Available at
http://pvamu.edu/aam
Appl. Appl. Math.
ISSN: 1932-9466

Vol. 11, Issue 1 (June 2016), pp. 45 - 60

Applications and
Applied Mathematics:
An International Journal
(AAM)

Color image encryption and decryption using Hill Cipher associated with Arnold transform

Rakesh Ranjan[1], R. K. Sharma[2] and M. Hanmandlu[1]
[1]Department of Electrical Engineering
Indian Institute of Technology
Delhi, Hauz Khas-110016
New Delhi, India
sweetatyagiaz@gmail.com, mhmandlu@ee.iitd.ac.in
[2]Department of Mathematics
Indian Institute of Technology
Delhi, Hauz Khas-110016
New Delhi, India
rksharma@maths.iitd.ac.in

Received: February 12, 2015; Accepted: January 13, 2016

Abstract

Image security over open network transmission is a big concern nowadays. This paper proposes another methodology for color image encoding and decoding using two stage Hill Cipher method which is connected with Arnold Transformation. The forgoing created a strategy for encryption and decryption of color image information and touched on just the premise of keys. In this plan, keys and the agreement of Hill Cipher (HC) are basic. Moreover, keys multiplication (pre or post) over an RGB image information framework is inevitable to know to effectively decrypt the first image information. We have given a machine simulation with a standard example and the result is given to support the stalwartness of the plan. This paper gives a detailed comparison between prior proposed methods and this methodology. The system has potential utilization in computerized RGB image transforming and security of image information.

Keywords: Color image encryption; Color image decryption; Cryptography; Arnold transform, Hill cipher

MSC 2010 No.: 92A64; 65T60; 68U10; 68P25

1. Introduction

Cryptographic frameworks are utilized broadly to guarantee secrecy and integrity of delicate data. Security of image information in an unstable network is a significant issue. Image information is very delicate and inclines to translate suddenly by gatecrashers. Several methods have been proposed to exchange image information safely, for example, digital techniques, and network and communication technologies. These images are utilized as a part of different zones for example: business reason, online training and preparing, military administrations, examination and exploratory reason. In all these regions, keeping up the fidelity and secrecy of original image information is a basic issue. In Kumar et al. (2014), the author has proposed RGB image security using random matrix affine cipher and discrete wavelet transform (DWT). Be that as it may, in our approach the encryption and decryption procedure is focused around Two Stage Hill Cipher (TSHC) over $SL_n(F)$ associated with Arnold Transform which is intended to guarantee secure transmission of color image information. We consider keys, course of action of HC, and position (pre or post) of multiplication of keys with image information for security. These parameters are exceptionally sensitive. Different schemes have been associated with encryption and decryption of image information safety. Authors, for example, Sui and Gao (2013), Hennelly and Sheridan (2003), Liu and Liu (2007) and Zhang et al. (2002), have proposed image encryption and decryption using Fourier transformation. Mishra and Sharma (2014), Antonini et al. (1992), Chen and Zhao (2008) and Kong and Shen (2014), have introduced image encryption by wavelet transform. Chen et al. (2013) have given RGB image encryption and decryption that focused on the affine transform in spinner space. Notwithstanding, late studies on the security of RGB images have uncovered vulnerability against attack such as known-plaintext attack, chosen-plaintext attack, chosen-ciphertext attack, and so forth. Attacks are not only limited to text data but also to image data, signals, and so forth.

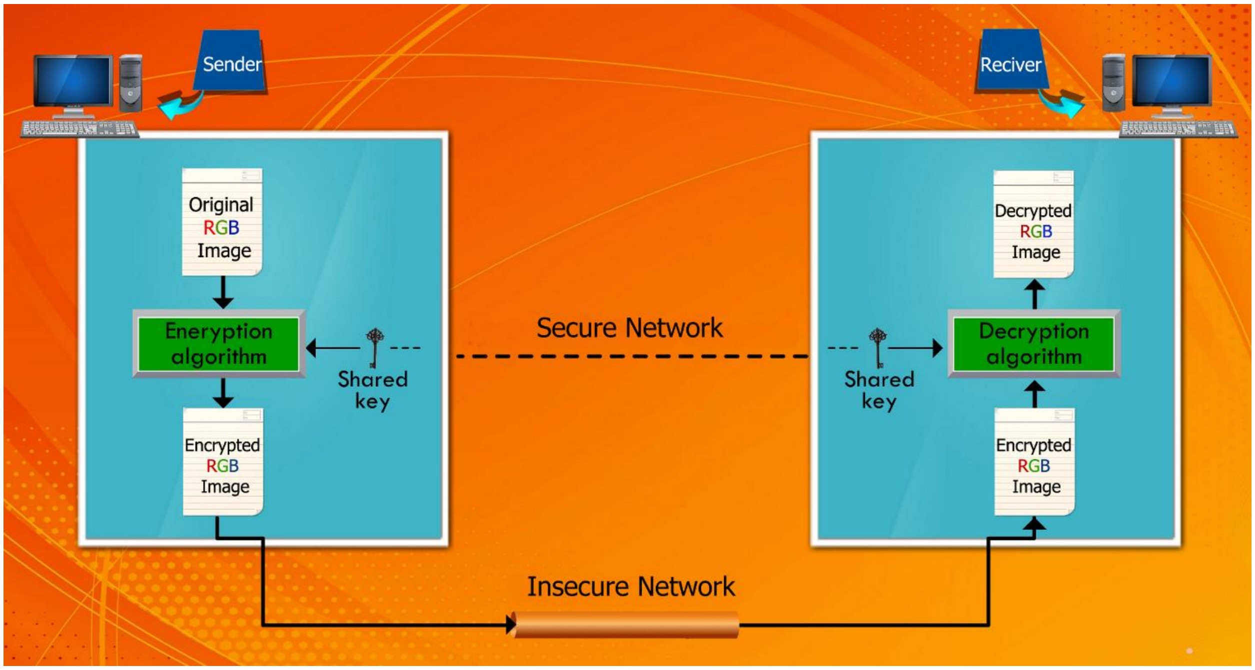

Figure 1. Procedure of transmission of information through open network

This technique is suitable for secure transmission of substantial size images that partitions the first image into equivalent block sizes such that block sizes (order of sub images) must be the same as the size (order) of Hill Cipher keys and the Hill Cipher keys are chosen from $S\,L_n(F)$ (Sherry (1977)). $S\,L_n(F)$ is an $n \times n$ matrix whose determinant is one and forms a group under multiplication over a field, F. Rosen (1984) and Stalling (2006) stand out among the most well-known systems for encryption and decryption of text information. The paper by Samson and Sastry (2012) portrays an RGB image encrypted using Hill Cipher and discrete wavelet transformation that considers involutory matrix for key. Muttoo et al. (2012) or Panduranga and Naveen (2012) discussed self-invertible matrix (likewise involutory matrix) for Hill Cipher key. Hill Cipher (HC) is particularly for images exhibited in matrix form and the Hill Cipher keys are chosen from $S\,L_n(F)$. Since $S\,L_n(F)$ is a non-abelian group and matrix multiplication is not commutative, then the multiplication of Hill Cipher keys with RGB image relies on pre or post multiplication to accurately decrypt the encrypted RGB image. To start with, random Hill Cipher is connected on every R, G, and B channel of a color image information before Arnold transform (AT), and secondly, it is connected after Arnold transform (AT). We characterize it as Two Stage Hill Cipher (TSHC), where our first stage is before applying Arnold transform (AT) and second stage is after applying Arnold transform. Experimental results, security analysis, and the correlation between the proposed system with Samson and Sastry (2012), Panduranga and Naveen (2012) are evidence for stalwartness and immenseness of the proposed methodology.

1.1. Organization of the paper

In Section 2, we clarify the proposed HC method and give the equation for color image encryption and decryption by Hill Cipher (HC) and Arnold Transform (AT), and we show in more details the thoughts and association of the proposed methodology. We then exhibit in Section 3 the system utilized as part of this paper for color image information encryption and decryption for the proposed method using TSHC connected with Arnold Transform. In section 4, we discuss the statistical analysis and stalwartness of the proposed methodology. Comparison between the proposed techniques with different related methods is given in Section 5. In Section 6, we draw the conclusion of this technique.

2. Hill Cipher and Arnold Transform

In the proposed cryptosystem, we have designed the security of RGB images of size $m \times m$ by Hill Cipher (HC) and Arnold transform (AT). The matrix of each one channel of RGB image of size $m \times m$ is separated into equivalent block of size $m \times m$ such that $m|m$, characterized by the user. We call it a block matrix (sub image), which is of the same size as the span of the key of Hill Cipher. In proposed cryptosystem, the multiplicative keys of Hill Cipher are looked over $S\,L_n(F_q)$ domain such that n divides m. Assume that the user chooses a type of block matrix (sub image), in which if the order of the block matrix does not divide the order of the original matrix $(n - m)$, then the model will automatically include required redundant rows and columns in the original matrix which will later on be naturally uprooted during the decryption process without giving any additional information. The strategy for block formation of RGB image information is delineated in Figure 2. $S\,L_n(F_q)$ is the set of all $n \times n$ matrix that contains those components of $GL_n(F_q)$ (Green (1977)) whose determinant is 1 over the field F_q. The mathematical formulation of $S\ L_n(F_q)$ is as follows:

$$SL_n(F_q) = \{A \in GL_n(F_q) |\ \det(A) = 1\},$$

where, $GL_n(F_q)$ is a general linear group over the domain F_q. Because $SL_n(F_q)$ contains those elements from $GL_n(F_q)$, whose determinant is equal to 1, for large size of $n,$ the order of $SL_n(F_q)$ is very large. If F_q is contains q elements then

$$|SL_n(F_q)| = \frac{|GL_n(F_q)|}{|GL_n(F_q)|/|GL_n(F_q)|} = \frac{|GL_n(F_q)|}{|GL_n(F_q) : SL_n(F_q)|} = \frac{|GL_n(F_q)|}{q-1} = \frac{q^H}{q-1}$$

$$= \prod_{j-1}^{n}(q^j - 1),$$

where $H = \sum_{j=1}^{n-1} j = \binom{n}{2}$ and F_q is a finite field containing q elements, where q is a large prime number. Since the determinant of every element of $SL_n(F_q)$ is 1, the inverse of Hill Cipher keys (k^{-1}) is equal to the adjoint of Hill Cipher keys $(adj(K))$ because $k^{-1} = \frac{adj(K)}{\det(K)}$. The formulation of Hill Cipher (HC) of a block matrix (sub image) of size $n \times n$ is given as:

$$C = C.K\ \ (mod\ N),$$

where, *B* is an *n* × *n* block matrix (sub image) of the color image of size *m* × *m*, *K* is an *n* × *n* key matrix from special linear group (1), and *C* be a cipher block of size *n* × *n*.

The formulation for inverse Random Hill Cipher (iRHC) of block matrix (sub image) of size *n* × *n* is given as:

$$B = C.adj(K)\ \ (mod\ N),$$

where, *ad j*(*K*) is adjoint of key matrix *K* ∈ *S Ln*(R), and *N* is a unit representation in single/double. Similarly, the same process is applied for the remaining block matrix (sub image) of the original color image. In Equation (4), the position of $adj(K)$ is fixed according to the position of *K* (3) because matrix multiplication is non-commutative (if attacker multiplies $adj(K)$ with C (4) without knowing the exact position of *K*, then the original image cannot be recovered correctly).

In this cryptosystem, we have also used discrete Arnold Transform or cat map transform [Dyson and Falk (1992)] to scramble each channel of the RGB image. For the size of *M* × *M* image, the Arnold Transform is defined as

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}\ \ (mod\ m),$$

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

Now, corresponding to the 2-dimensional inverse Arnold Transform (2D-iAT) of Equation 5 is defined as

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \ (mod\ m).$$

The additive inverse of a with respect to modulo a is equal to $m - a$ [Sharma et al. (2012)].

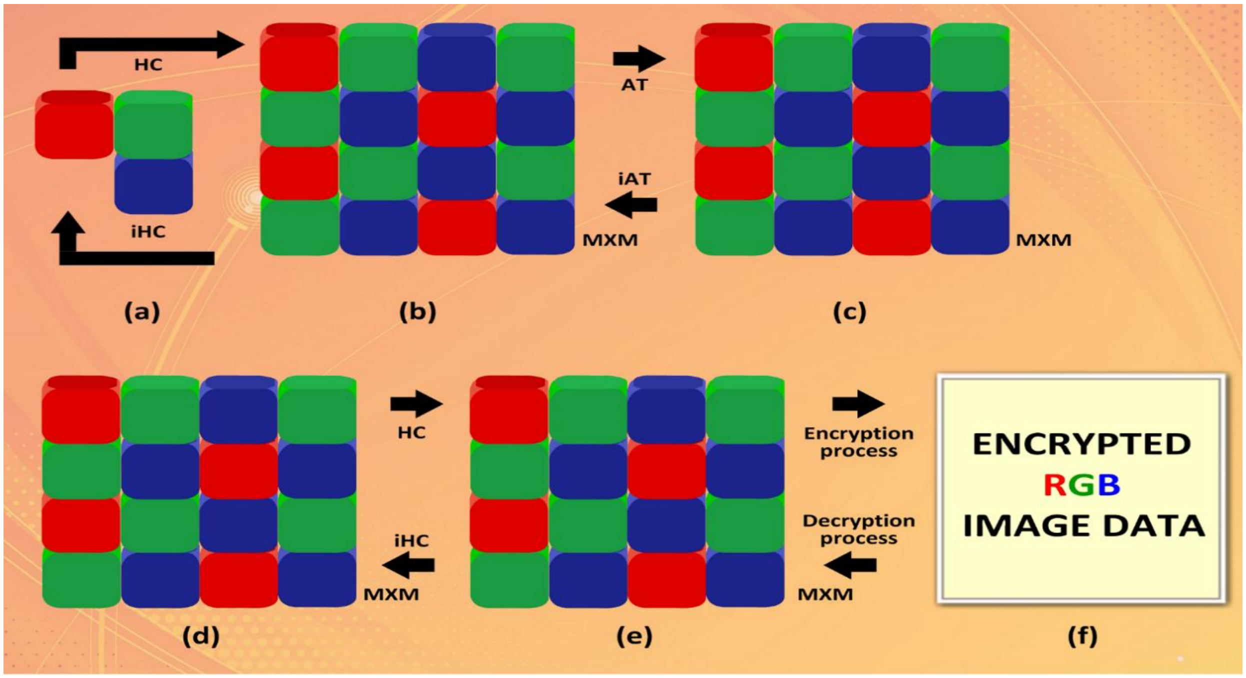

Figure 2. Block diagram of proposed model

In the block diagram of the proposed model (Figure 2) in step (a), the original image will be divided into 4×4 blocks, then the first stage HC will apply, and we get partially encrypted block image (b) and after using first stage HC, first stage AT will apply on partially encrypted block image and we get first stage final encrypted image (c). After that, second stage HC will apply and produce second stage partially encrypted block image (d). Then lastly, second stage AT will apply and generate final encrypted block image (e). In stage (f) encrypted block image will be converted into final encrypted image with original image size.

3. Encryption and decryption process

In this cryptosystem, we have outlined, the security of RGB images by two-stage Hill Cipher (TSHC) over $SL_n(F_q)$ domain with Arnold Transform (AT). In the encryption process, the proposed algorithm is applied on red (R), green (G), and blue (B) channels of an RGB image data exclusively. The system of encryption procedure applied on RGB images is delineated in the Figure 3, while methodology of decryption for an encrypted RGB image is illustrated in Figure 4. In the proposed cryptosystem, we are using 6 keys for Hill Cipher and 3 keys for Arnold Transform. In the first stage, we are using 3 keys for the Hill Cipher, which is applied on an RGB image. So also, in the following stage (second stage) 3 keys are additionally used by the Hill Cipher key. Hence, the aggregate number of conceivable outcomes of the Hill Cipher keys apply on RGB images including both stages is 6!. These alternatives (6!) said here structure a game plan of the Hill Cipher parameters, which is known as the course of action of HC parameters. Moreover, 3! alternatives are additionally accessible for arrangement of Arnold parameters, which are more sensitive. The

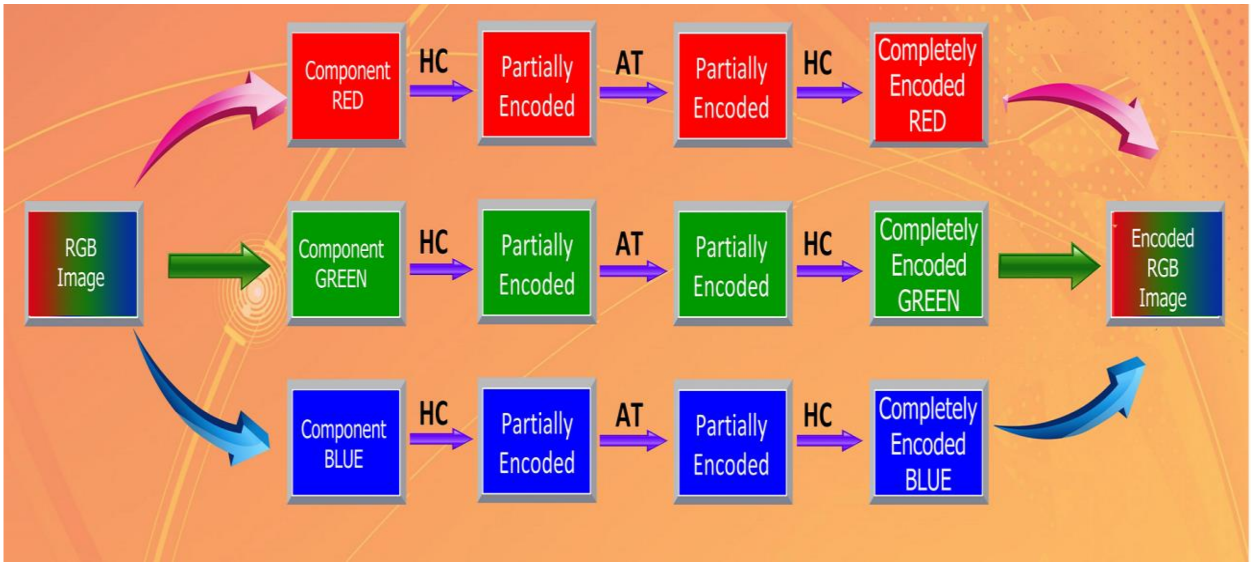

Figure 3. Encoding procedure for each component of RGB image data

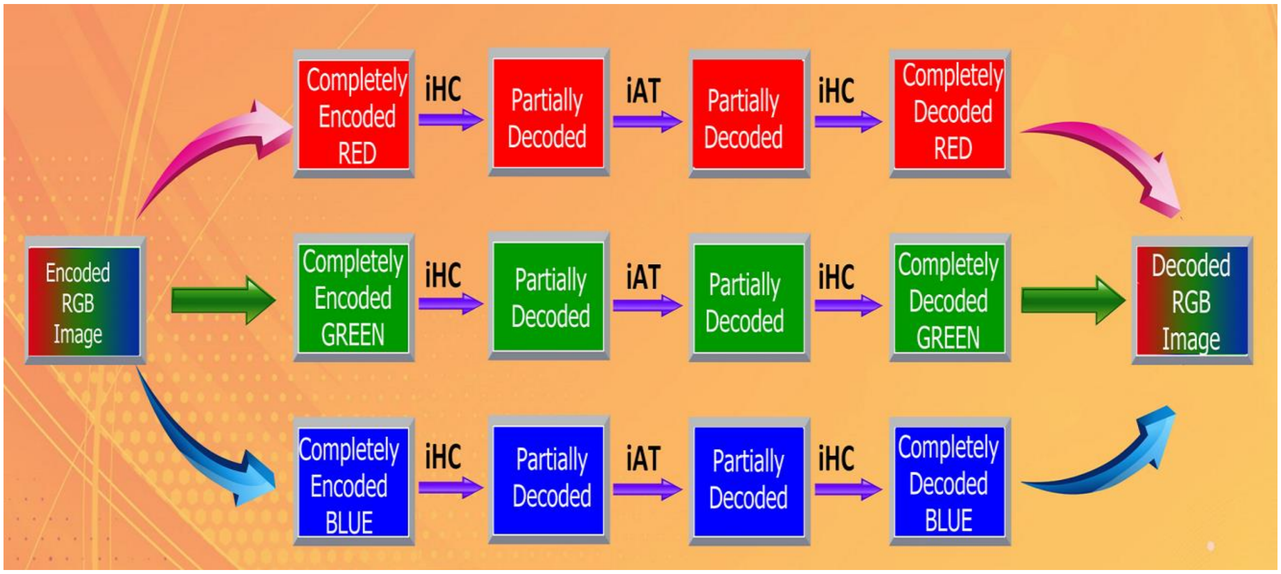

Figure 4. Decoding procedure for each component of RGB image data

encryption method for every component of RGB image data is given in Figure 3 and decryption process procedure for each part of RGB image data is portrayed in Figure 4. We have given the exploratory results in the Figure 5. Figure 5(a) is the original image, Figure 5(b) is the encrypted image, and Figure 5(c) is a correctly decrypted image while Figures 5(d), 5(e), and 5(f) were acquired using wrong Hill Cipher keys, Arnold keys, and course of action of HC keys, separately.

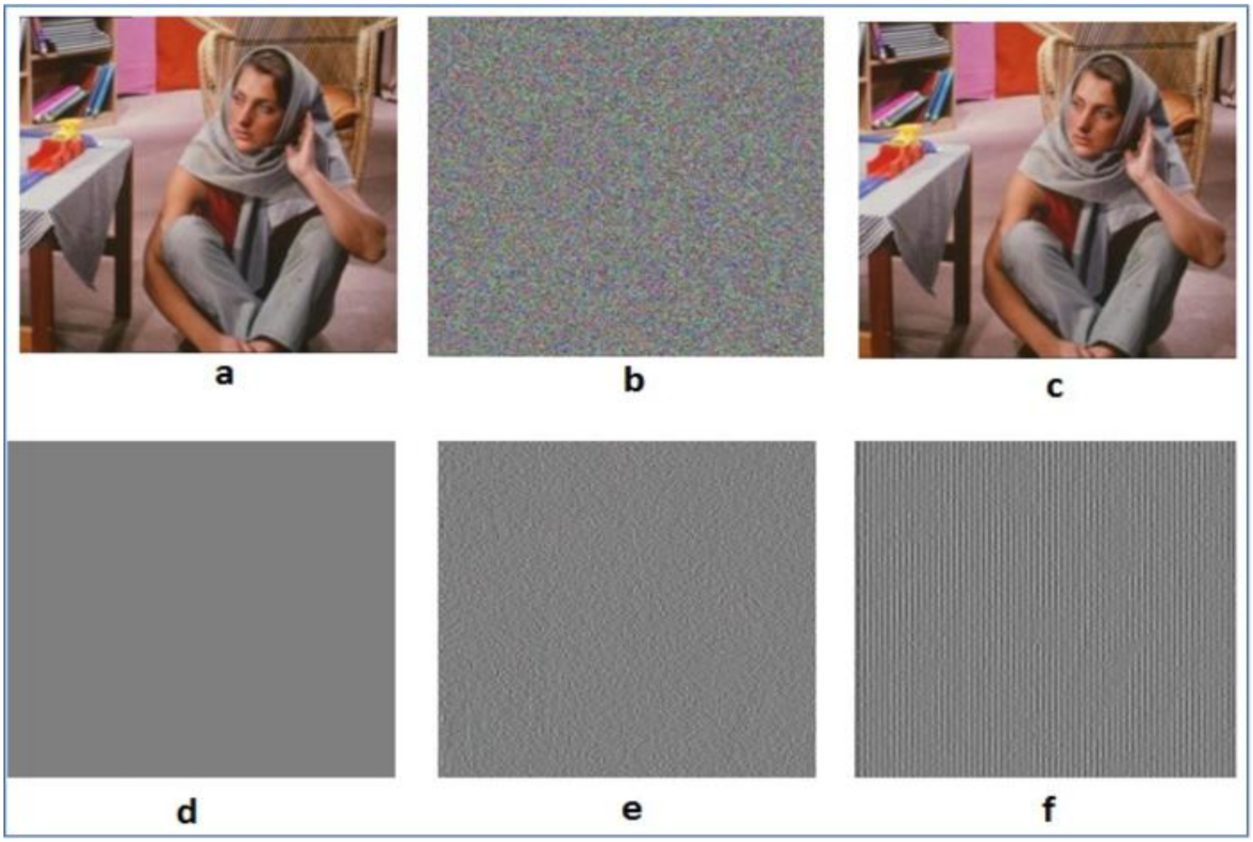

Figure 5. Final result of proposed method along with result with key error

4. Statistical analysis

The statistical analysis backs the vigor of the cryptosystem. In this segment, we examine the dissemination of information, previously, then after the fact encryption and decryption. We discuss the mean square error (MSE) analysis, peak signal noise ratio (PSNR), and correlation coefficient analysis between two images.

4.1. Robustness of the approach when encrypted RGB image data occluded

In this section, we discuss the asset of the proposed methodology when encrypted RGB image data impeded with 25% and 50% pixels. Encrypted RGB image Figure 5(b) is occluded from left and right with 25% pixels, which is given in Figure 6(a) and 6(b), respectively. Figure 6(e) is the decrypted image of Figure 6(a) when the exact keys and the right arrangement of HC parameters are coupled on occluded image; comparably, Figure 6(f) is the decoded image of Figure 6(b) when all the precise parameters are used. This analysis states that the proposed methodology is powerful against the 25% occluded encrypted RGB image data. Presently, scrambled RGB image data is congested with 50% pixels from left and right, which is indicated in Figures 6(c) and 6(d) separately, and the related unscrambled picture is introduced in Figures 6(g) and 6(h) respectively, with all the exact keys and the right course of action of AHC parameters.

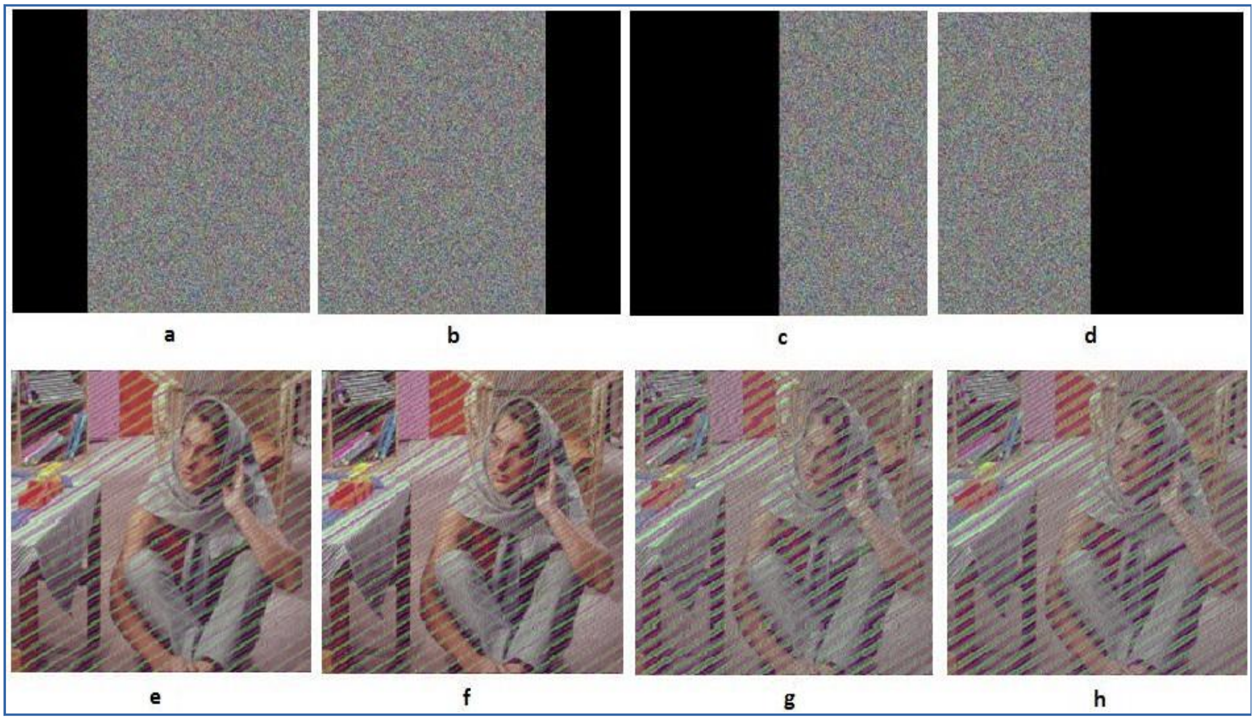

Figure 6. Exact keys and correct arrangement of HC parameters

Figures 7(e), (f), (g), and (h) are decrypted images of Figures 7(a), (b), (c), and (d), respectively. These decrypted images are acquired when precise keys and right strategy of AHC parameters are allowed on impeded images. The above examination shows that the proposed procedure is vigorous against the impediment of 25% and 50% encrypted data.

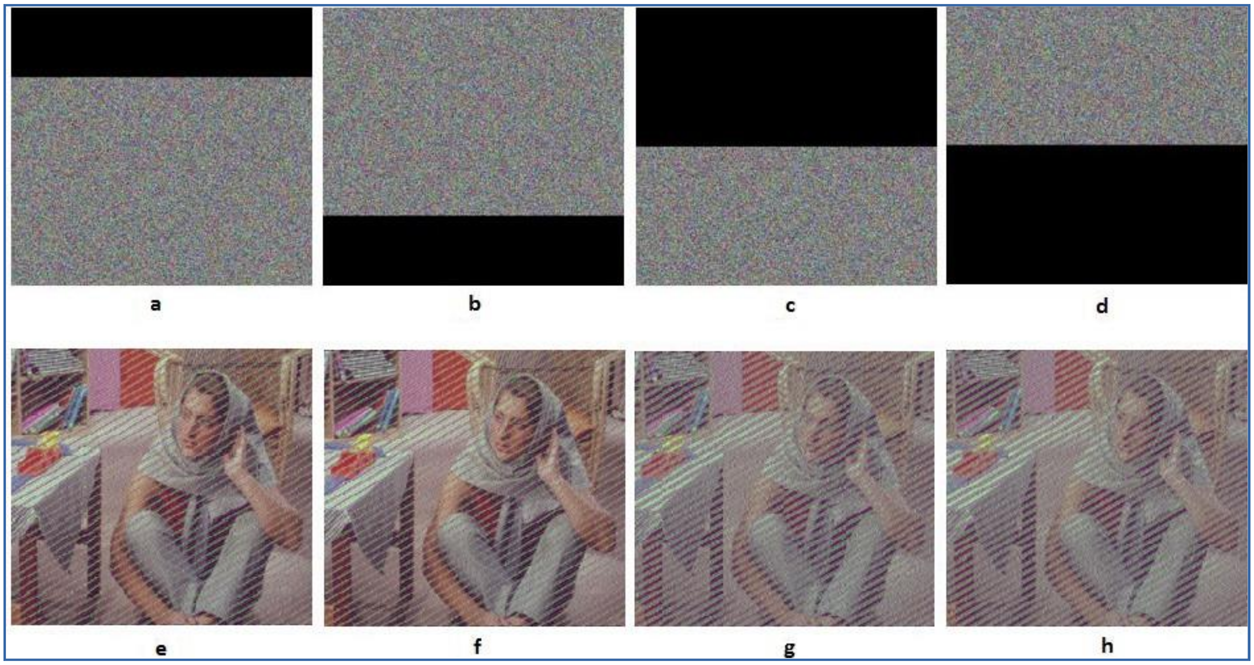

Figure 7. Exact keys and correct arrangement of HC parameters

In this way, it is affirmed that in all cases, the somewhat partially encrypted RGB image data can be effectively decrypted. By examining all the above actualities, we can say that the proposed methodology is powerful against such sorts of impediment attacks.

4.2. Mean square error, Peak signal-to-noise ratio, and Correlation analysis of color image

The mean square error (MSE) between the reconstructed color image data and the original color image data for red (R), green (G), and blue (B) components is computed from

$$MSE = \frac{1}{N \times M} \sum_{g=1}^{N} \sum_{h=1}^{M} [|f(g\Delta x, h\Delta y) - f_0(g\Delta x, h\Delta y)|^2],$$

where N and M are the pixels of an RGB image, Δx and Δy are the pixel sizes.

The peak signal-to-noise ratio (PSNR) between the reconstructed image and the original color image for red (R), green (G), and blue (B) components is computed by

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) = 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) = 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE)$$

Here, MAX_I is the maximum possible pixel value of the image. More generally, when samples are represented using linear PCM with B bits per sample, MAX_I is $2^B - 1$.

Now, the correlation coefficient (C_r) of red (R), green (G), and blue (B) channels of the original image and reconstructed image are computed by

$$C_r = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{[\sum_m \sum_n (A_{mn} - \bar{A})]^2 [\sum_m \sum_n (B_{mn} - \bar{B})]^2}}$$

where A and B are, respectively, the mean of output, and input images. The correlation coefficient between two images vary from −1 to +1, i.e. $-1 \leq C_r \leq +1$. Two images A and B have a strong positive linear correlation if the correlation coefficient C_r is close to +1. The −1 value of the correlation coefficient C_r indicates a negative relationship between the two images and the correlation coefficient of zero represents that there is no relationship between the two images. The MSE, PSNR, and C_r of red (R), green (G), and blue (B) channel of output and input color images are given in Tables 1.

Table 1. Statistical analysis between figure 5(b) and figure 5(a)

S.NO.	Component of color image	MSE	PSNR	Correlation
1.	Red component of color image	5.5332×10^3	10.7011	-0.043
2.	Green component of color image	5.6853×10^3	10.5833	4.4422×10^{-4}
3.	Blue component of color image	6.5395×10^3	9.9754	5.7411×10^{-4}

Table 2. Statistical analysis between figure 5(c) and figure 5(a)

S.NO.	Component of color image	MSE	PSNR	Correlation
1.	Red component of color image	0.00	∞	1.00
2.	Green component of color image	0.00	∞	1.00
3.	Blue component of color image	0.00	∞	1.00

Table 3. Statistical analysis between figure 5(d) and figure 5(a)

S.NO.	Component of color image	MSE	PSNR	Correlation
1.	Red component of color image	9.6847×10^3	8.2699	-6.1890×10^{-5}
2.	Green component of color image	9.7493×10^3	8.2411	-5.4639×10^{-5}
3.	Blue component of color image	1.0722×10^3	7.8278	-5.9923×10^{-5}

Table 4. Statistical analysis between figure 5(e) and figure 5(a)

S.NO.	Component of color image	MSE	PSNR	Correlation
1.	Red component of color image	9.6606×10^3	8.2808	0.0082
2.	Green component of color image	9.7797×10^3	8.2276	0.0043
3.	Blue component of color image	1.0747×10^3	7.8179	0.0048

Table 5. Statistical analysis between figure 5(d) and figure 5(a)

S.NO.	Component of color image	MSE	PSNR	Correlation
1.	Red component of color image	1.3018×10^3	6.9854	-6.9802×10^{-5}
2.	Green component of color image	1.1312×10^3	7.5955	-1.1859×10^{-5}
3.	Blue component of color image	9.4136×10^3	8.3932	-1.3820×10^{-5}

The mean square error values, PSNR, and correlation coefficient for red (R), green (G), and blue (B) channels of encrypted color image of Figure 5(b) are given in Table 1. High MSE and low PSNR, and the correlation coefficient 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 HC parameters. The mean square error values, PSNR, and correlation coefficient of decrypted color image in Figure 5(c) for red (R), green (G), and blue (B) channel are given in Table 2. The zero MSE values, infinite PSNR and a correlation coefficient of 1 of red, green, and blue shows that the original image has been recovered completely without any loss of sensitive information of the RGB image data. The mean square error values, PSNR, and the correlation coefficient for red (R), green (G), and blue (B) channel of Figure 5(d) are given in the Table 3, which shows that the Hill Cipher key is sensitive. The statistical analysis of Figure 5(e) is mentioned in Table 4, and we have discussed the mean square error values, PSNR, and correlation coefficient for red (R), green (G), and blue (B) channel of Figure 5(f) in table 5. These qualities demonstrate that the data about the original image cannot be grown regardless of the possibility that the decoder knows all the accurate keys, yet is not mindful of the right arrangement of HC parameters. In this manner, the statistical analysis of color image shows that the proposed methodology is vigorous against cryptanalysis on the grounds that security of this methodology relies on the keys, as well as on the position (pre or post) of keys multiplication, and the arrangement of HC parameters.

4.3. Pixels intensity distributions of the images at Horizontal, Vertical, and Diagonal pixels

The horizontal, vertical, and diagonal pixel intensity distributions of the original image (Figure 5(a)) are examined in Figure 8.

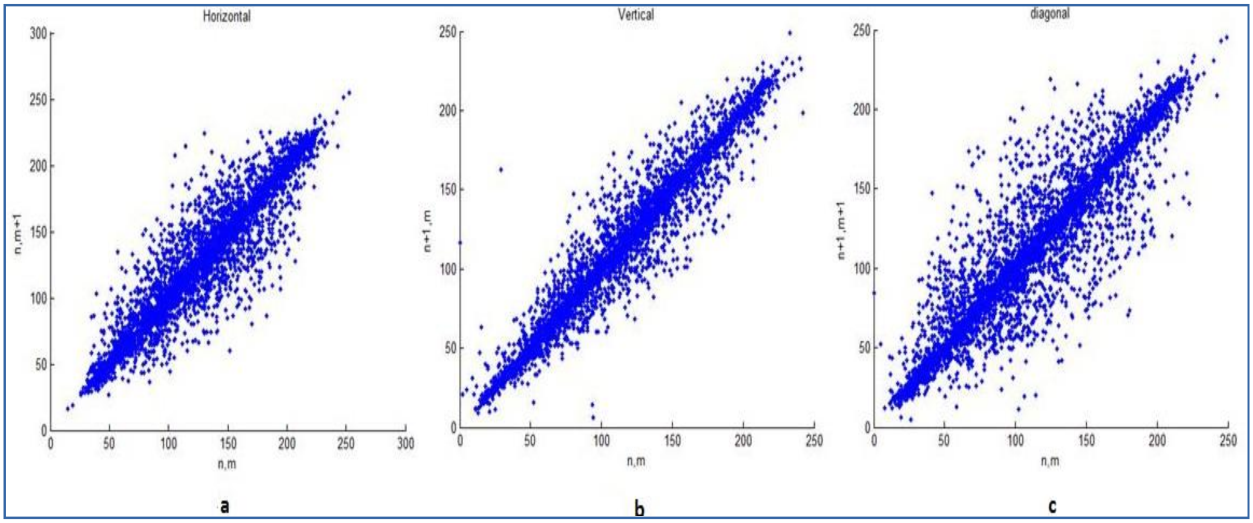

Figure 8. Distribution analysis at horizontal, vertical, and diagonal pixels of Figure 5(a)

Figure 9. presents the encrypted image pixel intensity distributions at horizontal, vertical, and diagonal format. The pixel intensity distributions of the encrypted image is consistently disseminated in the space, and totally unique in relation to pixels dispersions of the original image (Figure 8.). The conveyance of information of the scrambled image demonstrates that no data of the original image can be obtained from the encoded image. So the scrambled color image is secure from attacks.

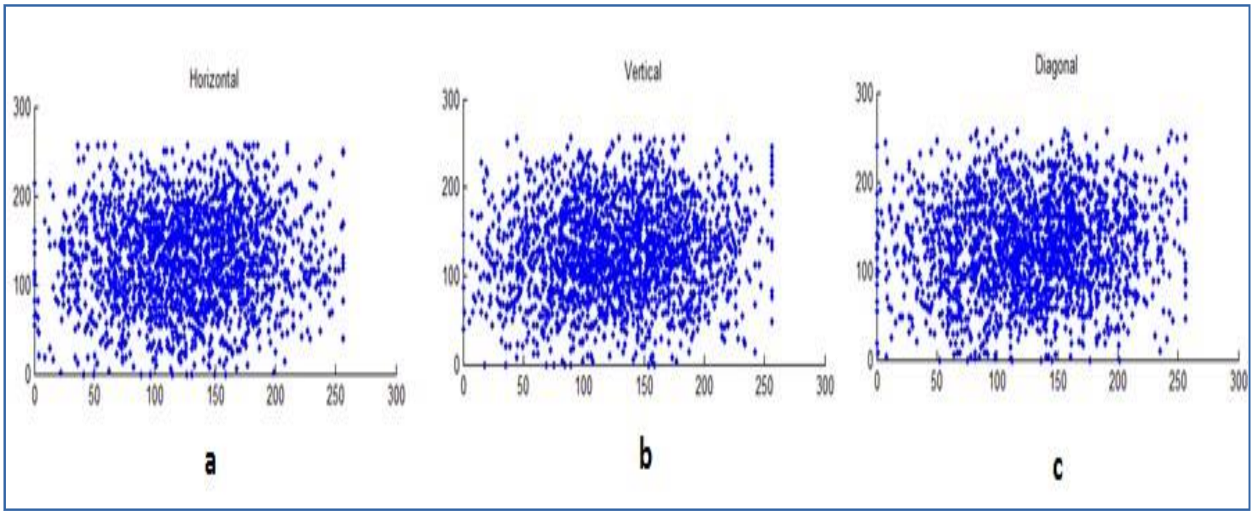

Figure 9. Distribution analysis at horizontal, vertical, and diagonal pixels of Figure 5(b)

The pixel intensity distributions of two neighboring pixels at horizontal, vertical, and diagonal directions of the accurately decrypted image is given in the Figure 10.

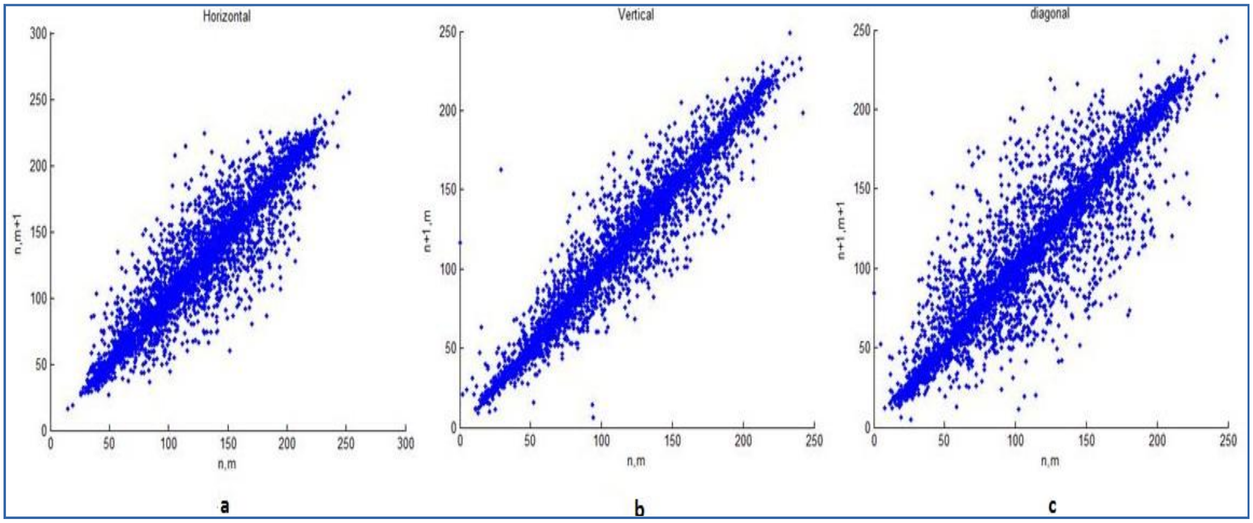

Figure 10. Distribution analysis at horizontal, vertical, and diagonal pixels of Figure 5(c)

The pixel intensity distributions of two neighboring pixels at horizontal, vertical, and diagonal directions of the correctly decrypted image is precisely like the pixel intensity distributions of the original image, which shows that the image is totally recovered on applying the exact keys and the right course of action of parameters.

4.4. Histogram analysis of color image data

An RGB image histogram is a graphical representation of the pixel intensity distribution of the RGB image. Consequently, an image histogram gives an acceptable outline of how the pixels in an image are distributed by plotting the number of pixels at every intensity level. The histogram of the original color image (Figure 5(a)) is given in Figure 11(a) and the histogram of the encrypted image (Figure 5(b)) is given in Figure 11(b). The histogram of the encrypted image is very

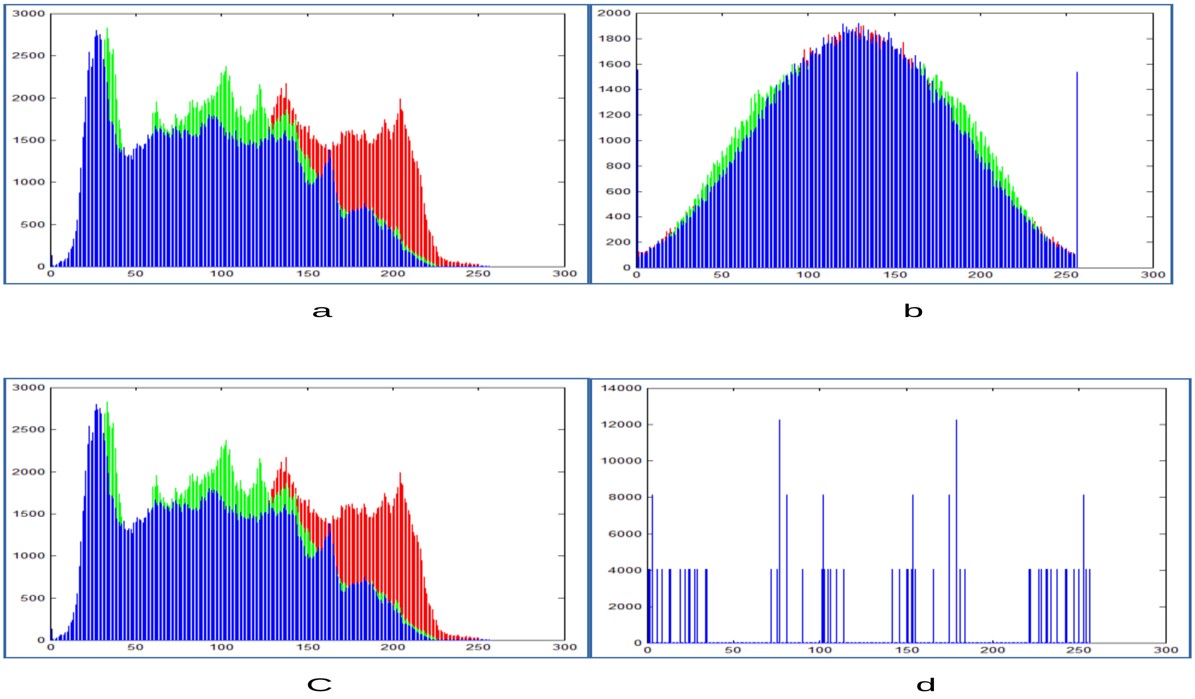

Figure 11. Histogram analysis of Figure 5

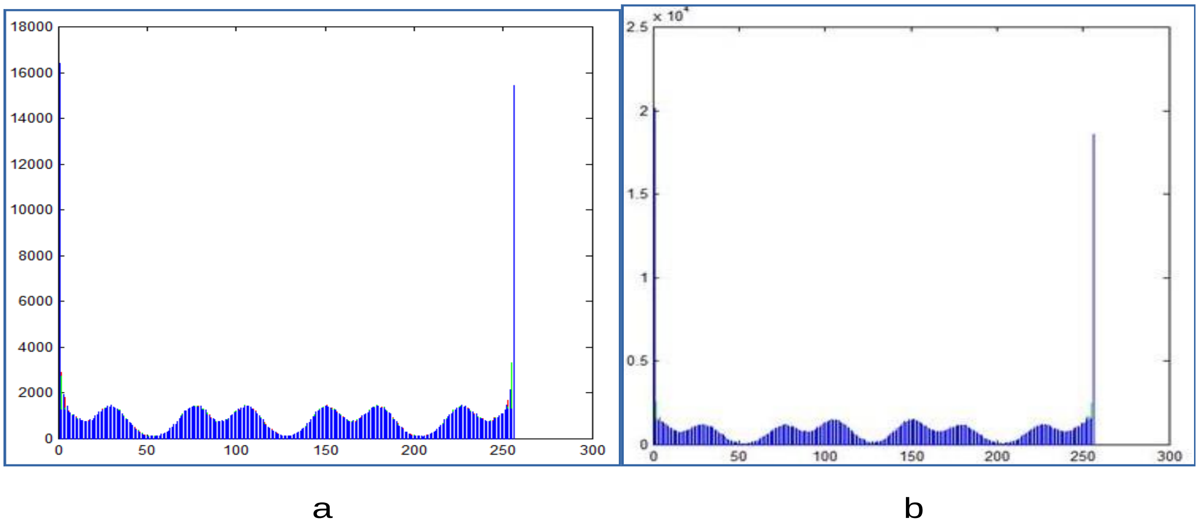

Figure 12. Histogram analysis of Figure 5(e) and (f)

different from the histogram of the original color image which means that the encrypted image data is totally transformed from the original image data. The histogram of correctly unscrambled image (Figure 5(c)) is given in Figure 11(c). The histogram of correctly decrypted image is precisely like the histogram of the original image, which means that the original image is totally recovered without loss of any data. The histogram of Figure 5(d) is given in Figure 11(d), which shows the robustness of the model when the wrong key is used for decryption. Figures 12(a) and 12(b) are the histograms of Figures 5(e) and 5(f), respectively. The distribution of data on these figures shows that the encrypted data is secure from attacks.

5. Comparison of proposed technique with available methods

The proposed approach compares with Samson and Sastry (2012) and Panduranga and Naveen (2012). Samson and Sastry (2012) has taken Hill Cipher key involutory matrix in which no information about block matrix (sub images) is given. Hence for a huge image the Hill Cipher key size will likewise be expensive. In the most pessimistic scenario the number of inputs for Hill Cipher key can be dependent upon the image size (for instance, a color image of size $512 \times 512 \times 3$, the total number of inputs required for Hill Cipher key is 786432). So it is unwieldy for the encoder to perform encryption and decryption procedure. Additionally, no data is given about mean square error analysis, histogram analysis, and robustness analysis of the methodology. Notwithstanding this, it is additionally projected to give enormous amount of inputs for extensive size images (as mentioned above). Panduranga and Naveen (2012) considered self-invertible Hill Cipher key which is likewise an involutory matrix. In Samson and Sastry (2012) and Panduranga and Naveen (2012), decryption process depends just on the key. If an attacker knows the precise key then the image can be unscrambled effectively. In our proposed methodology Hill Cipher keys are chosen from extraordinary linear group over a field $F(SL_n(F))$ and the size of Hill Cipher keys relies on the decision of the encoder. In this methodology, if an attacker carefully thinks about all the keys, however, and with no information about the correct arrangement of HC, then original image cannot be recouped. Again, information of pre or post multiplication of keys with image data is additionally obligatory.

Summing up, the certainties spoke to above, including all-experimental results, key's space analysis, sensitivity analysis, statistical analysis of the proposed cryptosystem of color image, and comparison with existing techniques, support the robustness and propriety of the introduced cryptosystem.

6. Conclusion

In this paper, we have exhibited a new cryptosystem for the color image of size $m \times m$, which is composed of Hill Cipher (HC) over $SL_n(F_q)$ domain with 2-dimensional Arnold Transform (AT). We have considered Hill Cipher keys from $SL_n(F_q)$ domain such that n divides the size of image matrix (m), which gives a gigantic key space to the introduced cryptosystem. In the proposed technique, the encryption strategy is usual; however, the decoding method is more severely arranged. There is no thought regarding the definite keys of Hill Cipher and the particular plan of HC parameters. Besides, regardless of the fact that the attacker has all the precise keys but is not mindful about the right plan of HC parameters, then he/she will not be able to recover the original data accurately from the ciphered data (encrypted image). Another advantage of this technique is that in Hill Cipher matrix multiplication, which is noncommutative and is used in our encryption process, the decryption process relies on the position (pre or post) of multiplication of inverse multiplicative keys with the encrypted image (on the same position of multiplicative keys utilized as a part of the encryption process). If there is no information about the particular position (pre or post) of keys multiplication, then the attacker cannot recover the original image. The proposed cryptosystem gives security of RGB image information by the keys, plans of HC parameters, and the position (pre or post) of keys multiplication. The security and statistical analysis support the robustness of the presented cryptosystem. Hence, the exhibited cryptosystem for color image can be used for secure transmission through unsecured channels without any lessening in the sensitive information.

Acknowledgment

The authors are thankful to both referees and the Editor-in-Chief Professor Aliakbar Montazer Haghighi for their valuable suggestion and constructive comments which helped us in revising the paper to its present form.

REFERENCES

Abuturab MR. (2013). Color image security system based on discrete Hartley transform in gyrator transform domain. Optics and Lasers in Engineering, 51:317-24.

Abuturab MR. (2012). Securing color information using Arnold transform in gyrator transform domain. Optics and Lasers in Engineering, 50:772-9.

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

Chen L, Zhao D. (2009). Color image encoding in dual fractional Fourier-wavelet domain with random Phases, Optics Communication, 282:3433-8.

Chen L, Zhao D. (2008). Image encryption with fractional wavelet packet method, Optik, 119:286-91.

Chen H, Du X, Liu Z, Yang C. (2003). Color image encryption based on the affine transform and gyrator Transform, Optics and Lasers in Engineering, 51:768-75.

Dyson FJ, Falk H. (1992). Period of a discrete cat mapping, Amer. Math. Mon., 99:603-24.

Hennelly B, Sheridan JT. (2003). Optical image encryption by random shifting in fractional Fourier Domains, Optics Letters, 28:269-71.

Kong D, Shen X. (2004). Multiple-image encryption based on optical wavelet transform and multichannel fractional Fourier transform, Optics & Laser Technology, 57:343-9.

Kumar M, Mishra D C, Sharma R K. (2014). A first approach of an RGB image encryption, Optics and Lasers in Engineering, 52:27-34.

Liu Z, Liu S. Random fractional Fourier transform, Optics Letters, 2007;32:2088–90.

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, Optics Communication, 2011; 284: 123-8.

Liu H, Liu Y. (2014). Cryptanalyzing an image encryption scheme based on hybrid chaotic system and cyclic elliptic curve, Optics & Laser Technology, 56:15-9.

Mishra D C, Sharma R K, Kumar M, Kumar K. (2014). Security of color image data designed by public-key cryptosystem associated with 2D-DWT, Fractals, 22:1450011-1-16.

Mishra D C, Sharma R K. (2014). Application of algebra and discrete wavelet transform in two-dimensional data (RGB-images) security, International Journal of Wavelets, Multiresolution and Information Processing, 12:1450040-1-25.

Mishra D C and Sharma R K. (2013). Grayscale-image encryption using Random Hill Cipher over $SL_n(F)$ associated with Discrete Wavelet Transformation, AAM, 08:777-91.

Mishra D C, Sharma R K, Ranjan Rakesh and Hanmandlu, M. (2015). Security of RGB image data by affine hill cipher over SLn(Fq) and Mn(Fq) domains with Arnold transform, Optik,126, No. 23, 3812-3822.

Muttoo S K, Aggarwal Deepika. Ahuja Bhavya. (2012). A Secure Image Encryption Algorithm Based on Hill Cipher System, Buletin Teknik Elektro dan Informatika, 1:51–60.

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

Rosen K H. (1984). Elementary Number Theory and Its Applications, Pearson, New York:171-5.

Samson Ch, Sastry V U K. (2012). An RGB Image Encryption Supported by Wavelet-based Lossless Compression, IJACSA, 3:36-41.

Sharma R K, Shah S K, Sanker A G. (2012). Algebra I, Pearson.

Sherry M. Green. (1997). Generators and Relations for the Special Linear Group Over a Division Ring, Proceedings of the American Mathematical Society, 62:229-232.

Singh N, Sinha A. (2009). Gyrator transform-based optical image encryption, using chaos, Optics and Lasers in Engineering, 47:539-46.

Singh M, Kumar A, Singh K. (2009). Encryption by using matrix-added, or matrix-multiplied input images placed in the input plane of a double random phase encoding geometry, Optics and Lasers in Engineering, 47:1293-300.

Stallings W. (2006). Cryptography and Network Security, Prentice Hall, New Jersey.

Sui L, Gao B. (2013). Single-channel color image encryption based on iterative fractional Fourier transform and chaos, Optics & Laser Technology, 48:117-27.

Zhang Y, Zheng CH, Tanno N. (2002). Optical encryption based on iterative fractional Fourier Transform, Optics Communication, 202:277-85.