Multimedia Tools and Applications (2021) 80:27829–27853
https://doi.org/10.1007/s11042-021-11003-x

Multi-layer color image encryption using random matrix affine cipher, RP2DFrHT and 2D Arnold map

Shazia Sabir[1] · Vandana Guleria[1]

Received: 13 February 2021 / Revised: 16 April 2021 / Accepted: 4 May 2021 /
Published online: 25 May 2021

Abstract

Confidentiality, integrity, authenticity, non-repudiation and storing and transmitting images over the unsecured channel has become a challenging task nowadays. In this scenario, a robust image encryption technique over open network has grasped a great deal of attention. In this paper to meet this challenge, we have established a new multi-layer robust color image encryption using random matrix affine cipher (RMAC), reality preserving two dimensional discrete fractional Hartley transform (RP2DFrHT) and two dimensional Arnold map. The first stage of encryption is designed through RMAC. RMAC provides security in co-ordinate domain as well as in geometrical domain. So if a hacker has knowledge about all the pixels of an image, but has no information about the mechanism of co-ordinate domain he/she cannot steal any information. The second stage of encryption is obtained incorporating the concept of RP2DFrHT. The reality preserving transform eliminates the complex-valued coefficients and provides the real-valued coefficients of encrypted image. The real-valuedness of data provides convenient platform for display, storage and transmission in digital domain. The third stage of encryption is done using 2D Arnold map, which not only enhances the security but also enlarges key space. Therefore, the proposed technique provides security in geometrical, co-ordinate, frequency and time domains simultaneously. The security of our proposed technique depends upon the secret keys as well as their correct arrangements. Simulation analysis provides the complete visual results of all stages of encrypted and decrypted images. Sensitivity analysis validates that our proposed technique is highly sensitive towards its secret keys and their arrangements. Statistical analysis such as histogram analysis, MSE, PSNR, correlation coefficient, entropy analysis and resistivity of classical attacks validates the effectiveness and feasibility of our proposed work. Moreover, comparison analysis testifies that our proposed technique functions significantly well as compared to existing similar techniques.

Keywords Random matrix affine cipher · Reality preserving two dimensional discrete fractional Hartley transform · 2D Arnold map · Image encryption and image decryption

✉ Vandana Guleria
vandana@bitmesra.ac.in

[1] Department of Mathematics, Birla Institute of Technology Mesra, Ranchi, India

1 Introduction

Internet is a valuable resource for us. In today's world, we rely too much on the Internet. It is very useful tool for work, education, shopping, personal entertainment, etc. Network and communication technologies are the important modes of transferring images over the Internet. Images are used in various fields such as engineering services, scientific experiments, medical imaging, advertising, art exhibition and online education, etc. With the increasing use of digital technologies for transmitting and storing images, secure transmission of images is a major concern. Image data is highly sensitive and prone to abrupt by intruders. Also image has high redundancy and strong correlation between the pixels. To protect sensitive data from an unauthorized access is a prime agenda nowadays. Therefore, secure communication is required for transmission of images over the Internet. In respond to this demand, cryptography and steganography are the two important security systems which offered a convenient platform for secure data transmission. Steganography is an efficient technique of hiding the fact that communication is taking place by hiding information in other information. It is profitable in various applications like government services, business communications, military services and medical services, etc. Abdulla [1] has contributed a significant work on the basis of steganography. In his work, he has developed secure and efficient image-based steganography approaches that enhance embedding efficient and improve message un-detectability. Whereas, cryptography enables us to transmit images over a public domain from a sender to a receiver in such a way that the opponent cannot guess what is being transmitted. The public channel could be telephone line, computer network, etc. The information that the sender wants to send to the receiver is called plaintext. The plaintext could be images, English text, numerical data, or anything. The plaintext is encrypted using a predetermined key and the resulting ciphertext is sent over the public channel. The opponent cannot guess the plaintext from the ciphertext. The receiver decrypts the ciphertext using the encryption key and reconstructs the plaintext. Image encryption plays an important role in the field of information hiding. While dealing with image encryption techniques, intrinsic properties of images such as high redundancy, bulk data capacity and strong correlation between the pixels must be considered. Due to intrinsic properties of images, techniques based on classical cryptography are less efficient for digital images. To overcome this issue, several methods have been proposed for secure transmission of images over the unsecured channel. Refregier and Javidi [29] was the first one who proposed optical image encryption using double random phase encoding (DRPE). This concept highlighted the encryption technique. DRPE was further extended from Fourier domain to the fractional Fourier domain [5, 12, 25, 26], Fresnel domain [13, 15, 32], gyrator domain [6, 21], Hartley transform [3, 4, 20], fractional wavelet transform [7, 9, 23], fractional Mellin transform [36, 43, 44], fractional Hartley transform [14, 27, 30, 31, 40, 42]. The aforementioned image encryption techniques on the basis of fractional transform have provided better performance and higher security. However the major drawback with these techniques is the complex-valued coefficients of encrypted images. The complex-valued coefficients of encrypted images not only make them inconvenient for display, but also increases the storage, computational and communication complexities in digital domain. To overcome these shortcomings, Venturini and Duhamel [37] proposed reality preserving fractional transform. The reality preserving fractional transform eliminates the burden of complex-valued coefficients and provides the real-valued coefficients of encrypted image. The real-valued nature of data is convenient for display and decreases the storage, computational and communication complexities of the encrypted image in digital environment. On the basis of this method, Guleria et al. [10] proposed a novel approach for security of multiple color images using asymmetric RSA cryptosystem, reality preserving fractional discrete cosine transform and Arnold transform.

Our contribution The concepts of RMAC, RP2DFrHT and 2D Arnold map are merged to design a new multi-layer robust color image encryption. The major contributions of our proposed encryption technique are as listed below.

1. Affine cipher is a well known and most commonly used encryption scheme. Earlier developed techniques [30, 46] using affine cipher are secured in geometrical domain only. However, in this paper the security system designed in the first stage of encryption through RMAC possesses security in co-ordinate domain as well as in geometrical domain. So if a hacker has knowledge about all the pixels of an image, but has no information about the mechanism of co-ordinate domain he/she cannot steal any information. The main reason is that in co-ordinate domain only the positions of the pixels are modified whereas the values of the pixels remain constant. In addition, arrangement of RMAC is very sensitive.
2. To provide next layer of security RP2DFrHT is implemented. Its inherent characteristic over other fractional transforms is the effective potential of real-valuedness which offers the convenient medium for display, storage and transmission over the unsecured public environment.
3. To provide extra layer of security in third stage of encryption Arnold map is used. The existing techniques [2, 11, 22] have used periodic property of Arnold map in decryption process, whereas in our proposed technique decryption process is done using inverse Arnold map. Moreover, we have used the generalized Arnold map which is faster. The encryption and decryption process require secret keys which enlarges our key space and enhances the security system significantly.

   To summarize this, our proposed encryption technique provides multi-layer security in geometrical, co-ordinate, frequency and time domains. It provides convenient medium for storage, display as well as transmission in digital domain. The security of the proposed technique depends not only upon the secret keys, but their arrangements also play a vital role. The secret keys and their arrangements are highly sensitive for robustness.

Paper organization We have organized the remaining sections of the paper as follows: Mathematical formulation of RMAC, RP2DFrHT and 2D Arnold map are explained in Section 2. The whole procedure of implementation of presented technique are covered in Section 3. In Section 4, simulation is provided. (i) Security analysis and (ii) Statistical analysis can be viewed through Sections 5 and 6 respectively. In Section 7, comparison analysis is provided. Lastly, the proposed technique is concluded in Section 8.

2 Preliminaries

In this section, we give a brief introduction of RMAC, RP2DFrHT and 2D Arnold map which are used in our proposed encryption technique.

2.1 Random matrix affine cipher (RMAC) [18]

Affine cipher is a well recognized mono-alphabetic substitution cipher mostly used for encryption of textual data. In our proposed technique RMAC [18] is used which performed better as compared to affine cipher. The proposed technique provides security in co-ordinate domain as well as in geometrical domain. The algorithm of RMAC is demonstrated in Fig. 1. The pixel intensity of $m \times n$ RGB image is given in matrix Y. The pixels of the image are categorized in even and odd numbered rows and columns. Even and odd numbered rows of the matrix Y are multiplied by the multiplicative parameters χ and η respectively. The co-ordinates of even and odd numbered rows are shifted by the shift parameters α and β respectively. The multiplicative parameters χ and η are coprime to n i.e $\gcd(\chi, n) = 1$ and $\gcd(\eta, n) = 1$ and $0 < \alpha \neq \beta < n$. Similar mechanism is adopted for even and odd numbered columns. Even and odd numbered columns of the matrix Y are multiplied by the multiplicative parameters λ and ω respectively. The co-ordinates of even and odd numbered columns are shifted by the shift parameters γ and δ respectively. The multiplicative parameters λ and ω are coprime to m i.e $\gcd(\lambda, m) = 1$ and $\gcd(\omega, m) = 1$ and $0 < \gamma \neq \delta < m$. The mathematical expression of RMAC on RGB image matrix Y is given as follows.

$$\begin{aligned} Y'_{\text{even row},\ p} &\equiv \chi Y_{\text{even row},\ i+\alpha (\text{mod } n)}, \\ Y'_{\text{odd row},\ q} &\equiv \eta Y_{\text{odd row},\ i+\beta (\text{mod } n)}, \\ Y'_{k,\ \text{even column}} &\equiv \lambda Y_{j+\gamma (\text{mod } m),\ \text{even column}}, \\ Y'_{l,\ \text{odd column}} &\equiv \omega Y_{j+\delta (\text{mod } m),\ \text{odd column}}. \end{aligned} \tag{1}$$

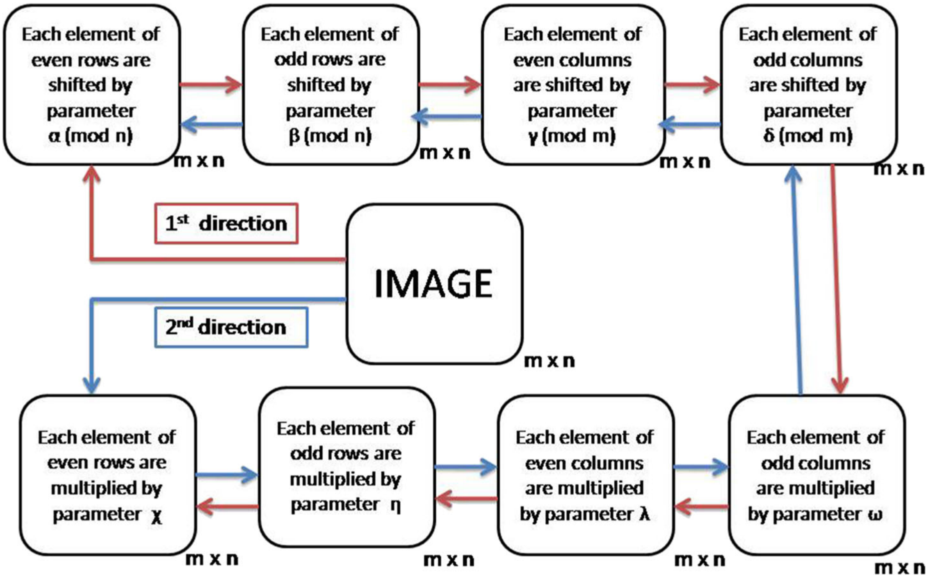

Each element of even rows are shifted by parameter α (mod n)
m x n
Each element of odd rows are shifted by parameter β (mod n)
m x n
Each element of even columns are shifted by parameter γ (mod m)
m x n
Each element of odd columns are shifted by parameter δ (mod m)
m x n
1st direction
IMAGE
m x n
2nd direction
Each element of even rows are multiplied by parameter χ
m x n
Each element of odd rows are multiplied by parameter η
m x n
Each element of even columns are multiplied by parameter λ
m x n
Each element of odd columns are multiplied by parameter ω
m x n

Fig. 1 Framework of RMAC for an RGB image of size $m \times n$

The inverse random matrix affine cipher (IRMAC) for decoding an RGB image Y' is provided below.

$$\begin{aligned} Y_{\text{even row},\ i} &\equiv \mu Y'_{\text{even row},\ p+n-\alpha (\text{mod } n)}, \\ Y_{\text{odd row},\ i} &\equiv \kappa Y'_{\text{odd row},\ q+n-\beta (\text{mod } n)}, \\ Y_{j,\ \text{even column}} &\equiv \nu Y'_{k+m-\gamma (\text{mod } m),\ \text{even column}}, \\ Y_{j,\ \text{odd column}} &\equiv \sigma Y'_{l+m-\delta (\text{mod } m),\ \text{odd column}}, \end{aligned} \tag{2}$$

where $\mu\chi \equiv 1(\text{mod } n)$, $\kappa\eta \equiv 1(\text{mod } n)$, $\nu\lambda \equiv 1(\text{mod } m)$ and $\sigma\omega \equiv 1(\text{mod } m)$. The matrix Y is an original RGB image whereas the matrix Y' is the matrix after using RMAC. Shift parameters and multiplier parameters are used as secret keys.

2.2 Reality preserving two dimensional discrete fractional Hartley transform (RP2DFrHT) [17, 45]

The elements of the $N \times N$ discrete Hartley transform (DHT) matrix H are as follows.

$$H_{ab} = \frac{1}{\sqrt{N}} \left[\cos\left(\frac{2\pi ab}{N}\right) + \sin\left(\frac{2\pi ab}{N}\right) \right], \tag{3}$$

where $0 \leq a, b \leq N - 1$.

Tridiagonal matrix S is given below.

$$S = \begin{bmatrix} 2 & 1 & 0 & \dots & 0 & 1 \\ 1 & 2\cos\left(\frac{2\pi}{N}\right) & 1 & \dots & 0 & 0 \\ 0 & 1 & 2\cos\left(\frac{4\pi}{N}\right) & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 2\cos\left[\frac{2(N-2)\pi}{N}\right] & 1 \\ 1 & 0 & 0 & \dots & 1 & 2\cos\left[\frac{2(N-1)\pi}{N}\right] \end{bmatrix}. \tag{4}$$

The eigen-decomposition of the $N \times N$ DHT matrix H [27] is given below.

$$H = UDU', \tag{5}$$

where U is a matrix obtained from the eigenvector of the tridiagonal matrix S given in (4), D is a diagonal matrix which consists of the eigenvalues of DHT matrix as its diagonal entries and U' is the transpose of the matrix U.

The discrete fractional Hartley transform H^c is obtained by taking the cth power of the matrix H as given below.

$$H^c = UD^cU', \tag{6}$$

where c is the fractional order.

The two dimensional discrete fractional Hartley transform (2DFrHT) for the $N \times N$ matrix X is

$$Z = H^c X (H^c)'. \tag{7}$$

The encrypted image obtained using 2DFrHT is a complex-valued image, whereas the original image is a real-valued image. To achieve real-valued encrypted image, reality preserving two dimensional discrete fractional Hartley transform (RP2DFrHT) [17, 45] is used.

The RP2DFrHT kernel matrix is given as

$$R_H^c = \begin{bmatrix} \mathrm{Re}(H^c) & -\mathrm{Im}(H^c) \\ \mathrm{Im}(H^c) & \mathrm{Re}(H^c) \end{bmatrix}. \tag{8}$$

The RP2DFrHT for the $N \times N$ matrix X is given as

$$E = R_H^c X R_H^d, \tag{9}$$

where c and d are the fractional orders.

The IRP2DFrHT for decoding the $N \times N$ matrix E is given as

$$X = R_H^{-c} E R_H^{-d}. \tag{10}$$

2.3 2D Arnold map [33]

The two dimensional (2D) Arnold map is enormously utilized in image encryption algorithms. It is used to dislocate the position of the pixels in an RGB image. The 2D Arnold map is shown below.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & v \\ u & uv+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}\ n), \tag{11}$$

The inverse Arnold map is given below.

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} uv+1 & -v \\ -u & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} (\mathrm{mod}\ n), \tag{12}$$

where u and v are the Arnold keys, (x, y) are the original pixels, (x', y') are the pixels after using 2D Arnold map and $u, v \in \mathbb{Z}^+$, $\mathbb{Z}^+$ is the set of positive integers.

3 Proposed method

We design a new multi-layer encryption technique for color image security. In the proposed technique, the concepts of RMAC, RP2DFrHT and Arnold map are merged. The proposed technique is discussed in two phases. First phase is an encryption process and second phase is a decryption process.

Phase 1: Encryption process Encryption is the phenomenon of converting plain image (original) into an unintelligible format of image called encrypted image. The whole encryption process is diagrammatically represented in the form of flowchart in Fig. 2. Firstly, three color components as red (R), green (G) and blue (B) are obtained by splitting the RGB image. Secondly, each component of RGB image is processed separately. A detailed description is given as below.

Stage-I (RMAC):- This stage involves the generation of the first stage encrypted image. The RMAC is implemented on each component of the original RGB color image. Two types of parameters are required in this stage. One is shift parameters and another is multiplier parameters. The shift parameters and multiplier parameters are as given below.

1. For red component (R): The shift parameters are α_R, β_R, γ_R, δ_R and the multiplier parameters are $\chi_R, \eta_R, \lambda_R, \omega_R$.
2. For green component (G): The shift parameters are α_G, β_G, γ_G, δ_G and the multiplier parameters are $\chi_G, \eta_G, \lambda_G, \omega_G$.

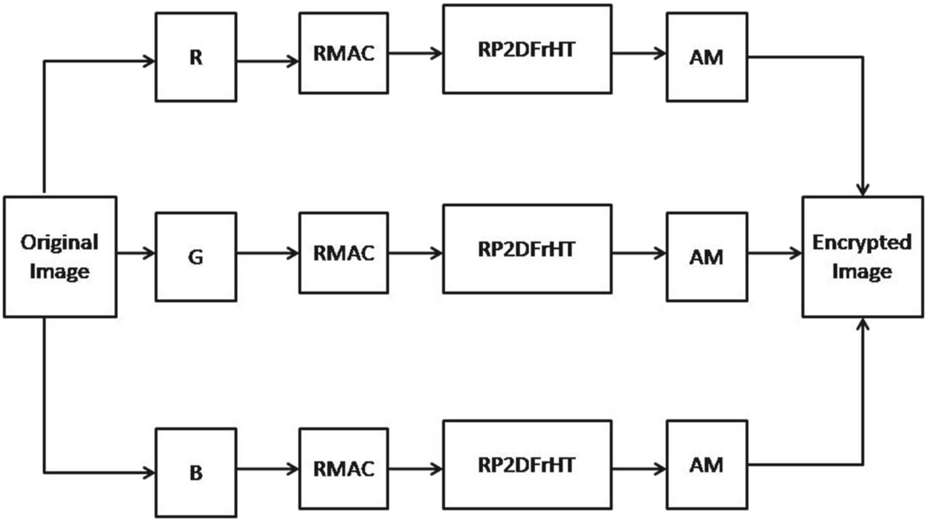


Fig. 2 Flowchart of Encryption process

3. For blue component (B): The shift parameters are α_B, β_B, γ_B, δ_B and the multiplier parameters are $\chi_B, \eta_B, \lambda_B, \omega_B$.

At the end of this stage, red, green and blue components of the first stage encrypted image are obtained for red, green and blue components of the original RGB image.

Stage-II (RP2DFrHT):- The second stage encrypted image is obtained by using RP2DFrHT. The RP2DFrHT is implemented on each component of the first stage encrypted image. The implementation is done using the fractional orders. The fractional orders for each component are as given below.

1. For red component (R): The fractional orders are c_R and d_R.
2. For green component (G): The fractional orders are c_G and d_G.
3. For blue component (B): The fractional orders are c_B and d_B.

At the end of this stage, red, green and blue components of the second stage encrypted image are obtained for red, green and blue components of the first stage encrypted image.

Stage-III (Arnold map):- The complete encrypted image is obtained by scrambling the pixels of each component of the second stage encrypted image. The scrambling is done using Arnold map. In this stage the Arnold keys are given as follows.

1. For red component (R): The Arnold keys are u_R and v_R.
2. For green component (G): The Arnold keys are u_G and v_G.
3. For blue component (B): The Arnold keys are u_B and v_B.

At the end of this stage, red, green and blue components of the third stage encrypted image are obtained for red, green and blue components of the second stage encrypted image. By combining red, green and blue components of the third stage encrypted image, we obtain the complete encrypted image.

Phase 2: Decryption process The process of converting an encrypted image into a plain image (original) is called decryption. It is basically a reverse process of the encryption. The whole decryption process is diagrammatically represented in the form of flowchart in Fig. 3. The whole procedure is processed using correct secret keys as well as their correct arrangements. A detailed description is given as below.

Stage-I (Reverse of Arnold map):- The complete encrypted image firstly segregated into red, green and blue components. The inverse Arnold map is applied on each component R, G, B of the encrypted image. At the end of this stage, scrambled pixels are converted into unscrambled pixels. The red, green and blue components of the first stage decrypted image are obtained for red, green and blue components of the complete encrypted image.

Stage-II (Reverse of RP2DFrHT):- In this stage IRP2DFrHT is applied to decrypt the image obtained in the first stage. The inverse fractional orders for each component are as given below.

1. For red component (R): The inverse fractional orders are c_R^{-1} and d_R^{-1}.
2. For green component (G): The inverse fractional orders are c_G^{-1} and d_G^{-1}.
3. For blue component (B): The inverse fractional orders are c_B^{-1} and d_B^{-1}.

At the end of this stage, red, green and blue components of the second stage decrypted image are obtained for red, green and blue components of the first stage decrypted image.

Stage-III (Reverse of RMAC):- Lastly inverse RMAC is applied to decrypt the image obtained in the second stage. The decryption keys involve in this process are as follows.

1. For red component (R): The inverse shift parameters are α_R^{-1}, β_R^{-1}, γ_R^{-1}, δ_R^{-1} and the inverse multiplier parameters are $\mu_R, \kappa_R, \nu_R, \sigma_R$.
2. For green component (G): The inverse shift parameters are α_G^{-1}, β_G^{-1}, γ_G^{-1}, δ_G^{-1} and the inverse multiplier parameters are $\mu_G, \kappa_G, \nu_G, \sigma_G$.

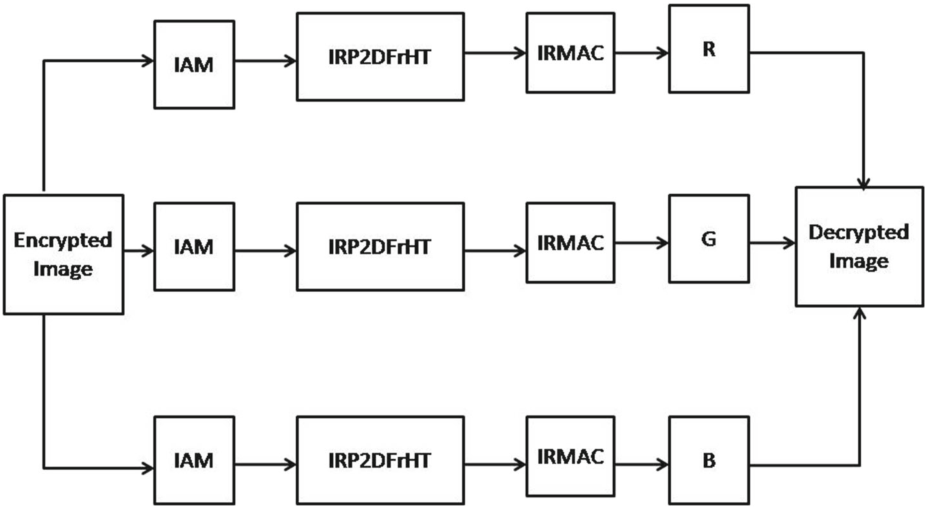


Fig. 3 Flowchart of Decryption process

3. For blue component (B): The inverse shift parameters are α_B^{-1}, β_B^{-1}, γ_B^{-1}, δ_B^{-1} and the inverse multiplier parameters are $\mu_B, \kappa_B, \nu_B, \sigma_B$.

As $\mu_R\chi_R \equiv 1 (\text{mod } N)$, $\kappa_R\eta_R \equiv 1 (\text{mod } N)$, $\nu_R\lambda_R \equiv 1 (\text{mod } N)$, $\sigma_R\omega_R \equiv 1 (\text{mod } N)$, $\mu_G\chi_G \equiv 1 (\text{mod } N)$, $\kappa_G\eta_G \equiv 1 (\text{mod } N)$, $\nu_G\lambda_G \equiv 1 (\text{mod } N)$, $\sigma_G\omega_G \equiv 1 (\text{mod } N)$, $\mu_B\chi_B \equiv 1 (\text{mod } N)$, $\kappa_B\eta_B \equiv 1 (\text{mod } N)$, $\nu_B\lambda_B \equiv 1 (\text{mod } N)$, $\sigma_B\omega_B \equiv 1 (\text{mod } N)$. At the end of this stage, red, green and blue components of the third stage decrypted image are obtained. By combining red, green and blue components of the third stage decrypted image, we obtain the complete decrypted image.

4 Simulation

In this section, simulation is done to examine the authenticity and feasibility of the proposed encryption technique. For simulation, Lena color image of size 512 × 512 × 3 is taken as shown in Fig. 4a. The first stage encrypted image obtained using RMAC is given in Fig. 4b. The shift parameters and multiplier parameters used in this stage are as follows.

1. For red component (R): The shift parameters are α_R=450, β_R=170, γ_R=145, δ_R=371 and the multiplier parameters are χ_R=233, η_R=147, λ_R=313, ω_R=291.
2. For green component (G): The shift parameters are α_G=151, β_G=71, γ_G=250, δ_G=300 and the multiplier parameters are χ_G=119, η_G=417, λ_G=505, ω_G=215.
3. For blue component (B): The shift parameters are α_B=399, β_B=501, γ_B=192, δ_B=497 and the multiplier parameters are χ_B=451, η_B=273, λ_B=337, ω_B=119.

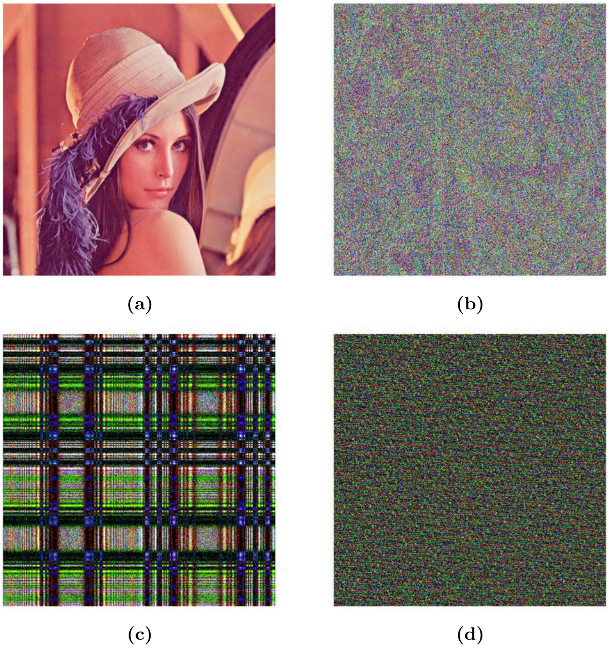


Fig. 4 Encryption results for Lena color image **a** The original Lena color image **b** The first stage Lena encrypted image **c** The second stage Lena encrypted image and **d** The complete Lena encrypted image

Figure 4c represents the second stage encrypted image by incorporating RP2DFrHT. The fractional orders used in this stage are as follows.

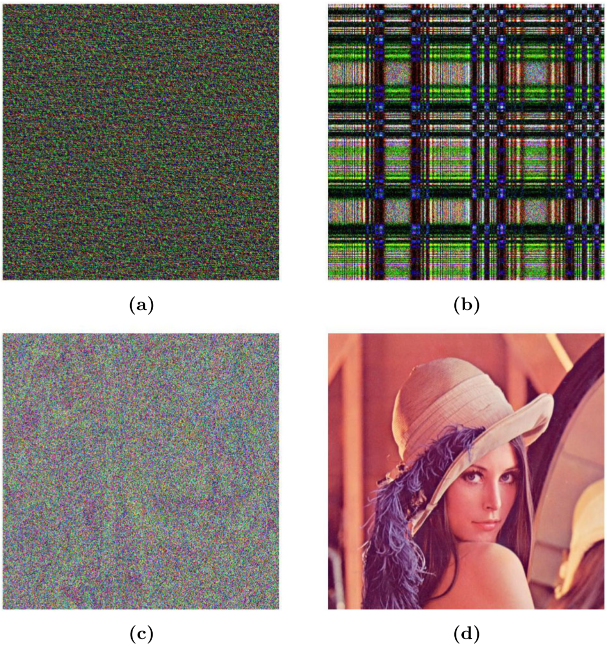
1. For red component (R): The fractional orders are c_R=0.7, d_R=0.3.
2. For green component (G): The fractional orders are c_G=0.4, d_G=0.5.
3. For blue component (B): The fractional orders are c_B=0.9, d_B=0.6.

Figure 4d represents the complete encrypted image obtained after using Arnold map. The Arnold keys used in this stage are as follows.

1. For red component (R): The Arnold keys are u_R=130, v_R=160.
2. For green component (G): The Arnold keys are u_G=97, v_G=100.
3. For blue component (B): The Arnold keys are u_B=99, v_B=110.

The Fig. 5 represents the correct demonstration of decrypted image for each stage employing correct secret keys and their correct arrangements. The complete encrypted image is given in Fig. 5a. The first stage decrypted image is obtained using inverse Arnold map as shown in Fig. 5b. The second stage decrypted image is obtained using IRP2DFrHT as shown in Fig. 5c. Lastly, Fig. 5d gives the complete decrypted image. This stage is obtained using inverse RMAC. The inverse shift parameters and inverse multiplier parameters are as given below.

1. For red component (R): The inverse shift parameters are α_R^{-1}=62, β_R^{-1}=342, γ_R^{-1}=367, δ_R^{-1}=141 and the inverse multiplier parameters are μ_R=345, κ_R=411, ν_R=265, σ_R=139.


(a)

(b)

(c)

(d)

Fig. 5 Decryption results for Lena color image **a** The complete Lena encrypted image **b** The first stage decrypted image **c** The second stage decrypted image and **d** The complete decrypted image

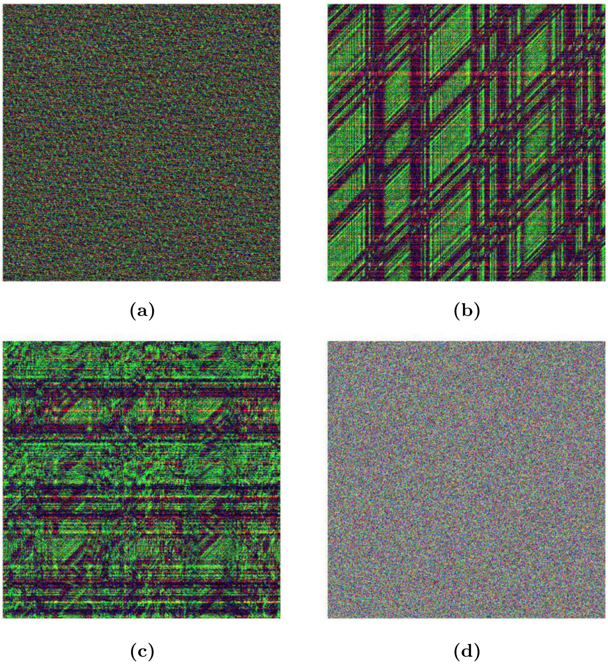
2. For green component (G): The inverse shift parameters are α_G^{-1}=361, β_G^{-1}=441, γ_G^{-1}=262, δ_G^{-1}=212 and the inverse multiplier parameters are μ_G=327, κ_G=97, ν_G=73, σ_G=231.
3. For blue component (B): The inverse shift parameters are α_B^{-1}=113, β_B^{-1}=11, γ_B^{-1}=320, δ_B^{-1}=15 and the inverse multiplier parameters are μ_B=235, κ_B=497, ν_B=433, σ_B=327.

5 Security analysis

The sensitivity analysis is done to validate the role of secret keys and their arrangements. The proposed technique is highly sensitive towards its secret keys and their arrangements. In other words, some simple modification in the secret keys or in the arrangements would provide a distorted version of the original image. The sensitivity analysis is done in five phases as given below.

Sensitivity analysis-I The sensitivity analysis-I is shown in Fig. 6. This stage is performed with incorrect Arnold keys while all other secret keys and their arrangements are kept same. The incorrect Arnold keys for each color component are taken as follows.

1. For red component (R): The Arnold keys are $u_R = 131$ and $v_R = 160$.
2. For green component (G): The Arnold keys are $u_G = 97$ and $v_G = 101$.
3. For blue component (B): The Arnold keys are $u_B = 100$ and $v_B = 111$.


(a) (b)

(c) (d)

Fig. 6 Results of Sensitivity analysis-I for incorrect Arnold keys **a** The complete Lena encrypted image **b** The first stage decrypted image **c** The second stage decrypted image **d** The complete decrypted image

The complete encrypted image is displayed in Fig. 6a. The outcome of the first stage decrypted image with incorrect Arnold keys of inverse Arnold map is given in Fig. 6b. The second stage decrypted image with correct decryption keys of IRP2DFrHT is given in Fig. 6c. The complete decrypted image with correct parameters and arrangements of IRMAC is shown in Fig. 6d. It is clear from Fig. 6 that the complete decrypted image is totally different from the original color image. Hence, Arnold keys are very sensitive for the proposed technique.

Sensitivity analysis-II This stage of sensitivity analysis is performed with approximate fractional orders of RP2DFrHT. However, Arnold keys and parameters of IRMAC are kept correct. The complete procedure is illustrated in Fig. 7. The approximate fractional orders for each color component are as follows.

1. For red component (R): The fractional orders are $c_R = 0.7$ and $d_R = 0.2$.
2. For green component (G): The fractional orders are $c_G = 0.3$ and $d_G = 0.5$.
3. For blue component (B): The fractional orders are $c_B = 0.8$ and $d_G = 0.5$.

The complete encrypted is represented in Fig. 7a. The outcome of the first stage decrypted image using accurate Arnold keys is shown in Fig. 7b. The outcome of the second stage decrypted image with approximate keys of IRP2DFrHT is shown in Fig. 7c. The complete decrypted image with correct parameters and the arrangements of IRMAC is shown in Fig. 7d. It is clear from Fig. 7 that the complete decrypted image is entirely different from the original color image. This stage shows that the fractional orders are highly sensitive.

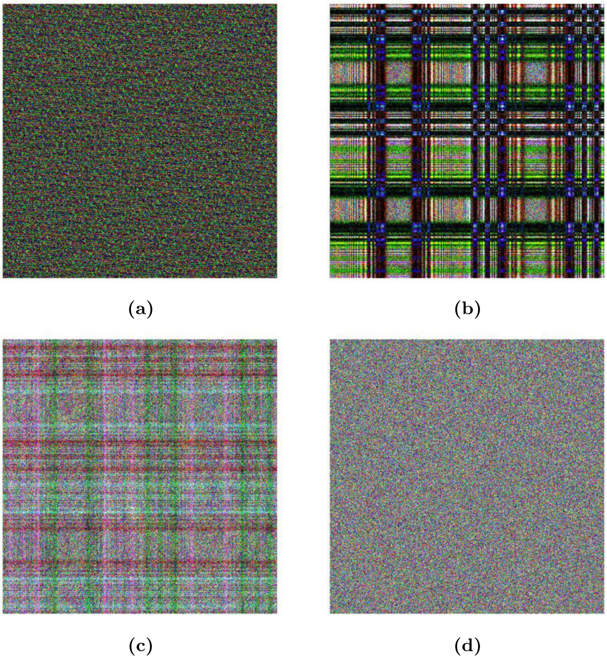


Fig. 7 Results of Sensitivity analysis-II for approximate fractional orders **a** The complete Lena encrypted image **b** The first stage decrypted image **c** The second stage decrypted image **d** The complete decrypted image

Sensitivity analysis-III This stage of sensitivity analysis is shown in Fig. 8. In this stage the sensitivity analysis is done using incorrect inverse shift parameters while remaining secret keys are kept same. The incorrect inverse shift parameters for each component are as follows.

1. For red component (R): The inverse shift parameters are α_R^{-1}=65, β_R^{-1}=341, γ_R^{-1}=360, δ_R^{-1}=100.
2. For green component (G): The inverse shift parameters are α_G^{-1}=364, β_G^{-1}=442, γ_G^{-1}=265, δ_G^{-1}=211.
3. For blue component (B): The inverse shift parameters are α_B^{-1}=110, β_B^{-1}=16, γ_B^{-1}=322, δ_B^{-1}=18.

The complete encrypted image is shown in Fig. 8a. The outcome of the first stage decrypted image using accurate Arnold keys is given in Fig. 8b. The outcome of the second stage decrypted image with correct IRP2DFrHT keys is given in Fig. 8c. The complete decrypted image is obtained using incorrect inverse shift parameters whereas inverse multiplier parameters and arrangements of IRMAC are kept same. This stage is displayed in Fig. 8d. It is clear from Fig. 8 that the complete decrypted image is completely different from the original color image. The sensitivity analysis-III interferences that the shift parameters are highly sensitive.

Sensitivity analysis-IV Sensitivity analysis-IV is done using approximate inverse multiplier parameters whereas inverse shift parameters, fractional orders and Arnold keys are not

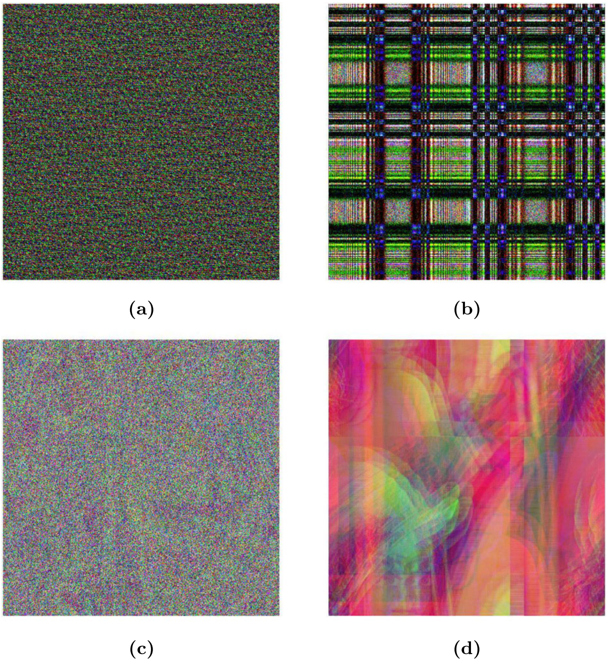


Fig. 8 Results of Sensitivity analysis-III for incorrect inverse shift parameters **a** The complete Lena encrypted image **b** The first stage decrypted image **c** The second stage decrypted image **d** The complete decrypted image

disturbed. The approximate inverse multiplier parameters for each color component are as follows.

1. For red component (R): The inverse multiplier parameters are μ_R=347, κ_R=151, ν_R=239, σ_R=459.
2. For green component (G): The inverse multiplier parameters are μ_G=239, κ_G=7, ν_G=211, σ_G=381.
3. For blue component (B): The inverse multiplier parameters are μ_B=431, κ_B=507, ν_B=143, σ_B=91.

The complete encrypted image is shown in Fig. 9a. The first stage decrypted image is displayed in Fig. 9b which is attained using accurate Arnold keys. The second stage decrypted image is displayed in Fig. 9c with correct IRP2DFrHT keys. The complete decrypted image is shown in Fig. 9d obtained using approximate inverse multiplier parameters whereas inverse shift parameters and arrangements of IRMAC are kept correct. The complete decrypted image is entirely different from the original image as shown in Fig. 9. Therefore, in this stage we conclude that the multiplier parameters are very sensitive.

Sensitivity analysis-V Sensitivity analysis-V is done using incorrect arrangements of IRMAC while other secret keys and their arrangements are kept correct. Incorrect arrangements for each color component are taken as follows.

1. For red component (R): The inverse shift parameters are α_R^{-1}=367, β_R^{-1}=342, γ_R^{-1}=141, δ_R^{-1}=62 and the inverse multiplier parameters are μ_R=345, κ_R=139, ν_R=411, σ_R=265.

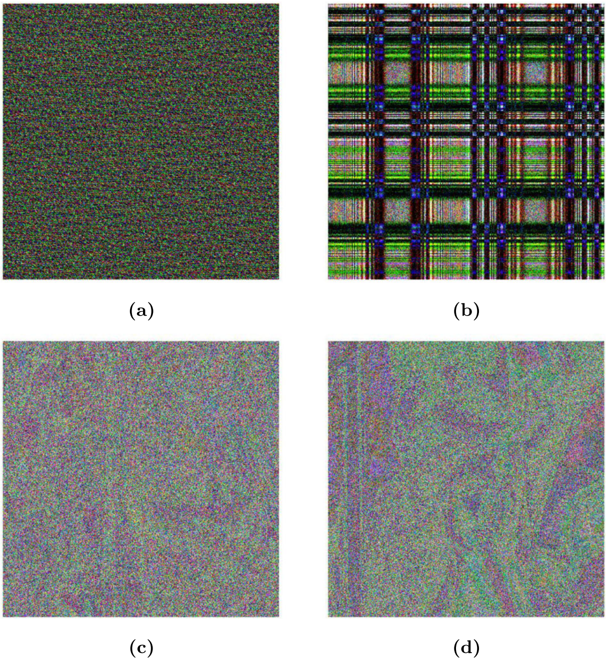


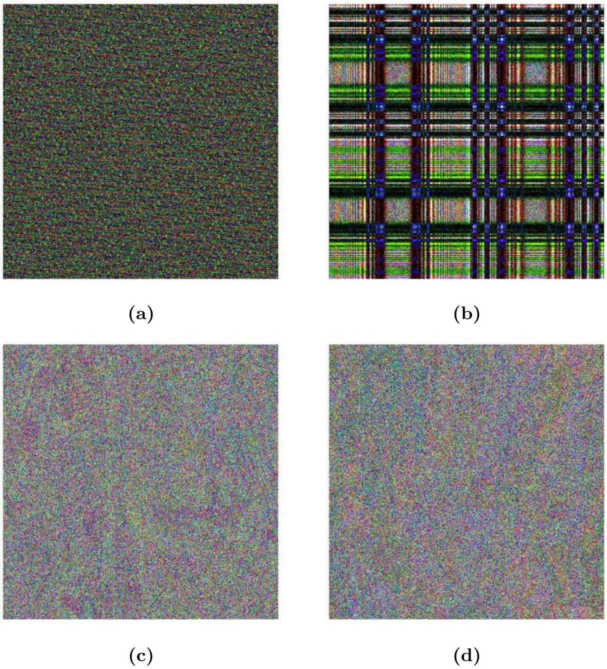
Fig. 9 Results of Sensitivity analysis-IV for approximate inverse multiplier parameters **a** The complete Lena encrypted image **b** The first stage decrypted image **c** The second stage decrypted image **d** The complete decrypted image

2. For green component (G): The inverse shift parameters are α_G^{-1}=441, β_G^{-1}=262, γ_G^{-1}=361, δ_G^{-1}=212 and the inverse multiplier parameters are μ_G=97, κ_G=327, ν_G=231, σ_G=73.
3. For blue component (B): The inverse shift parameters are α_B^{-1}=320, β_B^{-1}=113, γ_B^{-1}=15, δ_B^{-1}=11 and the inverse multiplier parameters are μ_B=497, κ_B=327, ν_B=235, σ_B=433.

The complete encrypted image is shown in Fig. 10a. The first stage decrypted image using correct Arnold keys is represented in Fig. 10b. The outcome of the second stage decrypted image using correct IRP2DFrHT keys is displayed in Fig. 10c. The complete decrypted image is obtained using incorrect arrangements of IRMAC whereas all other parameters are kept same. This stage is displayed in Fig. 10d. The complete decrypted image is entirely different from the original color image as displayed in Fig. 10. Hence, sensitivity analysis-V ensures that not only the magnitude of parameters but their arrangements are also very sensitive.

6 Statistical analysis

Visual differentiation between original and encoded/ decoded image is not possible. It would be possible in statistical analysis. An ideal encryption technique should resist all types of statistical attacks. To validate the effectiveness and feasibility of our presented encryption technique, we have done a statistical analysis in this section.


(a)

(b)

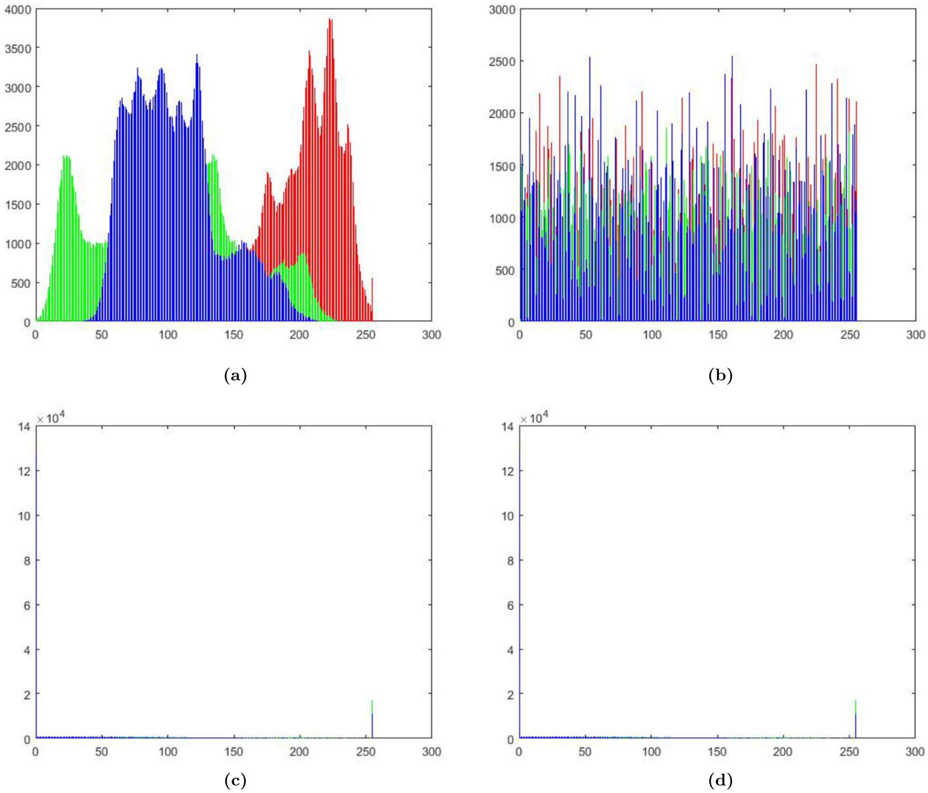
(c)

(d)

Fig. 10 Results of Sensitivity analysis-V for incorrect arrangements of IRMAC **a** The complete Lena encrypted image **b** The first stage decrypted image **c** The second stage decrypted image **d** The complete decrypted image

6.1 Histogram analysis

The statistical behaviour of input and output images are analyzed in histogram analysis. The histogram analysis is a graphical representation of the number of pixels against different intensity values found in an image. Figure 11a,b,c and d represent the histogram of the original Lena color image, the first stage Lena encrypted image, the second stage Lena encrypted image and the complete Lena encrypted image as given in Fig. 4a,b,c and d respectively. After analyzing all encrypted images, we have found that not only the histogram of the complete encrypted image, but also the histograms of different stages of the encrypted images are different from the original image. This ensures that the information about the original image cannot be leaked at any stage of the encrypted image. This also provides the robustness against potential attack. The histogram of the decrypted image is also obtained. Figure 12a,b,c and d represent the histogram of the complete Lena encrypted image, the first stage decrypted image, the second stage decrypted image and the complete decrypted image as shown in Fig. 5a,b,c and d respectively. The similarity between the histogram of the complete decrypted image and the histogram of the original image demonstrates the effectiveness of our proposed technique.



(a)

(b)

(c)

(d)

Fig. 11 Histogram results for encryption process **a** histogram of the original Lena color image **b** histogram of the first stage Lena encrypted image **c** histogram of the second stage Lena encrypted image **d** histogram of the complete Lena encrypted image

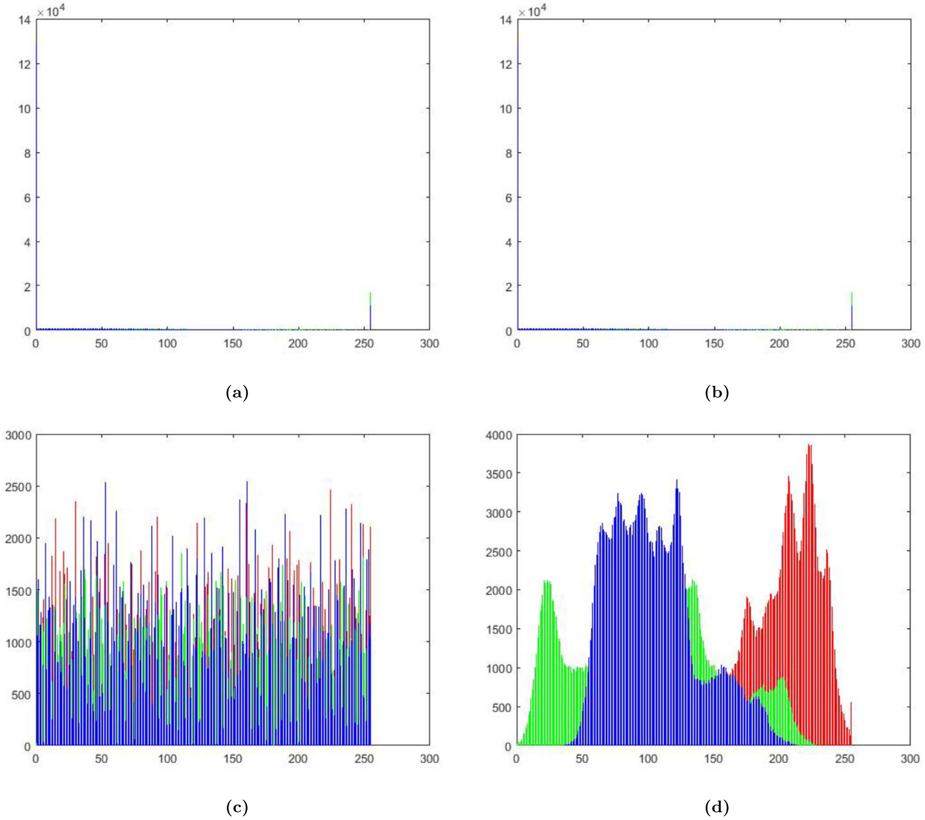


Fig. 12 Histogram results for decryption process **a** histogram of the complete Lena encrypted image **b** histogram of the first stage decrypted image **c** histogram of the second stage decrypted image **d** histogram of the complete decrypted image

6.2 Mean squared error (MSE)

The mean squared error between input RGB image and output RGB image for each red, green and blue component are mathematically calculated as.

$$MSE = \frac{1}{N \times M} \sum_{n=1}^{N} \sum_{m=1}^{M} |f(n,m) - \hat{f}(n,m)|^2, \tag{13}$$

where N and M are pixels of an RGB image, $f(n,m)$ is the input image and $\hat{f}(n,m)$ is the output image. Tables 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 and 11 represent the values of MSE between original image and output image for each RGB component. The MSE values between complete encrypted image shown in Fig. 4d and original image shown in Fig. 4a are given in Table 3. This table shows that the MSE values for each component of the RGB color image are very high. Higher values of MSE indicate that the original image is totally changed. The MSE values between complete decrypted image shown in Fig. 5d and original image are given in Table 6. This table shows that the MSE values for each component of RGB image is zero which guarantee that the original image and the complete decrypted image are both identical.

Table 1 $MSE_{(R,G,B)}$, $PSNR_{(R,G,B)}$ and $Correlation_{(R,G,B)}$ of Fig. 4b and a

S.No.	Image component	$MSE_{(R,G,B)}$	$PSNR_{(R,G,B)}$	$Correlation_{(R,G,B)}$
1.	R	1.0515e+04	7.9126	0.0071
2.	G	9.0633e+03	8.5579	0.0029
3.	B	7.1484e+03	9.5887	-0.0014

Table 2 $MSE_{(R,G,B)}$, $PSNR_{(R,G,B)}$ and $Correlation_{(R,G,B)}$ of Fig. 4c and a

S.No.	Image component	$MSE_{(R,G,B)}$	$PSNR_{(R,G,B)}$	$Correlation_{(R,G,B)}$
1.	R	4.7990e+04	1.3193	-0.0167
2.	G	2.5747e+04	4.0235	-0.0082
3.	B	3.3421e+04	2.8906	-1.5674e-04

Table 3 $MSE_{(R,G,B)}$, $PSNR_{(R,G,B)}$ and $Correlation_{(R,G,B)}$ of Fig. 4d and a

S.No.	Image component	$MSE_{(R,G,B)}$	$PSNR_{(R,G,B)}$	$Correlation_{(R,G,B)}$
1.	R	4.7748e+04	1.3413	1.5167e-04
2.	G	2.5633e+04	4.0428	-5.1979e-04
3.	B	3.3412e+04	2.8918	7.5117e-04

Table 4 $MSE_{(R,G,B)}$, $PSNR_{(R,G,B)}$ and $Correlation_{(R,G,B)}$ of Figs. 5b and 4a

S.No.	Image component	$MSE_{(R,G,B)}$	$PSNR_{(R,G,B)}$	$Correlation_{(R,G,B)}$
1.	R	4.7990e+04	1.3193	-0.0167
2.	G	2.5747e+04	4.0235	-0.0082
3.	B	3.3421e+04	2.8906	-1.5674e-04

Table 5 $MSE_{(R,G,B)}$, $PSNR_{(R,G,B)}$ and $Correlation_{(R,G,B)}$ of Figs. 5c and 4a

S.No.	Image component	$MSE_{(R,G,B)}$	$PSNR_{(R,G,B)}$	$Correlation_{(R,G,B)}$
1.	R	1.0515e+04	7.9126	0.0071
2.	G	9.0633e+03	8.5579	0.0029
3.	B	7.1484e+03	9.5887	-0.0014

Table 6 $MSE_{(R,G,B)}$, $PSNR_{(R,G,B)}$ and $Correlation_{(R,G,B)}$ of Figs. 5d and 4a

S.No.	Image component	$MSE_{(R,G,B)}$	$PSNR_{(R,G,B)}$	$Correlation_{(R,G,B)}$
1.	R	0	Inf	1
2.	G	0	Inf	1
3.	B	0	Inf	1

Table 7 $MSE_{(R,G,B)}$, $PSNR_{(R,G,B)}$ and $Correlation_{(R,G,B)}$ of Figs. 6d and 4a

S.No.	Image component	$MSE_{(R,G,B)}$	$PSNR_{(R,G,B)}$	$Correlation_{(R,G,B)}$
1.	R	1.0624e+04	7.8678	0.0032
2.	G	9.0729e+03	8.5533	-0.0018
3.	B	7.0812e+03	9.6297	0.0012

Table 8 $MSE_{(R,G,B)}$, $PSNR_{(R,G,B)}$ and $Correlation_{(R,G,B)}$ of Figs. 7d and 4a

S.No.	Image component	$MSE_{(R,G,B)}$	$PSNR_{(R,G,B)}$	$Correlation_{(R,G,B)}$
1.	R	1.0693e+04	7.8397	-0.0033
2.	G	9.0527e+03	8.5630	-6.6963e-05
3.	B	7.0967e+03	9.6202	0.0022

Table 9 $MSE_{(R,G,B)}$, $PSNR_{(R,G,B)}$ and $Correlation_{(R,G,B)}$ of Figs. 8d and Fig. 4a

S.No.	Image component	$MSE_{(R,G,B)}$	$PSNR_{(R,G,B)}$	$Correlation_{(R,G,B)}$
1.	R	3.2444e+03	13.0194	0.3307
2.	G	5.6516e+03	10.6091	-0.0211
3.	B	2.2769e+03	14.5574	0.0142

Table 10 $MSE_{(R,G,B)}$, $PSNR_{(R,G,B)}$ and $Correlation_{(R,G,B)}$ of Figs. 9d and 4a

S.No.	Image component	$MSE_{(R,G,B)}$	$PSNR_{(R,G,B)}$	$Correlation_{(R,G,B)}$
1.	R	1.1342e+04	7.5838	-0.0490
2.	G	9.1742e+03	8.5051	-0.0210
3.	B	7.0891e+03	9.6249	0.0113

Table 11 $MSE_{(R,G,B)}$, $PSNR_{(R,G,B)}$ and $Correlation_{(R,G,B)}$ of Figs. 10d and 4a

S.No.	Image component	$MSE_{(R,G,B)}$	$PSNR_{(R,G,B)}$	$Correlation_{(R,G,B)}$
1.	R	1.0574e+04	7.8882	-0.0021
2.	G	9.0777e+03	8.5511	-0.0049
3.	B	7.1170e+03	9.6078	0.0035

6.3 Peak signal-to-noise ratio (PSNR)

The peak signal-to-noise ratio between input RGB image and output RGB image for each RGB component are mathematically calculated as.

$$PSNR = 10 \; . \; \log_{10} \frac{(255)^2}{MSE}. \tag{14}$$

Tables 1–11 represent the values of PSNR between original image and output image for each RGB component. The PSNR values between complete encrypted image shown in Fig. 4d and original image shown in Fig. 4a are given in Table 3. This table shows that the PSNR values for each component of the RGB color image are low. Lower values of PSNR indicate that the original image is completely changed. The PSNR values between complete decrypted image shown in Fig. 5d and original image are given in Table 6. This table shows that the PSNR values for each component of RGB image is infinity which guarantee that the original image and the complete decrypted image are both identical.

6.4 Correlation coefficient

To measure linear relationship between the pixels of two images, correlation coefficient (C) is considered. The limiting value of C lies between -1 and +1 i.e. -1 ≤ C ≤ +1. If C is +1 it means the strong positive correlation. If C is -1 it means the negative relationship between two images. If C is 0 it means no relationship between two images. For the original image, the value of C is close to +1, whereas for the encrypted image, the value of C is close to 0.

Tables 1–11 represent the values of correlation coefficient between original image and output image for each RGB component. The values of C between complete encrypted image shown in Fig. 4d and original image shown in Fig. 4a are given in Table 3. This table shows that the values of C for each component of the RGB color image are tending to zero which indicate that the original image is totally changed. The values of C between complete decrypted image shown in Fig. 5d and original image are given in Table 6. This table shows that the values of C for each component of RGB image are +1 which guarantee that the original image and the complete decrypted image are both identical.

The results of the aforementioned statistical tools interference that without knowing correct secret keys and their correct arrangements, unauthorized person cannot obtain any information from the encrypted image. The ideal value of each statistical tool validates that using correct secret keys and their correct arrangements the complete correct original image has recovered. Tables 7–11 signify the sensitivity of secret keys and their arrangements mathematically. We have also obtained correlation coefficients in horizontal, vertical and diagonal directions which are given in Table 12.

6.5 Entropy analysis

To quantify the impulsiveness of the information, entropy analysis is done. The mathematical expression of entropy is given as follows.

$$H(s) = -\sum_{j=1}^{M} p(s_j) \log_2 p(s_j), \tag{15}$$

where $H(s)$ denotes the entropy of data s, $p(s_j)$ is the probability occurrence of the case s_j and M is the total number of all possible occurrences. The ideal value of $H(s)$ should be 8 bits. The entropy estimation should be near to ideal value to provide invulnerability

Table 12 Correlation coefficients in horizontal, vertical and diagonal directions

Data	Component of color image	H	V	D
Figure 4a	Red component	0.9753	0.9871	0.9634
	Green component	0.9748	0.9872	0.9630
	Blue component	0.9532	0.9741	0.9334
Figure 4d	Red component	0.0386	-0.0936	0.0083
	Green component	0.1305	-0.0222	-0.0195
	Blue component	0.0467	-00008	0.0059

from entropy attacks. The values of entropy estimation of red, green and blue components of the original image, the first stage encrypted image, the second stage encrypted image, the complete encrypted image and the complete decrypted image are listed in Table 13. It is justified that our proposed encryption technique is more secure against entropy based attacks.

6.6 Resisting classical attacks

While dealing with cryptanalysis, classical attacks are classified into four categories: chosen-plaintext attack (CPA), known-plaintext attack (KPA), chosen-ciphertext attack (CCA) and ciphertext-only attack (COA). In CPA, the cryptanalyst has tentative access to the encryption system and he tries to find a ciphertext corresponding to the randomly chosen plaintext. In KPA, the cryptanalyst has availability of both plaintext and ciphertext. The cryptanalyst randomly receives these samples instead of selecting. In CCA, the cryptanalyst has temporary access to decryption system to find comparative plaintext corresponding to the arbitrarily picked ciphertext. In COA, the cryptanalyst has access to a certain number of ciphertexts and have no information about the plaintext. Among them, chosen-plaintext is the most remarkable attack. If encryption algorithm restricts chosen-plaintext attack then it opposes other three attacks too. In this paper, our encryption technique is designed in such a way that the security of the system depends not only upon the secret keys, but also upon the correct arrangements of all secret keys. As the proposed technique has exceptionally huge key size. Therefore, it is difficult for hackers to analyze accurate secret keys and appropriate arrangements of all hidden keys. In Section 5, we have demonstrated the sensitivity analysis of our encryption technique. Therefore, owing to all these properties the proposed technique is unaffected by above all four typical attacks.

Table 13 Entropy values for red, green and blue components of Lena color image

RGB image	$Entropy_{(R,G,B)}$		
data	R	G	B
Figure 4a	7.2634	7.5899	6.9854
Figure 4b	7.8185	7.9122	7.7568
Figure 4c	5.4262	5.7184	4.8725
Figure 4d	5.4262	5.7184	4.8725
Figure 5d	7.2634	7.5899	6.9854

7 Comparison analysis

In this section, we have compared our proposed encryption technique with the existing similar techniques [7, 8, 11, 16, 18, 19, 22, 24, 28, 34, 35, 38, 39, 41, 42, 46].

S.No.	Existing techniques [7, 8, 11, 16, 18, 19, 22, 24, 28, 34, 35, 38, 39, 41, 42, 46]	Our proposed technique
1.	The security of the techniques [7, 8, 19, 22, 35, 39, 46] depend upon secret keys only.	The security of our proposed technique depends upon secret keys as well as their correct arrangements.
2.	The main secret keys of the techniques [16, 42] are fractional order and random phase.	The main secret keys of our proposed technique are shift parameters, multiplier parameters, fractional orders and Arnold keys.
3.	The techniques [8, 16, 18, 19, 35, 39] provide one or two layer of security.	Our proposed technique provides multi-layer security.
4.	The techniques [11, 16, 22, 28, 38, 39, 46] possess security either in co-ordinate domain, or in geometrical domain, or in frequency domain, or in spatial domain.	Our proposed technique maintains security in co-ordinate, geometrical, frequency and time domains.
5.	The techniques [11, 16, 24, 28, 34, 35, 41, 42] provide complex-valued coefficients.	Our proposed technique provides real-valued coefficients.
6.	In existing techniques [24, 28] the mean squared error between correctly decrypted image and original image is almost zero.	In our proposed technique the mean squared error between correctly decrypted image and original image is exactly equal to zero.

1. Chen and Zhao [7] proposed an encryption scheme in optical domain using fractional wavelet transform (FWT). Two series of keys are used in their scheme. The security of their scheme depends upon keys only.
2. Tao et al. [35] presented a cryptographic technique using multi orders of fractional Fourier transform (FRFT). The security of their technique depends only upon the keys. The nature of encrypted image is complex-valued. The security of their technique is given in the frequency domain.
3. Lang [19] developed a technique using the concept of reality preserving multiple-parameter fractional Fourier transform (RPMPFRFT). The security of his scheme depends upon the parameters of RPMPFRFT.
4. Liu et al. [22] introduced a scheme for color image in which Arnold transform and color-blend operation in discrete cosine transform domain play a vital role. The random angle data in color blend operation and parameters of Arnold transform are taken as a key. The security of their scheme depends in co-ordinate domain as well as in frequency domain.

5. Wu et al. [39] presented an encryption scheme using multiple-order discrete fractional cosine transform (MODFrCT). The security of their scheme depends upon fractional orders only. Their scheme provides security in frequency domain only.
6. Prasad et al. [28] introduced an encryption scheme using FRFT and wavelet transform. Final encoded image obtained in their scheme is complex-valued. Their scheme provides security in frequency domain only.
7. Zhu et al. [46] presented an algorithm for image security based on Arnold transform and affine cipher. Their scheme is secure in co-ordinate domain as well as in geometrical domain. The security depends upon secret keys only.
8. Kumar et al. [18] introduced their first encryption algorithm for RGB image using discrete wavelet transform and random matrix affine cipher. Their scheme provides two layers of security.
9. Zhao et al. [42] designed a scheme based on optical domain using two dimensional fractional Hartley transform (FRHT). The random phase codes and fractional orders are taken as keys. The final encrypted image is a complex-valued in their scheme.
10. Tao et al. [34] introduced double random amplitude encoding method using multiple-parameter discrete fractional Hadamard transform (MPDFrHaT). The ciphertext obtained in their scheme after encryption is complex-valued data.
11. Wu et al. [38] proposed a lossless cryptographic technique for color image utilizing two dimensional discrete wavelet transform and six dimensional hyperchaotic system. The system is secure in frequency domain as well as in spatial domain.
12. Mishra and Sharma [24] proposed an image encryption scheme utilizing random matrix shift cipher (RMSC) and discrete fractional Fourier transform (DFrFT). The secret keys as well as their arrangements are established for the immunity of the system. The nature of encrypted image is complex-valued.
13. Chen and Zhao [8] proposed an optical image encryption in accordance with wavelength multiplexing and lensless Fresnel transform holograms. The parameter of Fresnel transform and random phase masks are taken as a key.
14. Joshi et al. [16] designed a technique for color image data based on FRFT. The fractional order and random phase masks are taken as a key for the enhancement of security of the system.
15. Zhang and Xiao [41] proposed an image encryption scheme based on optical domain using discrete Chirikov standard map and chaos-based fractional random transform. The encrypted image obtained in their scheme has complex coefficients.
16. Guo et al. [11] introduced a technique for color image data using discrete fractional random transform (DFRNT) and Arnold transform (AT) in the intensity-hue-saturation (IHS) color space. The encrypted image obtained in their technique has complex coefficients.

8 Conclusions

In this paper, we have proposed a robust multi-layer color image encryption by merging the concepts of RMAC, RP2DFrHT and 2D Arnold map. The encryption has been done in three phases. Firstly, RGB image has been divided into its three components R, G, B. In the first phase, RMAC has been employed to transform the pixels in co-ordinate domain as well as in geometrical domain. In the second phase, RP2DFrHT has been used to transform the pixels in frequency domain. RP2DFrHT provides real-valued encrypted image.

The real-valuedness property of RP2DFrHT decreases the storage, computational and communication complexities of the encrypted image in digital environment. In the final phase, an additional layer of security has been provided using Arnold map. Arnold map provides chaotic behaviour in our proposed encryption technique. For correct image encryption, we have adopted the reverse steps of the encryption process. Moreover presented technique has provided security in geometrical domain, co-ordinate domain, frequency domain and time domain. Sensitivity analysis has been done to demonstrate the sensitivity of the secret keys and their arrangements. Statistical analysis has been done to prove the resistance against all types of statistical attacks.

References

1. Abdulla AA (2015) Exploiting similarities between secret and cover images for improved embedding efficiency and security in digital steganography. Ph.D. thesis, University of Buckingham
2. Abuturab MR (2012) Securing color information using Arnold transform in gyrator transform domain. Opt Lasers Eng 50(5):772–779
3. Abuturab MR (2013) Color image security system based on discrete Hartley transform in gyrator transform domain. Opt Lasers Eng 51(3):317–324
4. Abuturab MR (2015) An asymmetric single-channel color image encryption based on Hartley transform and gyrator transform. Opt Lasers Eng 69:49–57
5. Candan C, Kutay MA, Ozaktas HM (2000) The discrete fractional Fourier transform. IEEE Trans Signal Process 48(5):1329–1337
6. Chen H, Du X, Liu Z, Yang C (2013) Color image encryption based on the affine transform and gyrator transform. Opt Lasers Eng 51(6):768–775
7. Chen L, Zhao D (2005) Optical image encryption based on fractional wavelet transform. Opt Commun 254(4-6):361–367
8. Chen L, Zhao D (2006) Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms. Opt Express 14(19):8552–8560
9. Chen L, Zhao D (2008) Image encryption with fractional wavelet packet method. Optik 119(6):286–291
10. Guleria V, Sabir S, Mishra D (2020) Security of multiple RGB images by RSA cryptosystem combined with FRDCT and Arnold transform. J Inform Secur Appl 54:102524
11. Guo Q, Liu Z, Liu S (2010) Color image encryption by using Arnold and discrete fractional random transforms in IHS space. Opt Lasers Eng 48(12):1174–1181
12. Hennelly B, Sheridan JT (2003) Fractional Fourier transform-based image encryption: Phase retrieval algorithm. Opt Commun 226(1-6):61–80
13. Huang JJ, Hwang HE, Chen CY, Chen CM (2012) Optical multiple-image encryption based on phase encoding algorithm in the Fresnel transform domain. Opt Laser Technol 44(7):2238–2244
14. Hussain I (2016) Optical image encryption based on S-box transformation and fractional Hartley transform. J Vib Control 22(4):1143–1146
15. Hwang HE (2011) An optical image cryptosystem based on Hartley transform in the Fresnel transform domain. Opt Commun 284(13):3243–3247
16. Joshi M, Chandrashakher K (2007) Singh, Color image encryption and decryption using fractional Fourier transform. Opt Commun 279(1):35–42
17. Kang XJ, Han Z, Yu AW, Duan PQ (2017) Double random scrambling encoding in the RPMPFrHT domain. IEEE Int Conf Image Process (ICIP)4362–4366
18. Kumar M, Mishra D, Sharma R (2014) A first approach on an RGB image encryption. Opt Lasers Eng 52:27–34
19. Lang J (2012) Image encryption based on the reality-preserving multiple-parameter fractional Fourier transform. Opt Commun 285(10-11):2584–2590
20. Liu Z, Dai J, Sun X, Liu S (2010) Color image encryption by using the rotation of color vector in Hartley transform domains. Opt Lasers Eng 48(7-8):800–805
21. Liu Z, Xu L, Lin C, Dai J, Liu S (2011) Image encryption scheme by using iterative random phase encoding in gyrator transform domains. Opt Lasers Eng 49(4):542–546
22. Liu Z, Xu L, Liu T, Chen H, Li P, Lin C, Liu S (2011) Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains. Opt Commun 284(1):123–128

23. Mehra I, Nishchal NK (2015) Wavelet-based image fusion for securing multiple images through asymmetric keys. Opt Commun 335:153–160
24. Mishra DC, Sharma R (2016) An approach for security of color image data in coordinate, geometric, and frequency domains. Inform Secur J A Global Perspect 25(4-6):213–234
25. Nishchal NK, Joseph J, Singh K (2004) Securing information using fractional Fourier transform in digital holography. Opt Commun 235(4-6):253–259
26. Pei SC, Hsue WL (2006) The multiple-parameter discrete fractional Fourier transform. IEEE Signal Process Lett 13(6):329–332
27. Pei SC, Tseng CC, Yeh MH, Shyu JJ (1998) Discrete fractional Hartley and Fourier transforms. IEEE Trans Circ Syst II: Analog Digit Signal Process 45(6):665–675
28. Prasad A, Kumar M, Choudhury DR (2012) Color image encoding using fractional Fourier transformation associated with wavelet transformation. Opt Commun 285(6):1005–1009
29. Refregier P, Javidi B (1995) Optical image encryption based on input plane and Fourier plane random encoding. Opt Lett 20(7):767–769
30. Singh P, Yadav A, Singh K (2017) Color image encryption using affine transform in fractional Hartley domain. Opt Appl 47(3):421–433
31. Singh P, Yadav A, Singh K, Saini I (2017) Optical image encryption in the fractional Hartley domain, using Arnold transform and singular value decomposition. Math Sci Appl AIP Conf Proc 1802:020017-1–7
32. Situ G, Zhang J (2004) Double random-phase encoding in the Fresnel domain. Opt Lett 29(14):1584–1586
33. Soleymani A, Nordin MJ, Sundararajan E (2014) A chaotic cryptosystem for images based on Henon and Arnold cat map. The Scientif World J 2014
34. Tao R, Lang J, Wang Y (2009) The multiple-parameter discrete fractional Hadamard transform. Opt Commun 282(8):1531–1535
35. Tao R, Meng XY, Wang Y (2010) Image encryption with multiorders of fractional Fourier transforms. IEEE Trans Inform Forens Secur 5(4):734–738
36. Vashisth S, Singh H, Yadav A, Singh K (2014) Image encryption using fractional Mellin transform, structured phase filters, and phase retrieval. Optik 125(18):5309–5315
37. Venturini I, Duhamel P (2004) Reality preserving fractional transforms, International Conference on Acoustics. Speech Signal Process 5:205–208
38. Wu X, Wang D, Kurths J, Kan H (2016) A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system. Inf Sci 349-350:137–153
39. Wu J, Zhang L, Zhou N (2010) Image encryption based on the multiple-order discrete fractional cosine transform. Opt Commun 283(9):1720–1725
40. Yadav PL, Singh H (2018) Optical double image hiding in the fractional Hartley transform using structured phase filter and Arnold transform. 3D Research 9(2):20
41. Zhang Y, Xiao D (2013) Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform. Opt Lasers Eng 51(4):472–480
42. Zhao D, Li X, Chen L (2008) Optical image encryption with redefined fractional Hartley transform. Opt Commun 281(21):5326–5329
43. Zhou N, Wang Y, Gong L (2011) Novel optical image encryption scheme based on fractional Mellin transform. Opt Commun 284(13):3234–3242
44. Zhou N, Wang Y, Wu J (2011) Image encryption algorithm based on the multi-order discrete fractional Mellin transform. Opt Commun 284(24):5588–5597
45. Zhu Z, Wu C, Wang J, Hu K, Chen XD (2020) A novel 3D vector decomposition for color-image encryption. IEEE Photonics J 12(2):1–14
46. Zhu H, Zhao C, Zhang X, Yang L (2014) An image encryption scheme using generalized Arnold map and affine cipher. Optik 125(22):6672–6677

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.