ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

Encryption of RGB image using Arnold transform and involutory matrices

Anand Joshi[1], Maneesha Kumari[2]

Department of Mathematics, Dayalbagh Educational Institute, Agra, India[1,2]

Abstract: The security of image has become an important topic in the process of storage of an image and transmission of image over an unsecured channel such as internet. This paper proposes a new approach for colour image encryption and decryption using involuntary matrix associated with Arnold transformation. In this paper computer simulation with standard examples and the experimental results are given to support the robustness of the scheme. Sensitivity analysis and a comparison between earlier proposed techniques with our proposed approach is also given in this paper.

Keywords: Colour image encryption, Colour image decryption, involutory matrix, Arnold transforms, cryptosystem.

I. INTRODUCTION

With the fast development of computer network technology, it is so easy to obtain digital images through network and further use, process, reproduce and distribute them. The fascinating developments in digital image processing and network communications during the past decade have created a great demand for secure image transmission over the internet and through wire-less networks. Digital technology brings us much convenience, but it also gives attacker or illegal user an opportunity. Image data are highly sensitive and prone to decode abruptly by intruders. Several methods have been proposed to transfer image data securely in the world such as: digital techniques, network and communication technologies. These images are used in various areas for instance: commercial purpose, online education and training, military services, research and experimental purpose; in all these areas, maintaining the fidelity and confidentiality of original image data is a critical issue. So, the security of image data over an insecure network is a major issue.

To meet this challenge, a variety of encryption schemes have been pro- posed. In [2] authors developed the technique for RGB image security using random matrix affine cipher (RMAC) and Discrete Wavelet Transformation (DWT). In this [2] approach the encryption and decryption process is based on Two Stage Random Hill Cipher (TSRHC) over SLn(F) allied with Discrete Wavelet Transformation (DWT) to ensure secure transmission of colour image data. In [4, 5] authors have proposed image encryption and decryption using Fourier transformation, in [6,8] security of image data using gyrator transform domain combined with other different techniques is given, in [11] image encryption using Hartley transform is developed, in [12, 13] image coding by wavelet transform is given, and RGB image encryption and decryption based on the affine transform in gyrator domain is given by H. Chen et al. in [15]. In [16] some attacks like known-plaintext attack, chosen-plaintext attack, and chosen cipher text attack, etc. are discussed for the RGB images. In the approach of RGB image data encryption using random hill cipher (RHC) associated with discrete wavelet transform (DWT) is liberated to the known-plaintext attack and chosen cipher text attack, etc. This technique is appropriate for secure transmission of large size images. The paper [17] describes for a RGB image encrypted using hill cipher and discrete wavelet transformation. Here in this paper we consider keys arrangement of involutory matrices, and position (pre or post) of multiplication of keys with image data associated with the Arnold transformation. For security these parameters are highly sensitive. In the proposed approach we divide the original image into equal block sizes such that block sizes (order of sub images) must be same as size (order) of hill cipher keys and the hill cipher keys are selected from the set of involutory matrices.

Hill cipher [1] is one of the most well-known techniques for encryption and decryption of text data. But proposed Random Hill Cipher (RHC) is specifically for RGB images presented in matrix and the hill cipher keys are chooses from the set of involuntary matrices associated with the Arnold cat mapping. Since the matrix multiplication is non-commutative therefore the multiplication of hill cipher keys with RGB image depends on pre or post multiplication of random key matrices. The random hill key arrangement should also be known to correctly decrypt the encrypted RGB image. First, random hill cipher applied on each R, G, and B channels of a color image data, which are divided in different blocks, before Arnold transformation. Experimental results, security analysis, and comparison between proposed technique with [18, 19] is given in support for stalwartness an immenseness of the proposed approach.

II. ORGANIZATION OF PAPER

In section 2, we explain about the random Hill cipher and Arnold transformation. This section also describes the ideas and organization of the proposed approach. In section 3, the method used in this paper for colour image data encryption and decryption is presented. This section also discuss about the keys uses and arrangement of random hill cipher (RHC) for the proposed scheme and

DOI 10.17148/IJARCCE.2015.49108

about the keys generation 3.1. Demonstration of the procedure for image encryption and decryption is mentioned in section 4. In section 5 the sensitivity analysis of the proposed is given to show the robustness of the proposed method. In section 6, the analysis of some statistical measure such as mean square error (MSE), peak signal to noise ratio (PSNR), correlation, and histogram of pixels are given for the stalwartness and security analysis of the proposed approach is discussed. The Comparison between proposed techniques with other various related scheme is also given in section. In Section 7, we draw a conclusion of this paper.

III. RANDOM HILL CIPHER AND ARNOLD TRANSFORM

In the proposed cryptosystem, we have designed the security of RGB images of size m×m by random hill cipher (RHC) and Arnold transform (AT). The matrices used for the hill cipher are the involuntary matrices. The matrix of each channel of RGB image of size m×m is divided into equal blocks of size n × n such that n|m, we call it as block matrix (sub image), the size of sub image is same as the size of the key of random hill cipher, which is defined by the user. In proposed cryptosystem, the multiplicative keys of random hill cipher are chosen from set of involuntary matrices. Suppose the user chooses a type of block matrix (sub image), in which the order of block matrix dose not divide order of original image matrix (n m), then user needs to add some redundant rows or columns or both in the original image matrix.

Formulation for Random Hill Cipher (RHC) of a block matrix (sub image) of size $n \times n$ is given as:

$$C = B \cdot K(\mathrm{mod}\, N), \qquad (1)$$

where, B be a $n \times n$ block matrix (sub image) of the colour image of size $m \times m$, K is a $n \times n$ key matrix from the set of involutory matrices, and C be a cipher block of size $n \times n$. And formulation for inverse Random Hill Cipher (iRHC) of block matrix (sub image) of size $n \times n$ is given as

$$B = C \cdot K(\mathrm{mod\ N}), \qquad (2)$$

Here K is involutory matrix, the inverse of K is K itself. In this method there is no need to find the inverse of matrix $K \cdot N$ be unit representation in single/double. Similarly, the same process is applied for remaining block matrix (sub image) of the original colour image. In equation (2), the position of K is fixed according to the position of K (1), because matrix multiplication is non-commutative (if attacker multiplies K with C (2) without knowing the exact position of K, then original image cannot be recovered correctly).

In this cryptosystem, we have also used discrete Arnold transform or cat map transform [20] to scramble each channel of the RGB image. For the size of $M \times M$ image, the Arnold transform is defined as

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod{\mathrm{M}} \qquad (3)$$

Where $[x, y]^t$ and $[x', y']^t$ represent the position vector of image pixel before and after performing the Arnold transform, respectively.

Now, corresponding to the inverse Arnold transform of Eq. (3) is define as

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} \pmod{\mathrm{M}} \qquad (4)$$

Let A denote the left matrix in the right part of equation(3), $I(x, y)$ and $I(x', y')^{(n)}$ represent pixels in the original image and the encrypted image obtained by performing Arnold transform n times, respectively. Thus, image encryption using n times Arnold transforms can be written as

$$I(x', y')^{(k)} = AI(x, y)^{(k-1)} \pmod{\mathrm{M}} \qquad (5)$$

where $k = 0,1,\ldots,n$ and $I(x', y')^{(0)} = I(x, y)$. One can multiply the inverse matrix of A at each side of equation (5) to obtain $I(x, y)^{(k-1)}$. In other words, the encrypted image can be decrypted by iteratively calculating the following formula n times.

$$I(x, y)^{(k)} = A^{-1} I(x, y)^{(k-1)} \pmod{\mathrm{M}} \qquad (6)$$

IV. ENCRYPTION AND DECRYPTION PROCESS

In this cryptosystem, we design the security of RGB images by random hill cipher (RHC) over the set of involutory matrices associated with Arnold transform (AT). Proposed algorithm is applied on red (R), green (G), and blue (B) channels of an RGB image data in the encryption and decryption process. In the proposed cryptosystem, for encryption first we use hill cipher using involutory matrices on the image and get the partially encrypted image and then use Arnold transform on the partially encrypted image, combining these two keys on the image give the complete encryption. The procedure of encryption algorithm applied on RGB images is represented in the Fig. 1(a) and the procedure of decryption algorithm applied on RGB images is represented in the Fig. 1(b). The matrix of each channel of RGB image of size m×m is divided into equal blocks of size n×n such that n | m, we call it as block matrix (sub image), the size of sub image is same as the size of the key of random hill cipher, which is defined by the user. We applies keys $\mathrm{K}_{1\mathrm{R}}$ for red, $\mathrm{K}_{1\mathrm{G}}$ for green, and $\mathrm{K}_{1\mathrm{B}}$ for blue components of the image for hill cipher, these keys are the matrices and these matrices are from the set of involutory matrices, then Arnold transform (AT) is applied on

DOI 10.17148/IJARCCE.2015.49108

partially encrypted Red (R), Green (G), and Blue (B) components of RGB image. The similar inverse procedure is applied for decryption process which is also delineated in Fig. 4(b). For decryption of image inverse Arnold transform (iAT) is apply on the encrypted RGB image with the same key as used for the encryption and then we choose keys for the inverse random hill cipher (iRHC) for inverse process for different R, G, B component, the keys for the inverse hill cipher is same as the keys for encryption of the image because the matrices used in this process are involutory matrices and Combining these two decryption methods finally original image is recovered. The security of the proposed cryptosystem is based on the size of space of random hill cipher and on the number of times Arnold transformation is applies. The security of the proposed technique not only depends on the keys, but also on the arrangement of RHC parameters and position (pre or post) of keys multiplication with RGB image data, which are highly sensitive.

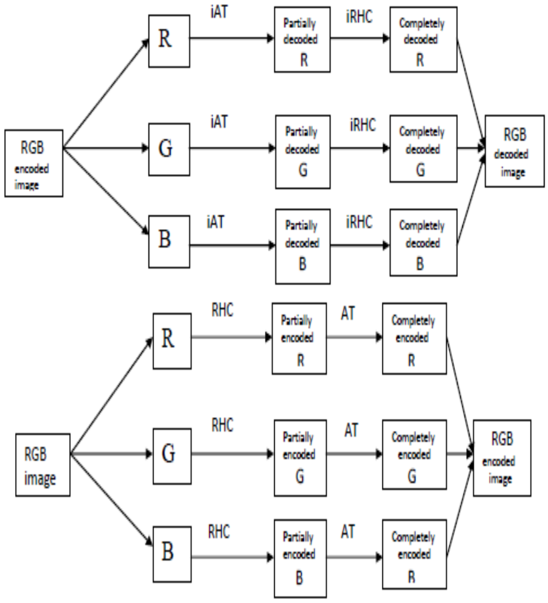

Figure 1: Encryption and decryption procedure for proposed method (a) The upper figure shows the encryption procedure for the RGB image (b) The lower figure shows the decryption procedure for the RGB image

A. Generation of keys

In the proposed method the keys for the hill cipher method is from the set of involutoy matrices. So, the generation of involutory matrices is important. This subsection is related to the generation of keys used in the proposed method. A matrix A is called involutory if $A^2 = I$. The analysis presented here for generation of involutory key matrix is valid for matrix of +ve integers that are the residues of modulo arithmetic of a number is given in the paper [3]. This algorithm can generate *involutory matrices* of order n× n, where n is even.

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & \cdots & a_{nn} \end{bmatrix}$$

be any n × n involutory matrix, where n is even. Let A is partitioned in the form

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$$ and the block matrice A_{11}, A_{12}, A_{21}, A_{22} are each of order $n_{/2} \times n_{/2}$ The algorithm for generation of involutory matrix A is given [3] as follows:

Algorithm

1. Select any arbitrary $n/2 \times n/2$ matrix A_{22}.
2. Obtain $A_{11} = -A_{22}$.
3. take $A_{12} = k(I - A_{11})$ or $k(I + A_{11})$ for k a constant.
4. Then $A_{21} = 1/k(I + A_{11})$ or $1/k(I - A_{11})$.
5. Form the matrix A completely.

Since the inverse of involutory a matrix is A itself, so in decryption method there is no need to find the inverse of matrix. This is the advantage of involutory matrices. The another key in this proposed method is Arnold algorithm, so the key k is any natural number which depends how many times Arnold transformation is applied on the different component of the of the RGB image. So the key space is the combination of key space of both above mentioned methods.

V. DEMONSTRATION OF THE PROCEDURE AND EXPERIMENTAL RESULTS

In this section we are giving the computer simulated results of the proposed method for different images. The figure 1 shows graphically the procedure of RGB image encryption and decryption. Figure 2 shows the experimental results for the Messi colour image of size $256 \times 256 \times 3$. Figure 3 shows the results for the lena colour image of size $256 \times 256 \times 3$. The proposed method is applied for the RGB image on different components red(R),Green(G), Blue(B)of colours. We take colour images of Messi and Lena of size 256 $\times 256 \times 3$ and apply the hill cipher method on the images using the involutory matrix by dividing the colour image in different blocks. The involutory matrix is generated by the method describe in the subsection 3.1. The computer simulated results of the encryption and decryption are shown in the figure 1.3. The figures 2 and 3 are divided into six parts (a), (b), (c), (d), (e), (f).The image encryption process of the image is as follows:(a) original image (b) image after random hill cipher encryption using involutory matrices (c) completely encrypted image after hill cipher and Arnold transformation. The second part of figures 2 and 3 of the figures show the computer simulated results of the decryption of images. The image decryption process of the encrypted image is as follows: (d) completely encrypted image as get from the encryption process (e) partially decrypted image after using the inverse Arnold transform (f) completely decrypted image after using inverse Arnold transformation and inverse hill transformation. Here for the Messi and Lena figures the Arnold transformation is applied on the images 8 times, so the value of key for the Arnold transformation is the number of times Arnold transformation is applied. We have tested this new approach on a number of images to check the robustness of the procedure but here we are showing the results related to the Messi and Lena images.

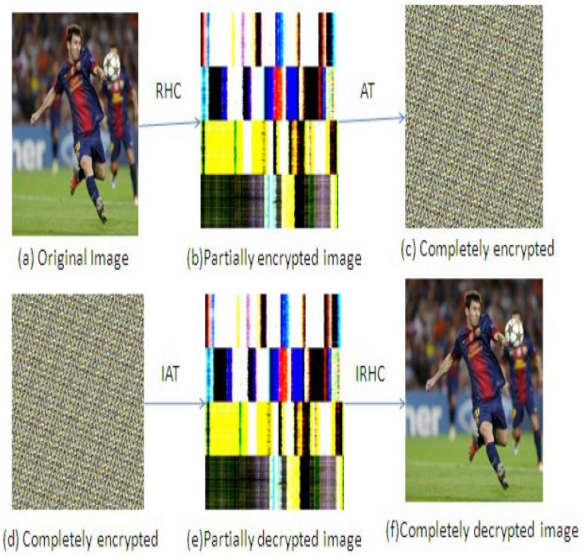
RHC
AT
(a) Original Image
(b)Partially encrypted image
(c) Completely encrypted
IAT
IRHC
(d) Completely encrypted
(e)Partially decrypted image
(f)Completely decrypted image

Figure 2: Results (Exact keys and correct arrangement of RHC parameters):
(a)Original Messi image of size 256×256×3 pixels; (b) encrypted image using involutory matrix; (c) completely encrypted image (d) completely encrypted image (e) partially decrypted image (f) completely decrypted image.

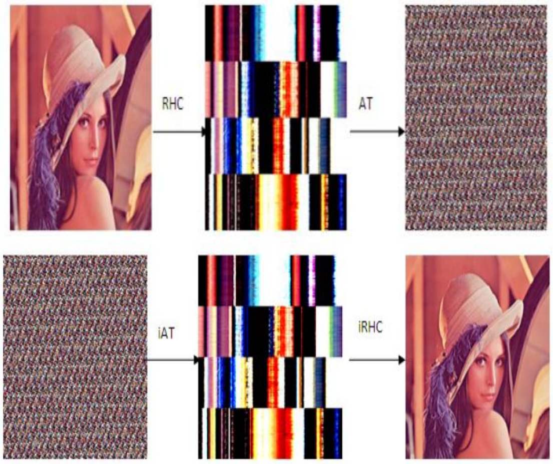

Figure 3: Results (Exact keys and correct arrangement of RHC parameters)
(a)Original Lena image of size 256×256×3 pixels;(b) encrypted image using involutory matrix; (c)completely encrypted image (d) completely encrypted image (e) partially decrypted image (f) completely decrypted image.

VI. SENSITIVITY ANALYSIS OF PROPOSED METHOD

The proposed method for RGB image encryption and decryption should be sensitive with respect to the parameters used for security. High sensitivity is required for unbreakable cryptosystem, i.e., the encrypted colour image cannot be decrypted correctly even though the exact parameters are slight changed. Images shown in the figure 4 are (a), (b), (c) respectively. Figure 4(a) is the completely encrypted Lena colour image of size 256 × 256×3, figure 4(b) and 4(c) are the decrypted image of the completely decrypted Lena image but slight changes in the parameters. Figure 4(a) is encrypted colour image of Lena, figure 4(b) is decrypted colour image with correct arrangement of Arnold transform parameter but slight changes in other parameter, and figure 4(c) is decrypted colour image with correct arrangement of random hill cipher but slight change in Arnold transform parameter. Similarly, the images shown in the figure 5 are (a), (b), (c) respectively. Figure 5(a) is the completely encrypted Messi colour image of size 256×256×3, figure 5(b) and5(c) are the decrypted image of the completely decrypted Messi image but slight changes in the parameters. These experimental results shows that the decrypted figures are totally different from the original figure, which shows that if slight changes are made in the parameters then the original image cannot be, recover from the decrypted image. The sensitivity analysis of the proposed cryptosystem shows that the technique used by us is highly sensitive to the parameters used for the security.

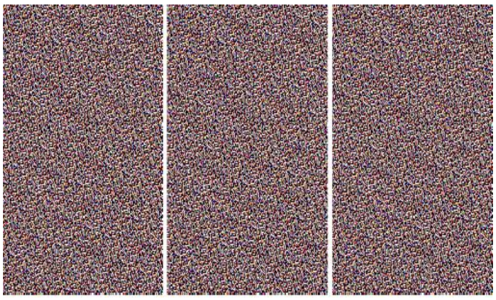

Figure 4: Sensitivity analysis:(a) encrypted colour image of Lena; (b) decrypted colour image with correct arrangement of Arnold transform parameter but slight changes in other parameter (c) decrypted colour image with correct arrangement of random hill cipher but slight change in Arnold transform parameter

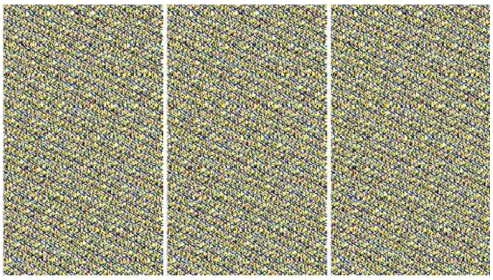

Figure 5: Sensitivity analysis:(a) encrypted colour image of Messi; (b) decrypted colour image with correct arrangement of Arnold transform parameter but slight changes in other parameter (c) decrypted colour image with correct arrangement of random hill cipher but slight change in Arnold transform parameter

VII. SENSITIVITY ANALYSIS OF PROPOSED METHOD

In this section we give the security analysis of the proposed method, statistical analysis of the proposed

DOI 10.17148/IJARCCE.2015.49108

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

method and comparison of the proposed method with the other methods. Hill cipher method is linear, so susceptible to known plain text attack. To avoid this attack we are using Hill cipher involving multiple key generation schemes, instead of single involutory matrix. The matrix of each channel of RGB image of size m×m is divided into equal blocks of size n×n such that n|m, we call it as block matrix (sub image), the size of sub image is same as the size of the key of random hill cipher, which is defined by the user. Suppose the user chooses a type of block matrix (sub image), in which the order of block matrix dose not divide order of original image matrix (n|m), and then user needs to add some redundant rows or columns or both in the original image matrix. If the pixel values are identical or very close, then after encryption they map to very close values or same values as before encryption in case of equal intensity values. To avoid this difficulty we are using Arnold chaotic mapping.

The commonly used measures for comparing the original image and modified image are Mean-Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) and correlation. The mean-squared error (MSE) between two images $g(x,y)$ and $g(\hat{x},y)$ is

$$MSE = 1/MN\sum_{i=0}^{m}\sum_{j=0}^{n}\left[g(m,n)-\hat{g}(m,n)\right]^2$$

Here MN is the size of the images.
The other measure is Peak Signal-to-Noise Ratio (PSNR) which is given by the following formula:

$$PSNR = -10\log_{10} MSE/s^2$$

where S is the maximum pixel value. PSNR is measured in decibels (dB). The mean square error (MSE) and PSNR of the different red, green and blue components of the Messi and Lena colour image original image and encrypted image are shown in the tables 1 and 2 respectively.

Table I: Messi original colour image and encrypted Messi image of size 256×256×3 pixels

Messi Image	RED	GREEN	BLUE
MSE PSNR	1.7912 e +004 5.6333	1.8924e+004 5.3947	2.0065e+004 5.1404a

Table II: Lena original colour image and encrypted Lena image of size 256×256×3 pixels

Lena Image	RED	Green	Blue
MSE PSNR	1.8447e+004 5.5055	1.7099e+004 5.8350	1.5127e+004 6.3673

The high MSE and low PSNR values indicate that the original image data is completely changed. Therefore, no information about the original image can be obtained from encrypted image without knowing the exact keys and the correct arrangement of Arnold transform parameters. The figure 6 shows the correlation of the vertical, diagonal and horizontal pixels of the original and encrypted Messi images. The correlation graph show that there is a high correlation in pixels of original image which are shown in the left portion of the figure 6 and there is very low correlation of pixels in the encrypted image which are shown in the right portion of the figure 6. Similar results are shown for the Lena colour image in figure 7.

Histogram analysis of the original image and completely encrypted is also given in the figure 8. Figure 8(a) is the histogram of the red, green and blue components of the original Messi image figure 8(b) is the histogram of the red, green and blue components of the completely encrypted Messi image figure 8(c) is the histogram of the red, green and blue components original Lena image and figure 8(d) is the histogram of the red, green and blue component completely encrypted Lena image. The histogram of the original image is totally different from the histogram of encrypted image.

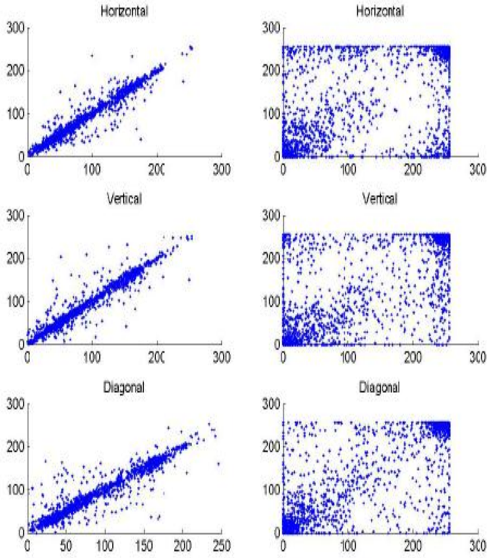

Figure 6: correlation of vertical, diagonal and horizontal pixels of the original Messi image and encrypted Messi image of size 256×256×3 pixels

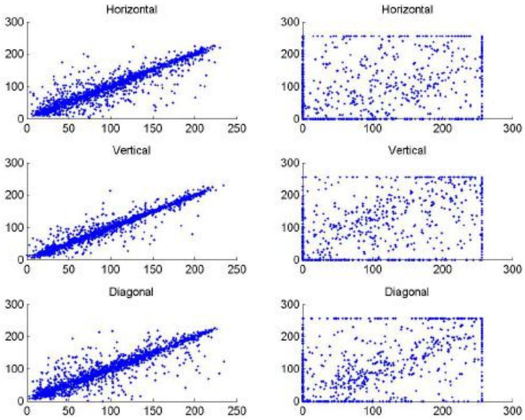

Figure 7: correlation of vertical, diagonal and horizontal pixels of the original Lena image and encrypted Lena image of size 256×256×3 pixels Comparison of these

DOI 10.17148/IJARCCE.2015.49108

histogram shows that encrypted image is completely different from the original image.

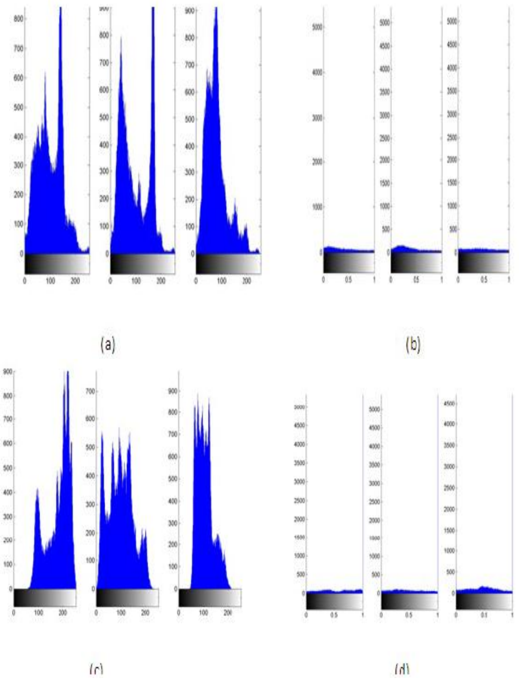

Figure 8: (a) histogram of original Messi image of size 256×256×3 pixels (b) histogram of completely encrypted Messi of size 256×256×3 pixels (c) histogram of original Lena image of size 256×256×3 pixels(d) histogram of completely encrypted Lena image of size 256×256×3 pixels.

The comparison of proposed method with the other existing methods is given in the table 3. The papers [18] and [19] consider self-invertible matrix for hill cipher key. But proposed Random Hill Cipher (RHC) is specifically for images presented in matrix and the hill cipher keys are chooses from the set of involutory matrices associated with the Arnold cat mapping. The key space of our proposed method not only depends on the set of involutory matrices but also on the arrangement of Arnold transformation. So, our propose method is better than the method describe in the [18] and [19].

Table III: Comparison of our approach with authors [18] and [19]

S.no.	Authors	Our approach
1	They have considered only keys for image security	We have considered keys an arrangements of random hill cipher parameters
2	Security of image depends only on the key of hell cipher	Security of image depends on the involuntary matrix key and the Arnold cat map key
3	If attacker knows about all exact keys then original image can be recovered	If attacker knows all exact keys but no information about the correct arrangement of RHC then original image cannot be recovered
4	No discussion about sensitivity analysis	Sensitivity analysis of every parameters is discussed

VIII. CONCLUSION

In this paper we have presented a novel approach of RGB image encryption and decryption. We have demonstrated the encryption and decryption procedure for the proposed method. The security analysis and sensitivity analysis of the proposed method is also discussed in this paper, sensitivity analysis shows that the proposed method is highly sensitive to the parameters used for the security. We have compared our proposed method with the some other existing methods and shown that our method is better than these methods. So, this method would have largely potential usage in digital RGB image processing and security of image data.

REFERENCES

[1] Stallings W. Cryptography and Network Security,Prentice Hall, New Jersey 2006.

[2] Kumar M, Mishra D C, Sharma R K. A first approach of an RGB image encryption. Opt Lasers Eng; 52:27-34, 2014.

[3] Bibhudendra Acharya, G.S.Rath,S.K.Patra, S.k.Panigrahy. Novel method of generatin self invertible matrix for hill cipher algorithm. Int. Journal of security; 1(1):14-21, 2007.

[4] Sui L, Gao B. Single-channel color image encryption based on iterative fractional Fourier transform and chaos. Optics & Laser Technology; 48:117-27, 2013.15

[5] Liu Z, Liu S. Random fractional Fourier transform. Opt Lett ; 32:2088-90, 2007.

[6] Abuturab MR. Color image security system based on discrete Hartley transform in gyrator transform domain. Opt Lasers Eng; 51:317-24, 2013.

[7] Abuturab MR. Securing color information using Arnold transform in gyrator transform domain. Opt Lasers Eng; 50:772-9, 2012.

[8] Singh N, Sinha A. Gyrator transform-based optical image encryption, using chaos. Opt Laser Eng; 47:539-46, 2009.

[9] Liu Z, Xu L, Liu T, Chen H, Li P, Lin C, Liu S. Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains. Opt Commun; 284: 123-8, 2011.

[10] Chen L, Zhao D. Color image encoding in dual fractional Fourier-wavelet domain with random phases. Opt Commun; 282:3433-8, 2009.

[11] Liu Z, Zhang Y, Liu W, Meng F, Wu Q, Liu S. Optical color image hiding scheme based on chaotic mapping and Hartley transform. Opt Lasers Eng; 51:967-72, 2013.

[12] Antonini M, Barlaud M, Mathieu P, Daubechies I. Image coding using wavelet transform, IEEE Transaction on Image Processing ; 1:205-20, 1992.

[13] Chen L, Zhao D. Image encryption with fractional wavelet packet method, Optik; 119:286-91, 2008.

[14] Singh M, Kumar A, Singh K. Encryption by using matrix-added, or Matrix multiplied input images placed in the input plane of a double random phase encoding geometry. Opt Laser Eng; 47:1293-300, 2009.

[15] Chen H, Du X, Liu Z, Yang C. Color image encryption based on the affine transform and gyrator transform. Opt Lasers Eng ; 51:768-775,2013.

[16] Peng X, Wei H, Zhang P. Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain. Opt Lett ; 31:3261-3,2006.

[17] Samson Ch, Sastry V U K. An RGB Image Encryption Supported by Wavelet-based Lossless Compression. IJACSA; 3:36-41, 2012.16

[18] Muttoo S K, Aggarwal Deepika. Ahuja Bhavya A Secure Image Encryption Algorithm Based on Hill Cipher System. Buletin Teknik Elektrodan Informatika; 1:51-60, 2012.

[19] Panduranga H T, Naveen Kumar S K. Advanced Partial Image Encryption using Two-Stage Hill Cipher Technique. International Journal of Computer Applications; 60:14-19, 2012.

[20] Dyson FJ, Falk H. Period of a discrete cat mapping, Amer. Math. Mon.;99:603-624, 1992.

DOI 10.17148/IJARCCE.2015.49108