The Nucleus ***52****, No. 2 (2015) 71-78*

www.thenucleuspak.org.pk

The Nucleus

ISSN 0029-5698 (Print)
ISSN 2306-6539 (Online)

A Novel Image Encryption Scheme Based on Orthogonal Vectors

N. Ahmed[1], Y. Saleem[1]*, H. A. Habib[2], S. M. Afzal[1] and S. K. Khurshid[1]

[1]*Department of Computer Science and Engineering, University of Engineering and Technology, Lahore, Pakistan*

[2]*Department of Computer Engineering, University of Engineering and Technology, Taxila, Pakistan*

*nisarahmedrana@yahoo.com,*ysaleem@gmail.com*

ARTICLE INFO

Article history:
Received :15 October, 2014
Revised : 30 April, 2015
Accepted :04 June, 2015

Keywords:
image encryption
orthogonal vectors
color images and cryptographic security

ABSTRACT

Image is an important utility of daily life. Use of internet and transmission of digital media over insecure channel such as broadcasting and unicasting through satellite pose a threat to security. Therefore, a novel encryption scheme is proposed for color images with the ability to tolerate noise and JPEG compressed. The algorithm operates in two phases. First phase is a transposition cipher that transposes the position of each pixel. The second phase uses orthogonal vectors for further processing in frequency domain to produce the cipher image. The tri-color image is separated into three channels and at the end, fused to produce the RGB cipher image. Due to the use of orthogonal vectors, it develops tolerance towards compression and channel noise. Experimental test are performed on a reasonable dataset of images to prove cryptographic security. The recovered image is tested based on a performance metric of image quality. The cryptographic analysis and performance evaluation has shown tolerance to noise and compression with adequate cryptographic security.

1. Introduction

Increasing growth of multimedia applications has created a need for security of multimedia information for storage and transmission. For security of multimedia information, two major technologies are used: encryption and digital watermarking. Image encryption techniques transform an image into a new image with no information and usability without the secret key. The encrypted image is called cipher text image. The original image without encryption is called plaintext image. Decryption is the process to obtain the plaintext image back from the cipher text image, usually with the help of secret key. Digital watermarking, on the other hand, does not change the original image. It is the process of hiding information into digital multimedia data for authentication and protection from manipulation or illegal copying. Watermarked information can be extracted for a range of purposes including authentication, control and copy prevention [1]. The watermark can be either visible or invisible, depending on the application.

Encryption algorithms are divided in two categories based on secret key naming symmetric-key and public-key [2]. In symmetric key cipher, the secret key is same for the process of encryption and decryption. Whereas in public-key cipher, secret key for encryption and decryption are different and are not related to each other [2]. The key for encryption is made public so anyone can encrypt an image but only intended recipient can decipher the image with private key. A large number of algorithms are proposed to achieve this objective. Image encryption algorithms are broadly classified into three categories based on their working principle[2]:

- Transposition based
- Value transformation based
- Visual transformation based

Transposition based cipher work on image pixels and change the position held by pixels with a complex regular system. Several techniques [3-6] based on transposition based cipher are presented in literature.

Digital images contain high redundancy and require some type of compression to reduce their size. An anticipated image encryption scheme must provide reduction in image size or ability to be compressed after encryption. Unfortunately, this property is not possessed by various image encryption schemes. Moreover, during wireless communication, there is a high possibility to corruption of some image pixels due to noisy channels. An image encryption scheme that is very sensitive to the cipher image would be unable to tolerate channel noise or any type of compression.

M. Prasad et al. [3] presented a chaos based transposition cipher. Chaotic system is highly random and unpredictable and they have utilized this property of chaotic system for scrambling. They scrambled the data based on random features obtained from chaotic map. An analysis of two different chaotic maps are also performed

[*] Corresponding author

and the one with superior performance is opted. Performance analysis is performed on the basis of correlation coefficient analysis and key sensitivity test.

YU [4] presented a chaos based image encryption scheme, which use hyper-chaotic sequence for randomness. They have performed encryption in two steps, one is the scrambling of image pixels and the second is transposition of grayscale value. Statistical test are performed to show the superiority of randomness of proposed hyper-chaotic system. Statistical, differential and key space & sensitivity test are performed to check the performance of the scheme.

Kester [5] also proposed a transposition based image cipher. The algorithm separate three RGB layers and convert them to a 1-dimensional array. These three arrays are combined to make a three-row matrix of elements n. After taking transpose of this matrix, it is converted to a 1-dimensional array. Then first $\frac{n}{3}$ elements of this array are arranged into original image dimension and assigned to R component of RGB image. Similarly next $\frac{n}{3}$ elements are assigned to G and leftover $\frac{n}{3}$ elements are assigned to B. These three RGB layers are combined to obtain an RGB image. RGB graph of encrypted images are shown to demonstrate performance.

Value transformation based ciphers modify the grayscale value of pixels to encrypt an image. Transposition only cipher are not secure enough to withstand statistical and differential attacks. Work of [7-9] has presented work based on value transformation or a hybrid of transposition and value transformation.

Sam et al. [7] presented an image cipher using the combination of manifold techniques. First part performs pixel permutation to achieve transposition. Second part performs block cipher based encryption using a 32 bit register. In third part, the resultant values are XORedwith chaotic key generated using transformed logistic maps. The proposed cipher encrypts the bits of image rather than pixels, making it a value transformation based cipher. Statistical, differential and time complexity is tested to demonstrate the performance of the cipher. Moreover, results of information entropy analysis are close to ideal values depicting trivial leakage of information.

He et al. [8] proposed an image cipher based on spatiotemporal chaos system specifically for colored images. One-way coupled map lattices (OCML) are used for generation of random sequence. The pseudorandom sequence chosen for encryption is highly sensitive to initial condition as it is taken by randomly iterating chaotic map for several times. Statistical, differential, entropy, time complexity and key sensitivity test are performed to demonstrate the performance of the proposed cipher.

Kwok et al. [9] have presented a chaos based image encryption scheme. The core of the algorithm is a key-stream generator based on cascade of chaotic maps. The rest of the working of algorithm is same as [8] but has superior performance with respect to speed and cryptographic security.

Visual transformation based schemes encrypt the images in such a way that mechanical operation is required for decryption. Moni Naor and Adi Shamir [10] has provided best known technique. Normally several shares are generated which may be combined digitally in certain way to obtain decrypted image.

Shahed et al. [11] presented a wavelet based image encryption technique. The algorithm encrypts four images in a single image of same dimension. In first step, Images are resized to a suitable square image and sub-band LL1 of wavelet transform of each image is computed. A new transposition image is created with dimension equal to original input image and block of pixels from all these images are copied to it according to user-defined sequence. Then zigzag pattern is used to convert a key image to a row vector that is further reshaped to a square image. This key image is then XORed with the transposed image to obtain compressed encrypted image. Correlation coefficient analysis, encryption speed, compression ratio are tested to demonstrate the performance. The cryptographic security is claimed to be enough but not fully secure.

Tedmori et al. [12] has presented a visual cryptography scheme, which operates in frequency domain (DCT). Input plaintext image is transformed to frequency domain using DCT and DC value is scattered to all the frequencies using a reversible weighting factor. Then each frequency is shuffled and their signs are reversed before transformation to spatial domain. Objective and subjective quality assessment test demonstrated high similarity in original and recovered images.

Lee et al. [13] presented a novel visual image encryption techniques based on Interferometer. The technique is designed for binary images, which divides the image into number of slides and they are further XORed with a random key. Their propose phase assignment rule is used to create phase mask for each slide. Mach-Zehnder interferometer is used in the decryption process to recover the original image by using phase mask.

Our proposed algorithm is a hybrid of transposition and value transformation methods. Transposition phase permute fixed size blocks to obtain a scrambled image. In value transformation phase, the image is processed in frequency domain with orthogonal vectors and resultant matrix is transformed to spatial domain. Scaling of image pixels is performed to obtain cipher image with good visual degradation and cryptographic security. The proposed schemes posses the ability to be compressed by JPEG and tolerate some amount of noise as well. The organization of paper is as follows. Section 2 explains the proposed algorithm. Section 3 presents some experimental results. In section 4, a discussion is made on the experimental results and analysis. The paper is concluded in section 5 along with some future work recommendation.

2. Proposed Technique

2.1 Encryption Algorithm

The input plaintext image should be square image. Zero padding can be used to make non-square image to a square image. Square image is required because the orthogonal matrix generated by singular value decomposition is also a square. SVD is the primal method which disintegrate $m \times n$ matrix φ and generates three matrices$U$, Σ and V^T such that$\varphi = U\Sigma V^T$. The matrix $\varphi$is generated through a secret key, which makes the proposed scheme a private key encryption scheme. Umatrix is a $m \times n$orthogonal matrix with column known as left singular vectors. Matrix V is a$n \times n$ orthogonal matrix with columns known as right singular vectors. Σ is a $m \times n$ diagonal matrix with diagonal singular values arranged in descending order. Once U or $V$are obtained, any of them can be used as matrixφ_i for multiplication with plaintext image.Following are the steps of encryption process.

Input the plain image I_0 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). The use of frequency domain (DCT) provides enhanced confusion.

Initialize an iteration count istarting from zero and going to N – 1.

1. Initialize a secret key k_i.
2. Generate pseudo random permutation sequence σ_i.
3. Perform pixel level permutation using random sequence $\sigma_i$separately on IR, IG and IB.
4. Generate a random vector Δ_0 using random sequence $\sigma_i$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 andI_B, separately.

Repeat step 1-5 for N number of times.

OnceN iterations are performed, inverse DCT of three RGB channel images I_R,I_G and$I_B$is taken separately to obtain spatial domain images.

Perform scaling and quantization of I_R, I_G andI_B with $\max(I) = 255$ and $\min(I) = 0$.

Fuse the three RGB channel images into a single RGB image.

N indicates the number of iteration that are used to repeat the encryption process. More iteration provides improved confusion and hence better encryption at the cost of time.

The similar process is demonstrated by flow chart given in Fig. 1. The three RBG layers follow the process depicted in Fig. 1 separately and they are combined at the end to obtain an encrypted RGB image.

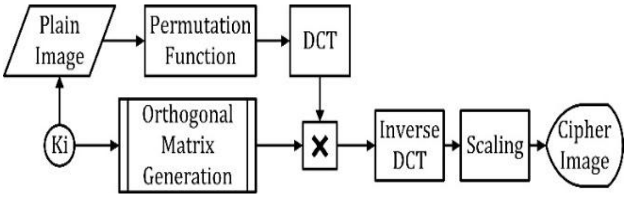

Fig. 1: Flowchart representation of encryption process

2.2 Decryption Algorithm

The decryption process is performed by applying all the transformation of encryption process in opposite order. If there is no distortion during transmission or storage, the received cipher image will be equal to transmitted or stored cipher image. 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 andC_B and take their DCT.

Initialize an iteration count i, which starts from zero and goes uptoN $- 1$

1. Initialize a secret key k_i.
2. Generate pseudo random permutation sequence σ_i.
3. Generate a random vector Δ_0 using random sequence $\sigma_i$of $m \times n$ elements.
4. Generate orthogonal matrix φ_i by using Gram-Schmidt algorithm.
5. Take transpose of matrix φ_i that is equivalent to ${\varphi_i}^{-1}$ in case of orthogonal matrix.
6. Multiply ${\varphi_i}^{-1}$ with C_R,C_G andC_B, separately.
7. Perform inverse pixel level permutation using random sequence $\sigma_i$separately on C_R,C_G andC_B.

Repeat step 1-5 for N number of times.

Once N iterations are performed, inverse DCT of three RGB channel images I_R,I_G and$I_B$is taken separately to obtain spatial domain images.

Perform scaling and quantization of C_R, C_G andC_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 Fig. 2. The three RBG layers follow the process depicted in Fig. 2 separately and they are combined at the end to obtain a decrypted output RGB image.

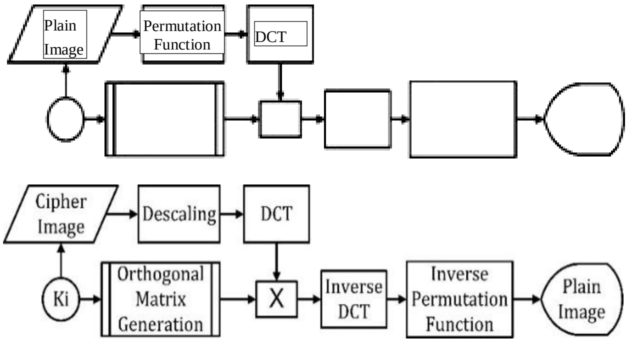

Fig. 2: Flowchart representation of decryption process

It is appropriate to state that the encrypted image is obtained after quantization so the decryption does not produce the exact replica of I_0. The goal of the proposed scheme is to perform image encryption resulting in decent reconstruction of the plain image I_0.

3. Experimental Results

A graphical user interface is designed in MATLAB ® 2010b to easily perform simulation and security analysis experiments for the proposed. 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.

Figs. 3-6(a) contain input plaintext image. The cipher images generated with proposed cipher are shown in Figs. 3-6 (b). The images in Figs. 3-6 (c) are the deciphered image. It is to be noted that deciphered images are not exact copy of input plaintext images. They are though the close approximation of the plaintext images, which are worthy enough for visual inspection. Their performance is demonstrated with performance metric of subsection 4.1.

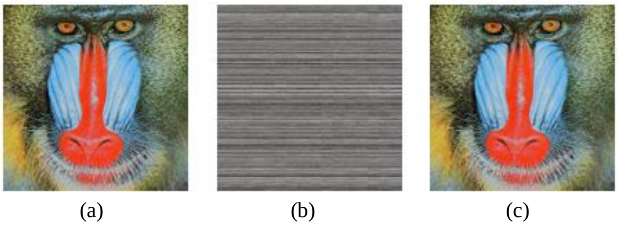

Fig. 3: (a) Plaintext image (Mandrill), (b) Ciphertext Image, (c) Deciphered Image

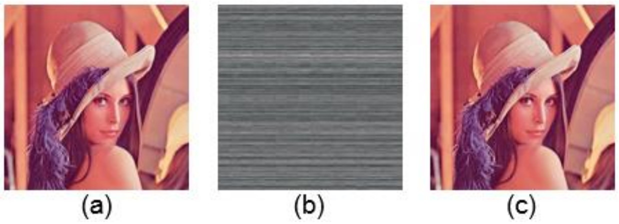

Fig. 4: (a) Plaintext image (Lena), (b) Ciphertext Image, (c) Deciphered Image

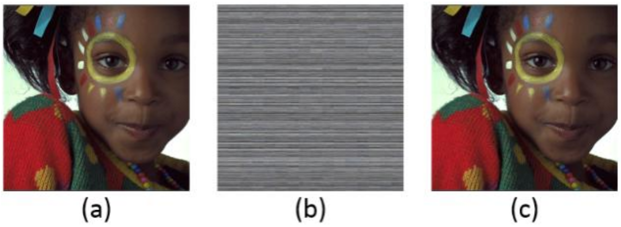

Fig. 5: (a) Plaintext image (Kodim15), (b) Ciphertext Image, (c) Deciphered Image

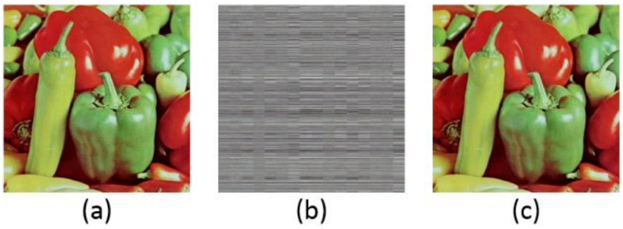

Fig. 6: (a) Plaintext image (Peppers), (b) Ciphertext Image, (c) Deciphered Image

3.1 *Performance Metric of Image Quality*

The proposed scheme recovers the image after deciphering that is not exact replica of input plaintext image as multiplication of orthogonal matrix in frequency domain and scaling result minor distortions. These variations in the recovered image are insignificant and do not affect the visual quality of image significantly. Since, imperceptibility depends on human visual system so perceptibility must be tested on the basis of some evaluation metric. These parameters are explained below. Table 1 provides the result of performance metric for the four test images.

3.1.1 *Euclidean Distance*

Euclidean distance is common distance between two points in a Euclidean space. Following formula can be used to successfully estimate the difference between two images by Euclidean distance.

$$ED(X,X') = \sum_{i=1}^{M}.\sum_{j=1}^{N}[X_{(i,j)} - X'_{(i,j)}]^2 \qquad (1)$$

3.1.2 *Mean Squared Error*

Mean squared error measures the average of the squares of the error in the original image and recovered image. It will provide a numeric value corresponding to the distortion in the recovered image for comparison of performance. Below formula is used to calculate MSE between two images.

$$M.S.E = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}[X_{(i,j)} - X'_{(i,j)}]^2 \qquad (2)$$

Here, X and X' denotes the original and recovered images respectively.

3.1.3 Peak-Signal-to-Noise Ratio

The problem with MSE is its values are strongly dependent on image intensity scaling and PSNR can scales the MSE according to image intensity range to avoid this. Formula for PSNR calculation is given below.

$$PSNR = 10\log_{10}\left(\frac{MAX_i^2}{MSE}\right) \qquad (3)$$

PSNR is an estimate to human view of reproduction quality. In spite of the fact that a higher PSNR shows that the recreation of image is of higher quality, sometimes it may not.

3.1.4 Normalized Correction

Normalized correction is a measure of similarity of two images as a function of a time-lag applied to one of them. Following formula is used to calculate normalized correction for two images.

$$NC(X,X') = \sum_i^M . \sum_j^N \frac{X_{(i,j)} * X'_{(i,j)}}{\sum_i^M . \sum_j^N (X_{(i,j)})^2} \qquad (4)$$

Table 1: Result of performance metric for the four test images

	Mandrill	Lena	Peppers	Kodim15
ED	211573	236643	263543	149804
MSE	0.8071	0.9027	1.0053	0.5715
PSNR	49.0616	48.5753	48.1077	50.5610
NC	0.9999	1.0000	0.9998	1.0006

3.2 Statistical Analysis

Histogram analysis of all four-test images is performed and result of Mandrill and Lena images are provided in Fig. 7&8. Statistical analysis is used to breakdown many kinds of image ciphers. The histogram and correlation of pixels in cipher image provide a clue during the analysis as pointed by Shannon in his classical masterwork [14].The histogram show the scattering of pixel values in the image. In an ideal case, a cipher should produce image with uniform histogram. It prevents the intruder from extraction of any expressive statistics from the histogram of cipher image.

In our case, the histogram is not uniform but is Gaussian for all the three layers of the image. Similar results are obtained for a large set of test images.

Table 2 provides the result of correlation coefficient analysis of a pair of random pixels. It is clear from the analysis that image has high correlation in horizontal direction as it can be seen in the cipher image Fig. 9 (b).As the columns of U are orthonormal basis vectors, their multiplication with cosine transformed image matrix results in this horizontal correlation. Hence, this correlation does not leak information of image, rather it depends on randomly generated matrix Δ_0. However, in vertical and diagonal direction correlation is good for cryptographic security. This correlation does not pose any threat to the security of the algorithm.

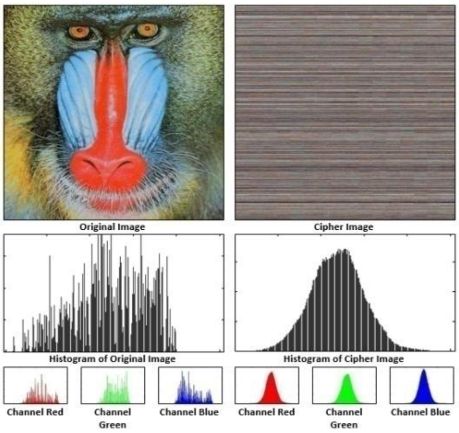

Fig. 7: Histogram Analysis of Mandrill Image

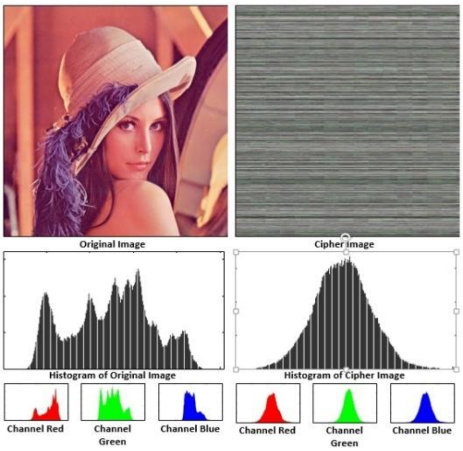

Fig. 8: Histogram Analysis of Lena Image

Correlation coefficient analysis of 10000 pair of random pixels is provided for Mandrill image in diagonal, horizontal and vertical directions. The results are shown in Figs. 9 (a), (b) and (c) respectively.

Table 1: Correlation coefficient analysis of two adjacent pixel: Mandrill Image

Direction of Adjacent Pixels	Plain Image	Cipher Image
Diagonal	0.9859	0.0323
Vertical	0.9921	0.0090
Horizontal	0.9721	0. 9825

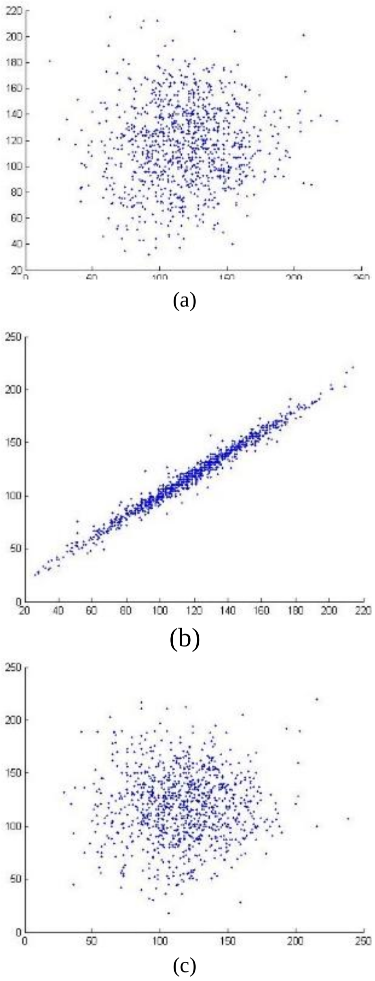

Fig. 9: Correlation coefficient analysis of Mandrill Image (a) correlation between diagonally adjacent pixels (b) correlation between horizontally adjacent pixels (c) correlation between vertically adjacent pixels

3.3 *Key Space Analysis*

Key space analysis is performed to check the strength of an encryption scheme against brute force attacks. A decent image encryption scheme must have high sensitivity to cipher key and large enough key space.

3.3.1 *Exhaustive Key Search*

Key size is the number of possible distinct cipher keys. A key space must be large enough to make exhaustive key search practically infeasible. The proposed encryption scheme has 128 bits key which means it requires 2^{128} number of operations to check for all the keys. This is a large enough key space size to resist brute-force attacks.

3.3.2 *Key Sensitivity Test*

Key sensitivity demonstrates the dependence of encryption scheme on cipher key. It can be tested in two different aspects; (i) 1-bit change in cipher key must produce entirely different cipher image, (ii) 1-bit change in cipher key must decrypt an entirely random image. Fig. x demonstrate the results of key sensitivity test for Mandrill image.

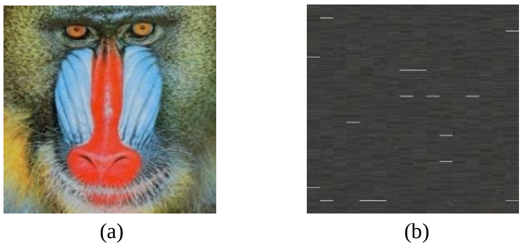

Fig. 10: Key Sensitivity test for Mandrill Image; (a) Plaintext Mandrill Image (b) decrypted image with 1-bit changed cipher key

3.3 *Tolerance to Noise and Compression*

Compression of digital images is highly desirable in field of image cryptography. It reduces the bandwidth requirement in wireless communication and in storage. Lossy compression is a type of compression, which removes the data that is not of much importance in visual inspection. Lossy compression hence introduces small variation in cipher image and result in improper decryption. The proposed algorithm reconstructs the original image in DCT domain so it preserves much of the useful image data. Moreover, the horizontal correlation in cipher image results in huge compression ratio and make it a suitable candidate for compression tolerant image encryption scheme. Fig. 11 provides the result of JPEG compressed image (90% quality factor) and its reconstructed image.

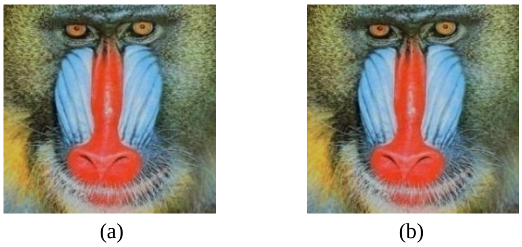

Fig. 11: Results of JPEG Compression; (a) Plain Image (Mandrill) (b) decrypted image from JPEG compressed cipher image (quality factor 90%)

Moreover, the algorithm is also robust to small variation due to channel noise and provides very good reconstruction of image as shown in Fig. 12.

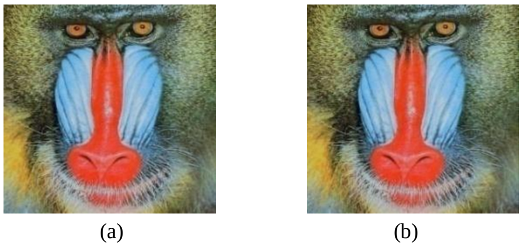

Fig. 12: Results of Noise; (a) Plain Image (Mandrill) (b) decrypted image from noisy cipher image (mean 0, variance 0.01)

4. Discussion

This research was intended to develop an image encryption scheme with tolerance to noise and compression. Security of multimedia content is an essential for transmission or storage in insecure media. The algorithm is simple and secure and has all the characteristics of a good image cipher. It is a hybrid of two popular image encryption categories naming; transposition cipher and value transformation cipher. The study is further continued to develop a comprehensive benchmark to test an image encryption scheme. Moreover, the application of the same technique on video and audio data is also performed and is waiting for its performance analysis and security evaluation.

In terms of performance, metric of image quality the proposed system outperforms on the image cipher does not recover the exact input image [10, 13]. Results of Table 1 provide the image quality recovered by the proposed scheme. ED of the four test images is provided which shows the recovered image is 0.394% to 0.224% different from the original image. The values of MSE and PSNR indicated the mean square value of the difference in recovered image from that of original image. The value of MSE depends upon the intensity range of the image whereas PSNR scales the intensity values. The acceptable value of PSNR is usually >25-30dB [15-16]. Image with PSNR >/30dB is indistinguishable by human eye. The theoretical maximum value of PSNR is 60dB however, 50dB is considered more than enough and the proposed algorithm has provided reconstruction close to 50dB. Normalized correction is another parameter for the measurement of similarity between two images and its results are very close to unity, indicating high similarity.

Statistical analysis is provided in terms of histogram and correlation coefficient analysis. Only [3,4,8,9] have provided the results of statistical analysis. Algorithms proposed by [4,9] has good results for histogram analysis and horizontal, vertical and diagonal correlation between adjacent pixels. In [3,8], results of correlation are good but they have not performed directional correlation analysis. Moreover, [3] have provided RGB intensity plots in place of histogram analysis. Histogram analysis of [8] is not spread to complete range but rather lies between100-250. Whereas, [5] has provided results of only RGB graph.

The proposed scheme has good characteristics concerning statistical analysis. Table 2 and Figs. 9-11 provides the results of correlation coefficient analysis which are good in vertical and diagonal directions and there is high correlation in horizontal direction. The horizontal correlation in the image is due to orthogonal vectors and is not related to image correlation. This does not leak out any information for analysis or attack as the orthogonal vectors are generated through SVD (using Gram Schmidt algorithm) from random sequence. The security of the orthogonal vectors depends on the random sequence, which is generated based on secret key.

The results of histogram of proposed scheme are Gaussian rather than the required uniform so the histogram does not reveal any information of plain image. This is again due to random vectors and the Gaussian shape due to central limit theorem. A range of different images is tested and obtained results are similar which indicate there is no relation in histogram of cipher image and plaintext image. The algorithm is cryptographically secure and does not pose any threat to the security of image. Moreover, the horizontal correlation can be used as a favorable feature in lossy compression and run length coding (lossless compression) which is a desired property in JPEG compression as it reduces the size of cipher image, by many folds. The same is demonstrated in section 3.4. Compression cannot be applied on completely uncorrelated image as it will result in increased in size because there is no room for compression.

5. 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 then unqualified security. The proposed algorithm performs position encryption as well as gray value encryption simultaneously. The experimental results demonstrate that the algorithm provide good visual degradation, tenability and cryptographic efficiency.

Although the proposed scheme is designed for digital images but it can be successfully used for encryption of audio and other multimedia data. The future directions to improve this work are provided below:

1. Implementation of the proposed technique on audio and other multimedia data
2. JPEG compression testing and performance compression with other compressible image encryption schemes
3. Incorporation of the proposed scheme after DCT step of JPEG compression to develop a secure compression algorithm.

References

[1] D. H. Brainard, D. G. Pelli and T. Robson, "Display characterization", Encyclopedia of imaging science and technology, pp. 172-188, 2002.

[2] W. Stallings, “Cryptography and network security: principles and practice”, Prentice Hall, 2010.

[3] P. Manjunath and K. L. Sudha, "Chaos image encryption using pixel shuffling", Computer Science & Information Technology (CS & IT) CCSEA, pp. 169-179, 2011.

[4] Y. Ming-yang, "Image encryption based on improved chaotic sequences", Journal of Multimedia, vol. 8, no. 6, p. 802-808, 2013.

[5] K. Quist-Aphetsi, "Image encryption based on the RGB PIXEL transposition and shuffling", International Journal of Computer Network and Information Security (IJCNIS), vol. 5, no. 7,p. 43-50, 2013.

[6] R. Pratyaksha, "Chaos image encryption using transposition and pixel shuffling", International Journal of Innovations in Engineering and Technology, vol. 4, no. 4, p. 259-265, December 2014.

[7] S.I. Shatheesh, P. Devaraj and R. S. Bhuvaneswaran, "Transformed logistic block cipher scheme for image encryption", Advances in Networks and Communications, Springer Berlin Heidelberg, pp. 70-78, 2011.

[8] H. Jun, Z. Li, and H. Qian, "Cryptography based on spatiotemporal chaos system and multiple maps", Journal of Software, vol. 5, no. 4, pp.421-428, 2010.

[9] H. S. Kwok and K. T. Wallace, "A fast image encryption system based on chaotic maps with finite precision representation", Chaos, Solitons & Fractals,vol. 32, no.4, pp.1518-1529, 2007.

[10] N. Moni and A. Shamir, "Visual cryptography", Advances in Cryptology—EUROCRYPT94. Springer Berlin Heidelberg, 1995.

[11] Shahed, A. Maytham, "Wavelet based fast technique for images encryption", Basrah Journal of Science, vol. 25, no. 2, pp. 126-141, 2007.

[12] T. Sara and Nijad Al-Najdawi, "Lossless image cryptography algorithm based on discrete cosine transform", International Arab Journal of Information Technology, vol. 9, no. 5, pp.471-478, 2012.

[13] L. Sang-Su et al., "Visual cryptography based on an interferometric encryption technique", ETRI Journal, vol. 24, no. 5, pp. 373-380, 2002.

[14] C.E.Shannon, “Communication theory of secrecy systems” Bell System Technical Journal, vol. 28, no.4, pp. 656-715, 1949.

[15] Welstead and T. Stephen, “Fractal and wavelet image compression techniques” Bellingham, WA: SPIE Optical Engineering Press, 1999.

[16] T. Nikolaos, V. Boulgouris and M. G. Strintzis, "Optimized transmission of JPEG2000 streams over wireless channels", IEEE Transactions on Image Processing, vol. 15, no.1 pp. 54-67, 2006.