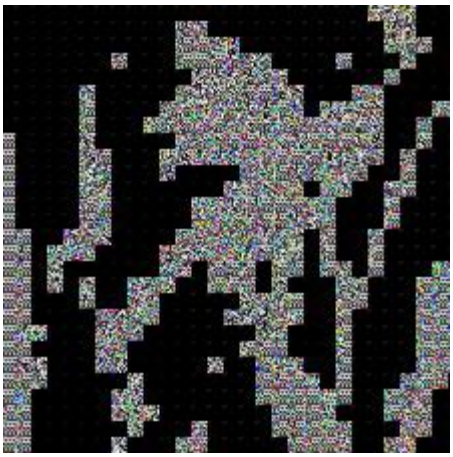


Figure 3.16 Encrypted Image (MSE=8736.6388, PSNR = 8.7174)

3.9 Permutation:

The image obtained after encrypting information content is permuted with the in-encrypted image that will shuffle the encrypted and un-encrypted bits to further enhance the image security. For permutation a randomly generated matrix will shuffle the image bits completely.

Consider a matrix of size n x n,

A = | 1 | 4 | 7 |
| --- | --- | --- |
| 2 | 5 | 8 |
| 3 | 6 | 9 |

=

10	11	12
13	14	15
16	17	18

A(1) = 10, A(2) = 13 and so on.

Another matrix that is randomly generated is,

B =

1	6	9
7	3	8
2	5	4

The statement becomes A(B) =A,

A

1	6	9
7	3	8
2	5	4

=A

1	4	7
2	5	8
3	6	9

Which means that A(1) = A(1), A(2) = A(7) and so on.

The shuffled matrix will be then

A =

10	17	18
12	16	15
13	14	11

Figure 3.17 Permuted Matrix

The original values for the image after permutation are shown in the Figure 3.19. Example of all the three layers of the first block are shown in the Figure 3.19 (a), 3.19 (b) and 3.19 (c).

	1	2	3	4	5	6	7	8
1	39	0	20	0	0	0	2	0
2	4	3	8	1	5	0	1	0
3	0	0	0	0	0	0	0	0
4	2	2	1	1	1	0	0	0
5	0	0	0	0	0	0	0	0
6	1	1	0	1	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	1	0	1	0	0	0	0

Figure 3.19 (a) Permuted Matrix layer 1

	1	2	3	4	5	6	7	8
1	43	0	22	0	0	0	2	0
2	3	3	9	1	6	0	1	0
3	1	0	0	0	0	0	0	0
4	2	3	1	1	1	0	0	0
5	0	0	0	0	0	0	0	0
6	1	2	0	1	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	1	0	2	0	1	0	0

Figure 3.19 (b) Permuted Matrix layer 2

	1	2	3	4	5	6	7	8
1	1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0

Figure 3.19 (c) Permuted Matrix layer 3

After permutation the resultant image is shown in the Figure 3.20.

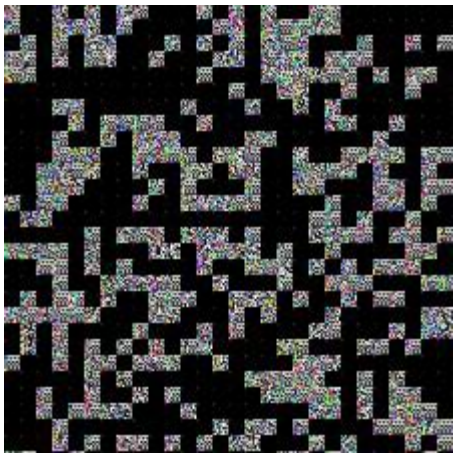


Figure 3.2018 Resultant Permuted Image (MSE= 8437.5269 PSNR = 8.8687)

Figure 3.19 Decrypted Image (MSE = 0.00090188 PSNR = 78.5793)

3.10 Decryption:

The decryption process is the same as the encryption process but in the reverse order. The same key will be used for decryption that was used in the encryption process and if there is a single bit changed in the decryption key then it will never give the original image.

First of all inverse permutation is used in order to decrypt the image. the permutation algorithm is known to the other side for decryption and if the permutation algorithm is

not used in the decryption that is used in the encryption then it will not give the desired output in the decryption process. After permutation the AES key that is used in the encryption will be used in the decryption. The encryption is already shared with the receiver for exact retrieval of the image. 128 bit AES key is used in the encryption / decryption. After applying the same key in the decryption that is used in the encryption resultant original image will be obtained.

If there is a single bit change in the decryption key then it will never give the desired output.

Figure 3.20 Original Image

In Figure 0.8, original image is shown. The image is encrypted using AES (16 bytes) key. After encryption we perform permutation in order to further shuffle the image and after permutation the result is shown in Figure 0.9

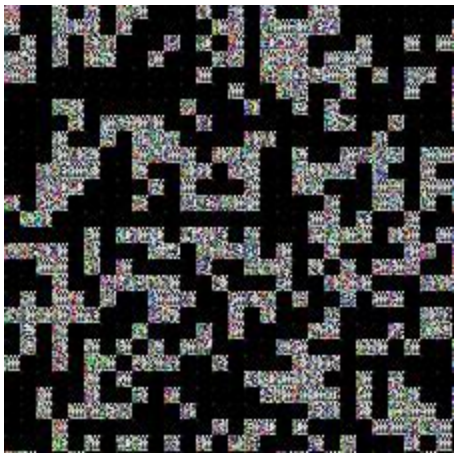


Figure 3.21 Encrypted Image

Figure 0.9 shows the original encrypted image. The Encrypted image is also processed for permutation and is send to the receiver for decryption.

Figure 3.22 Decrypted Image

In Figure 0.10 decrypted image is shown which is very different from the original image. This difference is because the original image is not decrypted using the same key that was used in the encryption process. If this key was used in the decryption process then it will give the same result that was required but this image is output of the image that was

decrypted using the original key with a single bit change. Last bit in the original key which is in hexadecimal form, is 5 and it is changed from 5 to 6 while the remaining bits remain the same with no single bit change and the result is very different as was desired.

3.11 Conclusion:

In this thesis selective image encryption is proposed based on a region that contains majority image information. A different approach is introduced for the selection of regions to be encrypted, the encryption algorithm AES is used in the encryption process. Permutation is applied to the encrypted image in order to further shuffle the encrypted image and increase one more level of security to the encrypted image. Different experiments were conducted on full images and selective image encryption which shows that algorithm proposed in thesis takes less encryption time than full image encryption and key sensitivity test in the next section shows that algorithm is secure against different attacks. Experiments were conducted on JPEG images using a new approach for the selection of area in the image. In Future the proposed encryption algorithm can be extended to medical and satellite images.

Chapter 4

Analysis of Proposed Selection Encryption Algorithm

4.1 Introduction:

In this chapter analysis of proposed encryption selective encryption algorithm is carried out in terms of time taken for encryption. A number of different experiments were conducted on different images both full images and selective images. Time taken by each experiment was recorded and compared which clearly shows the selection criteria and encryption process takes very less time in selective images as compared to full images. The proposed selective encryption algorithm takes very less time than full encryption algorithm and show a very good encryption result that cannot provide any meaningful information to the attacker.

4.2 Full Image Encryption:

In the Figure 4.1 Lena image is input for the process of full encryption.

Figure 4.1 Original Image

The histogram for original image is shown in the Figure 4.2.

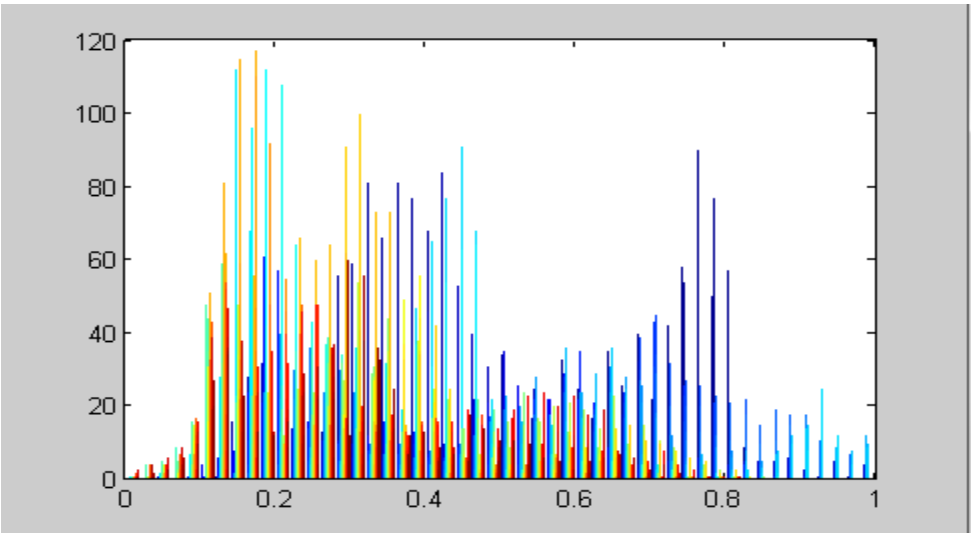


Figure 4.2. Original Image Histogram

Image is passed through a process of DCT transformation and the resultant image after DCT transformation and quantization is shown in the Figure 4.3 along with their histograms in the Figure 4.4.

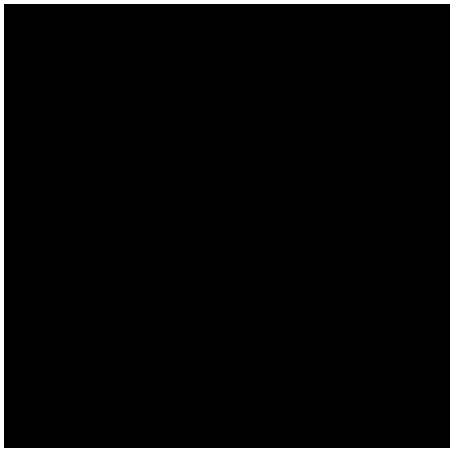


Figure 4.3 Resultant Image after DCT

During DCT transformation step image is converted from spatial to frequency domain and its mean square error is 45.5038 and its peak signal-to-noise ratio is 31.5503 which shows that image after DCT transformation is very similar to the original image

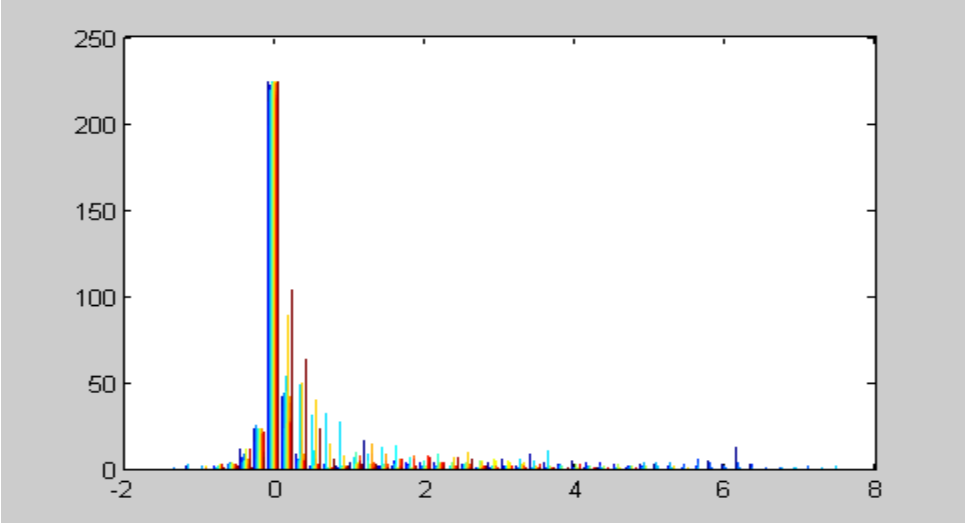


Figure 4.4 Histogram after DCT

In the Figure 4.5 resultant image after quantization is shown along with its histogram in the Figure 4.6, where an image size is further reduced by discarding the high frequency coefficients because human eye is very sensitive to lower frequency components but less sensitive to high frequency components. That is why in quantization high frequency components are converted to zero values by dividing the resultant image after DCT transformation using a standard quantized matrix.

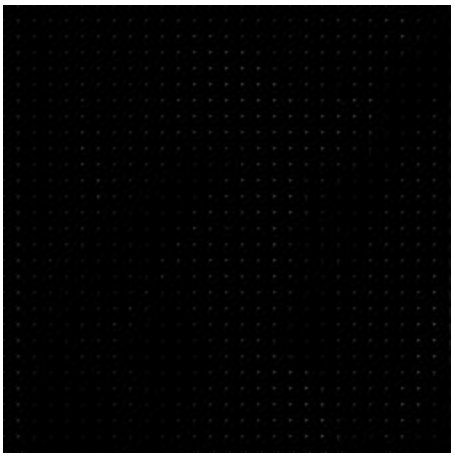


Figure 4.523 Resultant Image after quantization

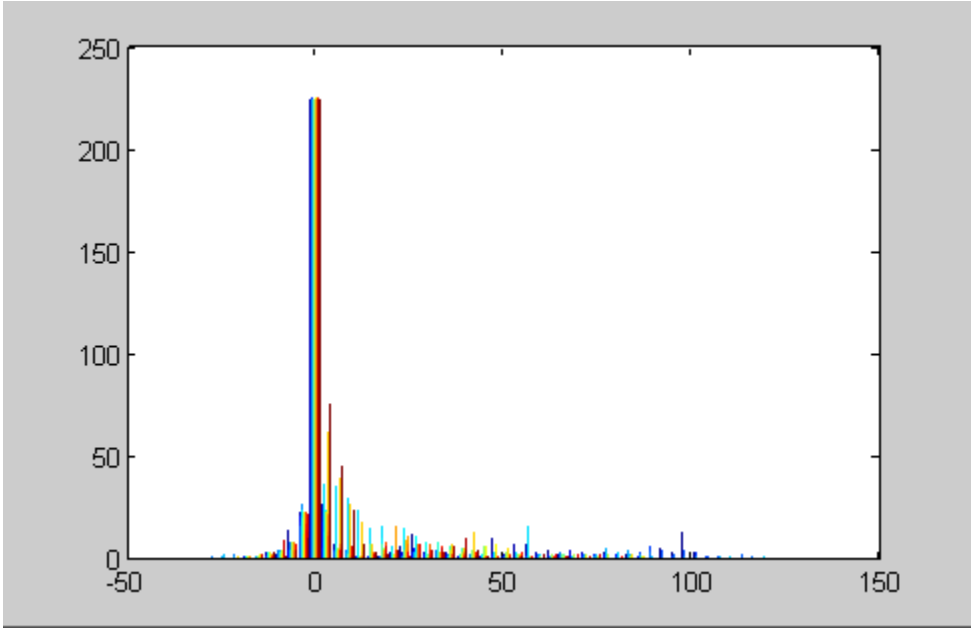


Figure 4.6 Histogram after quantization

In the Figure 4.7 full image encryption is shown. The total time taken to encrypt the image using AES key (16 bytes) is shown in the Table 8. The mean square error (MSE)

is 23162.0875 and the PSNR value is 4.483 which is very small value and shows that encrypted image is very different from the original image

Total Time taken is 8.5539 Seconds in encrypting full image using AES algorithm.

Figure 4.24 Full Image Encryption

In the Figure 4.8 histogram of the encrypted image is shown which clearly says that the histogram is a uniform one and is very different from the histogram of that of original image.

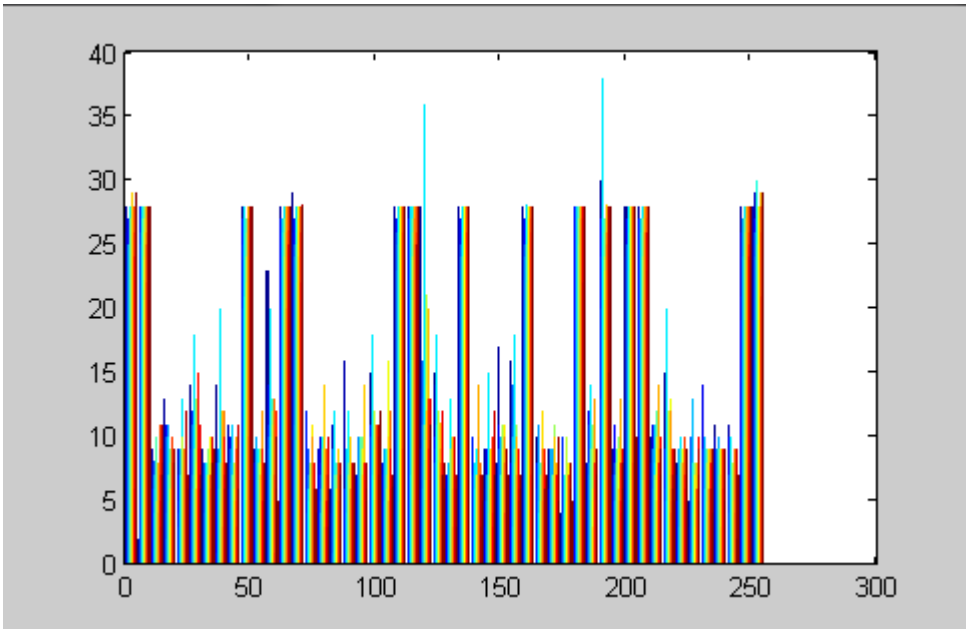


Figure 4.8 Histogram of encrypted image

In Figure 4.9 the permutation is shown that further increase the security level of the algorithm.

Figure 4.925 Permuted image

4.3 Selective Image Encryption:

In this section the proposed selective image encryption algorithm is applied to a number of different images to analyze the effect. Several experiments were conducted on different images and major findings achieved are highlighted. The security and efficiency parameters are highlighted in comparison with the full images encryption in this proposed encryption algorithm.

Figure 4.1026 Original Image

Original lena image is taken as input for the process of encryption. Total number of 841 blocks generated for processing. The histogram of original image is shown in the Figure 4.11.

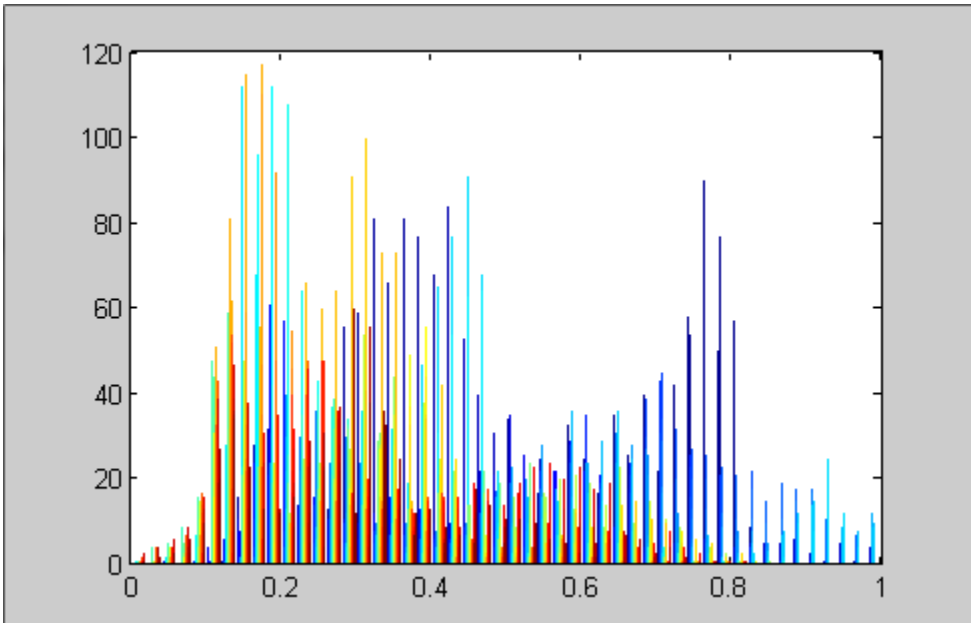


Figure 4.11 Original Image Histogram

After the image is taken as input an operation DCT is performed on the image in order to convert image from the spatial to the frequency domain. Figure 0.12 shows the resultant image after DCT transformation and Figure 0.13 shows the histogram of the DCT transformed image. After DCT transformation quantization is apply to the image that will reduce further the size of the image.

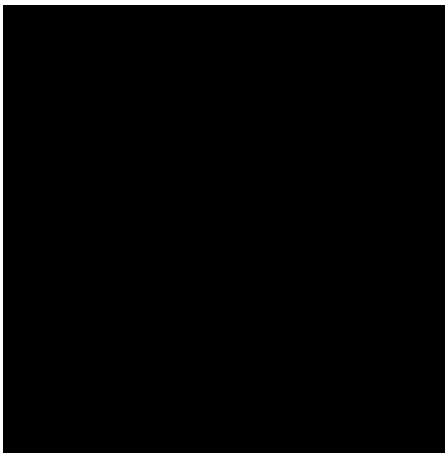


Figure 4.12 DCT transformed Image

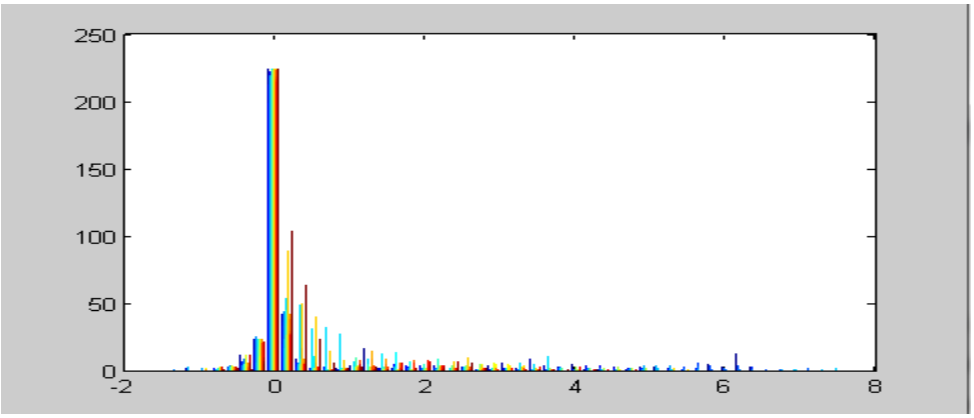


Figure 4.13 Histogram of DCT transformed Image

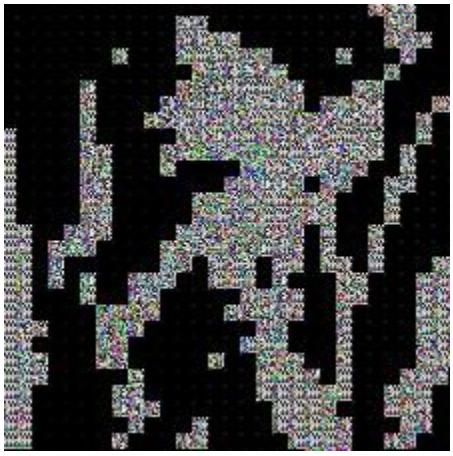


Figure 4.14 Selective Image Encryption

Figure 0.14 shows the resultant encrypted image which takes 3.6 second in the encryption which is very small time as compared to the total time taken by the full image encryption. The MSE and PSNR values show that the encrypted image is very different from the original image. In the Figure 0.15 the histogram of the encrypted image is shown.

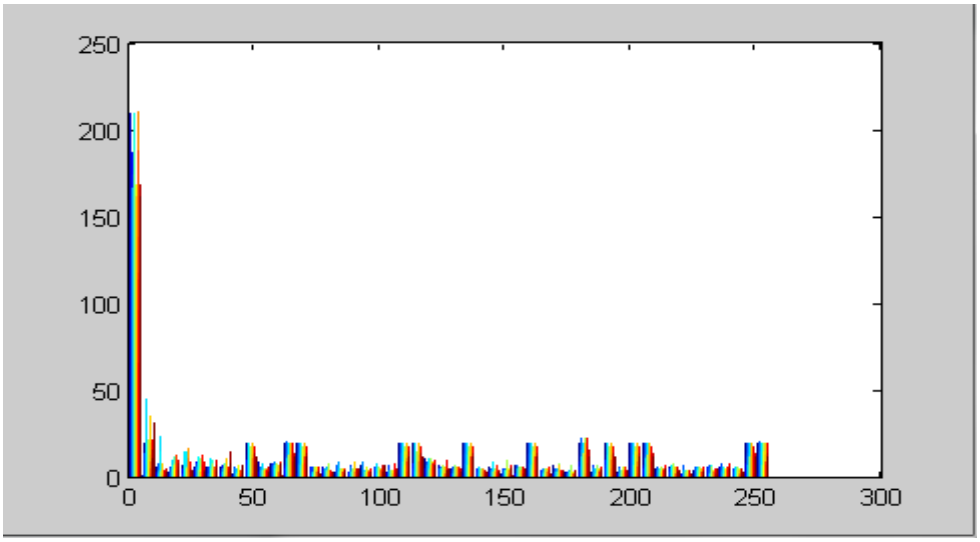


Figure 4.15 Histogram of Encrypted Image

The histogram shows the uniform nature of the image and also clearly shows that the encrypted image histogram is very different from the histogram of the original image. In the Figure 0.16 the final permuted image is shown which is further shuffled by the permutation algorithm to enhance the security of the image.

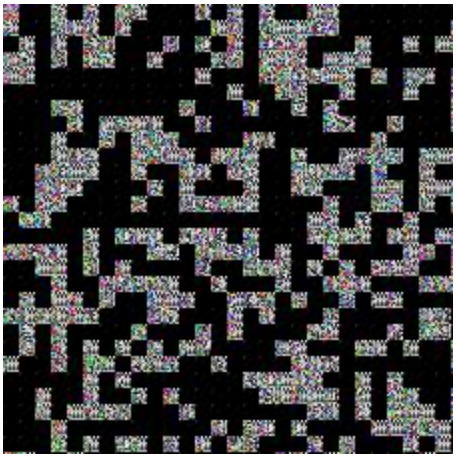


Figure 4.16 Permuted Image

Experiments were conducted on both full image encryption and selective image encryption and results of time taken are shown in Table 5.1 for both full image and selective image encryption. Some other experimental results of image is shown in the Figure 4.17.

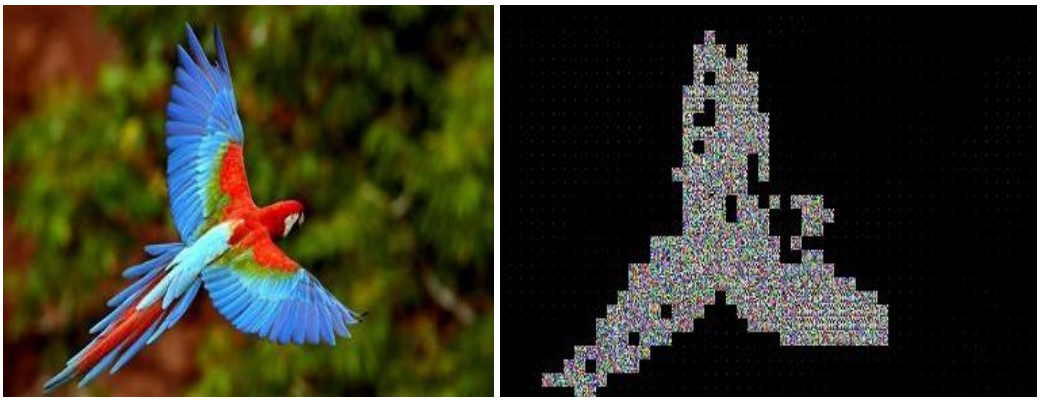


Figure 4.17 (a) Original Image (b) Encrypted Image

(c) Permuted Image (d) Decrypted Image

In the Figure 4.17 a colored parrot image is taken as input and it encrypt all the colored body part of image leaving the background unencrypted. Total time taken was very less as compared to the full image encryption. Total of 1450 blocks only 271 blocks were selected for encryption without compromising the security of the image.

Similarly an example of gray color image is selected and the result is shown in the Figure 0.18. Total time taken is very small and out of about 625 blocks only 194 blocks are selected for the process of encryption without compromising the security of the image.

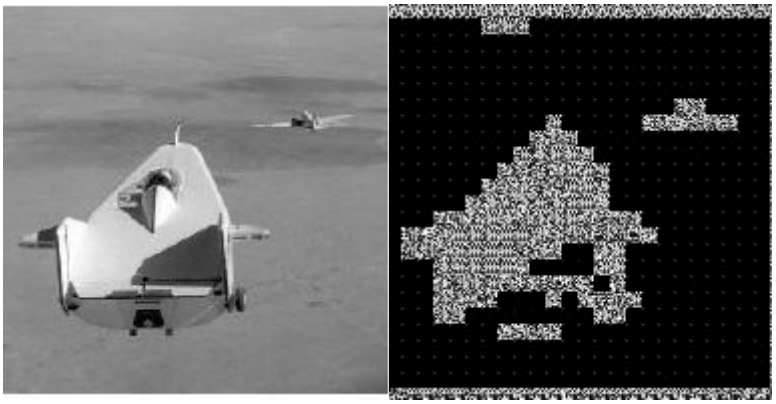
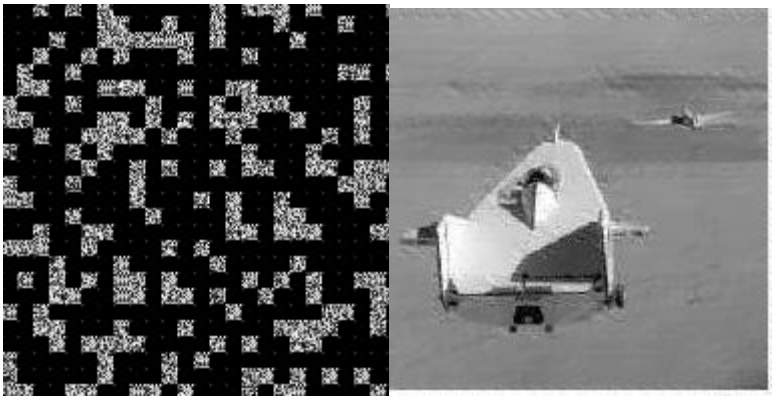


Figure 4.18 (a) Original image (b) Encrypted Image



(c) Permuted Image (d) Decrypted Image

The proposed encryption algorithm was applied to a number of different images and the resultant MSE and PSNR values calculated are shown in the Table. 4.1. The PSNR values for encrypted image is very different from the PSNR values of the original image showing the huge difference in between the original image and the encrypted image. the resultant MSE and PSNR values are shown in the Table 4.1.

Table. 4.1 Comparison of PSNR and MSE

Images	Proposed Selective Image Encryption		Proposed Selective Image Decryption	
	MSE	PSNR	MSE	PSNR
Lena	8814.3016	8.6789	0.00090188	78.5793
Bird	4021.5339	12.0869	0.00071114	79.6112
Flower	4660.987	11.446	0.0007197	79.5593
Skull	5885.2461	10.4332	0.00073378	79.4752
Gray Scale Image	6491.9496	10.0071	0.00075784	79..335

4.4 Time Analysis:

The proposed selective encryption scheme summarizes the different experimental results in Table 4.2 which shows total time taken in selecting sensitive area and encrypting the selected area with AES algorithm. The table also shows results of time taken for encrypting full image using AES encryption algorithm.

Table 4.2 Comparison of time (s) between full and selective image encryption.

Images	Full Image Encryption Time (Sec)	Proposed Selective Image Encryption Time (Sec)
Lena	8.5539	3.676021
Bird	14.6491	3.02769
Flower	12.1516	2.83967
Skull	8.5067	2.445685
Gray Scale image	6.3369	2.049593

The results in table 4.2 shows that proposed selective image encryption takes very less amount of time in both selecting and then encrypting the image, maintaining the security

of the transmitted image whereas, full image encryption takes more time as compared to the proposed selective image encryption algorithm.

The above results shows that proposed encryption algorithm is very efficient as compared to the full image encryption and the algorithm shows very good shuffling results ensuring the security of the images.

4.5 Future Work:

Selective image encryption in the recent research maintain the security of the transmitted image over an insecure network i.e. internet and save much time in both encrypting the image and decrypting the image because very less data is selected in encrypting the image as compared to the full images encryption. Considering these different features, selective image encryption provides a very good solution for transmitting multimedia images over the untrusted network and motivates research in this area. This research proposed region based encryption by encrypting certain blocks in the image based on the coefficients of the image information. The efficiency of the proposed encryption algorithm is proved in the results shown in table. 5.1, also the encryption of selected area and then permutation of selected and unselected area shows very good shuffling results ensuring the security of the proposed scheme.

This research work can be extended to different direction. The proposed algorithm can be used in encrypting the satellite images as satellite image information are very confidential information for military organization and need greater security when transmitted over the untrusted network during war, similarly this research can be extended to encrypt medical images because medical image information also needs greater security from transferring into unauthorized hands.

4.6 Conclusion:

This chapter presents an absolute overview of the results obtained during the course of this research work. The major findings achieved are highlighted. The security and efficiency parameters are highlighted in comparison with the full images encryption in this proposed encryption algorithm. In the end, a suggestion for continuing this research in future is presented. This chapter concludes the research.

BIBLIOGRAPHY

1. D. McGrew,M.Naslund, K.Norman, R.Blom,E.Carrara, and D.Oran “Secure Real time Transport Protocol ” Internet draft, 2001
2. H. Cheng and X. Li, “Partial Encryption of Compresed Images and Videos,” IEEE Transactions on Signal Processing, pp. 2439-2451.
3. M. Van Droogenbroeck and R. Benedett, “Techniques for a Selective Encryption of Uncompressed and Compressed Images,” Proceedings of Advanced Concepts for Intelligent Vision Systems (ACIVS) 2002, , September 9-11, 2002.
4. M. Podesser, H.-P. Shchmidt and A. Uhl, “Selective Bitplane Encryption for Secure Transmission of Image Data in Mobile Environments,” 5th Nordic Signal Processing Symposium, on board Hurtigruten, Norway, October 4-7, 2002
5. Panduranga H T, NaveenKumar S K, “Selective Image Encryption for Medical and Satellite Images”, “International Journal of Engineering and Technology (IJET), 5(1), 115 - 121” 2013.
6. Parameshachari B D, K M Sunjiv Soyjaudah, Chaitanyakumar M V, A Study on Different Techniques for Security of an Image, International Journal of Recent Technology and Engineering ™ (IJRTE), Volume- 1, Issue- 6,Jan 2013
7. Rodrigues, J.M. Puech, W. Bors, A.G. "Selective Encryption of Human Skin in JPEG Images", IEEE International Conference on Image Processing, 2006.
8. J.-M. Rodrigues, W. Puech, and A.G. Bors, “A Selective Encryption for Heterogenous Color JPEG Images Based on VLC and AES Stream Cipher,” in CGIV’06, Leeds, UK, 2006.
9. The International Telegraph and Telephone Consultative Committee “JPEG Standard (JPEG ISO/IEC 10918-1 ITU-T Recommendation T.81)” at http://www.w3.org/Graphics/JPEG/itu-t81.pdf

10. D. Taubman and M. Marcellin “JPEG2000: Image Compression Fundamentals, Standards and Practice” Page 200-246 Springer 2002.
11. J.Miano “Compressed Image File Formats: JPEG, PNG, GIF, Xbm, BMP” Chapter 9 Page 105-107 Addison-Wesley 1999
12. K.Sayood “Loss Compression Handbook” Chapter 18 Page 351-356 Academic Press 2003
13. B. Furht and, D. Kirovski “Multimedia Encryption And Authentication Techniques And Applications” Chapter 4 page 139-140 CRC Press 2006
14. G.Casella and E.L. Lehmann, "Theory of Point Estimation". Springer, (1999) Page 1 – 4
15. B Furht, D Socek and, AM Eskicioglu “Fundamentals of Multimedia Encryption Techniques” Multimedia Security Handbook, B. Furht and D. Kirovski, Eds. CRC Press, LLC, 2004, ch. 3, pp. 93 131.
16. H.Dobbertin, V.Rijmen and A.Sowa “Advanced Encryption Standard - AES: 4th International Conference, AES 2004” Page 34-96 Springer 2005
17. lC. Yen and lI. Guo, "The Design andRealization of a Chaotic Neural Signal Security System", Pattern Recognition and Image Analysis, 2002,Vol.12,No.1,pp.70-79.
18. F.Han, X.Yu, S.Han, “Improved Baker Map for Image encryption”, Proceeding of the first international symposium on systems and controls,Aerospace,2006,pp1273-76
19. P. Xu; J. Zhao; D. Wang; , "A selective image encryption algorithm based on hyper-chaos," Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on , pp.376-379, 27-29 May 2011.
20. Li, C. (2008) ‘On the security of some multimedia encryption schemes’, Doctoral Thesis, City university of Hong Kong

21. T. Xiang, K. wo Wong, X. Liao, Selective image encryption using a spatiotemporal chaotic system, Chaos: An Interdisciplinary Journal of Nonlinear Science 17 (2) (2007) 023115. (Pubitemid 46001017)
22. A. Massoudi, F. Lefebvre, C. De Vleeschouwer, and F. O. Devaux, "Secure and low cost selective encryption for JPEG2000," Multimedia, ISM, vol. 10, pp. 31-38, 2008
23. Lala Krikor, Sami Baba, Thawar Arif, Zyad Shaaban, "Image Encryption Using DCT and Stream Cipher", European Journal of Scientific Research, Vol.32, No.1, pp.47-57, 2009.
24. Fonteneau C., Motsch J., Babel M., and D´eforges O., "a hierarchical selective encryption technique in a scalable image codec", International Conference in Commun-ications, Bucharest, Romania 2008.
25. W. Puech and J. Rodrigues, "Crypto-compression of medical images by selective encryption of DCT", 13th European Signal Processing Conference, Turkey, September 2005.
26. C. Coconu, V. Stoica, F. Ionescu, and D. Profeta, "Distributed implementation of discrete cosine transform algorithm on a network of workstations", Proceedings of the International Workshop Trends & Recent Achievements in IT, Romania, pp. 116-121, May 2002.
27. JPEG, www.jpeg.org .
28. Howard Chi Ho Cheng. Partial encryption for image and video communication. Master thesis, Department of Computing Science, University of Alberta, Edmonton, Alberta, Canada, Fall 1998.
29. Nikolaos G. Bourbakis and Chris Alexopoulos. Picture data encryption using SCAN patterns. Pattern Recognition, 25(6):567–581, 1992.

30. Henry Key-Chang Chang and Jiang-Long Liu. A linear quadtree compression scheme for image encryption. Signal Processing: Image Communication, 10(4):279–290, 1997.
31. N. Bourbakis and C. Alexopoulos. Picture data encryption using scan patterns. Pattern Recognition, 25(6):567–581, 1992.
32. Chris Alexopoulos, Nikolaos G. Bourbakis, and N. Ioannou. Image encryption method using a class of fractals. J. Electronic Imaging, 4(3):251–259, 1995.
33. Kuo-Liang Chung and Lung-Chun Chang. Large encrypting binary images with higher security. Pattern Recognition Letters, 19(5-6):461–468, 1998.
34. Suchindran S. Maniccam and Nikolaos G. Bourbakis. Image and video encryption using SCAN patterns. Pattern Recognition, 37(4):725–737, 2004.
35. Dongxu Qi, Jiancheng Zou, and Xiaoyou Han. A new class of scrambling transformation and its application in the image information covering. Science in China - Series E (English Edition), 43(3):304–312, 2000.
36. Kenji Yano and Kiyoshi Tanaka. Image encryption scheme based on a truncated Baker transformation. IEICE Trans. Fundamentals, E85-A(9):2025– 2035, 2002.
37. Xiao-Yu Zhao and Gang Chen. Ergodic matrix in image encryption. In Proc. Second International Conference on Image and Graphics, Proc. SPIE, vol. 4875, pages 394–401, 2002.
38. Josef Scharinger. Fast encryption of image data using chaotic Kolmogorov flows. J. Electronic,Imaging,7(2):318–325,1998
39. G. Chen, Y. Mao, and C.K. Chui, “A symmetric image encryption based on 3D chaotic map,” Chaos Solitons Fractals 21, 2004, pp. 749-761.
40. F. Pichler and J. Scharinger, “Ciphering by Bernoulli shifts in finite Abelian groups,” in Contributions to General Algerbra: Proc. Linz- Conf., 1996, pp. 465-476.

41. F. Pichler and J. Scharinger, “Fast encryption of image data using chaotic Kolmogrov flows,” J. Elect. Imag. 7, 1998, pp. 318-325.
42. V. Patidar, N.K. Pareek and K.K. Sud, “A new substitution diffusion based image cipher using chaotic standard and logistic maps,” Commun Nonlinear Sci Numer Simulat 14, 2009, pp. 3056–307.
43. M. Sabery. K, and M. Yaghoobi, “A New Approach for Image Encryption using Chaotic Logistic Map,” icacte, International Conference on Advanced Computer Theory and Engineering, 2008, pp.585-590.
44. Tao, X., Liao, X.F. and Tang, G.P., “A novel block cryptosystem based on iterating a chaotic map,” Phys. Lett. A. v349, 2006, pp. 109-115.
45. A. Pande, P. Mohapatra, and J. Zambreno, “Using chaotic maps for encrypting image and video content,” in IEEE International Symposium on Multimedia (ISM) , dec. 2011, pp. 171–178.
46. Jakimoski, G. and L. Kocarev. 2001. ―Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps‖. IEEE Transactions on Circuits and Systems—I: Fundamental Theory and Applications. 48(2): 163-169.
47. Y.B. Mao, G. Chen, S.G. Lian, ―A novel fast image Encryption scheme based on the 3D chaotic baker map,‖ Int. J. Bifurcate Chaos, vol. 14, pp. 3613–3624, 2004.
48. H. Gao, Y. Zhang, S. Liang, and D. Li, ―A new chaotic algorithm for image encryption,‖ Chaos, Solutions &Fractals, vol. 29, no. 2, pp. 393–399, 2006.
49. N. K. Pareek, Patidar, and K. K. Sudd, An Image Encryption Using Chaotic Logestic Maps, Image and Vision Computing 24, 926-934, 2006
50. W. Zeng, H. Yu, and C.-Y. Lin, Eds., “Multimedia Security Technologies for Digital Rights Management” Academic Press, 2006
51. J.Gibson, “Digital Compression for Multimedia : Principles and Standards” Morgan Kaufmann, Chapter 9.5, page 300-304, 1998
52. B. Macq and J. Quisquater, “Cryptology for Digital TV broadcasting” Proceedings of the IEEE, 83(6)944–957, June 1995

53. A. Pommer and A. Uhl “Selective encryption of wavelet-packet encoded image data efficiency and security”
54. ACM Multimedia Systems (Special issue on Multimedia Security), 9(3)279–287, 2003
55. A. Uhl and A. Pommer. “Image and Video Encryption. From Digital Rights Management to Secured Personal Communication”, volume 15 of Advances in Information Security. Springer-Verlag, 2005.
56. M.Rabbani and P. Jones “Digital Image Compression Techniques” Page 114, SPIE Press 1991
57. I.Richardson “Video Codec Design: Developing Image and Video Compression Systems” Chapter 4 Page 49-57,JohnWiley and Sons 2002
58. W.Kou “Digital Image Compression: Algorithms and Standards” Chapter 5 Page 73, Springer 1995
59. J.Miano “Compressed Image File Formats: JPEG, PNG, GIF, Xbm, BMP” Chapter 9 Page 105-107 Addison-Wesley 1999
60. J.Daemen and V.Rijmen “The Design of Rijndael: AES--the Advanced Encryption Standard” Page2-221 Springer 2002
61. H.Dobbertin, V.Rijmen and A.Sowa “Advanced Encryption Standard - AES: 4th International Conference, AES2004” Page 34-96 Springer 2005
62. D. Taubman and M. Marcellin “JPEG2000: Image Compression Fundamentals, Standards and Practice” Page 200-246 Springer 2002
63. K.Sayood “Loss Compression Handbook” Chapter 18 Page 351-356 Academic Press 2003
64. B. Furht and, D. Kirovski “Multimedia Encryption And Authentication Techniques And Applications” Chapter4 page 139-140 CRC Press 2006
65. The International Telegraph and Telephone Consultative Committee “JPEG Standard (JPEG ISO/IEC 10918-1ITU-T Recommendation T.81)” at http://www.w3.org/Graphics/JPEG/itu-t81.pdf

66. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone “Handbook of Applied Cryptography” by CRC Press page 50-91
67. P. Rogaway and M. Bellare “Introduction to Modern Cryptography”US Deparpment of Commerce “Data Encryption Standard” page 7-20