Applications and Applied Mathematics: An International Journal (AAM)

Volume 15 | Issue 2 Article 29

12-2020

Multilayer Security of RGB Image in Discrete Hartley Domain

Umar H. Mir
Central University of Jammu

Deep Singh
Central University of Jammu

D. C. Mishra
Govt. P. G College, Jaiharikhal Lansdowne

Parveiz N. Lone
Central University of Jammu

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

Applications and Applied Mathematics:
An International Journal
(AAM)

Vol. 15, Issue 2 (December 2020), pp. 1213 – 1229

Multilayer Security of RGB Image in Discrete Hartley Domain

[1]Umar Hussain Mir, [2]Deep Singh, [3]D. C. Mishra and [4]Parveiz Nazir Lone

[1,2,4]Department of Mathematics
Central University of Jammu
Samba, Jammu and Kashmir, India - 181143
[1]umarcuj@gmail.com; [2]deepsinghspn@gmail.com; [4]parveizcuj@gmail.com

[3]Department of Mathematics
Govt. P. G College, Jaiharikhal Lansdowne
Uttrakhand, India - 246155
deepiitdelhi@gmail.com

Received: March 18, 2020; Accepted: July 28, 2020

Abstract

In this article, we present RGB image encryption and decryption using random matrix affine cipher (RMAC) associated with discrete Hartley transform (DHT) and random matrix shift cipher (RMSC). The parameters in RMAC and RMSC phases act as two series of secret keys whose arrangement is imperative in the proposed algorithm. The computer simulations with results and examples are given to analyze the efficiency of the proposed approach. Further, security analysis and comparison with the prior techniques successfully supports the robustness and validation of the proposed technique.

Keywords: Discrete Hartley transform; Image encryption; Image decryption; Random matrix affine cipher; Random matrix shift cipher

MSC 2010 No.: 94A60, 65T50, 68U10, 68P25

1. Introduction

The security of the digital image over transmission channels has been always a challenging problem because of various types of security attacks. Thus, the researchers are busy and trying to propose the secure methods for encryption and decryption of image data. The prime goal of this article is to construct efficient security algorithm for transmission of color images in an open unsecured network channel. In this paper, we propose a multilayered encryption and decryption method for color images based on random matrix affine cipher (RMAC) associated with discrete Hartley transform (DHT) followed by random matrix shift cipher (RMSC). Although there are several modes for transferring images all over the world provided by network and communication technologies, still their security is a challenge of the present era. In almost every field of science and technology, images are frequently used and their protection for confidentiality, integrity, authenticity and non-repudiation is a concerning issue. Several approaches have been proposed to encrypt and decrypt image data securely. The researchers in Chen and Zhao (2006); Liu et al. (2013) have introduced image encryption by using Hartley transform. In Abuturab (2012b); Abuturab (2013); Abuturab (2012a), the authors have presented image encryption over gyrator transform domain combined with other ciphers. The authors in Hahn et al. (2006); Hennelly and Sheridan (2003); Liu et al. (2011); Liu et al. (2007) have proposed image encryption and decryption using fractional Fourier transform. The authors in Liu et al. (2013); Liu et al. (2001) have set forth image encryption by optical transforms where as the authors in Antonini et al. (1992); Chen and Zhao (2008) have given image coding using wavelet transform. In Mishra et al. (2017); Ranjan et al. (2016), the authors presented the encryption techniques using Arnold map combined with reality preserving two dimensional discrete fractional Fourier transform (RP2DFRFT) and Hill cipher respectively. Color image encryption based on the affine transform in gyrator domain is given by Chen et al. (2013). Also, Liu et al. (2010a) have proposed double encryption using affine transform encoded into the gyrator domain. Recently, Sangavi and Thangavel (2019) have proposed a novel image encryption using fractal geometry where confusion is achieved by Julia set and Mandelbrot set, and the diffusion by XOR operation. However, vulnerability of images against many attacks like chosen-plain text attack, chosen-cipher text attack, statistical attacks, etc. have been revealed Peng et al. (2006b); Peng et al. (2006a), and even these attacks are also vulnerable to text data, signals, etc.

The color image encryption using random matrix affine cipher (RMAC) associated with discrete Hartley transform (DHT) and followed by random matrix shift cipher (RMSC) in the proposed approach is immune to the various attacks. The proposed approach is suitable for efficient and secure transmission of large size images assured by a large key space and correct arrangement of RMAC and RMSC parameters (for instance, there are about $8.7 \times 10^{20} \approx 1$ sextillion possible keys to decrypt an RGB image of size $512 \times 512 \times 3$).

Affine Cipher is known to be an imperative encryption and decryption technique for text and image data (Stallings (2006); Lone and Singh (2020)). The proposed RMAC is applied on even rows, even columns, odd rows and odd columns for each R, G, and B channel. Similarly, RMSC is a special case of RMAC. The procedure of our approach is divided into two stages, one applying RMAC

before DHT and second applying RMSC after DHT. The DHT (Villasenor (1994)) is a real valued transformation frequently used in image processing, data compression, signal processing, sound analysis, etc.

To support the robustness of the proposed approach, security analysis and comparison with the results in Ranjan et al. (2016); Mishra et al. (2017); Sangavi and Thangavel (2019); Lone and Singh (2020) is provided.

The remaining part of article is divided into six sections. In Section 2, we explain the concepts of RMAC, DHT and RMSC. In Section 3, we present the proposed method for image encryption and decryption using RMAC associated with DHT followed by RMSC. The primary focus of this section is on the keys formation used in proposed approach. In Section 4, in order to demonstrate and verify the approach on an RGB image, computer simulation and experimental results are provided. Security analysis and robustness of the approach is discussed in Section 5. Section 6 gives the comparison of proposed method with some existing methods. The conclusions drawn are given in Section 7.

2. Random matrix affine cipher, discrete Hartley transform and random matrix shift cipher

In the proposed approach, RMAC is applied on an RGB image of size $n \times m$, on each of its components red(R), green(G) and blue(B). The pixels of each component are given in matrix form in which even numbered and odd numbered rows are shifted by parameters α and β and multiplied by parameters μ and η, respectively, where

$$\alpha \neq \beta \text{ such that } \alpha,\ \beta \in Z_m - \{0\} \text{ and } \mu,\ \eta \in U(m).$$

Also, even numbered and odd numbered columns are shifted by parameters γ and δ and multiplied by parameters λ and σ, respectively, where

$$\gamma \neq \delta \text{ such that } \gamma,\ \delta \in Z_n - \{0\} \text{ and } \lambda,\ \sigma \in U(n),$$

with $U(r) = \{x \in \mathbb{N} : x < r \text{ and } \gcd(x, r) = 1\}$ is an abelian group under multiplication modulo r called group of units such that $|U(r)| = \phi(r)$, where $\phi(r)$ represents ***Eulers-phi*** function (Gallian (1999)).

The encryption formula for RMAC on an image matrix of size $n \times m$ is given as

$$\hat{X}_{even\ row,\ k} \equiv \mu X_{even\ row,\ j+\alpha(mod\ m)}, \tag{1}$$

$$\hat{X}_{odd\ row,\ l} \equiv \eta X_{odd\ row,\ j+\beta(mod\ m)}, \tag{2}$$

$$\hat{X}_{p\ ,\ even\ column} \equiv \lambda X_{i+\gamma(mod\ n),\ even\ column}, \tag{3}$$

$$\hat{X}_{q\ ,\ odd\ column} \equiv \sigma X_{i+\delta(mod\ n),\ odd\ column}, \tag{4}$$

and the decryption formula for RMAC known as inverse random matrix affine cipher(iRMAC) on an image matrix of size $n \times m$ is given as

$$X_{even\ row,\ j} \equiv \mu' \hat{X}_{even\ row,\ k+m-\alpha(mod\ m)}, \tag{5}$$

$$X_{odd\ row,\ j} \equiv \eta' \hat{X}_{odd\ row,\ l+m-\beta(mod\ m)}, \tag{6}$$

$$X_{i\ ,\ even\ column} \equiv \lambda' \hat{X}_{p+n-\gamma(mod\ n),\ even\ column}, \tag{7}$$

$$X_{i\ ,\ odd\ column} \equiv \sigma' \hat{X}_{q+n-\delta(mod\ n),\ odd\ column}, \tag{8}$$

such that $\mu\mu' = 1(mod\ m),\ \eta\eta' = 1(mod\ m),\ \lambda\lambda' = 1(mod\ n)$ and $\sigma\sigma' = 1(mod\ n)$, where X and $\hat{X}$ are old and new positions of pixel values of an image matrix before and after applying RMAC respectively. Clearly, the parameters of RMAC for each component matrix R, G and B act as keys for cryptosystem. So, the possible number of RMAC parameters of an RGB image of size $n \times m$ is given by

$$\mathcal{P}_1 = 3\{[(\phi(m))^2(\phi(n))^2 - 1](n-1)^2(m-1)^2\}. \tag{9}$$

In the proposed approach, the discrete Hartley transform (DHT) means two dimensional DHT (Villasenor (1994)). Let $f(x, y)$ for $x = 0, 1, 2, ..., n-1$ and $y = 0, 1, 2, ..., m-1$ denote a digital image of size $n \times m$. The discrete Hartley transform (DHT) of $f(x, y)$ denoted by $H(u, v)$ is a function

$$H : Z_n \times Z_m \to \mathbb{R}$$

given by

$$H(u, v) = Re\ \{F(u, v)\} + Im\ \{F(u, v)\}, \tag{10}$$

where Re and Im are the real and imaginary parts respectively of a discrete Fourier transform $F(u, v)$ given by

$$F(u, v) = \frac{1}{\sqrt{mn}} \sum_{x=0}^{n-1} \sum_{y=0}^{m-1} f(x, y) e^{-i2\pi(\frac{ux}{n} + \frac{vy}{m})}, \tag{11}$$

for $u = 0, 1, 2, ..., n-1$ and $v = 0, 1, 2, ..., m-1$(Gonzalez and Woods (2008)).

The inverse of discrete Hartley transform (iDHT) is its own inverse (Villasenor (1994)). At this stage, the DHT will act as key for cryptosystem, and thus, the number of keys at this stage is given by

$$\mathcal{P}_2 = 1. \tag{12}$$

The last phase of encryption is using random matrix shift cipher (RMSC) which is a special case of RMAC obtained by taking $\mu = \eta = \lambda = \sigma = 1$ in Equations (1) - (4) that is ignoring the multiplier parameters. However, we cannot use RMAC after DHT as done by Mishra and Sharma (2016) because in our case output will contain non integer values and multiplier parameters would

not work. Thus, we have specially proposed RMSC after DHT in our approach. The encryption formula for RMSC on an image matrix of size $n \times m$ is given as

$$\hat{Y}_{even\ row,\ k} \equiv Y_{even\ row,\ j+\alpha'(mod\ m)}, \tag{13}$$

$$\hat{Y}_{odd\ row,\ l} \equiv Y_{odd\ row,\ j+\beta'(mod\ m)}, \tag{14}$$

$$\hat{Y}_{p\ ,\ even\ column} \equiv Y_{i+\gamma'(mod\ n),\ even\ column}, \tag{15}$$

$$\hat{Y}_{q\ ,\ odd\ column} \equiv Y_{i+\delta'(mod\ n),\ odd\ column}, \tag{16}$$

and the decryption formula for RMSC known as inverse random matrix shift cipher (iRMSC) on an image matrix of size $n \times m$ is given as

$$Y_{even\ row,\ j} \equiv \hat{Y}_{even\ row,\ k+m-\alpha'(mod\ m)}, \tag{17}$$

$$Y_{odd\ row,\ j} \equiv \hat{Y}_{odd\ row,\ l+m-\beta'(mod\ m)}, \tag{18}$$

$$Y_{i\ ,\ even\ column} \equiv \hat{Y}_{p+n-\gamma'(mod\ n),\ even\ column}, \tag{19}$$

$$Y_{i\ ,\ odd\ column} \equiv \hat{Y}_{q+n-\delta'(mod\ n),\ odd\ column}, \tag{20}$$

such that

$$\alpha' \neq \beta' \text{ such that } \alpha',\ \beta' \in Z_m - \{0\},$$
$$\gamma' \neq \delta' \text{ such that } \gamma',\ \delta' \in Z_n - \{0\},$$

where Y and $\hat{Y}$ are old and new positions of pixel values of an image matrix before and after applying RMSC, respectively. Clearly, the parameters of RMSC for each component matrix R, G and B act as keys for cryptosystem. So, the possible number of RMSC parameters of an RGB image of size $n \times m$ is given by

$$\mathcal{P}_3 = 3\{(n-1)^2(m-1)^2\}. \tag{21}$$

Hence, the key space of the proposed cryptosystem for an RGB image of size $n \times m$ is as follows:

$$\begin{aligned} \mathcal{K} &= \mathcal{P}_1 + \mathcal{P}_2 + \mathcal{P}_3 \\ &= 3\{[(\phi(m))^2(\phi(n))^2 - 1](n-1)^2(m-1)^2\} + 1 + 3\{(n-1)^2(m-1)^2\} \\ &= 3\{(\phi(m))^2(\phi(n))^2(n-1)^2(m-1)^2\} + 1. \end{aligned} \tag{22}$$

3. Proposed encryption and decryption procedure

In the proposed approach, the RMAC is combined with DHT followed by RMSC is applied on an RGB image of size $n \times m \times 3$. The proposed approach is divided into two phases, in the first phase, RMAC is applied before DHT to achieve required confusion and diffusion. After applying DHT, RMSC is applied on the partially encoded image to further achieve the confusion property in the system. In the first phase, parameters applied on an RGB image have a maximum of $3 \times 8!$ choices, and in second phase of RMSC after DHT, the parameters have a maximum of $3 \times 4!$ choices. Thus, in the proposed approach, the total parameter choices are $3 \times (8! + 4!)$ and these choices are called parameter arrangements. In the first stage before DHT, we apply RMAC parameters $\alpha,\ \beta,\ \gamma,\ \delta,\ \mu,\ \eta,\ \lambda$ and σ on each channel of original image of size $n \times m \times 3$, after that DHT is applied on intermediate images which provide real matrices as output. Henceforth, after DHT, we finally apply RMSC with parameters $\alpha',\ \beta',\ \gamma'$ and δ' on partially encoded images. The encryption procedure of an RGB image is visualized in Figure 1. We will use same Greek letters for inverses of parameters in decryption procedure as used in encryption in order to avoid ambiguity. The decryption procedure of an encrypted image is visualized in Figure 2. Hence, in the proposed approach, it is very tough and troublesome to recover the original RGB image even if a decoder has correct keys but does not know the correct arrangement of parameters. The proposed encryption algorithm for a single color channel (say Red channel) is given below and the same follows for green and blue channels in the scheme. The decryption procedure is based on the same algorithm with inverse parameters using Equations (5)-(8), iDHT using Equation (11), and Equations (17)-(20).

Algorithm: Encryption procedure of the proposed approach on a single color channel.

▷ **Input**: $P_{i,j}$ (original image), keys $\{\alpha_i,\ \beta_i,\ \gamma_i,\ \delta_i\} \in \mathbb{Z}_n, \{\ \mu,\ \eta,\ \lambda, \sigma\} \in \mathbb{U}(n)$, $1 \leq i \leq 2$.
▷ **Output**: $C_{i,j}$ (cipher image).

---

(1) After, separation $P_{i,j}$ into color planes R, G and B.
(2) Select the R channel of size $n \times m$.
(3) Apply Equation (1) on even rows of R channel to shift the pixel position by parameter α_1 and multiply the value of pixels by μ.
(4) Apply Equation (2) on odd rows of partially encrypted image to shift the position of pixels by β_1 and change tha value of pixels by η.
(5) Apply Equation (3) on even columns of the partially encrypted image to shift the position of pixels by γ_1 and multiply the value of pixels by λ.
(6) Apply Equation (4) on the odd columns of partially encrypted image to shift the pixels by δ_1 and change tha value of pixels by σ.
(7) Apply DHT on the partially encoded image by using equation (11).
(8) Apply Equation (13) on even rows of the partialy encrypted image to shift the position of pixels by α_2.

(9) Apply Equation (14) on odd rows of the partialy encrypted image to shift the position of pixels by β_2.
(10) Apply Equation (15) on even columns of the partialy encrypted image to shift the position of pixels by γ_2.
(11) Apply Equation (16) on odd columns of the partialy encrypted image to shift the position of pixels by δ_2.
(12) After completion of step (11) complete encrypted image of R channel is obtained.
(13) Repeat the above procedure for G and B channels with a different set of key parameters.
(14) Concatenate the color channels R, G and B to form the completely encrypted image $C_{i,j}$.

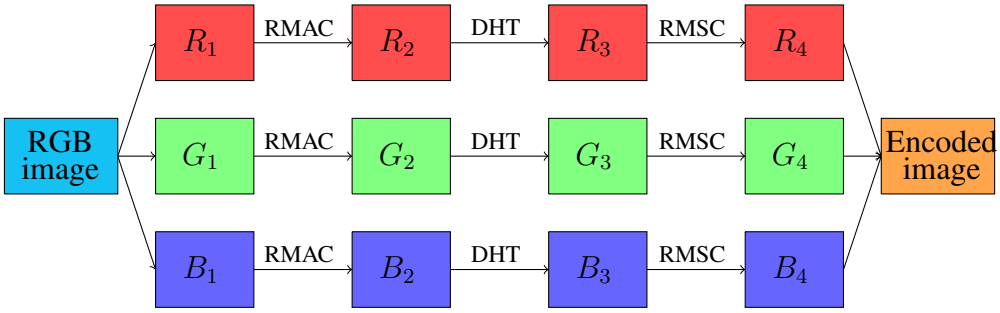

Figure 1. Encryption procedure for an RGB image

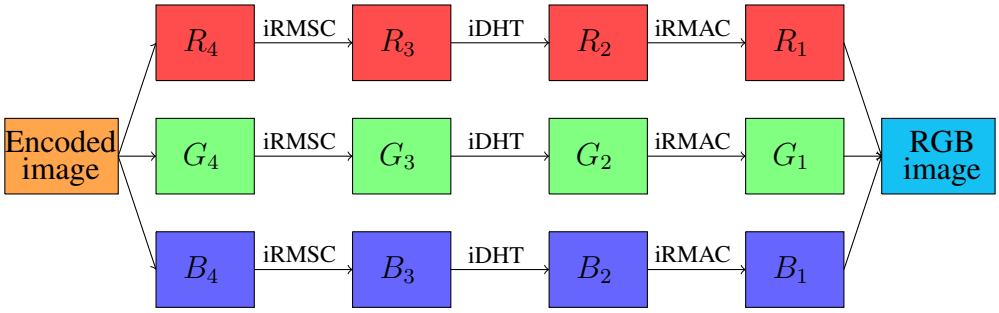

Figure 2. Decryption procedure for an RGB image

4. Demonstration of the procedure

The proposed approach is applied on a lena.jpg RGB image of size $256 \times 256 \times 3$ pixels as shown in Figure 3(a). Figure 3(b) shows encrypted RGB image with the following RMAC and RMSC parameters given in Table 1.

Figure 3(c) represents correctly decrypted RGB image with exact inverse parameters and their correct arrangement as given in Table 2.

Table 1. Parameters for the encrypted image in Figure 3(b)

R	G	B
$\alpha = 141$	$\alpha = 131$	$\alpha = 8$
$\beta = 171$	$\beta = 100$	$\beta = 240$
$\gamma = 209$	$\gamma = 25$	$\gamma = 100$
$\delta = 243$	$\delta = 217$	$\delta = 180$
$\mu = 29$	$\mu = 143$	$\mu = 101$
$\eta = 209$	$\eta = 13$	$\eta = 19$
$\lambda = 247$	$\lambda = 99$	$\lambda = 241$
$\sigma = 103$	$\sigma = 211$	$\sigma = 201$
$\alpha' = 43$	$\alpha' = 200$	$\alpha' = 245$
$\beta' = 78$	$\beta' = 15$	$\beta' = 190$
$\gamma' = 180$	$\gamma' = 171$	$\gamma' = 90$
$\delta' = 241$	$\delta' = 90$	$\delta' = 10$

Table 2. Parameters for correctly decrypted image in Figure 3(c)

R	G	B
$\alpha' = 213$	$\alpha' = 56$	$\alpha' = 11$
$\beta' = 178$	$\beta' = 241$	$\beta' = 66$
$\gamma' = 76$	$\gamma' = 85$	$\gamma' = 166$
$\delta' = 15$	$\delta' = 166$	$\delta' = 246$
$\mu = 53$	$\mu = 111$	$\mu = 109$
$\eta = 49$	$\eta = 197$	$\eta = 27$
$\lambda = 199$	$\lambda = 75$	$\lambda = 17$
$\sigma = 87$	$\sigma = 91$	$\sigma = 121$
$\alpha = 115$	$\alpha = 125$	$\alpha = 248$
$\beta = 85$	$\beta = 156$	$\beta = 16$
$\gamma = 47$	$\gamma = 231$	$\gamma = 156$
$\delta = 13$	$\delta = 39$	$\delta = 76$

Figure 3(d) represents incorrect decrypted RGB image with approximate inverse shift parameters in both RMAC and RMSC with correct multiplier parameters and arrangement as given in Table 3. Figure 3(e) represents incorrect decrypted RGB image with approximate inverse RMAC multiplier

Table 3. Parameters for incorrectly decrypted image in Figure 3(d) with approximate inverse shift parameters

R	G	B
$\alpha' = 214$	$\alpha' = 57$	$\alpha' = 12$
$\beta' = 178$	$\beta' = 242$	$\beta' = 67$
$\gamma' = 77$	$\gamma' = 86$	$\gamma' = 167$
$\delta' = 16$	$\delta' = 167$	$\delta' = 247$
$\mu = 53$	$\mu = 111$	$\mu = 109$
$\eta = 49$	$\eta = 197$	$\eta = 27$
$\lambda = 199$	$\lambda = 75$	$\lambda = 17$
$\sigma = 87$	$\sigma = 91$	$\sigma = 121$
$\alpha = 116$	$\alpha = 126$	$\alpha = 249$
$\beta = 86$	$\beta = 157$	$\beta = 17$
$\gamma = 48$	$\gamma = 232$	$\gamma = 157$
$\delta = 14$	$\delta = 40$	$\delta = 77$

parameters and with the same values of rest of the parameters with correct arrangement as given in Table 4.

Table 4. Parameters for incorrectly decrypted image in Figure 3(e) with approximate inverse RMAC multiplier parameters

R	G	B
$\alpha' = 213$	$\alpha' = 56$	$\alpha' = 11$
$\beta' = 178$	$\beta' = 241$	$\beta' = 66$
$\gamma' = 76$	$\gamma' = 85$	$\gamma' = 166$
$\delta' = 15$	$\delta' = 166$	$\delta' = 246$
$\mu = 54$	$\mu = 112$	$\mu = 110$
$\eta = 50$	$\eta = 198$	$\eta = 28$
$\lambda = 200$	$\lambda = 76$	$\lambda = 18$
$\sigma = 88$	$\sigma = 92$	$\sigma = 122$
$\alpha = 115$	$\alpha = 125$	$\alpha = 248$
$\beta = 85$	$\beta = 156$	$\beta = 16$
$\gamma = 47$	$\gamma = 231$	$\gamma = 156$
$\delta = 13$	$\delta = 39$	$\delta = 76$

Figure 3(f) represents incorrect decrypted RGB image with exact inverse parameters but with their incorrect arrangement as given in Table 5.

Table 5. Parameters for incorrectly decrypted image in Figure 3(f) with incorrect arrangement of parameters

R	G	B
$\alpha' = 11$	$\alpha' = 56$	$\alpha' = 213$
$\beta' = 66$	$\beta' = 241$	$\beta' = 178$
$\gamma' = 166$	$\gamma' = 85$	$\gamma' = 76$
$\delta' = 246$	$\delta' = 166$	$\delta' = 15$
$\mu = 109$	$\mu = 111$	$\mu = 53$
$\eta = 27$	$\eta = 197$	$\eta = 49$
$\lambda = 17$	$\lambda = 75$	$\lambda = 199$
$\sigma = 121$	$\sigma = 91$	$\sigma = 87$
$\alpha = 248$	$\alpha = 125$	$\alpha = 115$
$\beta = 16$	$\beta = 156$	$\beta = 85$
$\gamma = 156$	$\gamma = 231$	$\gamma = 47$
$\delta = 76$	$\delta = 39$	$\delta = 13$

The proposed approach is applied over JPEG RGB image of size $256 \times 256 \times 3$ as shown in Figure 3(a) performed in MATLAB **R2016b (9.1.0.441655)**. Using Equation (22), the maximum number of possible keys for an RGB image with $256 \times 256 \times 3$ pixels is given as:

$$\mathcal{K} = 3\{(\phi(256))^2(\phi(256))^2(256-1)^2256-1)^2\} + 1 \approx 3.405 \times 10^{18}.$$

Furthermore, the proposed approach is verified on a koala.jpg RGB image of size $192 \times 256 \times 3$ pixels given in Figure 4(a). Thus, it is quite evident from these experimental results that the proposed approach is applicable to any $n \times m \times 3$ size RGB image.

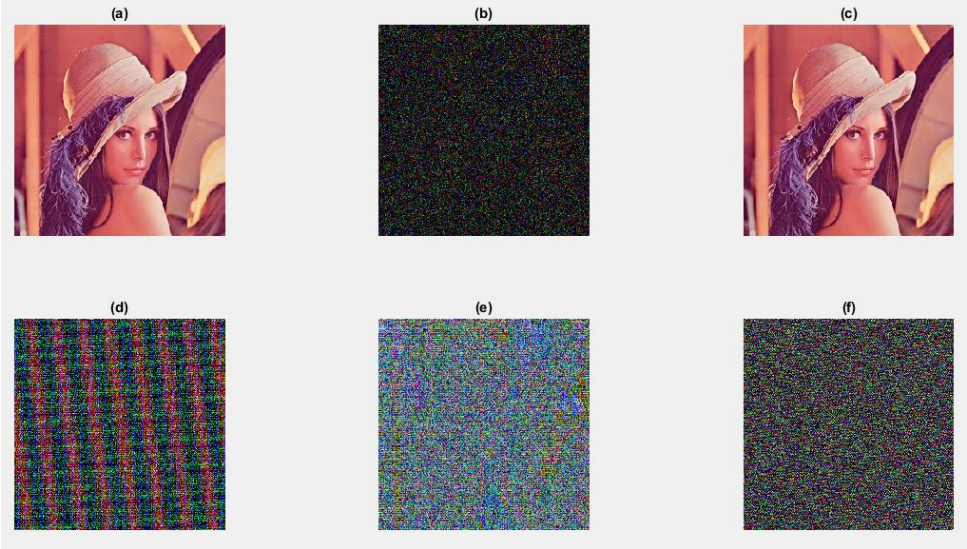

Figure 3. Demonstration results: (a) original image of size $256 \times 256 \times 3$ pixels; (b) encrypted image; (c) correctly decrypted image; (d) incorrectly decrypted image with correct multiplier parameters but approximated shift parameters; (e) incorrectly decrypted image with correct shift parameters but approximated multiplier parameters; (f) incorrectly decrypted image with correct parameters but without knowing the correct arrangement of these parameters. (Readers are advised to refer to the web version of this article for better color interpretation)

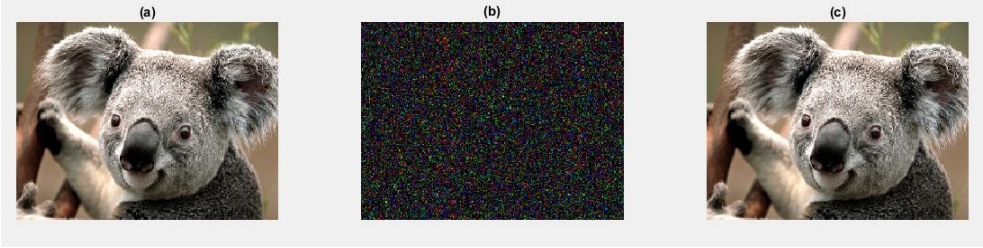

Figure 4. Demonstration results: (a) original image of size $192 \times 256 \times 3$ pixels; (b) encrypted image; (c) correctly decrypted image

5. Security analysis

5.1. Key sensitivity analysis

The proposed approach is highly sensitive to the key parameters. Indeed, high key sensitivity is needed in an efficient approach, so, if there is a slight change in the key parameters the original image cannot be decrypted correctly. Figure 3(a), Figure 3(b) and Figure 3(c) represent the original, the encrypted and correctly decrypted images respectively. Also, Figure 3(d) is an incorrectly decrypted image with mere approximate change in shift parameters $\alpha,\ \beta,\ \gamma,\ \delta,\ \alpha',\ \beta',\ \gamma'$ and δ'. The multiplier parameters $\mu,\ \eta,\ \lambda$ and σ being relatively prime to the order of image matrix are more sensitive, as a slight approximate change to them produce an incorrect decrypted image as shown in Figure 3(e). Last but not least, the arrangement of key parameters is most imperative as a slight change in arrangement will produce incorrect decrypted image as shown in Figure 3(f).

5.2. Mean square error

The mean square error (MSE) between the images of size $n \times m$ for each red(R), green(G) and blue(B) components is calculated from the formula

$$MSE = \frac{1}{nm} \sum_{r=1}^{n} \sum_{s=1}^{m} \{|f(r\Delta x, s\Delta y) - g(r\Delta x, s\Delta y)|^2\}, \tag{23}$$

where Δx and Δy are the pixel sizes and f and g are the image matrix of the original and reconstructed color image respectively. The more the value of MSE for the encrypted images, the more secure the system is against the attacks. Moreover, lower the value of MSE indicate much resemblance towards the original image.

5.3. Peak signal to noise ratio

The Peak signal-to-noise ratio (PSNR) is used as a quality measurement between the images and is computed for each component of RGB image by

$$\begin{aligned} PSNR &= 10 \log_{10} \left(\frac{max_i^2}{MSE} \right) \\ &= 20 \log_{10}(max_i) - 10 \log_{10}(MSE), \end{aligned} \tag{24}$$

where max_i is the maximum possible pixel value of the image. The maximum of max_i is $2^k - 1$, when samples are represented using Linear Pulse Code Modulation (LPCM) with $'k'$ bits per sample.

5.4. Correlation coefficient

The correlation co-efficient (C_r) between the images is used to find the correlation among the corresponding pixels of the images for each components (R, G, B) and can be computed by

$$C_r(X, Y) = \frac{\sum_n \sum_m (X_{nm} - \bar{X})(Y_{nm} - \bar{Y})}{\sqrt{[\sum_n \sum_m (X_{nm} - \bar{X})^2][\sum_n \sum_m (Y_{nm} - \bar{X})^2]}}, \tag{25}$$

where X is the original image and Y is the reconstructed image, $\bar{X}$ and $\bar{Y}$ are the mean of the original image and reconstructed image respectively. The range of correlation is $-1 \leq C_r \leq 1$ such that $C_r \to +1$ implies there is a strong positive relationship between the two images, $C_r \to -1$ implies there is a strong negative relationship among them and $C_r \approx 0$ implies there is no relationship between the images.

The MSE, PSNR and C_r between input image in Figure 3(a) and output images in Figures 3(b)-3(f) for each red(R), green(G) and blue(B) components are given in Tables 6-10 below.

Table 6. Analysis between Figure 3(a) and 3(b)

Color component	MSE	PSNR	C_r
R	2.7125×10^4	3.7971	-0.0014
G	9.4964×10^3	8.3552	1.7514×10^{-4}
B	8.9129×10^3	8.6306	-5.0679×10^{-5}

Table 7. Analysis between Figure 3(a) and 3(c)

Color component	MSE	PSNR	C_r
R	0	∞	1
G	0	∞	1
B	0	∞	1

Table 8. Analysis between Figure 3(a) and 3(d)

Color component	MSE	PSNR	C_r
R	2.2829×10^4	4.5460	-0.0093
G	1.0693×10^4	7.8397	0.0024
B	9.7951×10^3	8.2207	-3.0162×10^{-4}

Table 9. Analysis between Figure 3(a) and 3(e)

Color component	MSE	PSNR	C_r
R	1.7085×10^4	5.8046	0.0034
G	8.4341×10^3	8.8704	0.0037
B	7.1217×10^3	9.6049	-0.0032

Table 10. Analysis between Figure 3(a) and 3(f)

Color component	MSE	PSNR	C_r
R	2.2717×10^4	4.5674	-0.0013
G	1.0907×10^4	7.7538	0.0053
B	9.8039×10^3	8.2168	0.0060

The high MSE, low PSNR and low C_r values indicates that original color image is completely changed and no information can be obtained about original color image from output image. The MSE, PSNR and C_r of completely encrypted image Figure 3(b) for red(R), green(G) and blue(B) are given in Table 6 implying the high efficiency and robustness of the proposed approach. Table 7 represents MSE, PSNR and C_r of correctly decrypted image in Figure 3(c) for color components with correct keys and correct arrangement of RMAC parameters. The zero MSE value, infinite PSNR and C_r = 1 for each red(R), green(G) and blue(B) channels indicate that original color image has been reconstructed completely without loss of any information of color components of RGB image data. In Tables 8-10, the statistical analysis is provided about MSE, PSNR and C_r values for each red(R), green(G) and blue(B) channels of Figures 3(d)-3(f) respectively. The high MSE, low PSNR and low C_r values indicate that no information about original image can be obtained even if the attacker knows all the correct keys, but is unaware about correct arrangement of them. Thus, the statistical analysis of the proposed method for a color image supports the efficiency and robustness. Further, it shows that the security of the system depends not only on the keys but also on the correct arrangement of shift and multiplier parameters.

5.5. Entropy

The entropy is the measure of randomness of an image data. For the secure image encryption, the cipher images should be highly randomized. The good cipher images have an entropy value close to theoretical value of 8. The entropy is denoted by H and calculated from the equation

$$H(m) = \sum_{i=0}^{2^n-1} p(m_i) log \frac{1}{p(m_i)}, \tag{26}$$

where m_i is the gray value and $p(m_i)$ is the probability of occurrence of m_i expressed in bits. The Table 11 below shows the entropy value of the plain image and the corresponding cipher image. The entropy values of the cipher image are close to the ideal value which indicates that the proposed method can generate good random encrypted images.

Table 11. Entropy analysis of the scheme

Metrics	Color plane	Plain image	Cipher image
Lena	R	7.3033	7.9972
	G	7.6125	7.9973
	B	7.0862	7.9972

5.6. NPCR

The NPCR (Number of Pixels Change Rate) is a well known accepted parameter used to test the resistance of image encryption technique against the differential attacks. The high value of NPCR is considered as a high resistance toward the differential attacks. When a small change in the orginal image causes a big effect in its cipher image, so that the hacker cannot extract the information between the images then the NPCR value is approximate to theoretical value 100%. The following equation is used to calculate the value of NPCR,

$$\mathcal{N}(C_1, C_2) = \frac{1}{mn} \sum_{i,j} D(i,j) \times 100\%;\ D(i,j) = \begin{cases} 1, & \text{if } C_1(i,j) \neq C_2(i,j), \\ 0, & \text{elsewhere}, \end{cases} \tag{27}$$

where C_1 and C_2 are the cipher images before and after one pixel change in the plain image. Table 12 below shows the statistical values of the NPCR.

Table 12. NPCR analysis of the scheme

Metrics	Color plane	NPCR(%)
Lena	R	99.4043
	G	99.5468
	B	98.5443

5.7. Histogram analysis

The histogram of a digital image is a discrete function $h(r_k) = n_k$, where r_k is the k^{th} intesity value and n_k is the number of pixels in the image with intensity r_k (Gonzalez and Woods (2008)).

So, a histogram of a color image is defined as the graphical representation of the pixel intensity distribution at each intensity level.

The histogram of the original color image (Figure 3(a)) is given in Figure 5(a) and the histogram of the encrypted image (Figure 3(b)) is given in Figure 5(b). The histograms in Figure 5(a) and Figure 5(b) are totally different without any resemblance, so, the attacker cannot get any information from the encrypted image in order to reconstruct original image. Figure 5(c) is the histogram of the Figure 3(c) which is correctly decrypted image with correct keys and correct arrangement of parameters and is same as Figure 5(a) showing that the image data of correctly decrypted image is same as original image without loss of any information in RGB components. Similarly, the Figures 5(d)-5(f) are histograms of the Figures 3(d)-3(f) respectively. Clearly, these histograms show tremendous variation and no resemblance compared to Figure 5(a) because of an approximate change in key parameters and their arrangements. Therefore, the histogram analysis proves the high sensitiveness of the proposed approach and high security level of the encrypted data and hence the proposed technique is robust, fortified and appropriate.

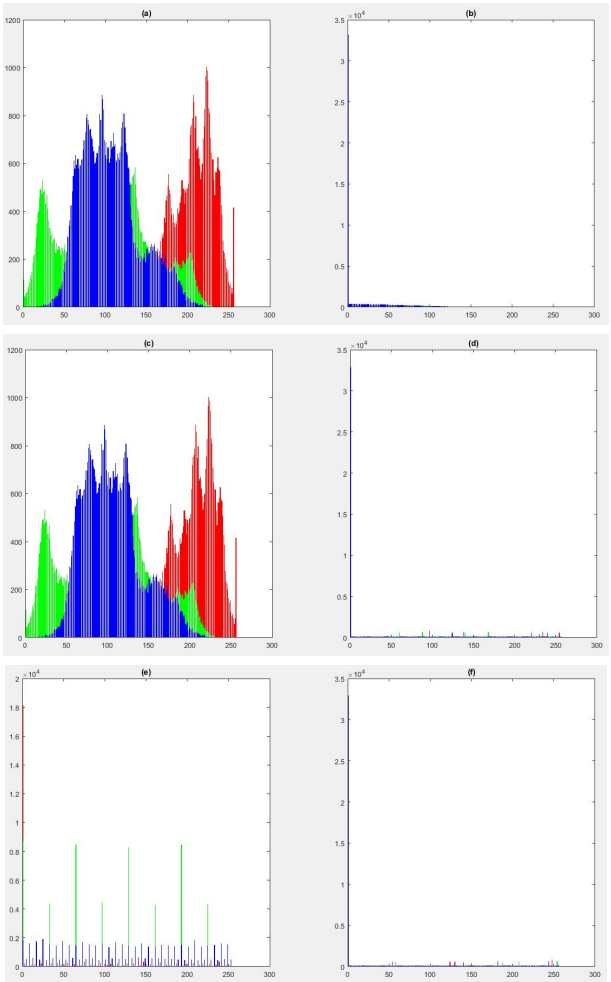

Figure 5. Histogram Analysis: (a) histogram of Figure 3(a); (b) histogram of Figure 3(b); (c) histogram of Figure 3(c); (d) histogram of Figure 3(d); (e) histogram of Figure 3(e); (f) histogram of Figure 3(f)

5.8. Pixel intensity distribution analysis of the images at horizontal, vertical and diagonal pixels

The pixel intensity distributions (PID) of two neighboring pixels at horizontal, vertical and diagonal directions of the original image in Figure 3(a) and the encrypted image in Figure 3(b) are shown in Figure 6 and Figure 7 respectively. The PID of the encrypted image in Figure 7 is accumilated on left-down corner in the domain, which is totally different from the PID of the original image in Figure 6. The PID of encrypted image indicates that no information can be retrieved regarding original image. So, the encrypted image is secure against crypto attacks. Also, the PID of the two neighboring pixels of the correctly decrypted image in Figure 3(c) is shown in Figure 8, which is exactly same as the PID of the original image in Figure 6 indicating that the original image can be completely reconstructed from the encrypted image without loss of any information by taking correct keys and correct arrangement.

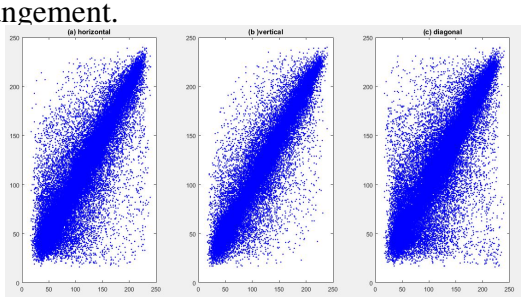

Figure 6. Pixel intensity distribution at diagonal, vertical and horizontal pixels of the original image Figure 3(a)

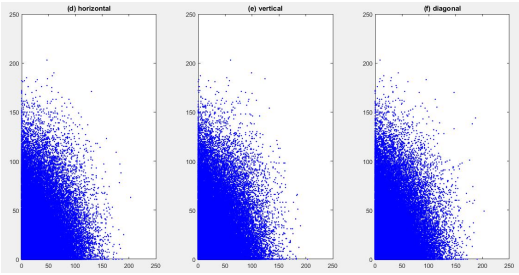

Figure 7. Pixel intensity distribution at diagonal, vertical and horizontal pixels of the encrypted image Figure 3(b)

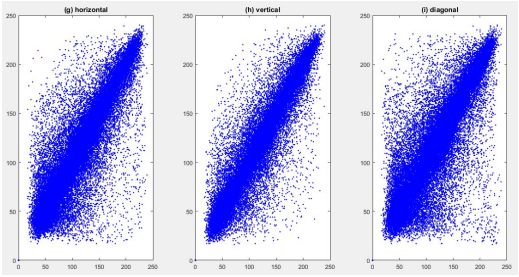

Figure 8. Pixel intensity distribution at diagonal, vertical and horizontal pixels of the decrypted image Figure 3(c)

6. Comparison of proposed approach with some existing methods

The proposed approach is compared with a number of existing techniques available in the literature (Sangavi and Thangavel (2019); Mishra et al. (2017); Ranjan et al. (2016); Lone and Singh (2020)).

The comparison has been done with reference to MSE, PSNR, correlation, entropy and NPCR by taking average values of the components in Table 13. From Table 13, one can conclude that the proposed technique is efficient, robust and can resist various cryptanalytic attacks as compared to the conventional methods.

Table 13. Comparison of the scheme with the existing methods

Metrics	MSE	PSNR	Entropy	correlation	NPCR
Ref. (Sangavi and Thangavel (2019))	7927.52	8.6000	7.9970	-0.00365	NA
Ref. (Mishra et al. (2017))	9950.76	8.1490	7.4739	0.00043	NA
Ref. (Ranjan et al. (2016))	5919.33	10.4199	NA	-0.0140	NA
Ref. (Lone and Singh (2020))	9425.16	8.3970	7.9974	-0.0001	99.6220
Proposed	15177.6	6.9276	7.9972	-0.00043	99.1651

7. Conclusion

The proposed approach is a multilayer security scheme for color image data based on random matrix affne cipher (RMAC) associated with discrete Hartley transform (DHT) and random matrix shift cipher (RMSC). This approach is applicable to any size of RGB image. The shift and multiplier parameters in RMAC and the shift parameters in RMSC act as key parameters in the proposed cryptosystem, and their arrangement is fundamental in the algorithm. The encrypted RGB image has a real nature because of Hartley transform, which can reduce the storage space and time complexity in practical applications. Also, the computer simulations demonstrate the validity, security, robustness and efficiency of the proposed technique.

Acknowledgment:

The authors are deeply thankful to the anonymous reviewer and the Editor-in-Chief for their valuable suggestion and comments which helped us to improve the quality of the paper in its present form.

REFERENCES

Abuturab, M. R. (2013). Color image security system based on discrete Hartley transform in gyrator transform domain, Opt Lasers Eng, Vol. 51, pp. 317-324.

Abuturab, M. R. (2012a). Color image security system using double random-structured phase encoding in gyrator transform domain, Appl Opt., Vol. 51, pp. 3006-3016.

Abuturab, M. R. (2012b). Securing color information using Arnold transform in gyrator transform domain. Opt Lasers Eng., Vol. 50, pp. 772-779.

Antonini, M., Barlaud, M., Mathieu, P. and Daubechies, I. (1992). Image coding using wavelet transform, IEEE Transaction on Image Processing, Vol. 1, pp. 205-220.

Chen, H., Du, X., Liu, Z. and Yang, C. (2013). Color image encryption based on the affine transform and gyrator transform, Opt Lasers Eng., Vol. 51, pp. 768-775.

Chen, L. and Zhao, D. (2006). Optical image encryption with Hartley transforms, Opt Lett., Vol. 31, pp. 3438-3440.

Chen, L. and Zhao, D. (2008). Image encryption with fractional wavelet packet method, Optik, Vol. 119, pp. 286-291.

Gallian, J. A. (1999). *Contemporary Abstract Algebra,* Narosa Publication House.

Gonzalez, R. C. and Woods, R. E. (2008). *Digital Image Processing* (3rd edition), Prentice Hall, Upper Saddle River, NJ.

Hahn, J., Kim, H. and Lee, B. (2006). Optical implementation of iterative fractional Fourier transform algorithm, Opt Express, Vol. 14, pp. 11103-11112.

Hennelly, B. and Sheridan, J. T. (2003). Optical image encryption by random shifting in fractional Fourier domains, Opt Lett., Vol. 28, pp. 269-271.

Liu, S., Mi, Q. and Zhu, B. (2001). Optical image encryption with multi stage and multi channel fractional Fourier-domain filtering, Opt Lett., Vol. 26, pp. 1242-1244.

Liu, Z., Chen, H., Liu, T., Li, P., Dai, J., Sun, X. and Liu, S. (2010a). Double-image encryption based on the affine transform and the gyrator transform, J Opt., Vol. 12, pp. 03540-03547.

Liu, Z., Dai, J., Sun, X. and Liu, S. (2010b). Color image encryption by using the rotation of color vector in Hartley transform domains, Opt Lasers Eng., Vol. 48, pp. 800-805.

Liu, Z. J. and Liu, S. T. (2007). Random fractional Fourier transform, Optics Letters, Vol. 32, pp. 2088-2090.

Liu, Z., Xu, L., Liu, T., Chen, H., Li, P., Lin, C. and Liu, S. (2011). Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains, Opt Commun., Vol. 284, pp. 123-128.

Liu, Z., Zhang, Y., Liu, W., Meng, F., Wu, Q. and Liu, S. (2013). Optical color image hiding scheme based on chaotic mapping and Hartley transform, Opt Lasers Eng., Vol. 51, pp. 967-972.

Lone, P. N. and Singh, D. (2020). Application of algebra and chaos theory in security of color images, Optik, Vol. 218, pp. 165155.

Mishra, D. C. and Sharma, R. K. (2016). An approach for security of color image data in coordinate, geometric, and frequency domains, Information Security Journal, Vol. 25, pp. 213-234.

Mishra, D. C., Sharma, R.K., Saurav, S. and Akhilesh, P. (2017). Multi-layer security of color image based on chaotic system combined with RP2DFRFT and Arnold Transform, J. Infor. Secur. Appl., Vol. 37, pp. 65-90.

Peng, X., Wei, H. and Zhang, P. (2006a). Chosen-plain text attack on lensless double-random phase encoding in the Fresnel domain, Opt Lett., Vol. 31, pp. 3261-3263.

Peng, X., Zhang, P., Wei, H. and Yu, B. (2006b). Known-plain text attack on optical encryption based on double random phase keys, Opt Lett., Vol. 31, pp. 1044-1046.

Rakesh, R., Sharma, R. K. and Hanmandlu, M. (2016). Color image encryption and decryption using Hill Cipher associated with Arnold transform, AAM, Vol. 11, No. 1, pp. 45 - 60

Sangavi, V. and Thangavel, P. (2019). An Image Encryption Algorithm Based On Fractal Geometry, Procedia Computer Science, Vol. 165, pp. 462-469.

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

Villasenor, J. D. (1994). Optical Hartley transforms, Proc IEEE, Vol. 82, pp. 391-399.