International Journal of Energy, Information and Communications
Vol.8, Issue 2 (2017), pp.1-18
http://dx.doi.org/10.14257/ijeic.2017.8.2.01

Design and Analysis of a Robust Compression Friendly Image Encryption Scheme

Gulshan Saleem*, Nisar Ahmed[1] and Hassan Khalid[2]

*Department of Computer Engineering,
CEME, National University of Science and Technology, Islamabad, Pakistan
[1]Department of Computer Engineering,
University of Engineering and Technology, Lahore, Pakistan
[2]Department of Electrical Engineering
University of Engineering and Technology, Lahore, Pakistan
*Gulshan.saleem14@ce.ceme.edu.pk, [1]nisarahmedrana@yahoo.com,
[2]engr_hassan09@ymail.com

Abstract

Encryption is the process of converting data into a disguised and unintelligible form for illicit use. Such security is needed in storage and transmission of digital images over an unreliable medium. Since, digital images have special features such as multiple channel information, high correlation, high redundancy and bulk data that enforce special requirements on image encryption schemes. This paper presents a robust color image encryption scheme using discrete cosine transform. In this technique, the image is split into three RGB channels and block based permutation is performed on an individual channel. This permuted image is further processed using orthonormal basis vectors in discrete cosine domain to generate cipher. Finally, these three channels are fused together to get the encrypted image. Furthermore, the performance of proposed technique is analyzed against Different parameters as information entropy analysis, correlation coefficient analysis; number of pixel change rate, unified average change intensity, compression friendliness and the security is evaluated against brute force, statistical and differential attacks. The experimental results are discussed in details and encryption scheme is found to have reasonable security against various attacks and have shown good performance.

Keywords: *Color Image Encryption, Cryptography, Multimedia security, Image security*

1.Introduction

Encryption is the procedure to transform information through an algorithm to an unreadable form except the intended recipient possessing the secret-key, to provide a way for storage or transmission of sensitive data over insecure channels [1, 2]. According to [1] despite the fact cryptography is the process to secure sensitive data, cryptanalysis performs analysis for contravention of confidential information.

The security of data is necessary for several applications together with multimedia data. The Internet, wireless and public network are not secure networks that are susceptible to eavesdropping. It is often true that large part of the digitally communicated information is confidential and requires protection. Therefore, the protection and security of data is a major problem addressed by researchers. The multimedia network applications that need protection are security cameras, multimedia database, internet telephony and teleconferencing conferencing [3].

In the past few decades, the researcher has provided numerous successful alphanumeric data protection schemes. Different type of data has its own features, requiring a different kind of techniques for cryptographic protection of confidential data [4]. The cryptographic

ISSN: 2093-9655 IJEIC

algorithms such as IDEA, AES, DES, and RSA were designed for alphanumeric data. In natural images, the value of adjacent pixels can be reasonably forecasted because of high correlation [5, 6]. Image data usually contains far less information value density than alphanumeric data. Furthermore due to real-time processing requirements, the lower computational cost is a critical constraint[7].

It may appear feasible for personal computers to perform multimedia encryption and compression swiftly, making total encryption schemes satisfactory for multimedia processing. Perhaps it is true, there is a trend of mobile and server computing applications requiring efficient multimedia encryption schemes. The servers have to handle numerous processes simultaneously so the reduction in computational cost will facilitate the execution of more tasks. In reality, special servers are designed to handle cryptographic operation to free the server from such computationally exhaustive tasks. The development of a fast and efficient encryption scheme will abolish the need for a dedicated server for cryptographic processing [7].

There are a variety of new encryption schemes proposed specifically for image data [8]. There are two reasons behind the fact that we are not using traditional encryption schemes for image data. The first of them is larger image size than the textual data, hence require more computational time. The second is the deciphered data should be the exact reconstruction of the original plaintext data whereas this is not required in image data. A close approximation to the plaintext image will suffice the purpose. The reason behind this acceptance is the characteristics of human perception [2, 8-10]. There are numerous image encryption schemes but none of them satisfies the different image types. The high correlation among the neighboring pixels of most natural images makes it possible to predict the value of a pixel from its neighbors [6, 11, 12].

Image encryption algorithms are mainly divided into two main groups:

1. Chaos-based methods
2. Non-chaos selective methods

Most of the image ciphers are designed for a specific encryption application. There are algorithms which are scalable and compressible and employee different approaches such as light encryption, strong encryption, and degradation [13]. Almost all the permutation only ciphers are doubtful against known plaintext attacks. In order to design a secure image encryption scheme, the permutation should be followed by other encryption variants. Maniccam *et al.*, [13] has proposed a multimedia encryption scheme for image and video data using SCAN patterns. Image pixels are permuted based on SCAN pattern and substituted with an iterated cipher. Maniccam *et al.*, [14] have presented another technique based on SCAN patterns. It performs encryption and lossless compression of digital grayscale and binary images. Guan *et al.*, [6] have proposed an image encryption technique which changes the gray value of pixels along with changing the spatial position to complicate the correlation between cipher and plaintext image. Mitra *et al.*, [4] have presented an encryption technique employing random combinational encryption approaches. It uses a bit, pixel and block level permutation to perform encryption. Ozturk *et al.*, [15] presented an image encryption scheme which improves visual cryptography and mirror like encryption algorithm by combining compression ability. Sinha *et al.*, [16] used jigsaw transform and fractional Fourier transform in image bit planes to generate image cipher. Droogenbroeck *et al.*, [17] have encrypted images using selective encryption technique as well as multiple selective encryptions. The proposed cipher uses pixel or block level permutation followed by other encryption operations in discrete cosine domain to make it a robust and secure encryption scheme.

Section 2 discusses in details, the literature survey of five popular image encryption schemes. Section 3 contains the proposed schemes and its algorithm and flow chart diagram. Section 4 contains experimental results and Section 5 includes performance

evaluation of the proposed encryption schemes against various security evaluation and encryption quality analysis parameters. Section VI concludes the work with some remarks to the proposed image cipher.

2. Literature Review

Extensive work has been done in the area of multimedia cryptography. Some significant works have been reviewed to provide a detailed analysis and help in analyzing and comparing the security and quality of the proposed image encryption scheme. It provides a glimpse of existing work in the area to justify the need for the proposed encryption scheme. The proposed algorithm in contrast to the other existing algorithm provides less noisy encryption technique as noise while encrypting and decrypting image is significantly less than other methods which is represented through experimentation as well in Section 5.

2.1. A Modified AES-Based Algorithm for Image Encryption

Zeghid *et al.*, [18] has analyzed the Advanced Encryption Standard for the protection of image data from illegal access and added a key stream generator for the enhancement of encryption performance. Most of the encryption schemes used in image encryption utilize vector quantization technique. The authors discussed the traditional techniques and proved the preeminence of the modified algorithm.

The algorithm uses multiple rounds for full encryption. Each round utilizes four transformations. The number of rounds is dependent on the length of the secret-key. The first round performs byte sub-transformation, a non-linear byte-substitutions, using a substitution table. The second round performs shift row transformation. It is a byte transposition, "which cyclically shifts the bytes in last three rows; the offset of left shift varies from one to three bytes" [18]. The third round multiplies a fixed matrix with all the column vectors. Bytes are treated as a polynomial rather than a number. In the fourth round, simple XOR is used for transformation of the key between the working state and round key.

They performed a security evaluation of proposed AES algorithm to check the performance of image encryption scheme. For the purpose of security evaluation, they have performed key space analysis and statistical analysis. In the former, the key space analysis is given much attention to drop the feasibility of brute force attack. AES has a large key space, as its secret key is very sensitive. In this typical case, the key space is of 10^{128} which is sufficiently large to repel all types of brute force attacks. The cipher image is changed completely with a minor change in secret key. They also performed correlation coefficient analysis and histogram analysis. The results indicate that the histogram of cipher image is uniform regardless of the histogram of plaintext image. This difference cancels out the probability of any statistical attack on the cipher image [18]. The correlation coefficient analysis is performed on pair of horizontally, vertically and diagonally adjacent pixels by using formula 1:

$$Cov(x, y) = E\big(x - E(x)\big)\big(y - E(y)\big) \quad (1)$$

The entropy of image falls below from maximum in Electronic Code Book (ECB) Mode as it contains textured zones because image containing homogeneous zones remain also the same after ciphering. In ECB, "ciphered block is a function of the plaintext block, the algorithm, and the secret key. Consequently, same data will be ciphered to the same value; which is the main security weakness of that mode and the image encryption scheme" [18].

The key stream generator was added for the enhancement of security of these algorithms. Two different forms of the key generator are used, W7 key stream generator and A5/1 key stream generator. The former is symmetric key technique having 128-bits key length. "It is optimized for efficient hardware implementation at reasonable data rates. Its architecture consists of functional unit and control unit" [25]. The function unit generates a synchronous key stream. In the later A5/1, three Linear Feedback Shift Registers (LFSR) R1 having

lengths 19 bits, R2 having 22 bits and R3 having 23 bits are used. LFSR shifts using clock cycles defined by a majority functions. Three bits are used by the majority functions naming; C1, C2 and C3. The initial state of LFSR's is mapped by the 64 bits key as [18]:

$$R1\ (19\ bits) : x19 + x5 + x2 + x + 1$$

$$R2\ (22\ bits): x22 + x + 1$$

$$R3\ (23\ bits): x23\ +\ x15\ +\ x2\ + x\ +\ 1$$

Finally, the output bits are produced by performing the XOR operation on each pre-initialized LFSR last bit. The efficiency and speed of encryption of AES algorithm are compared with MIE, N/KC, and the VC and demonstrated faster encryption. The A5/1 key stream generator has shown least area as shown experimentally due to its simpler architecture. The use of W7 key stream generator has resulted in enhancement of security of the proposed algorithm. The use of key stream generator has resulted in an increase of entropy value. The extended support of key stream generator for image cryptography in AES has resulted in enhanced security. Keystream generator has also overcome the problem of textured zones that exist in other known image cryptographic algorithms.

2.2. New Color Image Encryption Algorithm based on Chaotic Sequences Ranking

Meng Jian-liang *et al.*, [19] proposed an algorithm which creates a 1-1 relation between the image matrix and chaotic sequence by scrambling the position of color images. The privacy and security of cipher are improved by shuffling the pixel values of the scrambled image. The tricolor pixel values in the color image are interchanged to perform the color image encryption while shuffling operation and it is conducted by chaotic sequence. Most of the image cryptosystem are not highly secure due to the use of simple one-dimensional chaotic system whereas the higher dimensional chaotic systems have an efficient security.

Scrambling algorithm

Undertake a matrix for digital color image *i.e.*, A with dimension $M \times N$, having N column pixel value and M row value as shown in figure 1, so $A(i, j)$ is the image location. Scrambling is performed in row; link row of $i + 1$ to the tail of row i ($i = 2, 3, \ldots \ldots \ldots, M$), forming a sequence L1 ($a_{11}, a_{12}, \ldots, a_{1n}, a_{21}, \ldots, a_{M\times N}$) with dimension $M \times N$.

A chaotic sequence L2 is generated by utilizing appropriate initial value as a secret key. A consistent relation is established by the following rule.

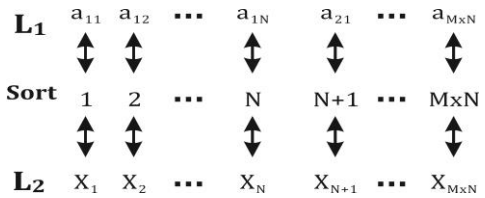


Figure 1. Generation and Sorting of Chaotic Sequence

L2' is obtained by sorting elements of L2 in ascending order with respect to their size. Serial number is obtained of each x_i in ordinal sequence $L2'$, forming an exchange set $T(t_1, t_2 \ldots t_{M\times N})$ and t_1 here is a member of $(1, 2, \ldots M \times N)$ [19]. L_1 is exchanged with respect to set T. L1' sequence is obtained by this mode. By application of the formula,

$$A'(i, j) = L_1'\big((i - 1) \times M + j\big)$$

here $i = 2, 3, \ldots M$ and $j = 1, 2, \ldots, N$ so A' can be acquired. On the same pattern column scramble column, the formula applied will be

$$A'(i, j) = L_1'((j - 1) \times N + 1).$$

The decryption follows the same process except it will use L1' instead of L2.

Shuffling algorithm

The shuffling operation is necessary to enhance the security of the ciphered color images. The tri-channel color image is broken down into 3-channels and the three-color values of each pixel are interchanged. Three tridimensional chaotic sequences are generated using Lorenz chaotic sequence. 1-1 relationship is computed between (ri, gi, bi) & (xi, yi, zi) and ascending order sorting with respect to size is performed. The exchange sequence is returned to matrix form according to the formula used during scrambling algorithm of encryption process after interchanging the tricolor values of pixels. The tricolor shuffled image is used to generate the color image. The result will be the cipher image. Decryption follows the similar process.

The authors analyzed the both algorithms using parameters like statistical analysis, emulation experiment, execution efficiency and correlation coefficient analysis. The experimentation demonstrated high security, confidentiality, and efficiency. The isolation of chaotic sequence from high-dimensional chaotic sequence resulted in enhancement of the encryption rate.

2.3. A New Image Encryption Arithmetic Based on a Three-dimensional Map

Feng Huang *et al.*, [20] introduces a 2-D map based technique which is further extended to 3-D. A tetragonal image is separated into two isosceles triangles, sliced along the diagonal. Stretching and folding are used to perform the encryption process. Initially, N×N plain image is transformed to a line of N^2pixels. This line is folded over to a new N×N image by inserting individual pixels of one column to the next column. Obtained two-dimensional image is composed of two sub-maps; right map and the left map. The process is demonstrated by the figure 2 by utilizing image with 4×4 pixels.

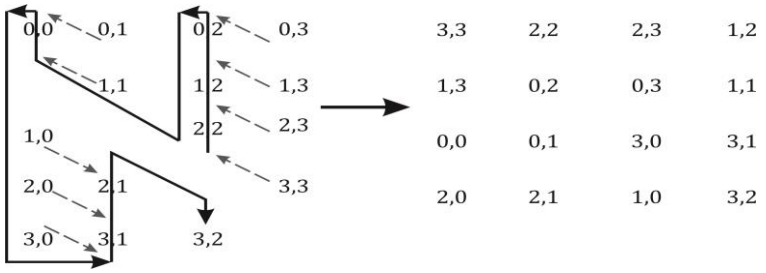


Figure 2. 4×4 Pixels Process of the Left Map

Pixel (3, 3) is inserted before (2, 2) and pixel (2, 3) between (2, 2) and (1, 2) and so on. This line of pixels is folded over to a new N×N image, same in size as the plain image [20]. The 2-D algorithm is extended to 3-D. The algorithm has gray values in decimal for N×N square image with L gray values. These decimal values are represented into binary form using the following formula:

$$A = \sum \mathrm{Kn2n}$$

The image gray levels are used to fragment plain image into layers. The initial layer contains smallest binary values and the succeeding layers with larger and the process continue [20]. Then image layers are confused using left and right map. Finally, the line is converted to a square image by using the below-mentioned formula.

$$\mathrm{Kn(i,j)} = \mathrm{I(i \times N + j).}$$

These maps produce cipher image similarly as permuted image. The numbers of left and right maps are used as a cipher key. Decimal digits of cipher key represent the amount of

iteration of right and left map alternatively. The cipher key 47 will iterate left map 4 times and right map seven-time in order to complete the operation [20]. Just in case of binary digits, the right and left map are iterated. Every four digits of the binary image iterated from least to most significant bits (from 0 to 15 bit) alternatively.

In the case of three-dimensional maps, if the cipher key is presumed to be "3294"; the odd number layers are enciphered by iterating left map by 3 times and right map by 2 times. Whereas the even numbered layers, the mapping will be performed by iterating left map by 9 times and right map by 4 times [20]. Image encryption is performed by extending the image to a three-dimensional image. The key is designed and plotted to a square image of the same size. The cipher image is obtained by combining these layers. Diffusion can also be added to obtain a better quality encryption.

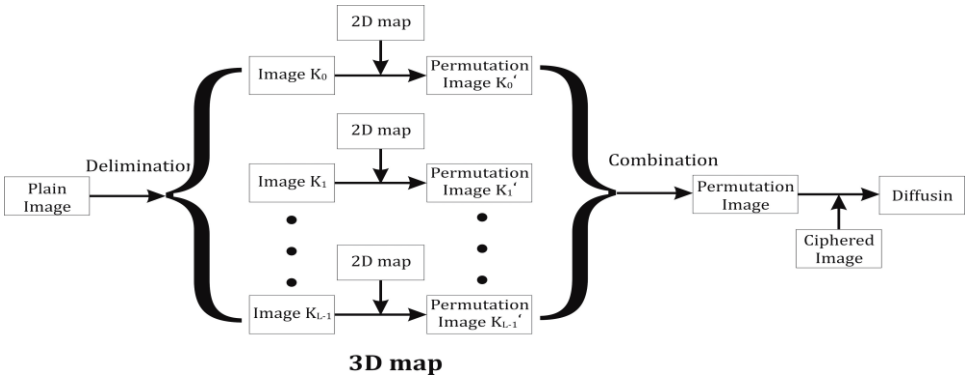


Figure 3. The Process of Image Encryption

The efficiency of the algorithm is proved experimentally. The algorithm possesses good confusion properties. The correlation between vertical, horizontal and diagonal pixels is also insignificant, making it a good encryption algorithm.

2.4. Analysis and Comparison of Image Encryption Algorithms

Ismat *et al.*, [15] have discussed and analyzed numerous image encryption algorithms on the basis of their security and efficiency. They classified all the discussed techniques into three major types namely position permutation, value transformation, and visual transformation. Mirror-like image encryption (MIE) performs the scrambling by determining the chaotic system and determining the binary sequence based on that chaotic sequence. Swap function rearranges the image pixels with respect to binary sequence. Human visual characteristics are used in visual cryptography to decipher the encrypted image. Halftone image is obtained by transformation of gray level image and two transparencies of visual cryptography are generated. The plain image cannot be detected without stacking the both transparencies. There are three methods in visual cryptography. In the first one, cyan, magenta, yellow and black are used to share the plain image. The secret image can't be perceived from any single sharing image. The second method uses two sharing images and is poor then the first one as that keep image contrast.

The authors also analyzed the advantages and disadvantage of their proposed algorithm. The digital signatures in this scheme do not incorporate any type of compression despite the fact the authenticity is verified. The size of the image increases as a drawback due to the introduction of redundancy. Medical imaging and military application use SCAN due to its lossless compression and robust encryption capabilities. The current scheme performs both compression as well as encryption with the cost of encryption speed. In chaotic encryption scheme and mirror-like encryption scheme, a binary sequence is used. Vector Quantization (VQ) requires less bitrate resulting in optimal utilization of storage space and channel bandwidth. The decoding process is fast as VQ is based on uncomplicated hardware

structure. In the case of double random phase encoding, only one channel is utilized for the encryption of multi-channel color image. Hence it decreases the complexity and increases the reliability of cipher. The key advantage of this technique is the image is recovered without any reckoning. The image is compressed before transmission to reduce the channel bandwidth. The decompression is performed before deciphering the image at receiving end. Compression is a more important issue for VC then MIE as it produces two or more sharing images can be produced which are twice the size of original image [15]. It has been shown experimentally that both VC and MIE can be improved if compression follows the encryption process. JPEG compression with 100% quality factor cannot compress the noise in image productively. The JPEG compression results in loss of color even in the case of 100% quality factor so PNG lossless compression is ultimate for compression of color images in MIE. The compression algorithm used in VC should be selected carefully as it is not a lossless cipher.

2.5. Wavelet Based Image Encryption

Flayh *et al.*, [21] have presented a new encryption scheme for digital images based on Wavelet transform. It hides the processing steps of the most efficient transform that offer a prevailing time-frequency depiction. The authors presented an encryption technique based on hiding wavelet packet tree and alternative technique of hiding filter type. The image data is of enormous size that poses a restriction of time complexity and makes it an important parameter for image cryptography. The promising entity of this technique is that the intruder cannot construct the plain image without the knowledge of processing steps.

Hiding Filter Types Encryption Scheme (HFT)

The technique is based on a pool of filter and the selection of filter is performed randomly. The filter is used differently at different decomposition level. They have used haar, biorthogonal, daubechies, coiflet and smylet filter families. The decomposition depth and the filter library determines the size of keyspace. The disintegration depth is kept secret for efficiency and security. In each disintegration level, the index of filter is selected arbitrarily. Reintegration using the correct filter generates a smooth image. The incorrect filter selection during reintegration produces a noisy image. The proposed scheme has been applied to four grayscale and four color images to demonstrate the experimental results. The results of experimentation demonstrated that the cipher image has much less correlation as compared to a plain image or deciphered image. The correlation coefficient of the tricolor image is calculated through reconstruction of three-color spaces (Red, Green, and Blue). The correlation of reconstructed tricolor image is generated by averaging the correlation of three different color channels. The following formula is used to perform the stated correlation calculation:

$$\text{Corr\_RGB} = \frac{\text{Corr\_red} + \text{Corr\_green} + \text{Corr\_blue}}{3}$$

Hiding Wavelet Packet Tree Encryption Scheme (HWPT)

The technique is based on disintegration that is decided randomly by using best-basis algorithm initially and then random changes are made to it. Reintegration of image requires the tree structure. The technique is applied to a set of color and grayscale images and has demonstrated highly uncorrelated cipher image. The key space size in this algorithm is 22^{2n}.

The study consists of the application of both techniques on color and grayscale images. The security of this technique is based on the selection of filter types, sequences, and quantity. The structure of tree also plays important role in defining the security of this technique. An analysis has been performed by applying both of these techniques together and separately on a set of color and grayscale images. The results of analysis demonstrate

the security of the technique and provided a better result when both techniques are used together. The correlation result of the plain image and reconstructed image are close to unity indicating the high accuracy of reconstruction. Moreover, the cipher image provides worthy confusion properties to protect the confidential image data [21].

3. Proposed Technique

3.1. Encryption Algorithm

Input the plain image I0 with dimension $m \times n \times 3$.
Separate the three RGB channels into 2-Dimensional images IR, IG, and IB with dimension $m \times n$ and take their discrete cosine transform DCT.
Initialize an iteration count i that starts from zero and goes up to $N - 1$

1. Initialize a secret key k_i.
2. Generate pseudorandom permutation sequence σ_i.
3. Perform pixel level permutation using random sequence σ_i separately on IR, IG, and IB.
4. Generate a random vector Δ_0 using a random sequence σ_i of $m \times n$ elements.
5. Generate orthogonal matrix φ_i by using Gram-Schmidt algorithm.
6. Multiply φ_i with I_R, I_G and I_B, separately.

Step 1 to 5 are repeated N times.
After performing N iterations, inverse DCT of three RGB channel images I_R,I_G and I_B is taken to get the spatial domain images.
Perform scaling and quantization of I_R, I_G and I_B with $\max(I) = 255$ and $\min(I) = 0$.
Fuse the three RGB channel images into a single RGB image.
The similar process is demonstrated by flow chart given in Figure 4. The three RBG layers follow the process depicted in Figure 4 separately and they are combined at the end to obtain an encrypted RGB image.

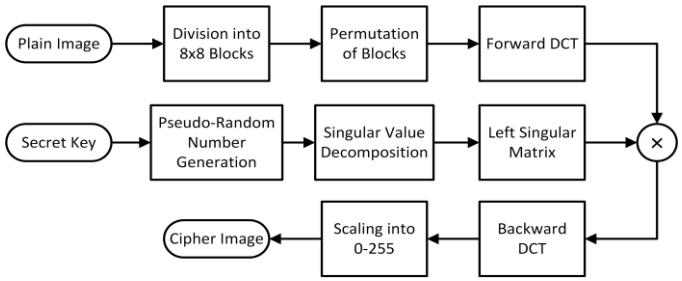


Figure 4. Flowchart Representation of Encryption Process

3.2. Decryption Algorithm

The decryption process is performed by applying all the transformation of the encryption process in converse order. If there is no distortion during transmission or storage, the received cipher image will be equal to transmitted or stored cipher image. The type of distortion is caused by JPEG compression only in this scenario. The secret key k_i along with the number of iterations N and scaling parameters are also required along with the cipher image C_0 to perform the decryption process.

Separate the three RGB channels of cipher image C_0 into 2-Dimensional images C_R,C_G

and C_B and take their DCT.
Initialize an iteration count i which starts from zero and goes up to $N - 1$

7. Initialize a secret key k_i.
8. Generate pseudorandom permutation sequence σ_i.
9. Generate a random vector Δ_0 using random sequence σ_i of $m \times n$ elements.
10. Generate orthogonal matrix φ_i by using Gram-Schmidt algorithm [x13]
11. Take transpose of matrix φ_i that is equivalent to φ_i^{-1} in the case of an orthogonal matrix.
12. Multiply φ_i^{-1} with C_R, C_G and C_B, separately.
13. Perform inverse pixel level permutation using random sequence σ_i separately on C_R,C_G and C_B.

Step 1 to 5 are repeated N times.
After performing N iterations, inverse DCT of three RGB channel images C_R, C_G and C_B is taken to get the spatial domain images.
Perform scaling and quantization of C_R, C_G and C_B with $\max(I) = 255$ and $\min(I) = 0$.
Fuse the three RGB channel images into a single RGB image.
The similar process is demonstrated by flow chart given in Figure 5. The three RBG layers follow the process depicted in Figure 5 separately and they are combined at the end to obtain a decrypted output RGB image.

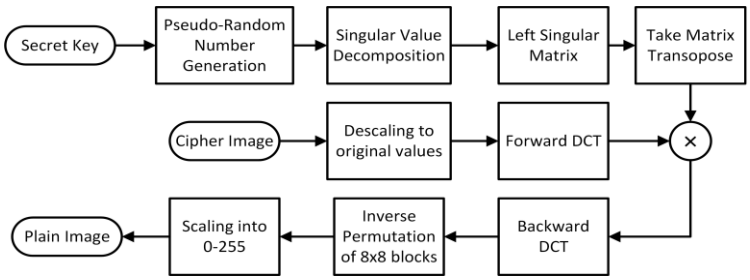


Figure 5. Flowchart Representation of Decryption Process

It is appropriate to state that the encrypted image is obtained after quantization so the decryption doesn't produce the exact input image I_0. The goal of the proposed scheme is to perform multimedia encryption in image domain resulting in excellent reconstruction of the plain image I_0.

4. Experimental Results

A graphical user interface is designed in MATLAB ® 2010b to easily perform simulation and security analysis experiments for the proposed technique as shown in Figure 6. The practicality of the proposed encryption scheme is verified by performing the encryption experiment on a large set of images. The result of encryption shows good quality encryption with other suitable encryption parameters.

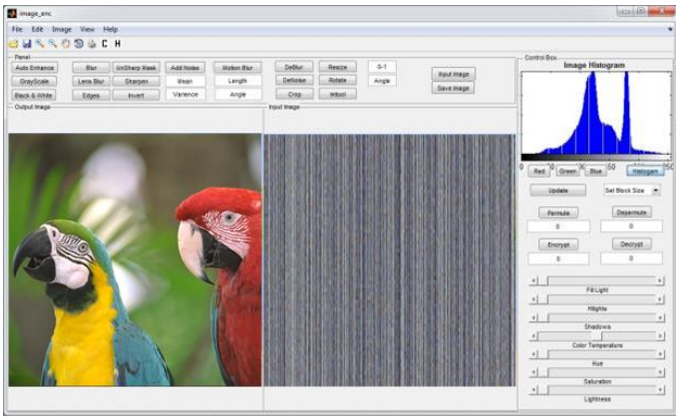


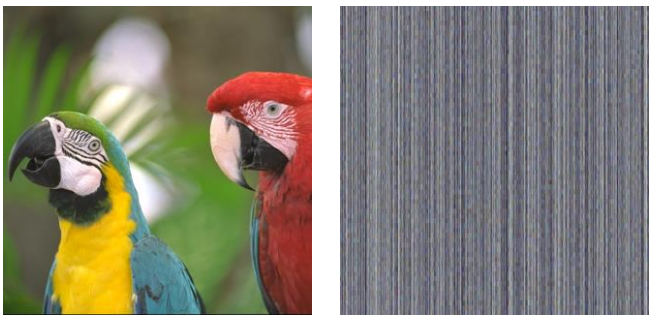
Figure 6. The MATLAB ® 2010b Based GUI for the Proposed Scheme

Figure 7 (a) contains Kodim19 (lighthouse) image as a plaintext input image. The ciphertext image after encryption of Kodim19 is shown in Figure 7 (b). The decrypted image has slight variation in intensity values due to requantization but it causes no visual degradation. PSNR between original and decrypted images are calculated and found out to be 42.82dB, which is quite high.

(a) (b)

Figure 7. (a) Plaintext Image, (b) Ciphertext Image

Figure 8 provides the original Kodim23 image (a) and ciphertext version of the same image (b). The PSNR between original and decrypted image is 41.1dB, which is quite good for visual observing.



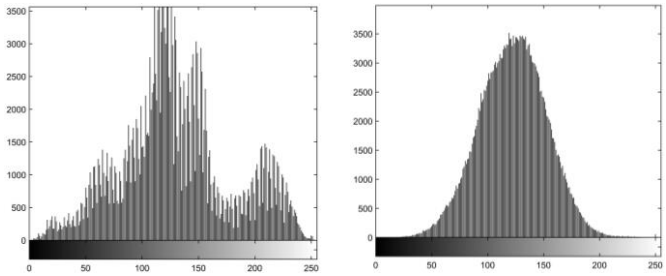
(a) (b)

Figure 8. (a) Plaintext image, (b) Ciphertext Image

5. Comparative Analysis

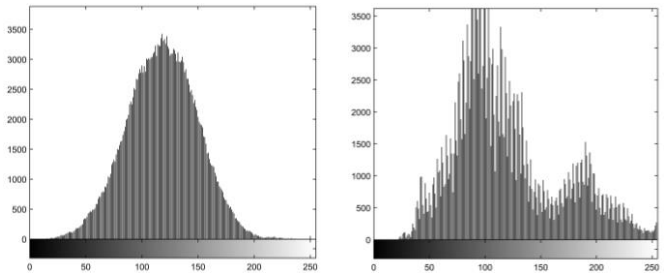
5.1. Histogram Analysis

Many kinds of ciphers can be broken down by performing statistical analysis. The histogram and correlation of pixels in cipher image provide a clue during the analysis as pointed by Shannon in his classical masterwork [18]. The histogram shows the range of pixel values in the image. In an ideal case, a cipher should produce an image with the uniform histogram. It prevents the intruder from extraction of any expressive statistics from the histogram of cipher image. The proposed algorithm generates a Gaussian curve like histogram for all the cipher images regardless of plaintext-image. The histograms of the three RGB channels are also independent of the input plaintext-image. The results of histogram analysis are provided for Kodim19 image and Kodim23 images respectively in Figure 9 and 10.



(a) (b)

Figure 9. Histogram Analysis Results of Kodim15 Image; (a) Histogram of Original Image, (b) Histogram of Ciphertext Image



(a) (b)

Figure 10. Histogram Analysis Results of Kodim23 Image; (a) Histogram of Original Image, (b) Histogram of Ciphertext Image

The histogram analysis is performed on a set of test images and results for two of them are shown here. It is evident that all the histograms are of bell shaped and are independent of input image histogram so they don't leak any information to the intruder. The permuted DCT image is multiplied with an orthogonal matrix that produces normally distributed histogram. All the features of the input color image are covered and the input cannot be guessed from the output instead of the non-uniform histogram. The algorithm has complicated the dependence of the statistics of the output on the statistics of the input.

5.2. Correlation Coefficient Analysis

The correlation coefficient in image domain is a measure that tells the degree of similarity between two images. The correlation of image with itself is called self-correlation. The self-correlation of the adjacent pixel for a meaningful image is always high as the value of the adjacent pixel is close to each other in such case. The correlation analysis

was performed on two diagonally adjacent, horizontally adjacent and vertically adjacent pixels of cipher image as well as plaintext image. 1000 pairs of random pixels were selected from cipher and plaintext image to perform the analysis. The following formula was used to perform correlation coefficient analysis:

$$C.C = \frac{Cov(x,y)}{\sigma_x \times \sigma_y}$$

The analysis was performed on numerous 512×512 cipher images. However, the correlation result of 1000 random pair of pixels is shown in Figure 11 for diagonal direction, Figure 12 for the vertical direction and Figure 13 for the horizontal direction. Cipher image of Peppers is used for this analysis. The result of the correlation coefficient for a cipher image is 0. 0076 in vertical direction and 0.0105 in a diagonal direction. Whereas, the horizontal correlation coefficient for cipher image is 0.9861, which is much higher due to horizontally correlated pixels in the cipher image.

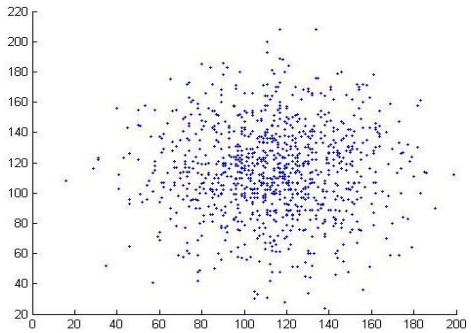


Figure 11. Diagonal Correlation of 1000 Random Points

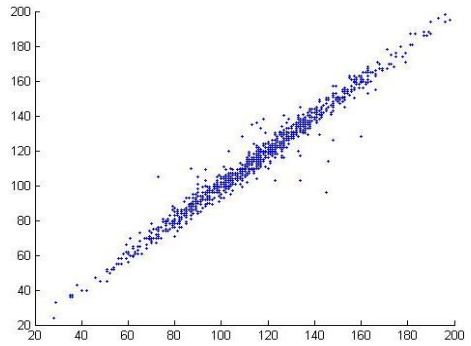


Figure 12. Horizontal Correlation of 1000 Random Points

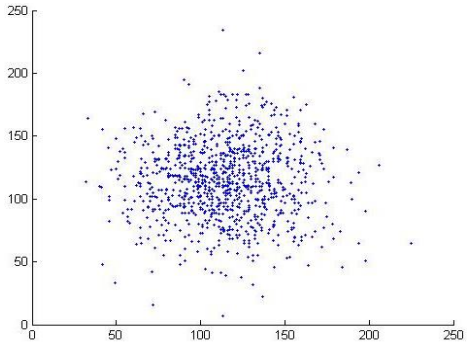


Figure 13. Vertical Correlation of 1000 Random Points

The higher correlation in horizontal adjacent pixels is a favorable feature to get high compression rate in case of JPEG compression that is discussed later in this paper. The results of Table 1 & 2 show the value of correlation coefficient that is close to one in the case of plaintext images. However, the cipher image has low correlation in the vertical and diagonal direction. Conversely, the correlation in the horizontal direction is much high, close to one. The reason behind this phenomenon is the multiplication of permuted image with orthogonal matrices. Regardless of higher horizontal correlation, the image security is not compromised; as it does not leak any information to be used for deduction of the plaintext image or the secret key.

Table 1. Correlation Coefficient Analysis of Two Adjacent Pixels: Kodim19 Image

Direction of Adjacent Pixels	Plain Image	Cipher Image
Diagonal	0.9821	0.0105
Vertical	0.9830	0.0076
Horizontal	0.9746	0. 9861

Table 2. Correlation Coefficient Analysis of Two adjacent pixels: Kodim23 Image

Direction of Adjacent Pixels	Plain Image	Cipher Image
Diagonal	0.9679	0.0376
Vertical	0.9756	0.0141
Horizontal	0.9750	0. 9803

5.3. Information Entropy Analysis

The entropy of a source provides information about the source itself [22]. It indicates the degree of uncertainty of a system [23]. Shannon [24] proposed his information theory which is used in network security, cryptography, data compression and other related areas. The entropy of an image I [25] can be calculated as:

$$H(I) = -\sum_{i=0}^{255} h_N(i)\log_2(h_N(i))$$

Where $h_N(i)$ is the normalized histogram of the color level i in the image I.

In an ideal case, the information entropy of an image should be 24 bits for an RGB color image. The entropy value less than 8 bits may result in the leakage of the information which intimidates the security [26, 27]. The results of the information entropy analysis are provided in Table 3.

Table 3. Information Entropy of Cipher Images

Cipher Image	**Entropy Analysis**
Kodim19	0.9830
Kodim23	0.9746

5.4. Key Space Analysis

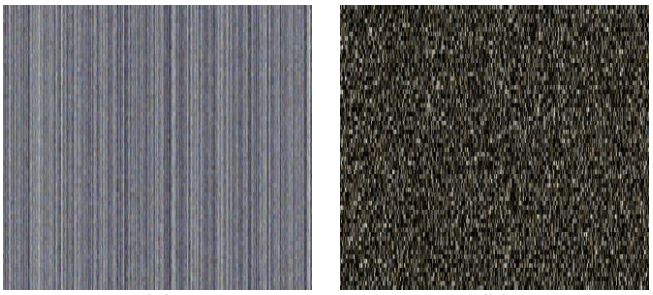
A good algorithm should have a large enough key space to make brute force attacks practically infeasible and the algorithm should be much sensitive to the secret key. Keyspace analysis has been performed on a large set of data for the proposed algorithm and some of the results are concisely given below.

5.5. Key Space

The proposed image encryption technique has 9×10^{308} different combination of a secret key. The key space of this algorithm is large enough for practical use to resist all kinds of brute force attacks.

5.6. Key Sensitivity Test

Ideally, an encryption technique should be sensitive to secret key, i.e. a single bit change in secret key should produce a significantly dissimilar cipher image. Following steps are carried out to perform the key sensitivity test of the proposed algorithm and its results are shown in Figure 14.



(a) (b)

Figure 14. Key Sensitivity Test; (a) Encrypted image. (b) Decrypted with Wrong Secret Key

i. The plaintext image, Kodim15, is encrypted with a secret key "33945087255" and the cipher image obtained is shown in Figure 14 (a).
ii. The cipher image obtained in the previous step is decrypted with 1-bit changed secret key "33945087256" and the decrypted image obtained is shown in Figure 14 (b).
iii. It is clear from the Figure 14 that the proposed image encryption scheme is very sensitive to change in secret key.

5.7. Differential Analysis

The differential analysis is ineffective if a minor change in plain image produces a large change in cipher image. Two common measures are used to check the effect of one-pixel change on the entire image. These two tests are NPCR and UACI that are widely used in security analysis by the cryptographic community. NPCR measure the absolute number of pixels that changes value whereas UACI measures the average difference between two cipher images.

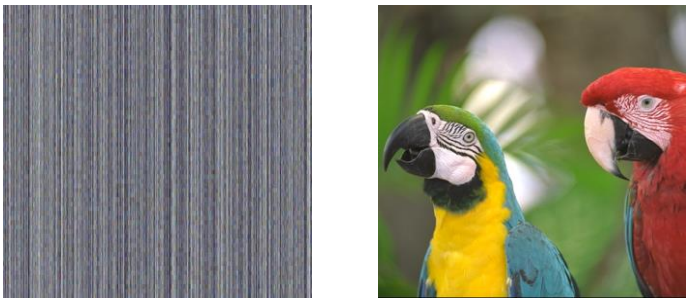
Table 4. Quantitative Score of NPCR and UACI Tests

Image	NPCR Quantitative	UACI Quantitative
Kodim19	0.989669799804688	0.122380395029105
Kodim23	0.990264892578125	0.137299062691483

Differential analysis test provides quantities as well as qualitative values for the pair of cipher images. The qualitative value for NPCR and UACI are positive for both images, indicating that the cipher image is secure to differential analysis. The NPCR quantitative score is satisfactory. The NPCR value 0.9896 for Kodim19 cipher image in table 4 produced by proposed scheme indicates that 98.96 percent of the pixels are different in second cipher image from that of first cipher image. The UACI scores is comparatively lower for the proposed scheme; means the average difference between the two cipher images is not significant.

5.8. Noise Tolerance

Noise tolerance is the desired parameter of a good image encryption scheme. The effect of noise on the cipher images and their decryption quality is explored in this section. The figure 15 and 16 shows the results of noise resistant on cipher images. Additive white Gaussian noise is added to the cipher image followed by the decryption process. Simulation results indicate that the proposed system is tolerant to noise and can be used in noisy channels.



Cipher Image with 30dB AWGN Reconstructed Image

Figure 15. Result of Cipher Image with AWGN and its Deciphered Image

Cipher Image with 30dB AWGN Reconstructed Image

Figure 16. Result of Cipher Image with AWGN and its Deciphered Image

5.9. Compression Friendliness

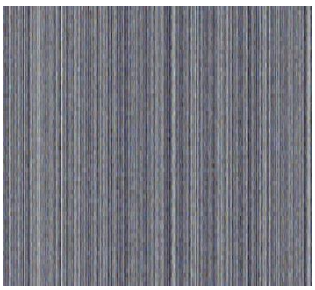
The matter of image compression is of vital importance in the area of cryptography. The compression of the image reduces the requirement of transmission bandwidth and storage space. Various compression-coding techniques are in use based on the entropy theory. If the encryption does not affect the compression efficiency significantly and nor does it introduce additional data, then it is said to be compression friendly. Entropy-based methods are used to compress the image data having lots of redundancy. The proposed algorithm is compression friendly as it produces the cipher image with the same size as the input plaintext image. An added property of this algorithm is that it is tolerant to lossy compression.

Lossy compression is much important in the case of image data to reduce the requirement of transmission bandwidth and storage space. It is possible to reconstruct the image with enough visual quality that the error between the original and reconstructed image is small when the image is compressed through lossy compression technique such as JPEG. Much of the conventional image ciphers cannot work in lossy compression. Due to horizontal correlation in cipher image, it gives significant compression whereas highly uncorrelated images JPEG compression doesn't give a significant reduction in image size. The result of JPEG compressed cipher image and its reconstructed image is shown in Figure 17 and 18. The image size after JPEG compression at different quality factors is tabulated in Table 5.

Table 5. Cipher Image (Kodim19) Size at Different Quality Factors of JPEG Compression

Quality Factor	Image Size	
	Kodim15	Peppers
Bitmap Image	768 KB	768 KB
100	219 KB	211 KB
90	80 KB	76 KB
70	50 KB	49 KB
50	40 KB	41 KB
30	32 KB	33 KB
10	17 KB	18 KB

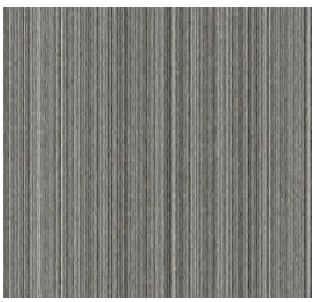
The size of the original bitmap image was 768 kB. It is clear from the Figures 17 and 18 that the encrypted images can be recovered with good quality even after JPEG compression with different quality factors. The table shows that when the size of encrypted image decreases with the decrease in quality factor.



JPEG Compressed Cipher Image

Reconstructed Image from JPEG

Figure 17. JPEG Compression is Performed at 75% Quality Factor



JPEG Compressed Cipher Image

Reconstructed Image from JPEG

Figure 18. JPEG Compression is Performed at 75% Quality Factor

6. Conclusion

The security requirements of an encryption algorithm are much different from an image to a text file. The reason for this is the intrinsic characteristics of the image cryptosystems such as the speed of encryption and easiness of algorithm are taken as more important parameters than unqualified security. The algorithm performs position encryption as well as gray value encryption simultaneously. The algorithm produces cipher image with good vertical and horizontal correlation whereas the horizontal correlation is high. This does not pose any security threat on the cipher as this horizontal correlation is due to the property of orthogonal basis vector. This horizontal correlation provides a superior advantage over the other popular ciphers as it can result in significant compression is a case of lossy

compression such as JPEG.

It has been demonstrated experimentally, the algorithm has many promising parameters. It provides sufficiently large key space, higher security, consistent histogram, robustness to noise and lossy compression. It also maintains a worthy compromise between visual degradation, tenability, compression friendliness, cryptographic security and computational efficiency.

References

[1] C. Harris, "ITN584 Access Control & Smart Cards", in Research Paper2001.
[2] G. C. Kessler, "An overview of cryptography", **(1998)**.
[3] G. Ye, "Image scrambling encryption algorithm of pixel bit based on chaos map. Pattern Recognition Letters", vol. 31, no. 5, **(2010)**, pp. 347-354.
[4] A. Mitra, Y. V. S. Rao and S. Prasanna, "A new image encryption approach using combinational permutation techniques", International Journal of Computer Science, vol. 1, no. 2, **(2006)**, pp. 127-131.
[5] A. L. Vitali, "Video over IP using standard-compatible multiple description coding: an IETF proposal", Journal of Zhejiang University SCIENCE A, vol. 7, no. 5, **(2006)**, pp. 668-676.
[6] R. C. Gonzalez and E. Richard, "Woods, digital image processing", ed: Prentice Hall Press, ISBN 0-201-18075-8, **(2002)**.
[7] C.-P. Wu and C.-C. J. Kuo, "Efficient multimedia encryption via entropy codec design", Photonics West 2001-Electronic Imaging, International Society for Optics and Photonics, **(2001)**.
[8] K. Wang, "On the security of 3D Cat map based symmetric image encryption scheme", Physics Letters A,vol. 343, no. 6, **(2005)**, pp. 432-439.
[9] Y. Shuangyuan, L. Zhengding and H. Shuihua, "An asymmetric image encryption based on matrix transformation", Communications and Information Technology, ISCIT 2004. IEEE International Symposium on. 2004. IEEE, **(2004)**.
[10] D. Salomon, "Data compression: the complete reference2004: Springer-Verlag New York Incorporated",
[11] S. P. Nanavati and P. K. Panigrahi, "Wavelets: Applications to image compression-I", Resonance, vol. 10, no. 2, **(2005)**, pp. 52-61.
[12] A. L. Vitali, "Video over IP using standard-compatible multiple description coding: an IETF proposal", Journal of Zhejiang University-Science A, vol. 7, no. 5, **(2006)**, pp. 668-676.
[13] S. S. Maniccam and N. G. Bourbakis, "Image and video encryption using SCAN patterns", Pattern Recognition, vol. 37, no. 4, **(2004)**, pp. 725-737.
[14] S. Maniccam and N. Bourbakis, "Lossless image compression and encryption using SCAN", Pattern Recognition, vol. 34, no. 6, **(2001)**, pp. 1229-1245.
[15] I. Ö ztürk and İ. Soğukpınar, "Analysis and comparison of image encryption algorithms", International Journal of Information Technology, vol. 1, no. 2, **(2004)**, pp. 108-114.
[16] A. Sinha and K. Singh, "Image encryption by using fractional Fourier transform and jigsaw transform in image bit planes", Optical Engineering, vol. 44, no. 5, **(2005)**, pp. 057001-057001-6.
[17] M. Van Droogenbroeck and R. Benedett, "Techniques for a selective encryption of uncompressed and compressed images", ACIVS Advanced Concepts for Intelligent Vision Systems, Proceedings, **(2002)**.
[18] M. Zeghid, "A modified AES based algorithm for image encryption", International Journal of Computer Science and Engineering, vol. 1, no. 1, **(2007)**, pp. 70-75.
[19] M. Jian-liang, P. Hui-jing and G. Wan-qing, "New color image encryption algorithm based on chaotic sequences ranking", Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP'08 International Conference on. 2008. IEEE.
[20] F. Huang, C. Wang and S. Li, "A new image encryption arithmetic based on a three-dimensional map", Cybernetics and Intelligent Systems, IEEE Conference, **(2008)**.
[21] N. A. Flayh and S. I. Ahson, "Wavelet based image encryption", Signal Processing, ICSP 2008. 9th International Conference, IEEE, **(2008)**.
[22] N. F. El Fishawy and O. M. A. Zaid, "Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms", IJ Network Security, vol. 5, no. 3, **(2007)**, pp. 241-251.
[23] S. H. Kamali, "A new modified version of Advanced Encryption Standard based algorithm for image encryption", Electronics and Information Engineering (ICEIE), 2010 International Conference, IEEE, **(2010)**.
[24] R. M. Gray, "Entropy and information theory", Springer, **(2011)**.
[25] A. Benjeddou, "A fast color image encryption scheme based on multidimensional chaotic maps", in Information Infrastructure Symposium, 2009. GIIS'09. Global, IEEE, **(2009)**.
[26] X. Shu-Jiang, "A novel image encryption scheme based on chaotic maps", Signal Processing, ICSP 2008. 9th International Conference, IEEE, **(2008)**.
[27] C. E. Shannon, "Communication theory of secrecy systems", Bell system technical journal, vol. 28, no. 4, **(1949)**, pp. 656-715.

Authors

Gulshan Saleem,
MS- Software Engineering,
Department of Computer Engineering,
College of Electrical and Mechanical Engineering,
National University of Science and Technology Islamabad, Pakistan.

Nisar Ahmed
PhD Scholar,
Department of Computer Engineering,
University of Engineering and Technology, Lahore, Pakistan.

Hassan Khalid
MS Student,
Department of Electrical Engineering,
University of Engineering and Technology, Lahore, Pakistan.