An Investigation of the Use of MJEA in Image Encryption

Jamal N. Bani Salameh
Computer Engineering Department
Mu'tah University
Mu'tah – Karak, P.O.Box (7)
Jordan
jbanisal@mutah.edu.jo

Abstract:- In today's digital world, electronic communication means are susceptible to attacks and eavesdropping, where security problems such as modification and forgery have reached critical extents. Encryption has been used for securing data communication and it is considered as one of the best tools to help people to protect their sensitive information from cryptanalysts when it is stored or transmitted via insecure communication channels. Most of the encryption algorithms available are generally used for text data and not suitable for multimedia data. Multimedia data contains different types of data that includes text, audio, video, graphic, and images. With the increasing use of multimedia data over the Internet, here comes a demand of securing multimedia data. The main goal of this work is to investigate the use of our encryption algorithm (MJEA) to be a new approach for image encryption. MJEA will try to dissipate the high correlation among pixels and increase the entropy value by dividing the image into blocks and shuffles their positions. In this research I am going to use the correlation, histograms and entropy to measure the security level of the encrypted images. Experimental results show the possibility of applying MJEA for digital image encryption. MJEA was able to achieve high embedding capacity and high quality of the encrypted image. A comparison has been conducted between MJEA and other block ciphers like RC5 and RC6 for encrypting Lena image by considering correlation coefficients. From the obtained results, I noticed that MJEA algorithm achieved minimum correlation coefficient and maximum encryption quality. A detailed description of the design process together with results and analyses are given to define the proposed technique precisely.

Key-words:- Image encryption, Image Correlation, Image Entropy, Information Security, Encryption Algorithm

1 Introduction

The huge growth of computer networks and the latest advances in digital technologies allowed not only information to be exchanged through the Internet but also large files, such as digital images.

The Internet and other electronic communication means are susceptible to attacks and eavesdropping, make the security matters nowadays more important than before.

Information security plays an important role in telecommunication, storage of text, and multimedia data including images, audio and video. Classic methods of securing information mainly depend on cryptography. Cryptography is the science that studies the mathematical techniques for keeping message secure and free from attacks [1]. It encrypts plain text to generate cipher text. However, the transmission of cipher text may easily be intercepted, attacked or decrypted violently. Most of the encryption algorithms available are generally used for text data and not suitable for securing images and other multimedia data.

The primary intention of keeping images protected is to maintain confidentiality, integrity and authenticity [2]. Encryption is a common technique for image security. Generally, Encryption is a procedure that transforms an image into a cryptic image by using a key. Furthermore, a user can retrieve the initial image by applying a decryption method on the cipher image, which is usually a reverse execution of the encryption process [1].

Here, in this paper I am attempting to extend the use of our encryption algorithm MJEA (for Modified Jamal Encryption Algorithm) to be a new approach for image encryption [3]. It is expected that MJEA will produce imperceptible encrypted images; with high embedding capacity and high quality; that could be sent securely to the other party. MJEA is expected to dissipate the high correlation among pixels and increase the entropy value by dividing the image into blocks and shuffles their positions. In this work I am going to use the correlation, histograms and entropy to measure the security level of the encrypted images.

The rest of the paper is organized as follows: Section 2 gives a brief survey of image encryption techniques and gives an overview of MJEA. Section 3 describes in detail the proposed image encryption technique. Section 4 shows experimental results and discusses the efficiency of the proposed mechanism. Finally, section 5 provides some concluding remarks and future work.

2 Background

In this section I will give a brief survey about some image encryption techniques and an overview about the encryption algorithm (MJEA) that will be used in this research.

2.1 Survey about Image Encryption Techniques

Image encryption has a wide range of applications in various fields including internet communication, multimedia systems, medical imaging, Tele-medicine and military communication. The security of digital images has attracted more attention recently and it becomes an integral part of the image delivery process.

Many different encryption methods have been used to protect image data from unauthorized access like SCAN-based methods, chaos-based methods, tree structure-based methods, and other miscellaneous methods [4]. All of these techniques try to encrypt the original image by scrambling its contents. On the other hand, the receiver tries to decrypt the encrypted image in order to retrieve the original image.

Each type of images has its own characteristics include high correlation among pixels, bulk data capacity and high redundancy. Many encryption algorithms have been used for image encryption in the literature; no single algorithm satisfied different types of images. Most of these algorithms are designed for a specific image format compressed or uncompressed, and some of them are even format compliant. There are methods that offer light encryption (degradation), while others offer strong form of encryption. Some of the algorithms are scalable and have different modes ranging from degradation to strong encryption [5].

Zhi-Hong and Guanet al. [6] have presented a new image encryption scheme, in which shuffling the positions and changing the grey values of image pixels are combined to confuse the relationship between the cipher image and the plain image.

Ozturk I. and Sogukpinar I. [7] proposed new schemes which add compression capability to the mirror-like image encryption and visual cryptography algorithms. Jui-Cheng Yen and Jiun-In Guo [8] have proposed a new image encryption scheme based on a chaotic system. The chaotic image encryption algorithm is used for encryption of text and images. But this algorithm does not have any compression scheme and authenticity verification.

Sinha A. and Singh K. [9] proposed a technique to encrypt an image for secure transmission using the digital signature of the image. Digital signatures enable the recipient of a message to authenticate the sender of a message and verify that the message is intact. Droogenbroeck M.V. and Benedett R. [10] have proposed two methods for the encryption of an image; selective encryption and multiple selective encryption.

Shujun Li et al. [11] have pointed out that all permutation-only image ciphers were insecure against known/chosen-plaintext attacks. In conclusion, they suggested that secret permutations have to be combined with other encryption techniques to design highly secured images.

A.Mitra, Y.V. Subba Rao and S.R.M. Prasanna [12] have proposed a new random combinational image encryption approach using pixel and block permutations. The permutation of pixels and blocks are good at producing higher security level of the image compared to bit permutation. S.S.Maniccam and N.G. Bourbakis [13] have presented an image encryption using SCAN pattern. The image encryption is performing by SCAN based permutation of pixels and a substitution rule which together form an iterated product cipher.

Recently, however many new block ciphers have been proposed using chaotic maps and they achieve better security and performance: Alireza J. and Abdolrasoul M. [14] have proposed a new image encryption using Chaos and Block Cipher. Bhavana A., Himani A. and Monisha M. [15] have proposed an implementation of various cryptosystem using Chaos.

2.2 Overview about MJEA

This section gives a brief overview of MJEA block cipher. MJEA is symmetric encryption algorithm, which means that the same key is used for encryption and decryption. The data to be encrypted is divided into blocks of equal length. MJEA is an abbreviation for (Modified Jamal Encryption Algorithm). It is a novel block encryption algorithm proposed by Jamal Bani Salamehin [3]. It encrypts a 64-bit plaintext (Pt) to a 64-bit ciphertext (Ct) in 8 rounds for encryption or decryption process under the control of key (K) that has a size of 120-bit. The motivation for MJEA was to design a novel encryption algorithm that uses good features of JEA encryption algorithm [16], and try to correct the weakness in its performance.

The MJEA cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

In this Algorithm as shown in Fig. 1, a series of transformations have been used depending on S-BOX and XOR Gates. The cipher itself consists of the following: An initial permutation followed by 8 rounds of encryption, each round consisting of a key mixing operation, a pass through S-boxes and a linear transformation and the last step in this process is the final permutation.

MJEA satisfies the basic requirement of a good algorithm that each ciphertext bit depend upon all bits of the plaintext and all bits of the key, although the degree of dependence is uneven.

The design philosophy behind MJEA is that simplicity of design which yields an algorithm that is easier to implement, achieves a good Avalanche Effect as quickly as possible, achieves better security properties, and complete the encryption/decryption process with a high speed.

MJEA is proved to counter two types of attacks: a passive attack and active cryptanalysis directed to recovery of the current key (brute force attack). The security of this algorithm relies on the key and the S-box for thorough scrambling of the plaintext to produce the ciphertext.

A series of simulations were done to demonstrate the effectiveness of MJEA. The algorithm achieves its goals of thoroughly scrambling the plaintext with the key when run for at least four rounds. MJEA achieved a good Avalanche Effect when it is tested separately; on average more than 50% of bits were changed when I change a bit in the plaintext, key or the ciphertext. A comparison has been conducted between MJEA and different encryption algorithms. Simulation results clearly showed the superiority of MJEA when compared with (JEA, TEA and MTEA) encryption algorithms in terms of Avalanche Effect.

In the next section I will describe the proposed image encryption technique in more details.

3 Description of the Proposed Image Encryption Technique

Here in this section, I am proposing MJEA algorithm to be used for image encryption, and I am going to give a detailed description about the encryption and decryption process. MJEA is a symmetric block algorithm; it has a block size of 64 bits and 120-bit key. All operations in MJEA are XORed on 8-bit words. MJEA has been analyzed considerably as plain text encryption algorithm and I believe that its characteristics making it ideal to be used effectively for image encryption.

3.1 Encryption Process

Fig. 2 shows a block diagram of the proposed algorithm to perform the encryption process. The original image and the (120-bit) encryption key are the two main inputs of this algorithm. The original image data bit stream is divided into a number of 64-bit blocks. Those blocks are stored in a file to be used as input to the encryption algorithm (MJEA). Each block of the original image is encrypted separately; the 64-bit block of original image goes in one end of the algorithm, and then the algorithm runs to produce the 64-bit of ciphered image at the end.

As we see in Fig. 2; each 64-bit block of the original image is divided into eight 8-bit blocks. The algorithm operates on each of the eight bytes of the 64-bit word individually. These eight blocks become the input to the first round of the algorithm. MJEA performs the encryption process in 8 rounds under the control of the main key. Each round needs sixteen 8-bit subkeys. The subkeys generation process starts with the 120-bit main key (K); which is divided into two parts K_L and K_R. Furthermore, K_L is divided into seven 8-bit subkeys and K_R is divided into eight 8-bit subkeys. MJEA is based upon a basic function, which is iterated eight times. The first iteration (round) operates on eight input 8-bit blocks and the successive iterations also operate on the 8-bit blocks that come from the previous iteration. At each round, each byte of the original image is XORed with one or more of the other data bytes, and two 8-bit subkeys (one produced by $K_L$and the other produced by K_R). The result is then translated using a (256x8) bit substitution table (S-box). After the last iteration, a final transform step produces the 64-bit cipher image block.

The process of encryption is continued with other blocks of the original image from top to bottom. After I am done with encrypting all blocks of original image; the newly transformed image (ciphered image) is obtained by assembling all ciphered 64-bit blocks that goes out of the encryption algorithm (MJEA).

Note that the internal structure of MJEA takes care about the transformation process that refers to the operation of dividing and replacing an arrangement of the original image.

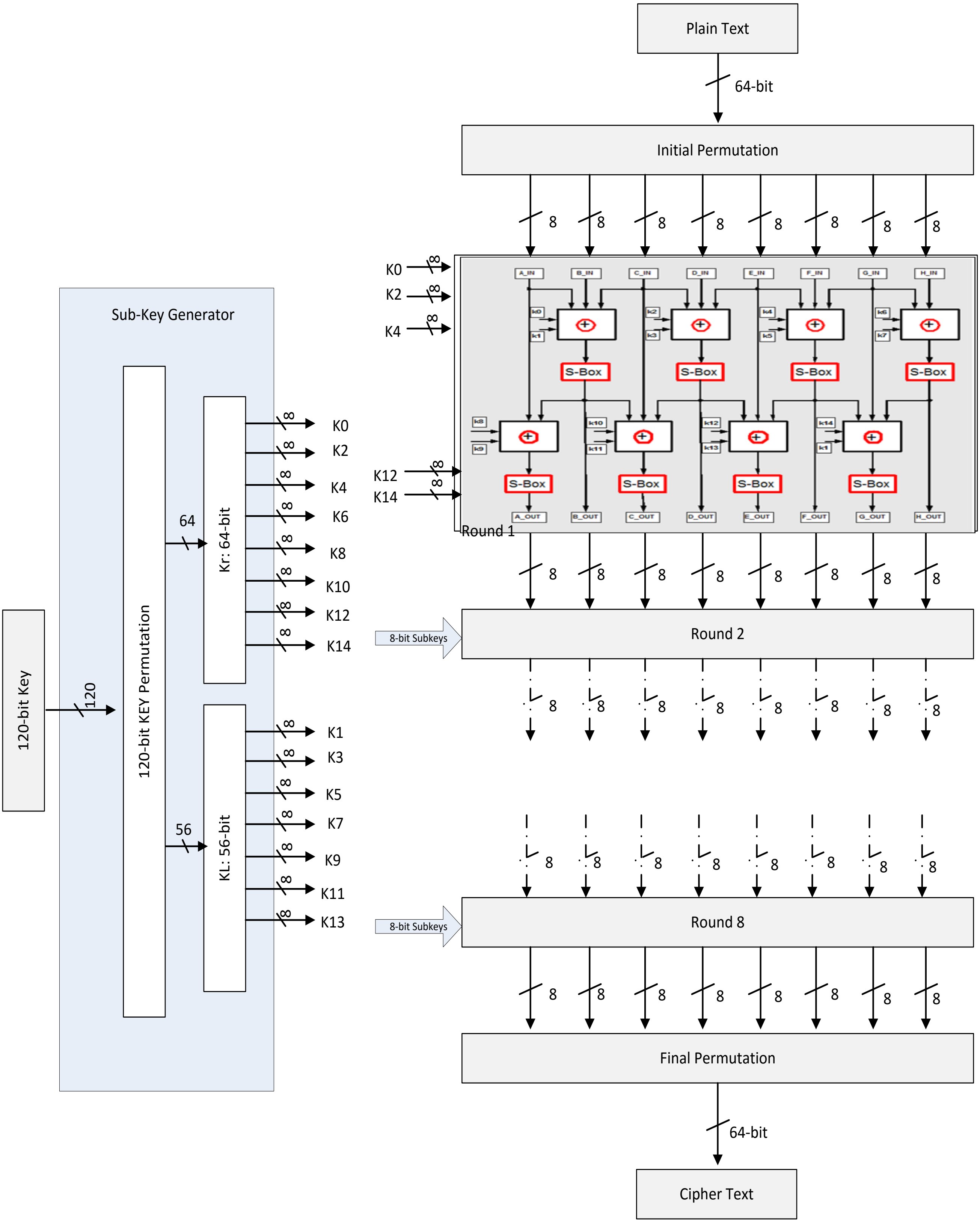


Figure 1: Block Diagram of MJEA

3.2 Decryption Process

Decryption process is different from encryption in that the inverse of the S-boxes must be used in the reverse order, as well as the inverse linear transformation and reverse order of the subkeys.

Decryption for MJEA is relatively straightforward beginning with the ciphered image as input. The encrypted image is divided into the same block length of MJEA algorithm from top to bottom.

The first block of the ciphered image is entered to the decryption function and the same 120-bit secret key is used as input to provide the algorithm with the same sub-keys as in the encoder side; the sub-keys are used in reverse order. Each block of ciphered image is decrypted separately; the 64-bit block of ciphered image goes in one end of the algorithm, and then the algorithm runs in the reverse direction, which reconfigures the 64-bit of deciphered image at the end. Note that the starting point in the key vectors must be pre-computed, based upon the number of rounds performed, and that the bytes are used in reverse order.

The process of decryption is continued with other blocks of the ciphered image from top to bottom. After I am done with decrypting all blocks of ciphered image; the original image is extracted by assembling all deciphered 64-bit blocks that goes out of the decryption algorithm (MJEA).

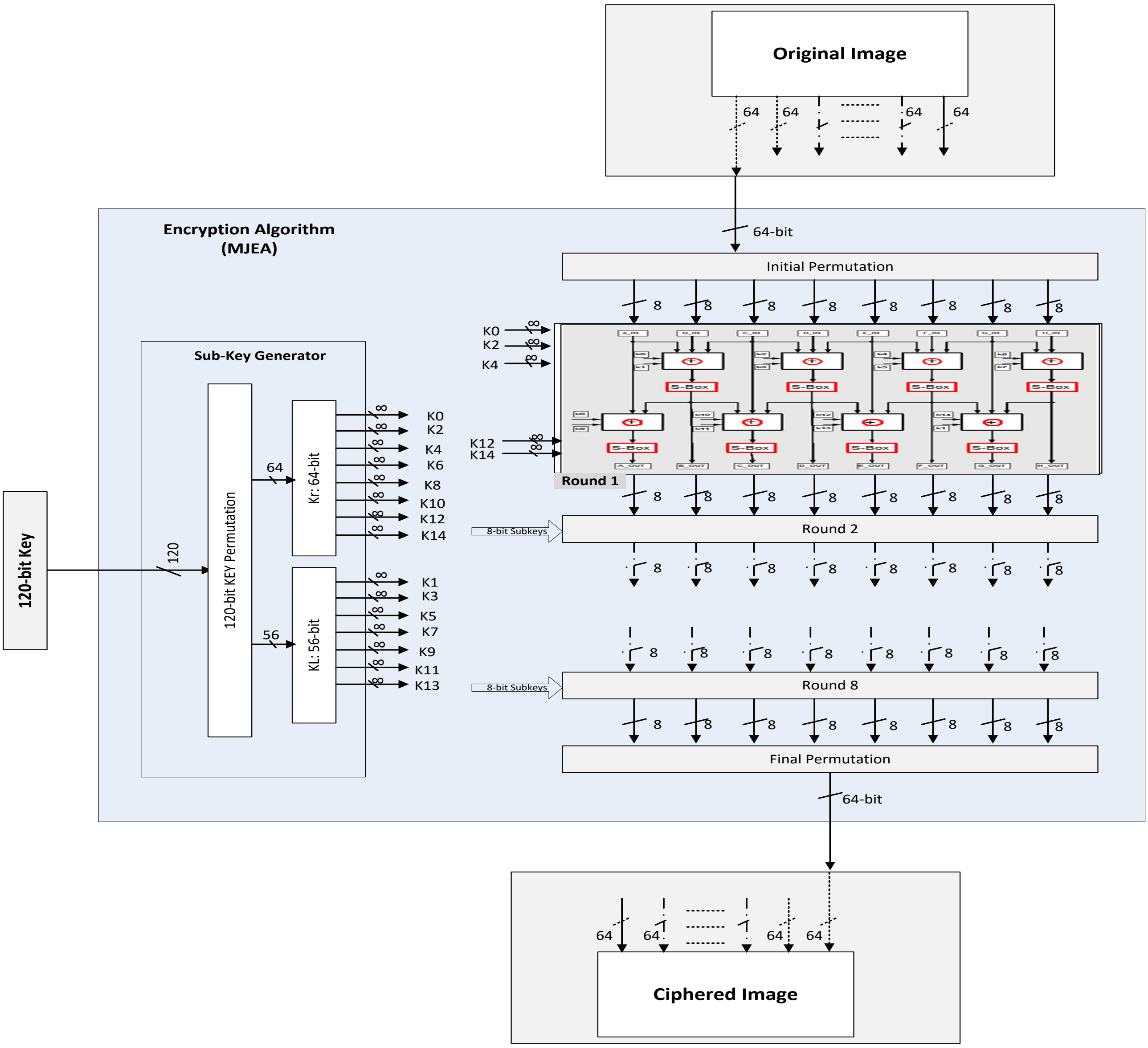


Figure 2: A block Diagram of the the Proposed Technique to Perform the Image Encryption Process.

4 Experimental Results

In this section; the performance of the proposed techniques will be evaluated by considering different metrics.

4.1 Visual Testing for the Use of MJEA for Image Encryption

Series of experiments were conducted to test the encryption/decryption quality of MJEA for application to digital images. I selected several grey-scale images having different contents. I made my tests using well-known images: Lena, Peppers, Cman, Baboon and Rose images each of size (512x512) pixels, as the original images and apply MJEA algorithm for encryption/decryption process.

Figs. 3-7 show results of applying MJEA to the original images in both encryption and decryption. Figs. 3a-7a show the original images that are considered to be input images for MJEA algorithm, then I run the encoder of MJEA to encrypt each one of those input images. The encrypted images are depicted in Figs. 3b-7b. As shown, the encrypted images (cipher images) regions are totally invisible. Afterthat I took the encrypted images to be the input for the decoder of MJEA in order to recover the original images out of the encrypted images. The decrypted images are shown in Figs. 3c-7c. Based on the results shown in Figs. 3-7:

- Clearly in all cases, there is no loss of image quality after performing the decryption step.
- The encrypted image is decrypted successfully and the decoder is able efficiently to recover the original image.
- There is no visual information observed in the encrypted image, and the encrypted images are visual indistinguishable even with a big difference with respect to the original images.

So, the visual inspection of Figs. 3-7 show the possibility of applying the proposed MJEA algorithm successfully in both encryption and decryption for digital images.

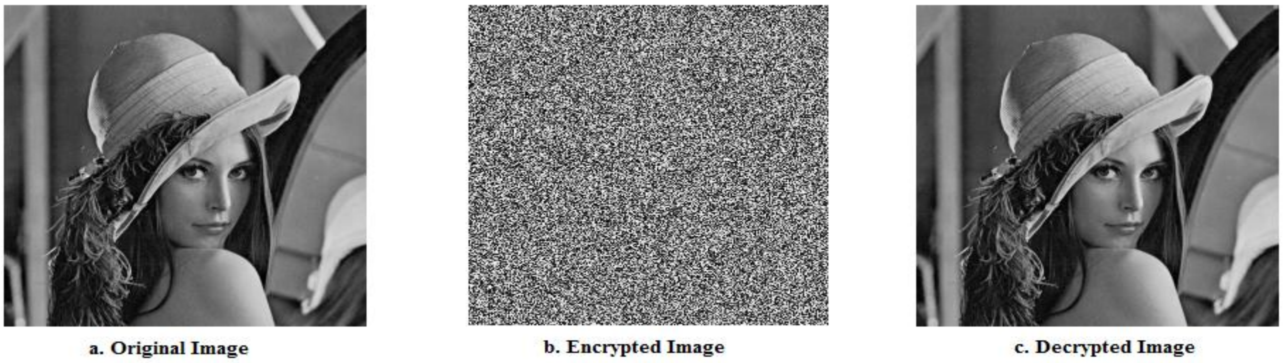

a. Original Image b. Encrypted Image c. Decrypted Image

Figure 3: Application of MJEA on Lena Image

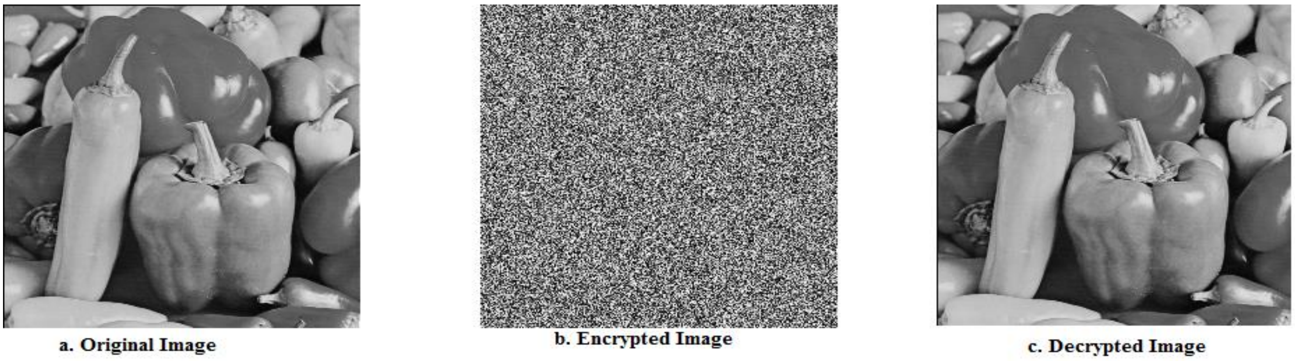
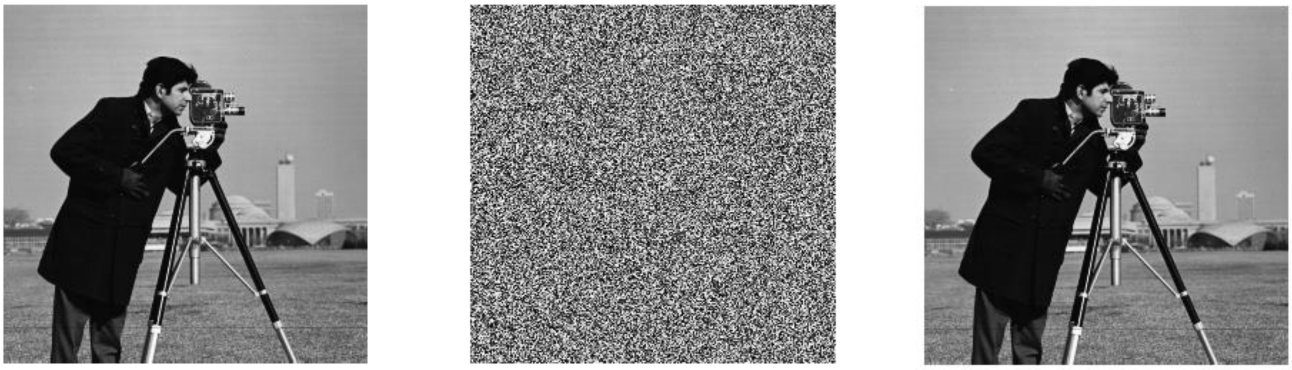
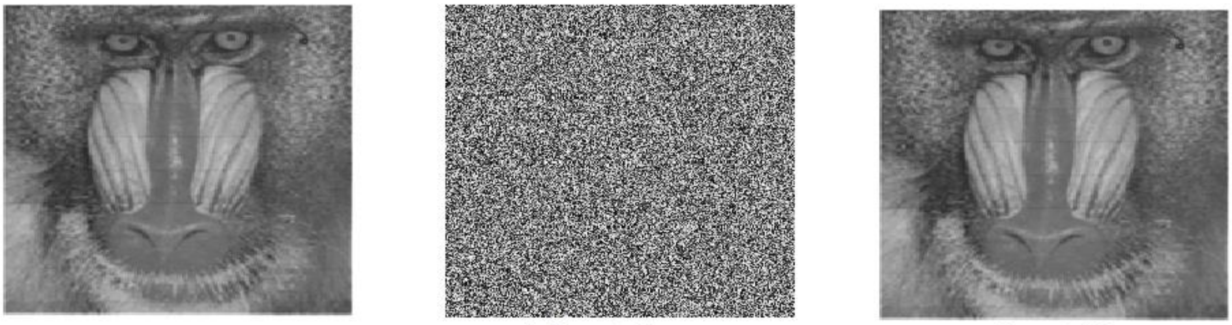

a. Original Image b. Encrypted Image c. Decrypted Image

Figure 4: Application of MJEA on Pepper Image



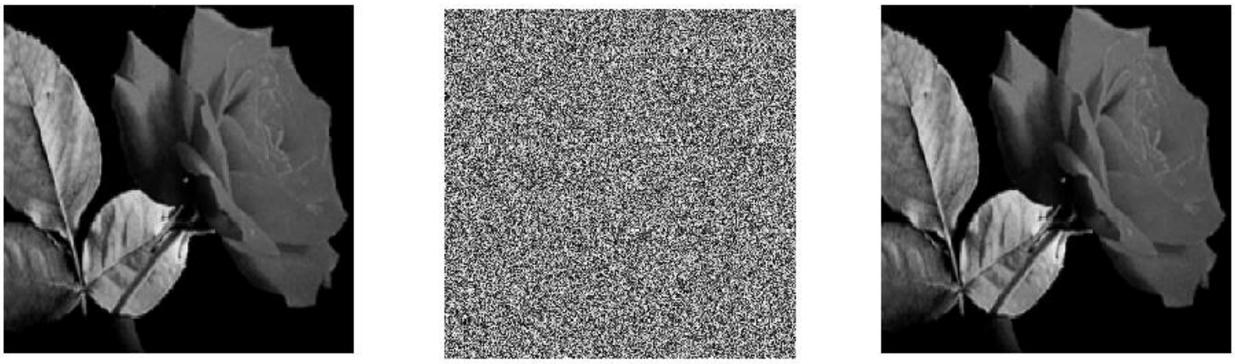
a. Original Image b. Encrypted Image c. Decrypted Image

Figure 5: Application of MJEA on Cman Image



a. Original Image b. Encrypted Image c. Decrypted Image

Figure 6: Application of MJEA on Baboon Image



a. Original Image b. Encrypted Image c. Decrypted Image

Figure 7: Application of MJEA on Rose Image

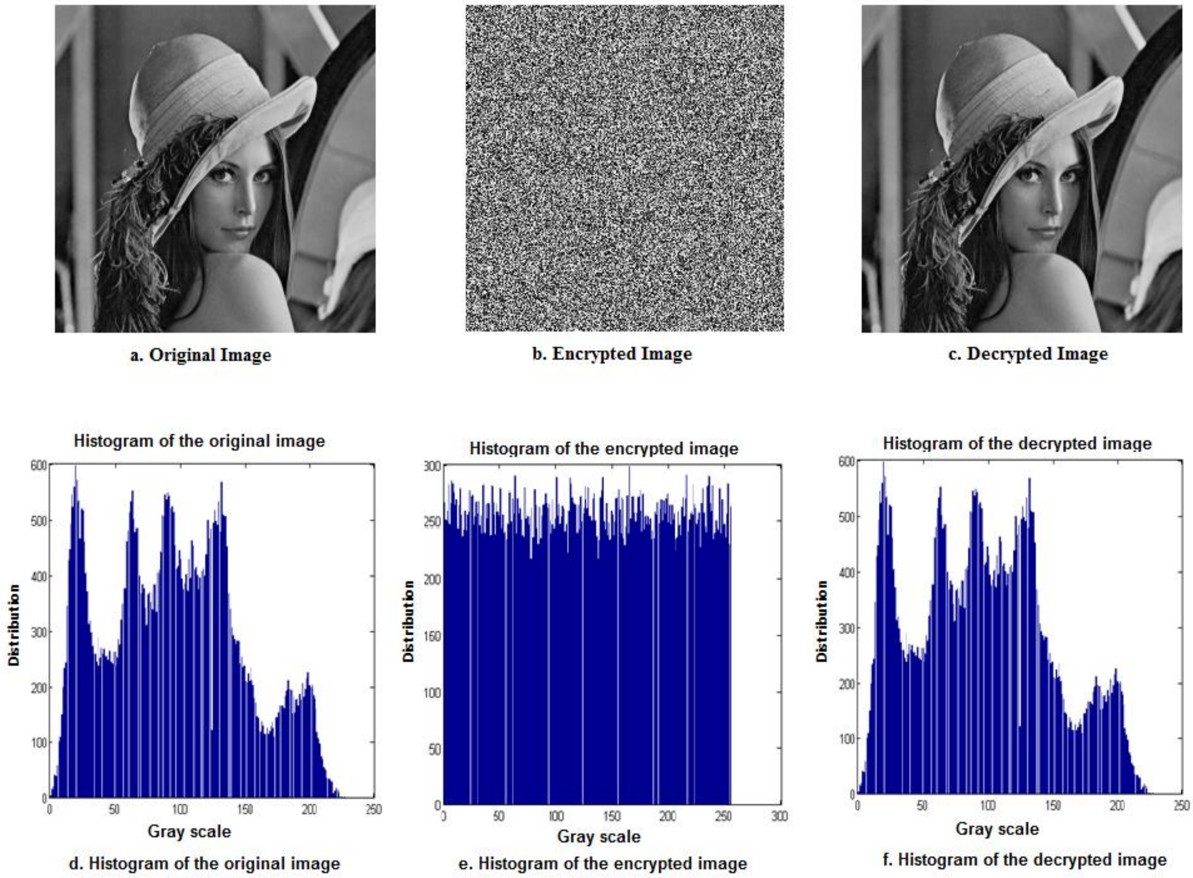
4.2 Image Security Parameters

Generally, a good encryption algorithm should qualify various security criteria and some of them will be tested over MJEA in this section:

4.2.1 Histogram Analysis

A good image encryption scheme should always generate a cipher image of uniform histogram for any original images. I calculated and analyzed the histograms of several encrypted images as well as its original images that have widely different content. One typical example among them is shown in Fig. 8. I selected the image of Lena (512 X 512 pixels), grey-scale image, and I calculated its histograms.

It is clear from Fig.8 that the decrypted image is same as the given input image, and the corresponding histograms are also same. Furthermore, it is clear from Fig. 8e that the histogram of the encrypted image is fairly uniform and significantly different from the respective histograms of the original image and the decrypted image. Histogram of the cipher image does not contain any statistical resemblance to the original image and hence does not provide any clue to employ any statistical attack on the proposed image encryption procedure. This is consistent with the perfect security defined by Shannon [17] and the proposed encryption scheme resists against the known-plaintext attack. The histogram uniformity in the results of the proposed algorithm ensures the success of the proposed method in achieving the required randomness.



a. Original Image

b. Encrypted Image

c. Decrypted Image

d. Histogram of the original image

e. Histogram of the encrypted image

f. Histogram of the decrypted image

Figure 8: Original/Encrypted Images and their Histograms

4.2.2 The Correlation Coefficient

A useful metric to assess the encryption quality of any encryption algorithm is the correlation coefficient between pixels at the same positions in the original and the cipher images.

Correlation is a measure of the relationship between two variables. If the two variables are the original image and cipher image, then they are in perfect correlation if they are highly dependent. In this case the cipher image is the same as the original image and the encryption process failed in hiding the details of the original image. If the correlation coefficient equals zero, then the original image and its cipher image are totally different. If the correlation coefficient equals -1, this means the cipher image is the negative of the original image. So, success of the encryption process means smaller values of the correlation coefficient.

For example, x_i and y_i are two pixel pair then the correlation coefficient can be calculated by the following equations [18]:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{1}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x_i))^2 \tag{2}$$

$$COV(x, y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x_i))(y_i - E(x_i)) \tag{3}$$

The Correlation Coefficient:

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{4}$$

$$r_{xy} = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{(\sum_{i=1}^{N}(x_i - E(x))^2)}\sqrt{(\sum_{i=1}^{N}(y_i - E(y))^2)}} \quad (5)$$

Where , x_i and y_i are gray level value of two adjacent pixels of the original image and cipher image, N is the number of pairs (x_i , y_i) and E(x) is the mean of x_i and E(y) is the mean of y_i .

The procedure to test the correlation between two vertically adjacent pixels, two horizontally adjacent pixels, and two diagonally adjacent pixels in original image/cipher image is as follows. First, randomly select 1000 pairs of two adjacent pixels from an image. Then, calculate their correlation coefficient. The encryption quality for MJEA block cipher algorithm is estimated using the correlation coefficient of two horizontally, two vertically and two diagonally adjacent pixels in the original image/cipher image with Lena image are illustrated in Table 1.

Fig. 9 shows Correlation Coefficients for Lena Image: (a) shows the correlation of two horizontal adjacent pixels of original image, (b) shows the correlation of two vertical adjacent pixels of original image, (c) shows the correlation of two diagonal adjacent pixels of original image, (d) shows the correlation of two horizontal adjacent pixels of encrypted image, (e) shows the correlation of two vertical adjacent pixels of encrypted image, and (f) shows the correlation of two diagonal adjacent pixels of encrypted image.

Table 1: Correlation Coefficients for Lena Image

Image name	Direction of adjacent pixels	Plain-image	Encrypted Image Using MJEA
Lena	Horizontal	0.984	0.0023
	Vertical	0.971	0.0022
	Diagonal	0.942	0.0018

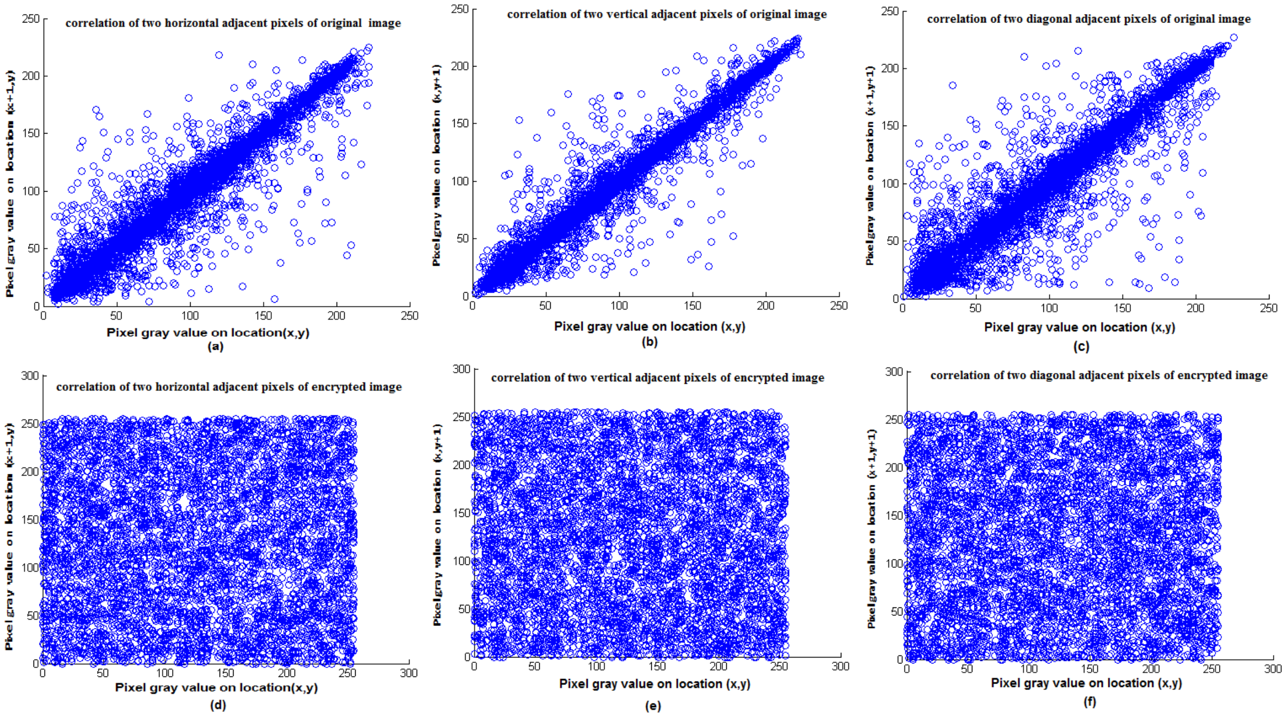


Figure 9: Correlation Coefficients for Lena Image

An encryption quality comparison has been conducted between the proposed algorithm and other block ciphers like RC5 and RC6. Table 2 shows the encryption quality Comparison of MJEA, RC5 and RC6 for Lena image using correlation coefficients.

From the obtained results, I can conclude that the MJEA algorithm obtained minimum correlation coefficient and maximum encryption quality with respect to RC5 and RC6.

Table 2: Comparison of MJEA, RC5 and RC6 for Lena Image using Correlation Coefficients

Image name	Direction of adjacent pixels	Plain-image	Encryption Algorithm		
			MJEA	RC5	RC6
Lena image	Horizontal	0.984	0.0023	0.0041	0.0038
	Vertical	0.971	0.0022	0.0034	0.0032
	Diagonal	0.942	0.0018	0.0028	0.0027

4.2.3 Key Space Analysis

A good encryption scheme should be sensitive to the secret keys, and the key space should be large enough to make brute force attacks infeasible. In our case; for MJEA; the key space size is 2^{120}. It is large enough to resist all type of brute force attacks. The MJEA encryption algorithm is analyzed thoroughly [3]. One of the tests that was made to check the average number of ciphertext bits changed for single-bit changes in the key. From a series of simulations, I found that the algorithm achieves its goal of thoroughly scrambling decrypted plaintext given a single-bit change in key; it needs at least 4-rounds to give a strong Avalanche Effect on the ciphertext (more than 50% of the ciphertext bits were changed).

The experimental results also demonstrate that MJEA is very sensitive to the secret key when it used for image encryption. Table 3 illustrates the sensitivity of MJEA to the secret key(ki) when encrypting Lena image using different keys.

Table 3: Correlation coefficients of two adjacent pixels in two images (Original image and the same image encrypted in different keys)

Correltion	Horizontal	Vertical
Original Image	0.94	0.97
Image encrypted by K1	0.002	0.007
Image encrypted by K2	0.012	0.011
Image encrypted by K3	0.044	0.048
Image encrypted by K4	0.033	0.037

As can be seen in the table, when the secret key is changed slightly, the correlation coefficients also changed which indicates that the encrypted image becomes absolutely different. The sensitivity to key which is the main characterization of MJEA algorithm guarantees the security of our scheme

4.2.4 Image Entropy

Entropy measures the uncertainty association with random variable. As for grayscale image in Block Based Image Encryption decreases the mutual information among encrypted image variables (i.e. high contrast) and thus increases the entropy value. A secure cryptosystem should fulfil a condition on the information entropy that is the ciphered image should not provide any information about the plain image. The information entropy is calculated using equation (6).

$$H_e = -\sum_{K=0}^{G-1} P(K).\log_2(P(K)) \qquad (6)$$

Where:
He: Entropy of image
G: Gray value of an input image (0-255)
P(k): Represents the probability of the occurrence of symbol *(k)*

Suppose that a random source emits symbols with equal probability, after evaluating Eq. 6, I obtained its entropy (*He= 8*), corresponding to a truly random source. Actually, given that a practical information source seldom generates random messages, in general its entropy value is smaller than the ideal one. However, when the messages are encrypted, their entropy should ideally be 8. If the output of such a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security.

For the entropy test, I select the image of Lena (512 X 512 pixels), grey-scale image to be tested by using MJEA. As I said before MJEA is a block encryption algorithm, it has a 64-bit block size; so the original image data bit stream is divided into (8192 - blocks) each block has 64-bit.

The entropy for ciphered images encrypted by using different encryption keys are calculated using Eq. 6 and are listed in Table 4. Even MJEA is very sensitive to the secret key; the information entropy obtained in all cases by using different keys is very close to the theoretical value of 8. This means that information leakage in the encryption process is negligible and the encryption system is secure against entropy attack.

Table 4: Entropy for Lina Image Encrypted in Different Keys

Encryption key	Entropy for encrypted image
K1	7.9974
K2	7.9972
K3	7.9970
K4	7.9972

5 Conclusions and Future Work

In this paper I investigated the use of MJEA for image encryption. A number of evaluation parameters proposed in the literature were systemically presented to form a frame work for evaluating our proposed image encryption algorithm.From the small series of simulations that was done in this work, several points could be concluded:

- Experimental results show the possibility of applying our encryption algorithm (MJEA) to digital images encryption; MJEA was able to achieve high embedding capacity and high quality of encoded image. It was able to replace and transform of all pixels in the original-image by the help of the (120-bit) secret key. As seen in decrypted images; there is no loss of the image quality after performing the decryption step. This means that the encrypted image is decrypted successfully and the decoder is able efficiently to recover the original image.
- I have calculated and analyzed the histograms of several encrypted images as well as its original images. By comparing the histograms together; I noticed that the probabilities of appearance of every gray level are equitably distributed and the histogram of the encrypted-image is flat. The histogram uniformity in the results ensures the success of the proposed algorithm preprocessing method in achieving the required randomness.
- A comparison has been conducted between MJEA and other block ciphers like RC5 and RC6 for encrypting Lena image by considering correlation coefficients. From the obtained results, I noticed that the MJEA algorithm obtained minimum correlation coefficient and maximum encryption quality with respect to RC5 and RC6. The disturbance of the strong correlation among the adjacent pixels assures high security of the images
- The entropy for ciphered images encrypted by using different encryption keys are calculated; I found that the information entropy obtained in all cases by using different keys is very close to the theoretical value of 8. This means that information leakage in the encryption process is negligible and the encryption system is secure against entropy attack.

Further work would include the following:

- More thorough testing and analysis to get better performance
- To extended the use of the proposed algorithm in trying to handle other image formats and sound data.
- Calculate the execution time for encryption and decryption for the proposed algorithm and compare it with other well-known algorithms.
- Design sophisticated software based on this technique which will target to use in highly secure multimedia data transmission applications.

References:

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Prentice Hall, 2013

[2] M. A. Bani Younes and A. Jantan, Image Encryption Using Block-Based Transformation Algorithm, *IAENG International Journal of Computer Science*, Vol. 35, No. 1. 2008

[3] J. N. Salameh, A New Symmetric-Key Block Ciphering Algorithm, *Middle-East J. Sci. Res.*, Vol. 12, No. 5, 2012, pp. 662-673.

[4] W. Lee, T. Chen and C. Chieh Lee, Improvement of an Encryption Scheme for Binary Images, *Pakistan Journal of Information and Technology*, Vol. 2, No. 2, 2003, pp. 191-200.

[5] S.S. Maniccam, N.G. Bourbakis, Image and Video Encryption using SCAN Patterns, *Journal of Pattern Recognition Society*, vol. 37, No. 4, 2004, pp.725–737.

[6] G. Zhi-Hong, H. Fangjun, and G.Wenjie, Chaos - Based Image Encryption Algorithm, *Elsevier*, 2005, pp. 153-157.

[7] I. Ozturk, I.Sogukpinar, Analysis and Comparison of Image Encryption Algorithm, *Journal of transactions on engineering, computing and technology*, Vol. 3, 2004, pp.38.

[8] Jui-Cheng Yen, Jiun-In Guo, A new Chaotic Image Encryption Algorithm, *IEEE Int. Conf. Circuits and Systems*, Vol. 4, 2000, pp. 49-52.

[9] A. Sinha, K. Singh, A technique for Image Encryption Using Digital Signature, *Source: Optics Communications*, Vol.218, No. 4, 2003, pp.229-234.

[10] M. V. Droogenbroech, R. Benedett, Techniques for A selective Encryption of Uncompressed and Compressed Images, *In ACIVS’02, Ghent, Belgium. Proceedings of*

Advanced Concepts for Intelligent Vision Systems, 2002.

[11] Li. Shujun, Li. Chengqing, C. Guanrong, Nikolaos, G. Bourbakis and Lo Kwok-Tung, A general Quantitative Cryptanalysis of Permutation-only Multimedia Ciphers Against Plaintext Attacks, *Signal Processing: Image Communication*, Elsevier, Vol. 23, No. 3, 2008, pp. 212-223.

[12] A. Mitra, Y V. Subba Rao, and S. R. M. Prasnna, A new Image Encryption Approach using Combinational Permutation Techniques, *Journal of computer Science*, Vol.1, No. 1, 2006, pp.127.

[13] S.S. Maniccam, N.G. Bourbakis, A Lossless Image Compression and Encryption using SCAN, *Pattern Recognition*, Vol. 34, 2001, pp. 1229-1245.

[14] A. Jolfaei , A. Mirghadri, Image Encryption Using Chaos and Block Cipher, *Computer and Information Science*, Vol. 4, No. 1, 2011

[15] B. Agrawal, H. Agrawal, and M. Mishra, Implementation of Various Cryptosystem Using Chaos, *Journal of Computer Engineering (IOSR-JCE)*, Volume 13, Issue 4, 2013, PP 77-84.

[16] J. N. Salameh, JEA-128: A novel Encryption Algorithm Using VHDL, *WSEAS Transactions on Computers*, Vol. 12, No. 8, 2009, pp. 1875-1885.

[17] C. E. Shannon, Communication theory of secrecy systems, *Bell Systems Technical Journal*, Vol. 28, 1940, pp. 656-715.

[18] K. Loukhaoukha, J. Chouinard and A. Berdai, A Secure Image Encryption Algorithm Based on Rubik's Cube Principle, *Journal of Electrical and Computer Engineering*, Vol. 2012 (2012), Article ID 173931, 2012, 13 pages.