Optica Applicata, Vol. LV, No. 1, 2025
DOI: 10.37190/oa/200434

Secure cryptosystem based on improved Yang–Gu algorithms in gyrator domain

ARCHANA TOBRIA[1,*], PHOOL SINGH[2]

[1] Department of Mathematics, Central University of Haryana,
Mahendergarh, Haryana 123031, India

[2] Department of Mathematics, SOET, Central University of Haryana,
Mahendergarh, Haryana 123031, India

[*] Corresponding author: archana191216@cuh.ac.in

A secure cryptosystem based on improved version of Yang–Gu algorithm has been proposed along with lower–upper (LU) decomposition for compression in gyrator transform. Yang–Gu algorithm introduces nonlinearity whereas LU decomposition leads to compression in the proposed scheme. Two random phase masks and binary phase modulators are used in the encryption process. Random phase masks act as public keys and binary phase modulations are applied to generate private keys. Grayscale and medical images are used to validate the proposed cryptosystem against different types of attacks. The statistical attack including information entropy, histogram analysis, correlation distribution plots, and 3-D plots are analyzed for the robustness of the proposed scheme. The quality of the retrieved image is compared with original image using the value of the correlation coefficient. The proposed scheme also showed resistance against data shuffling attack and basic attacks. Key sensitivity analysis demonstrated that the scheme is highly sensitive to its private keys and gyrator transform parameters. Therefore, based on above discussed results, the proposed scheme enhances the security.

Keywords: image compression, gyrator transform, LU decomposition, improved Yang–Gu mixture amplitude-phase retrieval algorithm.

1. Introduction

The developments in internet and advanced communication technology have made human life easy and attracted a lot of society's attention. Nowadays, a massive amount of data has been sent via communication channels or the internet. At the same time, the security of data from illegitimate users is a crucial problem and attracted a lot of attention from researchers. Several security methodologies have been proposed to protect the data from unintended access; encryption is one of them. During encryption, the original information is changed into corresponding unreadable form to secure it from illegal users. Many optical and digital encryption cryptosystems have been proposed to protect the data from illegitimate users. Optical encryption techniques are getting high attention because of their parallel processing and high speed. In 1995, Refregier and Javidi proposed first optical encryption cryptosystem, referred to as double random phase encoding (DRPE) [1]. DRPE is symmetric in nature because the same key is used for encryption and decryption process, therefore, it is vulnerable to basic attacks [2-5]. Thus, an asymmetric cryptosystem is designed to secure the data from an unintended user.

In optical sense, Qin and Peng proposed the first asymmetric cryptosystem based on nonlinear operations such as phase truncation and phase reservation operation in the Fourier domain (phase-truncated Fourier transforms, PTFT) [6]. Due to its nonlinear and asymmetric nature, the PTFT scheme achieves high robustness against basic attacks. However, PTFT-based encryption algorithms are breakdown to a special attack based on phase retrieval algorithm (PRA) [7-9]. Researchers have proposed several nonlinear encryption algorithms based on PRA to address this issue. Rajput and Nischal proposed an optical nonlinear scheme based on the Gerchberg–Saxton algorithm in Fresnel transform [10]. In 2013, Liu *et al.* [11-13] proposed an iterative scheme based on Yang–Gu mixture amplitude-phase retrieval algorithm (Yang–Gu algorithm). Further Yang–Gu algorithm, was used in various cryptosystems by the researchers [14-19]. Wang *et al.* [20] proposed an improved amplitude-phase retrieval algorithm (improved Yang–Gu algorithm) which is an improved version of Yang–Gu algorithm.

Now-a-days, many research groups are working in the area of image compression [21]. It is of two types: lossless and lossy compression. In lossless compression [22,23], there is no loss of information in image before and after compression whereas in lossy compression, some information may be lost, but the recovered image is similar to the input image. Some loss of information is because the image compression algorithms remove the redundant pixels from an image. For image compression, various compressive techniques have been developed by researchers including compressed sensing [24-28], semi-tensor product compressed sensing [29], fractal-based compression, *etc.* [30-32]. Moreover, image compression algorithms are explored in various domains including discrete cosine transform (DCT) [33-35], vector quantization [36], discrete wavelet transform (DWT) [37], *etc.* An asymmetric scheme based on compression using DCT in Fresnel transform was proposed by Kumari *et al.* [38] for color images. From the literature, it has been observed that sparse matrices are more convenient for compression and storage than other dense matrices. Rakheja *et al.* [39] reported an asymmetric technique based on the sparse matrix concept in a hybrid multi-resolution wavelet domain using the QR-decomposition technique. In this paper, the lower–upper (LU) decomposition process is applied to produce a sparse matrix and the product of lower and upper matrix acts as a private key in the decryption process.

This paper proposes a hybrid (symmetric and one-time-pad) cryptosystem based on an improved Yang–Gu algorithm and LU decomposition in gyrator transform. First, an improved version of Yang–Gu algorithm is used to get the real-valued image, and later LU decomposition is applied for compression which yields a permutation matrix (sparse matrix) and lower–upper matrices. The input image has size of 256×256 pixels whereas corresponding encrypted image is 16×16 pixels. The proposed scheme works for grayscale as well as medical images. The structure of paper is given as follows:

Section 2 discusses gyrator transform and LU decomposition technique. Section 3 provides a detailed description of the proposed scheme and its numerical simulation through MATLAB are presented in Section 4. A comparative analysis with existing scheme has been done for the proposed scheme in Section 5. The main contributions of the paper and findings are concluded in the last section.

2. Theoretical background

2.1. Gyrator transform

The gyrator transform (GT) [40] is a linear canonical transform widely used in image encryption algorithms. Mathematically, the gyrator transform of an image $f(x, y)$ is defined as

$$\begin{aligned} F(u, v) &= G^{\alpha}\Big[f(x, y)\Big](u, v) \\ &= \frac{1}{|\sin\alpha|}\iint f(x, y)\exp\left[2\pi i\,\frac{(xy+uv)\cos\alpha-(xv+yu)}{\sin\alpha}\right]\mathrm{d}x\,\mathrm{d}y \end{aligned} \tag{1}$$

where α stands for the rotation angle and its value between the interval $[0, 2\pi]$ and provides an extra key to an encryption algorithm. The (u, v) and (x, y) represent coordinates in the frequency and spatial domain, respectively. Figures 1(b) and (c) illustrate the effect of GT on grayscale image with dimensions 256 × 256 pixels, shown in Fig. 1(a), with rotation angles $\alpha = 2.14$ and $\alpha = 1.25$, respectively. Figure 1(d) displays the corresponding recovered image.

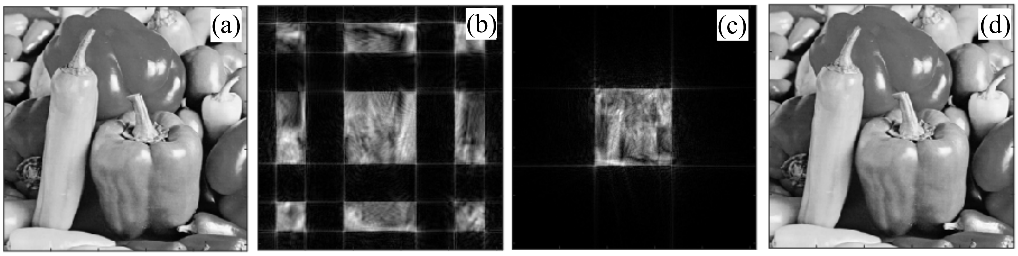

Fig. 1. (a) Grayscale image with dimensions 256 × 256 pixels. The effect of GT on grayscale image with dimensions 256 × 256 pixels and with rotation angles (b) $\alpha = 2.14$, and (c) $\alpha = 1.25$. (d) The corresponding recovered image.

2.2. LU decomposition

In mathematics, especially linear algebra and numerical analysis, lower–upper (LU) decomposition [41] is a method that factorizes a non-singular square matrix into lower and upper triangular matrices. Sometimes, a permutation matrix is also included in which every row and column contains only the unit element, and rest all elements are zeroes. The elements above the principal diagonal are zero and on principal diagonal are one in lower triangular matrix whereas in upper triangular matrix elements below the principal diagonal are zero. Mathematically, the upper matrix U and lower matrix L of size $n \times n$ are as follows:

$$U = \begin{bmatrix} u_{11} & u_{12} & \dots & u_{1n} \\ 0 & u_{22} & \dots & u_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & u_{nn} \end{bmatrix}, \quad L = \begin{bmatrix} 1 & 0 & \dots & 0 \\ l_{21} & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ l_{n1} & l_{n2} & \dots & 1 \end{bmatrix}$$

The LU decomposition is also applied on a grayscale image as shown in Fig. 1(a). Figure 2 depicts the results of LU decomposition on the grayscale image. The lower and upper triangular matrices of LU decomposition are depicted in Figs. 2(a) and (b), respectively, whereas Fig. 2(c) shows the permutation matrix. Result corresponding to inverse LU decomposition is displayed in Fig. 2(d).

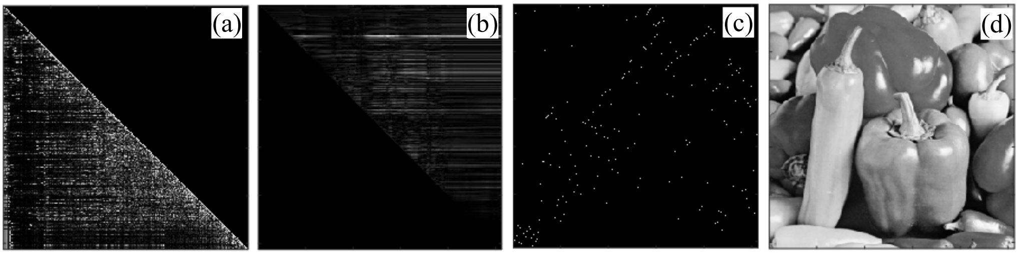

Fig. 2. The results of LU decomposition on the grayscale image: (a) lower and (b) upper triangular matrices, (c) permutation matrix, and (d) result corresponding to inverse LU decomposition.

3. Proposed scheme

In this section, a hybrid cryptosystem based on an improved Yang–Gu algorithm and LU decomposition in GT domain is discussed in detail. During the iterative loop, an input image and two random phase masks RPM1 and RPM2 served as public keys and are used as the constraints. Figure 3 displays the flowchart of encryption and decryption process. The encryption process involves the following steps.

Step 1: Initially, an $e_1(x, y)$ is allocated as amplitude image having values between 0 and 1. At the k-th iteration, public key RPM2 is bonded with amplitude $e_k(x, y)$ subjected to the gyrator transform with angle α. Mathematically,

$$g_k(u, v) = G^{\alpha}\Big[e_k(x, y)\,\mathrm{RPM2}(x, y)\Big] \tag{2}$$

$$g'_k(u, v) = \mathrm{PT}\Big[g_k(u, v)\Big] \tag{3}$$

$$\varphi'_k(u, v) = \mathrm{PR}\Big[g_k(u, v)\Big] \tag{4}$$

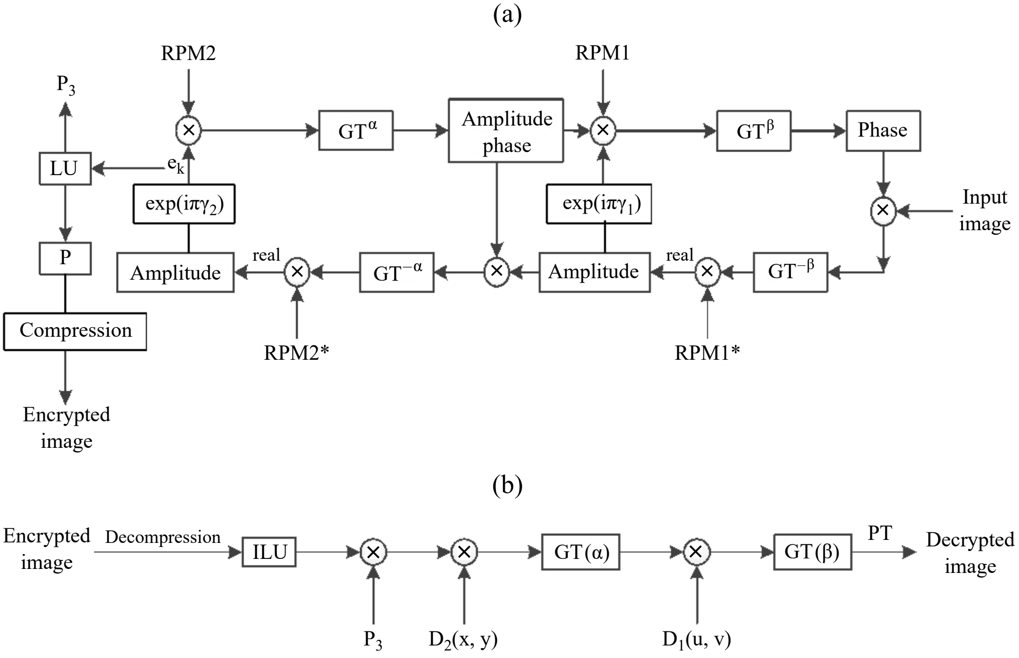

Fig. 3. The flowchart of (a) encryption and (b) decryption process.

where $G^{\alpha}[\cdot]$ represents the GT operator, and PT, PR denote the phase truncate and phase reserved part, respectively.

Step 2: The part PT $g_k'(u, v)$ is combined with another public key RPM1(u, v) and a private phase modulator $\exp(i\pi\gamma_{1,k-1})$. The combined image undergoes another gyrator transform with angle β. Mathematically,

$$h_k(x, y) = \mathrm{GT}^{\beta}\Big[g_k'(u, v)\,\mathrm{RPM1}(u, v)\exp(i\pi\gamma_{1,\,k-1})\Big] \tag{5}$$

$$h_k'(x, y) = \mathrm{PT}\Big[h_k(x, y)\Big] \tag{6}$$

$$\varphi_k(x, y) = \mathrm{PR}\Big[h_k(x, y)\Big] \tag{7}$$

Step 3: The plaintext $I(x, y)$ is multiplied by phase $\varphi_k(x, y)$ and undergoes inverse gyrator transform with angle $-\beta$:

$$H_k(u, v) = \mathrm{GT}^{-\beta}\Big\{I(x, y)\exp\Big[i\varphi_k(x, y)\Big]\Big\} \tag{8}$$

Step 4: $H_k(u, v)$ is bonded with RPM1$^*(u, v)$ and its real part is stored as $R_{k1}(u, v)$:

$$R_{k1}(u, v) = \mathrm{Re}\Big[H_k(u, v)\,\mathrm{RPM1}^*(u, v)\Big] \tag{9}$$

where asterisk and Re denote the complex conjugate operation and real part operator, respectively. $R_{k1}(u, v)$ may contain types of elements such as positive and negative. Thus, we performed a one-way binary phase modulator operator $\exp(i\pi\gamma_{1,k}(u, v))$ on $R_{k1}(u, v)$, to get positive elements of it. The binary phase modulator $\gamma_{1,k}(u, v)$, is generated by

$$\gamma_{1,k}(u, v) = \begin{cases} 1, & R_{k1}(u, v) < 0 \\ 0, & R_{k1}(u, v) > 0 \end{cases} \tag{10}$$

Thus, the following equation gives the modified amplitude as

$$R'_k(u, v) = R_{k1}(u, v)\exp\left[i\pi\gamma_{1,k}(u, v)\right] \tag{11}$$

Step 5: The phase $\varphi'_k(u, v)$ obtained from Eq. (4) is bonded with $R'_k(u, v)$ and undergo inverse gyrator transform with angle $-\alpha$:

$$I_k(x, y) = \mathrm{GT}^{-\alpha}\left\{R'_k(u, v)\exp\left[i\varphi'_k(u, v)\right]\right\} \tag{12}$$

Step 6: $I_k(x, y)$ is bonded with $\mathrm{RPM2}^*(x, y)$ and its real part is stored as $R_{k2}(x, y)$:

$$R_{k2}(x, y) = \mathrm{Re}\left[I_k(x, y)\,\mathrm{RPM2}^*(x, y)\right] \tag{13}$$

Step 7: Another one-way binary phase modulator $\gamma_2(x, y)$ is bonded with $R_{k2}(x, y)$ as it may contain negative elements. The modulator $\gamma_2(x, y)$ is calculated as follows:

$$\gamma_2(x, y) = \begin{cases} 1, & R_{k2}(x, y) < 0 \\ 0, & R_{k2}(x, y) > 0 \end{cases} \tag{14}$$

$$e_k(x, y) = R_{k2}(x, y)\exp\left[i\pi\gamma_2(x, y)\right] \tag{15}$$

If values of the correlation coefficient (CC) between $h'_k(x, y)$ and $I(x, y)$ are larger than a predetermined threshold value, the iterative loop from Steps 1 to 7 may end here. The following equation can be used to determine the CC value:

$$\mathrm{CC} = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\left[h'_k(x, y) - \overline{h'_k(x, y)}\right]\left[I(x, y) - \overline{I(x, y)}\right]}{\sqrt{\sum_{x=1}^{M}\sum_{y=1}^{N}\left[h'_k(x, y) - \overline{h'_k(x, y)}\right]^2}\;\sqrt{\sum_{x=1}^{M}\sum_{y=1}^{N}\left[I(x, y) - \overline{I(x, y)}\right]^2}} \tag{16}$$

here M, N are dimension of plaintext image, and overline is an average operator.

Here, two binary phase modulators $\gamma_1(u, v)$ and $\gamma_2(x, y)$ form two private keys $P_1(u, v)$ and $P_2(x, y)$, respectively are:

$$P_1(u, v) = \exp\left[-\varphi'(u, v)\right]\exp\left[i\pi\gamma_1(u, v)\right] \tag{17}$$

$$P_2(x, y) = \exp\left[i\pi\gamma_2(x, y)\right] \tag{18}$$

Step 8: The LU decomposition is performed on $e_k(x, y)$ if CC is greater than a threshold value. A pair of lower and upper triangular matrices and a permutation matrix are obtained through LU decomposition:

$$[L, U, P] = \mathrm{LU}\left[e_k(x, y)\right] \tag{19}$$

where LU denotes the lower–upper decomposition operator. The lower and upper matrix is represented by L and U, respectively, and the permutation matrix is denoted by P. Due to sparse matrix P, the ciphertext alone cannot provide sufficient information to the attacker in an iterative attack using phase retrieval technique, even if the attacker has access to the actual ciphertext. As a result, without knowledge of private keys, decrypting the plaintext from a known ciphertext will be challenging, which enhances the proposed scheme security level [42].

Step 9: The encrypted image $E(x, y)$ of size 16×16 is obtained by compressing the permutation matrix:

$$P_3 = L_{i,j} \times U_{i,j} \tag{20}$$

$$E(x, y) = \mathrm{compressed}(P) \tag{21}$$

The combination of lower and upper triangular matrix acts as a private key P_3 as shown in Eq. (20). As P is a sparse matrix and location of its non-zero entries can be stored and saved as encrypted image as shown in Fig. 3(a).

The following steps are used for the decryption process listed below.

Step 1: The matrix P is restored from the encrypted image $E(x, y)$ by using its address values as its elements. For this, a zero matrix of size 256×256 is considered. Location entries of $E(x, y)$ in zero matrix are stored in the form of one get to get P matrix. Therefore, performing the inverse LU decomposition using private key P_3 and P as

$$C_1(x, y) = P \times P_3 \tag{22}$$

Step 2: The image $C_1(x, y)$ is bonded with decryption key $D_2(x, y)$, which is generated by bonding private key $P_2(x, y)$ with public key RPM2(x, y). The resultant image undergoes gyrator transform with angle α:

$$C_2(u, v) = \mathrm{GT}^{\alpha}\left[D_2(x, y)\, C_2(x, y)\right] \tag{23}$$

where $D_2(x, y) = P_2(x, y)\,\mathrm{RPM2}(x, y)$.

Step 3: Another decryption key $D_1(u, v)$ is bonded with $C_2(u, v)$ and followed with gyrator transform of angle β:

$$C_3(x, y) = \mathrm{GT}^{\beta}\Big[D_1(u, v)\, C_2(u, v)\Big] \tag{24}$$

where $D_1(u, v) = \mathrm{RPM1}(u, v) P_1(u, v)$.

Step 4: To obtain the decrypted image $D(x, y)$, perform the phase truncation operation on $C(x, y)$, as shown in Fig. 3(b), and

$$D(x, y) = \mathrm{PT}\Big[C_3(x, y)\Big]$$

4. Results and discussion

The validation and resistance of the presented scheme are investigated against various attacks. MATLAB has been used to do numerical simulation for the proposed cryptosystem. The proposed cryptosystem results are shown corresponding to grayscale and medical images of size 256×256 pixels. During encryption process, the threshold value of CC is considered 0.98 in the improved Yang–Gu algorithm.

The validation outcomes corresponding to input images such as grayscale and medical images are displayed in Figs. 4 and 5, respectively. The input grayscale image is depicted in Fig. 4(a) whereas Fig. 4(e) shows its corresponding encrypted image of size 16×16 pixels. The recovered image is presented in Fig. 4(i). The corresponding lower, upper, and permutation matrices after LU decomposition for the proposed cryptosystem are illustrated in Figs. 4(b)–(d), respectively. Three private keys namely, P_1, P_2, and P_3, are generated, during the encryption process that are shown in Figs. 4(f)–(h), respectively. Figure 5 shows the validation outcomes for the medical

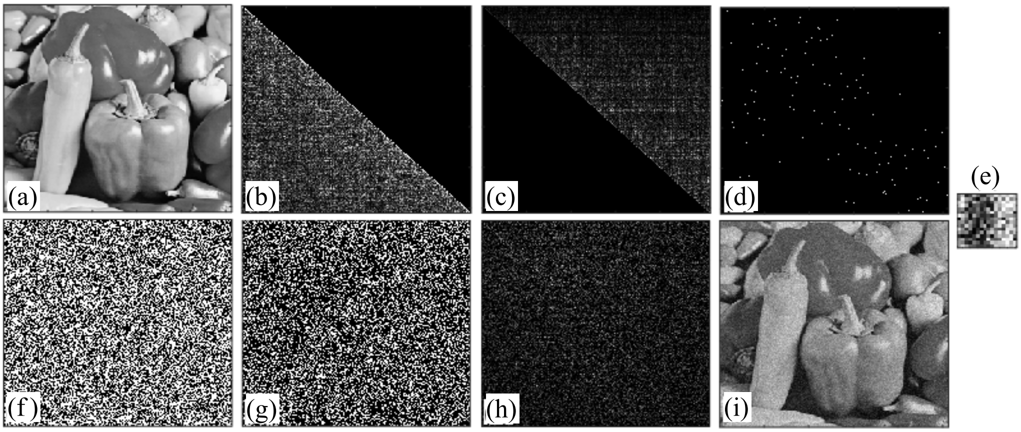

Fig. 4. The validation outcomes corresponding to grayscale image. (a) Input image. (b) Lower, (c) upper, and (d) permutation matrices after LU decomposition for the proposed cryptosystem. (e) Encrypted image of size 16×16 pixels. Private keys (f) P_1, (g) P_2, and (h) P_3 generated during the encryption process. (i) Recovered image.

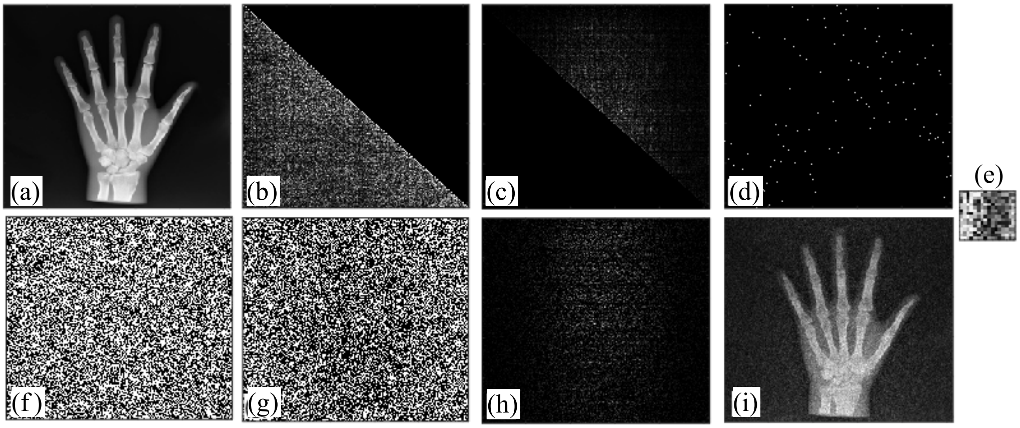

Fig. 5. The validation outcomes corresponding to medical image. (a) Input image. (b) Lower, (c) upper, and (d) permutation matrices after LU decomposition for the proposed cryptosystem. (e) Encrypted image of size 16 × 16 pixels. Private keys (f) P_1, (g) P_2, and (h) P_3 generated during the encryption process. (i) Recovered image.

image. Figures 4(i) and 5(i) indicate that the retrieved images are visible even with compressed encrypted image. They are almost the same as an input image. Thus, Figs. 4 and 5 demonstrate that the proposed scheme effectively retrieves the input image with compressed encrypted image.

The quality of recovered image is analysed through statistical metric [43] such as correlation coefficient. The CC value gives the relationship between pixels of two images. It used to determine the how these two images are related to each other and its lies between –1 and 1. The value of CC approaching –1 indicates that images are negatively correlated whereas CC = 0 shows that they are not correlated to each other. The value of CC approaching to 1 indicates that images are positively correlated and shows perfect relationship between them. For the proposed cryptosystem, value of CC for grayscale and medical images are 0.9668 and 0.9680 between the original and retrieved images, respectively.

Also, the proposed scheme is based on LU decomposition which leads to its compression. The compression ratio provides a numerical value that how much data has been compressed in size as compared to its original size. Therefore, the compression ratio is computed using the following equation:

$$\text{Compression ratio} = \frac{\text{Bits per pixels / Number of pixels}_{\text{original}}}{\text{Bits per pixels / Number of pixels}_{\text{compressed}}} \tag{25}$$

Thus, for proposed scheme's value of compression ratio is computed by using Eq. (25) and given as

$$\text{Compression ratio} = \frac{65\,536}{256} = 256 \tag{26}$$

The values of statistical metric CC and compression ratio show the efficacy of the proposed scheme.

4.1. Statistical attack analysis

The effectiveness of the proposed scheme is tested against statistical attacks including histogram, correlation distribution, 3-D plots, and information entropy. For an ideal cryptosystem, histogram of ciphertext is altogether different from input image and is uniformly distributed. The histogram plots of the original grayscale and medical images are shown in Figs. 6(a) and (b), and their corresponding encrypted image histogram plots are depicted in Figs. 6(c) and (d), respectively. Figure 6 indicates that the histograms of encrypted images are uniformly distributed and differ entirely from input image plots. Thus, the proposed scheme offers sturdiness and robustness against the histogram analysis.

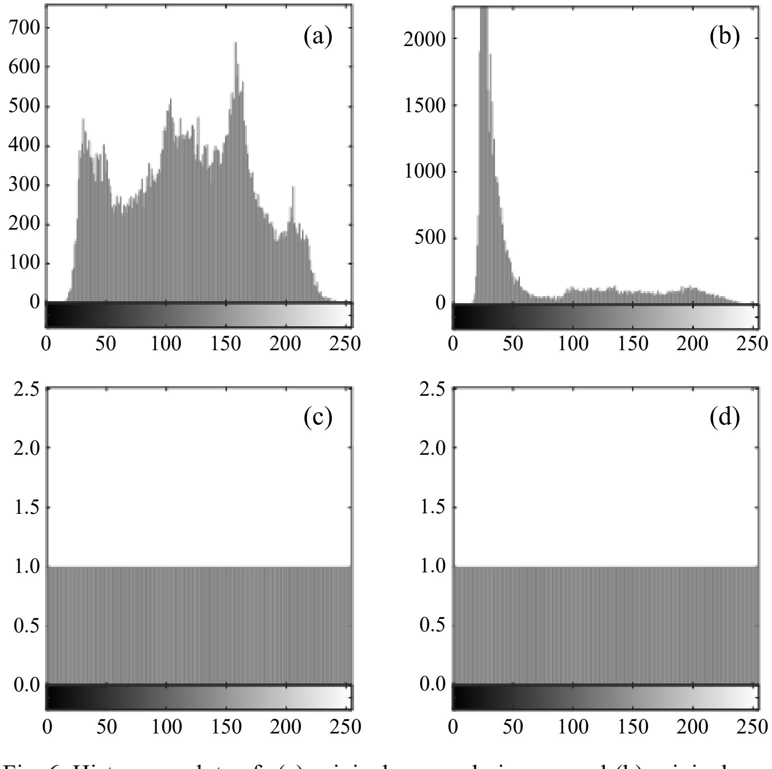

Fig. 6. Histogram plots of: (a) original grayscale image, and (b) original medical image. (c, d) Corresponding encrypted image histogram plots.

Figures 7(a) and (b) display the 3-D plots of input grayscale and medical images. The corresponding 3-D plots of the encrypted image are shown in Figs. 7(c) and (d) whereas retrieved image 3-D plots are demonstrated in Figs. 7(e) and (f), respectively. Figure 7 reveals that the 3-D plots of the input and retrieved images are similar, where-

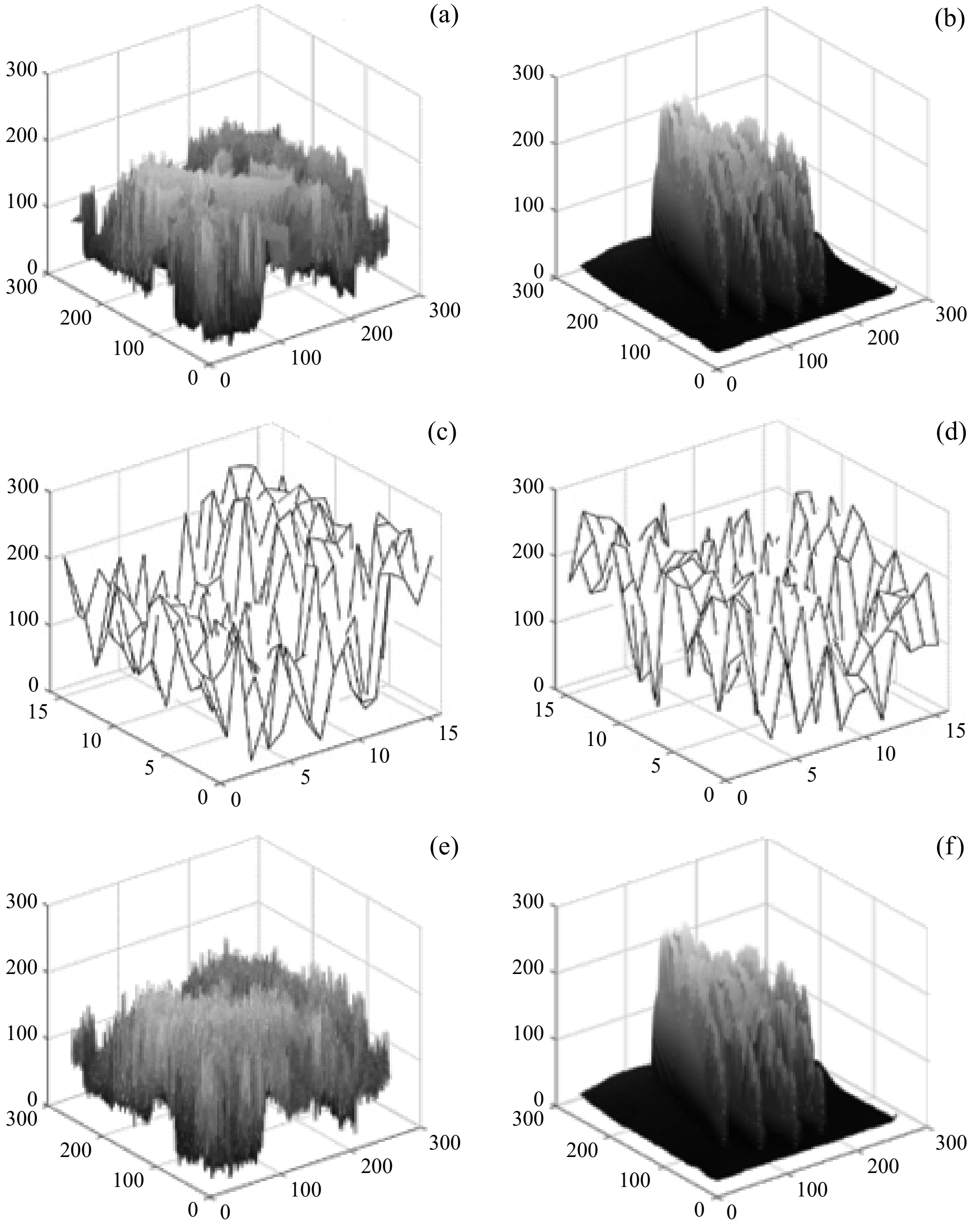

Fig. 7. 3-D plots of input images: (a) grayscale, and (b) medical. (c, d) The corresponding 3-D plots of the encrypted image. (e, f) The corresponding retrieved image 3-D plots.

as the 3-D plots of the encrypted images differ significantly. Thus, 3-D plots do not expose any information about input image.

Another statistical attack, *i.e.*, correlation distribution plots are also analysed for the scheme. An adversary can obtain helpful information from the strong correlation present in adjacent pixels of ciphertext. For a secured cryptosystem, the correlation of neighbouring pixels of ciphertext image must be low. For the evaluation, 5000 adjacent pixels were arbitrarily selected from the input images in the diagonal direction. Figures 8(a) and (b) demonstrate the correlation distribution plots of input images: grayscale and medical. The correlation plots of the corresponding ciphertext are displayed in Figs. 8(c) and (d), respectively. Also, the values of CC between input and encrypted images are calculated in horizontal, diagonal, and vertical directions and presented in Table 1. Figure 8 and Table 1 indicate that for input images value of correlation is high, whereas it is low for the encrypted images. From the above discussion, the observation about cryptosystem is that it successfully resists the statistical attacks.

The proposed cryptosystem performance is also evaluated in terms of information entropy. The uncertainty level of randomness in pixel distribution is examined by in-

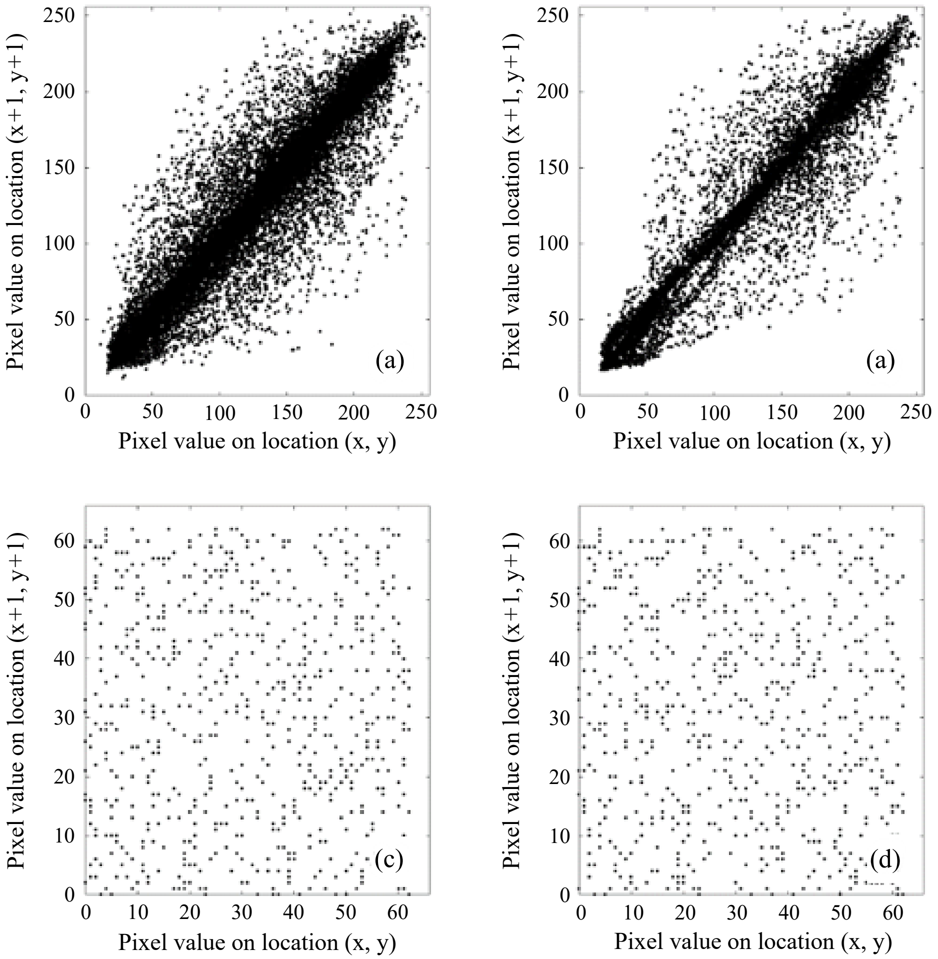

Fig. 8. The correlation distribution plots of input images: (a) grayscale and (b) medical. (c, d) The correlation plots of the corresponding ciphertext.

Table 1. Values of correlation coefficient between plaintext and ciphertext.

	Plaintext		Ciphertext	
	Grayscale image	Medical image	Grayscale image	Medical image
Diagonal	0.9269	0.9765	0.4245	0.2077
Horizontal	0.9500	0.9809	0.4487	0.2415
Vertical	0.9658	0.9942	0.4967	0.2472

formation entropy. The minimum value of entropy is 0 while 8 is the maximum value for a 8 bit image. The entropy value approaching 8 signifies a high level of randomness. The entropy value of the proposed cryptosystem for original grayscale and medical images are 7.6021 and 5.8862 whereas for corresponding encrypted images are 7.9922 and 7.9931, respectively. Values of entropy in encrypted images approach to its maximum value, which reflects the strength of proposed scheme.

4.2. Key sensitivity analysis

The proposed cryptosystem has three private keys P_1, P_2, P_3 and two gyrator transform parameters α and β. Kerckhoff's principle states that the security of a scheme depends upon the strength of keys. Therefore, the sensitivity of private keys and gyrator transform parameters for the proposed scheme need to be examined. Figure 9 depicts the retrieved image when one of the private keys is wrong. Figure 9(a) illustrates the retrieved image when private key P_1 is wrong, whereas the retrieved image corresponding to the wrong key P_2 and P_3 are display in Figs. 9(b) and (c), respectively. Also, the key sensitivity analysis is presented in terms of CC plots for the gyrator parameters α and β. Figures 10(a) and (b) show the CC plots of α and β when the original value of the gyrator parameter is slightly changed in order of 0.001 to its original value. From the Fig. 10, it is observed that only at the correct value of gyrator parameters the value of CC is almost one whereas with the slight change in the value of α and β the value of CC sharply drops. The key sensitivity analysis of encryption parameters of the reported scheme shows the strength of private keys, and gyrator parameters are not susceptible.

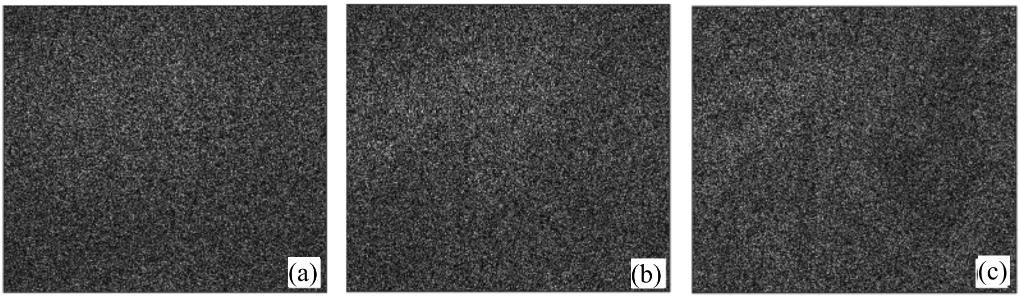

Fig. 9. The retrieved images corresponding to the wrong private key (a) P_1, (b) P_2, and (c) P_3.

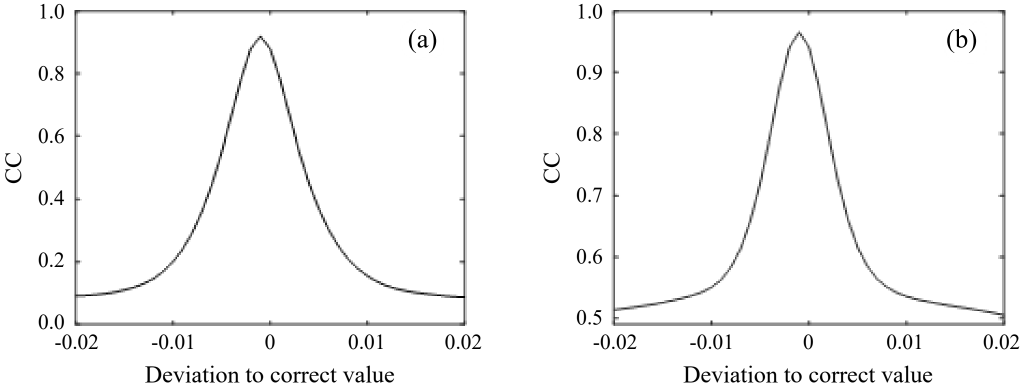

Fig. 10. The CC plots of (a) α and (b) β when the original value of the gyrator parameter is slightly changed in order of 0.001 to its original value.

4.3. Pixel shuffling attack

The efficacy of the presented cryptosystem is analysed against the shuffling of encrypted image pixels. Usually, the occlusion attack is used to test the performance of a cryptosystem. In occlusion attack, occluded portion is replaced by zeros. But, in the proposed scheme, the pixel position is transferred with a restriction that it cannot be zero. Thus, the proposed cryptosystem is evaluated against data shuffling attack. The encrypted images when 20%, 40%, and 60% of data are shuffled with rows displayed in Figs. 11(a)–(c) whereas Figs. 11(d)–(f) illustrate the corresponding retrieved images, respectively. The retrieved image quality is low when the number of pixels shuffled are increased, however, the decrypted image is still identifiable. Thus, the presented cryptosystem successfully endured the shuffling attack.

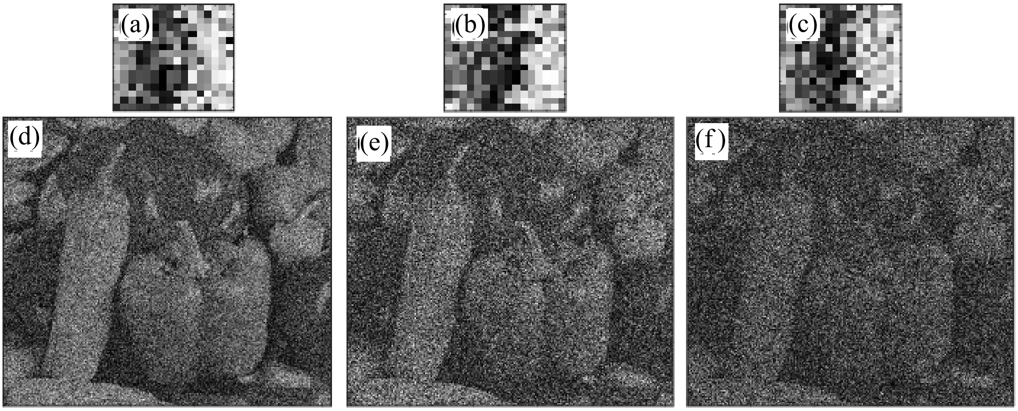

Fig. 11. The encrypted images when (a) 20%, (b) 40%, and (c) 60% of data are shuffled with rows, and (d–f) the corresponding retrieved images.

4.4. Basic attack analysis

The basic attacks are mainly: known-plaintext attack (KPA), ciphertext-only attack (COA), and chosen-plaintext attack (CPA). It is well known that if the cryptosystem can endure the CPA, then it can also endure the other basic attacks such as KPA, and COA. The proposed cryptosystem is based on improved version of Yang–Gu algorithm, and WANG *et al.* [20] have shown that the improved Yang–Gu algorithm resists against the CPA. Figure 12 displays the recovered image corresponding to the CPA for the proposed cryptosystem. Thus, the presented scheme resists the basic attacks.

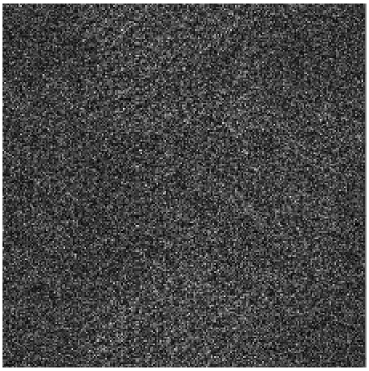

Fig. 12. The recovered image corresponding to the CPA for the proposed cryptosystem.

4.5. Time complexity analysis

The complete cryptosystem comprises the encryption and decryption process of the proposed scheme, time taken by grayscale and medical images are 37.03 and 35.93 sec with 1000 number of iterations, respectively. The decryption process takes time only 0.126 and 0.077 sec of grayscale and medical images, which reflects the complexity of encryption process and simplicity of decryption process.

5. Comparison analysis

The comparison of proposed cryptosystem is performed with some recent similar cryptosystems *i.e.*, XU *et al.* [45], GONG *et al.* [44], RAKHEJA *et al.* [39], and KUMARI *et al.* [38], and explained in Table 2. The comparison has been done on various criteria such as transform domain, compression technique, applied approaches, compression ratio, implementation, types of images, and performance against basic attacks. Table 2 reveals that the reported cryptosystem has been validated for grayscale and medical images whereas another cryptosystems are silent about medical image. Proposed cryptosystem also shows a high compression ratio and high key sensitivity against its private keys and gyrator transform parameters. The proposed scheme is also a well-coped pixel-shuffled data attack.

Table 2. Comparison analysis of the proposed cryptosystem.

Parameters	Xu *et al.* [45]	Gong *et al.* [44]	Rakheja *et al.* [39]	Kumari *et al.* [38]	Proposed cryptosystem
Transform domain	Discrete wavelet domain	Discrete fractional random transform	Hybrid multi-resolution wavelet	Fresnel	Gyrator
Applied approach	Symmetric	Symmetric	Asymmetric	Asymmetric	Hybrid
Types of images	Grayscale	Grayscale	Grayscale	Color	Grayscale and medical
Compression technique	Compressive sensing	Discrete cosine transform	Compressed sparse row	Discrete cosine transform	Compressed sparse
Compression ratio	0.75	4	127.502	–	256
Performance against basic attacks	Robust against chosen/known plaintext, minor occlusion, and low-intensity noise	Endure a small degree of occlusion, noise attack	Robust against occlusion and noise attack	Robust against occlusion, noise, and special attack	Robust against pixel shuffling and basic attacks

6. Conclusion

In this paper, a hybrid (symmetric and one-time-pad) cryptosystem based on improved Yang–Gu algorithm and compression using gyrator transform is proposed. The Yang –Gu algorithm makes the cryptosystem nonlinear. The LU decomposition process is used for compression, which not only provides a compressed ciphertext but also provides a private key. During encryption process, three private keys are obtained, one from LU decomposition and the other two are generated through binary phase modulators. The gyrator parameters also provide extra security to the encryption algorithm. The validation and performance of the proposed cryptosystem are examined on different types of images including grayscale and medical images through MATLAB. The statistical attacks are analysed in terms of information entropy, 3-D, histogram, and correlation distribution plots. The cryptosystem also offers high robustness against pixel shuffling attack. It is also well performed against all private keys and gyrator transform parameters. The proposed cryptosystem also resists the basic attacks. Therefore, the proposed cryptosystem will offer a more secure and robust image transfer process in real life because of its capability to offer a shield against various attacks.

Fundings

This work was supported by the award reference number 1172(CSIR-UGC NET DEC.2018) from University Grants Commission, Ministry of Human Resource Development.

References

[1] Refregier P., Javidi B., *Optical image encryption based on input plane and Fourier plane random encoding*, Optics Letters **20**(7), 1995: 767-769. https://doi.org/10.1364/OL.20.000767

[2] Frauel Y., Castro A., Naughton T.J., Javidi B., *Resistance of the double random phase encryption against various attacks*, Optics Express **15**(16), 2007: 10253-10265. https://doi.org/10.1364/OE.15.010253

[3] Carnicer A., Montes-Usategui M., Arcos S., Juvells I., *Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys*, Optics Letters **30**(13), 2005: 1644-1646. https://doi.org/10.1364/OL.30.001644

[4] Peng X., Wei H., Zhang P., *Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain*, Optics Letters **31**(22), 2006: 3261-3263. https://doi.org/10.1364/OL.31.003261

[5] Gopinathan U., Monaghan D.S., Naughton T.J., Sheridan J.T., *A known-plaintext heuristic attack on the Fourier plane encryption algorithm*, Optics Express **14**(8), 2006: 3181-3186. https://doi.org/10.1364/OE.14.003181

[6] Qin W., Peng X., *Asymmetric cryptosystem based on phase-truncated Fourier transforms*, Optics Letters **35**(2), 2010: 118-120. https://doi.org/10.1364/OL.35.000118

[7] Wang X., Zhao D., *A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms*, Optics Communications **285**(6), 2012: 1078-1081. https://doi.org/10.1016/j.optcom.2011.12.017

[8] Wang X., Chen Y., Dai C., Zhao D., *Discussion and a new attack of the optical asymmetric cryptosystem based on phase-truncated Fourier transform*, Applied Optics **53**(2), 2014: 208-213. https://doi.org/10.1364/AO.53.000208

[9] Wang Y., Quan C., Tay C.J., *Improved method of attack on an asymmetric cryptosystem based on phase-truncated Fourier transform*, Applied Optics **54**(22), 2015: 6874-6881. https://doi.org/10.1364/AO.54.006874

[10] Rajput S.K., Nishchal N.K., *Fresnel domain nonlinear optical image encryption scheme based on Gerchberg–Saxton phase-retrieval algorithm*, Applied Optics **53**(3), 2014: 418-425. https://doi.org/10.1364/AO.53.000418

[11] Liu W., Liu Z., Liu S., *Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang–Gu algorithm*, Optics Letters **38**(10), 2013: 1651-1653. https://doi.org/10.1364/OL.38.001651

[12] He W., Meng X., Peng X., *Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang–Gu algorithm: Comment*, Optics Letters **38**(20), 2013: 4044. https://doi.org/10.1364/OL.38.004044

[13] Liu W., Liu Z., Liu S., *Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang–Gu algorithm: Reply*, Optics Letters **38**(20), 2013: 4045. https://doi.org/10.1364/OL.38.004045

[14] Sui L., Liu B., Wang Q., Li Y., Liang J., *Double-image encryption based on Yang–Gu mixture amplitude-phase retrieval algorithm and high dimension chaotic system in gyrator domain*, Optics Communications **354**, 2015: 184-196. https://doi.org/10.1016/j.optcom.2015.05.071

[15] Sui L., Liu B., Wang Q., Li Y., Liang J., *Color image encryption by using Yang–Gu mixture amplitude-phase retrieval algorithm in gyrator transform domain and two-dimensional Sine logistic modulation map*, Optics and Lasers in Engineering **75**, 2015: 17-26. https://doi.org/10.1016/j.optlaseng.2015.06.005

[16] Abuturab M.R., *Securing multiple information using wavelet transform and Yang–Gu mixture amplitude-phase retrieval algorithm*, Optics and Lasers in Engineering **118**, 2019: 42-51. https://doi.org/10.1016/j.optlaseng.2019.01.015

[17] Wang Y., Quan C., Tay C.J., *Nonlinear multiple-image encryption based on mixture retrieval algorithm in Fresnel domain*, Optics Communications **330**, 2014: 91-98. https://doi.org/10.1016/j.optcom.2014.05.032

[18] Rakheja P., Yadav S., Tobria A., *A novel image encryption mechanism based on umbrella map and Yang–Gu algorithm*, Optik **271**, 2022: 170152. https://doi.org/10.1016/j.ijleo.2022.170152

[19] Tobria A., Singh P., *A comparative analysis of phase retrieval algorithms in asymmetric double image cryptosystem in gyrator domain*, Optical and Quantum Electronics **56**, 2024: 33. https://doi.org/10.1007/s11082-023-05524-y

[20] Wang Y., Quan C., Tay C.J., *Asymmetric optical image encryption based on an improved amplitude–phase retrieval algorithm*, Optics and Lasers in Engineering **78**, 2016: 8-16. https://doi.org/10.1016/j.optlaseng.2015.09.008

[21] Sayood K., *Introduction to Data Compression*, 3rd Ed., Morgan Kaufmann Series in Multimedia Information and Systems, Elsevier, Amsterdam, Boston, 2006.

[22] Rhee H., Jang Y.I., Kim S., Cho N.I., *Lossless image compression by joint prediction of pixel and context using duplex neural networks*, IEEE Access **9**, 2021: 86632-86645. https://doi.org/10.1109/ACCESS.2021.3088936

[23] Otair M., Abualigah L., Qawaqzeh M.K., *Improved near-lossless technique using the Huffman coding for enhancing the quality of image compression*, Multimedia Tools and Applications **81**, 2022: 28509-28529. https://doi.org/10.1007/s11042-022-12846-8

[24] Chai X., Zheng X., Gan Z., Han D., Chen Y., *An image encryption algorithm based on chaotic system and compressive sensing*, Signal Processing **148**, 2018: 124-144. https://doi.org/10.1016/j.sigpro.2018.02.007

[25] Wang H., Xiao D., Li M., Xiang Y., Li X., *A visually secure image encryption scheme based on parallel compressive sensing*, Signal Processing **155**, 2019: 218-232. https://doi.org/10.1016/j.sigpro.2018.10.001

[26] Huang S., Jiang D., Wang Q., Guo M., Huang L., Li W., Cai S., *High-quality visually secure image cryptosystem using improved Chebyshev map and 2D compressive sensing model*, Chaos, Solitons & Fractals **163**, 2022: 112584. https://doi.org/10.1016/j.chaos.2022.112584

[27] Ye G., Liu M., Wu M., *Double image encryption algorithm based on compressive sensing and elliptic curve*, Alexandria Engineering Journal **61**(9), 2022: 6785-6795. https://doi.org/10.1016/j.aej.2021.12.023

[28] Abuturab M.R., Alfalou A., *Multiple color image fusion, compression, and encryption using compressive sensing, chaotic-biometric keys, and optical fractional Fourier transform*, Optics & Laser Technology **151**, 2022: 108071. https://doi.org/10.1016/j.optlastec.2022.108071

[29] Chai X., Fu J., Gan Z., Lu Y., Zhang Y., Han D., *Exploiting semi-tensor product compressed sensing and hybrid cloud for secure medical image transmission*, IEEE Internet of Things Journal **10**(8), 2023: 7380-7392. https://doi.org/10.1109/JIOT.2022.3228781

[30] Saad A.-M.H.Y., Abdullah M.Z., *High-speed implementation of fractal image compression in low cost FPGA*, Microprocessors and Microsystems **47**, 2016: 429-440. https://doi.org/10.1016/j.micpro.2016.08.004

[31] Zhou N.-R., Tong L.-J., Zou W.-P., *Multi-image encryption scheme with quaternion discrete fractional Tchebyshev moment transform and cross-coupling operation*, Signal Processing **211**, 2023: 109107. https://doi.org/10.1016/j.sigpro.2023.109107

[32] Ping P., Yang X., Zhang X., Mao Y., Khalid H., *Generating visually secure encrypted images by partial block pairing-substitution and semi-tensor product compressed sensing*, Digital Signal Processing **120**, 2022: 103263. https://doi.org/10.1016/j.dsp.2021.103263

[33] Jridi M., Alfalou A., Meher P.K., *Optimized architecture using a novel subexpression elimination on Loeffler algorithm for DCT-based image compression*, VLSI Design, Vol. 2012, 2012: 209208. https://doi.org/10.1155/2012/209208

[34] Xue J., Yin L., Lan Z., Long M., Li G., Wang Z., Xie X., *3D DCT based image compression method for the medical endoscopic application*, Sensors **21**(5), 2021: 1817. https://doi.org/10.3390/s21051817

[35] Rajprabu R., Prathiba T., Deepa Priya V., Rajkumar A., Rajkannan C., Ramalakshmi P., *Transforming pixels: Crafting a 3D integer discrete cosine transform for advanced image compression*, International Journal of Advanced Computer Science and Applications **15**(5), 2024: 819-826. https://doi.org/10.14569/IJACSA.2024.0150582

[36] Huang Z., Zhang X., Chen L., Zhu Y., An F., Wang H., Feng S., *A vector-quantization compression circuit with on-chip learning ability for high-speed image sensor*, IEEE Access **5**, 2017: 22132 -22143. https://doi.org/10.1109/ACCESS.2017.2762399

[37] Kim H., No A., Lee H.-J., *SPIHT algorithm with adaptive selection of compression ratio depending on DWT coefficients*, IEEE Transactions on Multimedia **20**(12), 2018: 3200-3211. https://doi.org/10.1109/TMM.2018.2832604

[38] Kumari E., Mukherjee S., Singh P., Kumar R., *Asymmetric color image encryption and compression based on discrete cosine transform in Fresnel domain*, Results in Optics **1**, 2020: 100005. https://doi.org/10.1016/j.rio.2020.100005

[39] Rakheja P., Singh P., Vig R., *An asymmetric image encryption mechanism using QR decomposition in hybrid multi-resolution wavelet domain*, Optics and Lasers in Engineering **134**, 2020: 106177. https://doi.org/10.1016/j.optlaseng.2020.106177

[40] Rodrigo J.A., Alieva T., Calvo M.L., *Gyrator transform: Properties and applications*, Optics Express **15**(5), 2007: 2190-2203. https://doi.org/10.1364/OE.15.002190

[41] Su Q., Wang G., Zhang X., Lv G., Chen B., *A new algorithm of blind color image watermarking based on LU decomposition*, Multidimensional Systems and Signal Processing **29**, 2018: 1055-1074. https://doi.org/10.1007/s11045-017-0487-7

[42] Xiong Y., Quan C., *Hybrid attack free optical cryptosystem based on two random masks and lower upper decomposition with partial pivoting*, Optics & Laser Technology **109**, 2019: 456-464. https://doi.org/10.1016/j.optlastec.2018.08.033

[43] Wang Z., Bovik A.C., Sheikh H.R., Simoncelli E.P., *Image quality assessment: From error visibility to structural similarity*, IEEE Transactions on Image Processing **13**(4), 2004: 600-612. https://doi.org/10.1109/TIP.2003.819861

[44] Gong L., Deng C., Pan S., Zhou N., *Image compression-encryption algorithms by combining hyper-chaotic system with discrete fractional random transform*, Optics & Laser Technology **103**, 2018: 48-58. https://doi.org/10.1016/j.optlastec.2018.01.007

[45] Xu Q., Sun K., Cao C., Zhu C., *A fast image encryption algorithm based on compressive sensing and hyperchaotic map*, Optics and Lasers in Engineering **121**, 2019: 203-214. https://doi.org/10.1016/j.optlaseng.2019.04.011

Received January 1, 2025
in revised form January 23, 2025