Hindawi
International Journal of Optics
Volume 2021, Article ID 5510125, 19 pages
https://doi.org/10.1155/2021/5510125

Research Article

A Secure Asymmetric Optical Image Encryption Based on Phase Truncation and Singular Value Decomposition in Linear Canonical Transform Domain

Anshula Sangwan [1] **and Hukum Singh** [2]

[1]*Department of Computer Science and Engineering, The NorthCap University, Sector 23-A, Gurugram 122 017, India*
[2]*Department of Applied Sciences, The NorthCap University, Sector 23-A, Gurugram 122 017, India*

Correspondence should be addressed to Hukum Singh; hukumsingh@ncuindia.edu

Received 27 January 2021; Revised 27 February 2021; Accepted 19 March 2021; Published 16 April 2021

Academic Editor: Paramasivam Senthilkumaran

A new asymmetric optical double image encryption algorithm is proposed, which combines phase truncation and singular value decomposition. The plain text is encrypted with two-stage phase keys to obtain a uniformly distributed cipher text and two new decryption keys. These keys are generated during the encryption process and are different from encryption keys. It realizes asymmetric encryption and improves the security of the system. The unscrambling keys in the encryption operation are mainly related to plain text. At the same time, the system is more resistant to selective plain text attacks; it also improves the sensitivity of decryption keys. With the application of phase truncation, the key space expanded and the security of the cryptographic system is enhanced. The efficacy of the system is calculated by evaluating the estimated error between the input and retrieved images. The proposed technique provides innumerable security keys and is robust against various potential attacks. Numerical simulations verify the effectiveness and security of the proposed technique.

1. Introduction

With the rapid development of modern online transactions, protecting information security has become increasingly difficult. Unauthorized users may access the data, so information hiding techniques are required to conceal the multimedia data from unintended users. To overcome this problem, many encoding methods have been developed in the field of optical security, biometrics, and holographic storage. Parameters such as phase, amplitude, wavelength, frequency, and polarization have multiple degrees of freedom, thus increasing the key space. Therefore, optical techniques are the prime requirement, where a given data will be transmitted secretly on it, and any attacker in the middle cannot obtain the data. In the previous years, many encoding techniques were developed [1–6]. The double random phase encoding (DRPE) method [1] suggested by Refregier and Javidi in 1995 is the most effective image coding scheme. DRPE is an effective solution because the information is encrypted into an unrecognizable format. In DRPE, the original images are multiplied by randomly generated phase keys by using the input domain and the Fourier domain and a random phase mask (RPM) used as a security key. Use the conjugate of the encrypted image or the conjugate of the RPM to decrypt and return to tracing the optical path. In addition, DRPE - based coding methods are prolonged from Fourier transform (FT) to many other domains, such as fractional Fourier transform [7–12], Fresnel transform [13, 14], Fresnel wavelet transform [15], fractional Mellin transform [16–19], gyrator transform (GT) [20–25], gyrator wavelet transform (GWT) [26, 27], ghost Holography [28], etc.

In all these techniques, the indistinguishable RPM acts as a key during the decryption process. Similarly, due to the inherent nature of attacks, symmetrical schemes are used to deal with attacks, such as chosen cipher attack

(CCA), chosen plain attack (CPA), and known plain attack (KPA) [29–31] because of an immanent stretch; it faces the problem of precondition administering and conducts. To address aforesaid matter, some dissymmetric optical cryptosystems have been proposed. Qin and Peng [32] put forward one of the pioneering work about asymmetric phase reservation (PR) and amplitude-truncation (AT) techniques to make the linearity of symmetric routines better. Since the decryption keys differ from the encryption keys, the author [33] claims that the PTFT-based cryptosystem is nonlinear. In 2013 [34], a speech restoration based on the AM-FM model in the linear canonical transform (LCT) domain was proposed. One relies on linear canonical transform domain filtering; the other relies on restoring the speech signal in the LCT domain. Kumar et al. [35] proposed an asymmetric method that uses two-dimensional nonseparable linear canonical transform (2D-NSLCT) and an iterative phase retrieval algorithm for duplex image encryption. First, PRA generates an encryption security key. Here, two intensity images are combined to form a complex image. Rakheja et al. [36] proposed a duplex image encoding based on the 3D Lorenz chaotic system and QR decomposition in the two-dimensional nonseparable linear canonical transform domain. In this communication, the unconventional framework of the 2D–NSLCT extends the key-size of the initiate scheme and enhances the robustness against brute-force attacks. The phase truncation part will continue for further processing, whereas the phase reserve part is used as the decryption key. After the intermediate cipher text is multiplied by a random phase mask, the inverse two-dimensional inseparable canonical transform will be performed. The output obtained is QR decomposition to get the final cipher text and another private key. Rajput and Matoba [37] proposed optical voice encryption in the other optical domains such as fractional Fourier, Fresnel and gyrator transforms, which convert input information into different mixed space-frequency domains. They also analyzed the experimental recording conditions of the human voice and some security aspects of the scheme. Their results show that the original voice cannot be retrieved unless the correct keys and correct domain orders are used. Number of papers published in the linear canonical transform have been studied [38–49]. Wang et al. [50–61] proposed the high-dimension Lorenz chaotic system and perceptron model, a chaotic image encryption system. Image encryption and various analysis have also been performed by authors [62, 63]. They describe the algorithm flow in detail and analyze the cryptographic security. Some of the papers on image encryption in different context have been noted [64, 65].

In this communication, we have introduced an unpredictable method for narrating duplex picture encryption using two-dimensional LCT and DPM besides esteem deterioration. The proposed LCT has comparable properties, such as numerous well-known scientific changes. We know that the classical DRPE experiences issue of key space and optical hub arrangement. To overcome these issues and to extend the key space, we favor utilizing a deterministic phase mask (DPM) [56, 62] rather than conventional RPM. The use of LCT has advantages such as computational ease and convenience in their optical implementation. The variations of LCT orders are achieved by rotation of the lens system because there is no need to change the distance like the optical implementation of fractional Fourier transform. The proposed scheme provides enhanced security by increasing the key space through the use of a deterministic phase mask. Such phase masks are easier to position in the decoding and provide their own security parameters.

In this article, the security of the cryptosystem depends on the linear canonical transform domain. The rest of the manuscript is organized as follows: Section 2 reflects the conceptual framework of the suggested scheme, Section 3 gives the proposed encryption and decryption methods, Section 4 indicates the various simulation results and robustness of DPM, and the concluding remarks are given in Section 5.

2. Principle

2.1. Generation of Deterministic Phase Mask (DPM). The deterministic phase mask (DPM) is produced by characterizing the arrangement (m), which is given by the number of subkeys (NSK) in a single stage cover, where NSK = $(2^m \times 2^m)$. As described in [19, 66, 67], the upcoming DPM can consist of a combination of the 16 submasks $M(i, j)$ represented. DPM for the specific esteem of $m = 4$ is displayed in Figure 1

$$\mathrm{DPM} = \sum_{i=0}^{2^m} \sum_{j=0}^{2^m} M_{i,j}(d \times d), \tag{1}$$

where $M_{i,j}$ is defined as follows:

$$M_{i,j}(x, y) = e^{2i\pi\left(u_k \cdot x_+ v_k \cdot y\right)}, \tag{2}$$

where $k = 1, 2, \ldots\ldots\ldots\ldots$ NSK (number of subkeys) and u_k and v_k are randomly generated in the interval $[1, d]$, where k is defined into the interval. $[1, 2^m]$.

For simplicity, we display the example when the order of encryption $m = 2$, 3 and 4. If $m = 2$, deterministic masks are considered (256×256) with 16 NSK of size (64×64). Each DPM_1 or DPM_2 is combined with 16 submasks M_{ij}, as k interval is from 1 to 4, u_k and v_k are randomly generated in the interval from 1 to 64. If $m = 3$, deterministic masks (256×256) are constructed with 8 NSK of size (32×32). Each DPM_1 or DPM_2 is combined with 64 submasks $M_{i,j}$, k interval is from 1 to 8; u_k and v_k are randomly generated in interval from 1 to 32.

2.2. Theoretical Background of LCT. LCT is generated by ABCD transform, generalized Fresnel transform, and amplified fractional Fourier transform. LCT may be directly changing course, with three parameters characterized as follows [38, 42]:

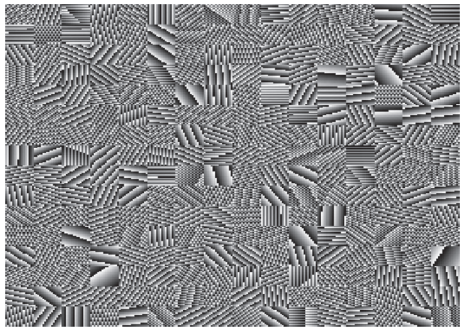

Figure 1: Generation of deterministic phase mask (DPM) for $m = 4$.

$$\begin{aligned}&\mathrm{LCT}_{\alpha,\beta,\gamma}\{f(x,y)\}\\&= k(u,v) = \sqrt{\beta}e^{-i\pi/4}\iint_{\infty}^{\infty}\exp\{i\pi[r(x,u,y,v)]\}f(x,y)\mathrm{d}x\mathrm{d}y,\end{aligned} \tag{3}$$

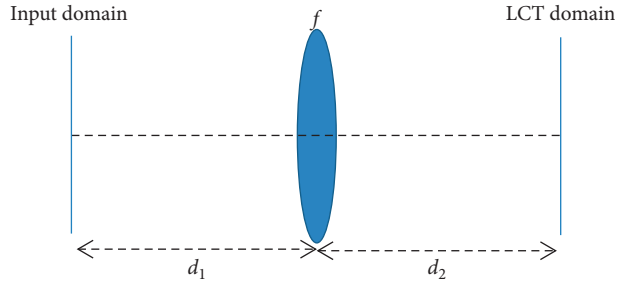

Figure 2: Representation of single lens LCT.

where kernel $r(x,u,y,v) = \alpha(x^2+y^2) - 2\beta(ux+vy) + \gamma(u^2+v^2)$

$\mathrm{LCT}_{(\alpha,\ \beta,\ \gamma)}$ [] indicate that the LCT administrator has three genuine change parameters. These three parameters are independent of (x, y) and (u, v) domains. Inverse two-dimensional LCT is written as follows:

$$\begin{aligned}\mathrm{LCT}_{(-\alpha,-\beta,-\gamma)}\{k(u,v)\} = f(x,\ y) = \sqrt{\beta}e^{i\pi/4}\iint_{\infty}^{\infty}\exp\{-i\pi[s(x,u,y,v)]\}k(u,v)\mathrm{d}u\mathrm{d}v,\\ s(x,u,y,v) = \alpha\left(x^2+y^2\right) - 2\beta(ux+vy) + \gamma\left(u^2+v^2\right),\end{aligned} \tag{4}$$

where $\mathrm{LCT}_{(-\alpha,\ -\beta,\ -\gamma)}$ [] denotes the inverse LCT. If $(\alpha, \beta, \gamma, d) = (0, 1, -1, 0)$, the 2D LCT is simplified to the FT with a multiplier factor $\sqrt{-i}$, where α, β and γ are constants and are related by unit determinant matrix. The elements α, β, γ convey three parameters as the order of LCT. These orders are considered as the key parameters for image encryption purposes. LCT is a unitary transform, a special case, including FT, FrFT, FrT, and operations including scaling and chirp multiplication. The optical LCT system can be implemented using an arbitrary number of thin lenses and propagate through free space. The implementation belongs to the quadratic phase system (QPS) category [68].

The optical implementation of an LCT using a single lens is shown in Figure (2).

The LCT parameters α, β, and γ can be directly related to the distances d_1 and d_2, and the focal length f is as given below:

$$\begin{aligned}\alpha &= \frac{d_1 - f}{\lambda[f(d_1+d_2) - d_1d_2]},\\ \beta &= \frac{f}{\lambda[f(d_1+d_2) - d_1d_2]},\\ \gamma &= \frac{d_2 - f}{\lambda[f(d_1+d_2) - d_1d_2]}.\end{aligned} \tag{5}$$

2.3. Singular Value Decomposition (SVD). The SVD may be a numerical method utilized to diagonalizable matrices. It breaks down a $m \times m$ real matrix A into a product of three matrices as follows [69–73]:

$$\begin{aligned}A = \mathrm{USV}^T = [u_1, u_2, u_3, \ldots, u_m] \times \begin{bmatrix}\sigma_1 & 0 & \cdots & 0\\ 0 & \sigma_2 & \cdots & 0\\ \vdots & 0 & \ddots & 0\\ 0 & 0 & \cdots & \sigma_m\end{bmatrix}\\ \times [v_1, v_2, v_3, \ldots, v_m]^T.\end{aligned} \tag{6}$$

The matrix U and V are orthogonal matrices (i.e., $\mathrm{UU}^T = 1$ and $\mathrm{VV}^{\mathrm{T}} = 1$) having sizes $m \times n$ and $n \times n$, respectively, while S could be an $m \times n$ diagonal matrix with nonnegative real values called singular values. Moreover, the arrangement of USV multiplication is very critical for the input image to be recouped accurately. Amid encryption, USV is made for cipher image $C(x, y)$. At the time of decoding, perform reverse singular value decomposition.

$$\begin{aligned}[\mathrm{USV}] &= \mathrm{SVD}(C(x,y)),\\ \mathrm{ISVD} &= \mathrm{USV}^T.\end{aligned} \tag{7}$$

If the multiplication arrangement has been changed to [UVS], [VUS], and [VSU], you cannot recompose the image. Finally, if the multiplication order is USV, the image can be

restored. Because of multiplication, order plays an important role, so if the door opener gets any components from any channel, he will not be able to determine the first image.

2.4. Nonlinear Phase Truncation Fourier Transform (PTFT). PTFT can be a preparation of Fourier transform, but it has phase truncation, which means that because it only retains the amplitude (modulus part) of the Fourier spectrum, the phase part of the spectrum is truncated. Let $f(x, y)$ denote the image to be encoded, LCT [ ] the operator of linear canonical transform, PT [ ] the operator of the phase truncated, and PR [ ] denote phase reservation. The phase truncation operation of the image $f(x, y)$ in the two-dimensional linear canonical transform can be written as follows:

$$F(u, v) = \mathrm{LCT}[f(x, y)] = |F(u, v)| \cdot e^{[i\varnothing(u,v)]}. \tag{8}$$

The phase truncation (PT) and the phase reservation (PR) operations can be expressed, respectively, as follows:

$$\begin{aligned} \mathrm{PT}[F(u, v)] &= |F(u, v)|, \\ \mathrm{PR}[F(u, v)] &= e^{[i\varnothing(u,v)]}. \end{aligned} \tag{9}$$

3. Proposed Cryptosystem Technique

3.1. Asymmetric Cryptosystem for Encryption. The input image $f(x, y)$ is multiplied by RPM, i.e., $[\exp^{i(2\pi n_1(x,y))}]$ and then linear canonical transformation is performed in the order α_1, β_1, γ_1. Here, $n_1(x, y)$ is statistically independently and randomly distributed in [0, 1]. The PTFT separates the obtained complex spectrum into amplitude and phase. The amplitude-truncation (AT) value helps generate the first decryption key (DK_1) and the phase truncation (PT) value, bonded with another phase mask DPM (for the set $m = 4$), and then proceed to α_2, β_2, γ_2 order then further take linear canonical transformed which give the encrypted image, which is further amplitude-truncated to generate a second decryption key (DK_2). Also, at the conclusion, SVD is connected; steps are appearing underneath. Finally, the encrypted image $E(x, y)$ is obtained. Improper selection of any of these parameters during decryption comes out with negative results. Presence of number of encryption keys helps in making the system more secure against unauthorized attacker. The steps (Figure 3) of encryption of an input image $f(x, y)$ can be expressed as follows:

$$E(u, v) = \mathrm{PT}\left[\mathrm{LCT}^{\alpha_1,\beta_1,\gamma_1}\left\{\left\{f(x, y) \times \exp^{i(2\pi n_1(x,y))}\right\}\right\}\right], \tag{10}$$

$$C(x, y) = \mathrm{PT}\left[\mathrm{LCT}^{\alpha_2,\beta_2,\gamma_2}\left\{E(u, v) \times \sum_{i=0}^{2^m}\sum_{j=0}^{2^m} M_{i,j}(d \times d)\right\}\right], \tag{11}$$

$$\mathrm{DK}_1(u, v) = \mathrm{AT}\left[\mathrm{LCT}^{\alpha_1,\beta_1,\gamma_1}\left\{\left\{f(x, y) \times \exp^{i(2\pi n_1(x,y))}\right\}\right\}\right], \tag{12}$$

$$\mathrm{DK}_2(x, y) = \mathrm{AT}\left[\mathrm{LCT}^{\alpha_2,\beta_2,\gamma_2}\left\{E(u, v) \times \sum_{i=0}^{2^m}\sum_{j=0}^{2^m} M_{i,j}(d \times d)\right\}\right], \tag{13}$$

$$e(\xi, \eta) = \mathrm{SVD}[C(x, y)], \tag{14}$$

where PT denotes a phase truncation operator, $\mathrm{LCT}^{\alpha_1,\beta_1,\gamma_1}$ and $\mathrm{LCT}^{\alpha_2,\beta_2,\gamma_2}$ represent the linear canonical transform of order $\alpha_1, \beta_1, \gamma_1$ and inverse linear canonical transform order $\alpha_2, \beta_2, \gamma_2$, respectively. The decryption keys (DKs) are obtained during the encryption process. Within the proposed strategy, the two encryption keys are treated as open keys and are not utilized within the unscrambling handle. The two decoding keys utilized are given by equations (12) and (13).

3.2. Asymmetric Cryptosystem for Decryption. The decryption process is shown in Figure 4. First, perform inverse singular value decomposition on the image, then multiply it by second decryption key (DK_2), and then LCT. Then multiply with the asymmetric key DK_1 again perform LCT.

Steps for decryption is as follows:

$$\begin{aligned} €(u, v) &= \mathrm{ISVD}\{e(\xi, \eta)\}, \\ f_{(x,y)} &= \mathrm{LCT}^{\alpha_2,\beta_2,\gamma_2}\left[\mathrm{LCT}^{\alpha_1,\beta_1,\gamma_1}\{€(u, v)\} \times \mathrm{DK}_1 \times \mathrm{DK}_2\right]. \end{aligned} \tag{15}$$

3.3. Optoelectronic Realization. An optoelectronic experimental setup of the proposed encryption scheme has appeared in Figure 5. In encryption, the image $f(x, y)$ and RPM are first displayed on phase only spatial light-modulator (PO-SLM) associated with the machine and lit up by a He-Ne laser source ($\lambda = 632.8$ nm). LCT order $\alpha_1, \beta_1, \gamma_1$ is performed optically. The resulting spectrum and DPM are displayed on to second $\mathrm{PO\text{-}SLM}_2$, which is additionally connected with the computer and after that performing an inverse LCT. The resultant spectrum is recorded by the charged coupled device (CCD) camera and stored in the computer system. The phase truncated part may be made by CCD. The amplitude-truncated part may be done by phase-shifting interferometry. In the decryption process, the digitally acquired image $E(x, y)$ is multiplied with asymmetric key DK_1 is displayed on $\mathrm{PO\text{-}SLM}_1$ irradiated with a laser source, and then subjected linear canonical transform through, then information is displayed on SLM_2 is associated with computer and intensity of the decrypted image is recorded in the output plane.

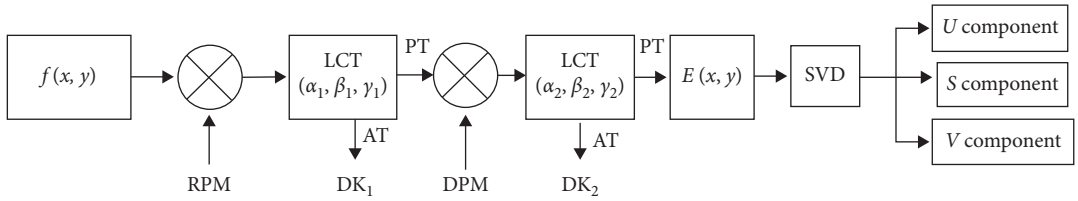

Figure 3: Flow chart for the encryption scheme.

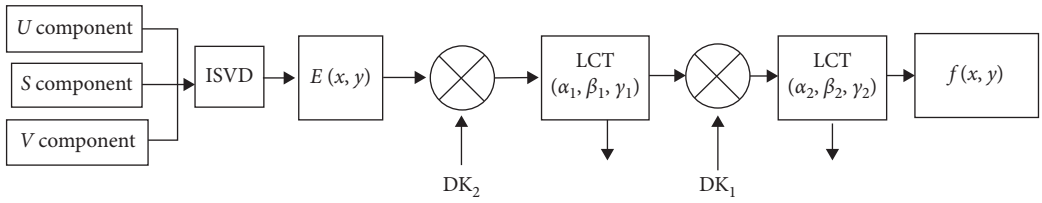

Figure 4: Flow chart for decryption scheme.

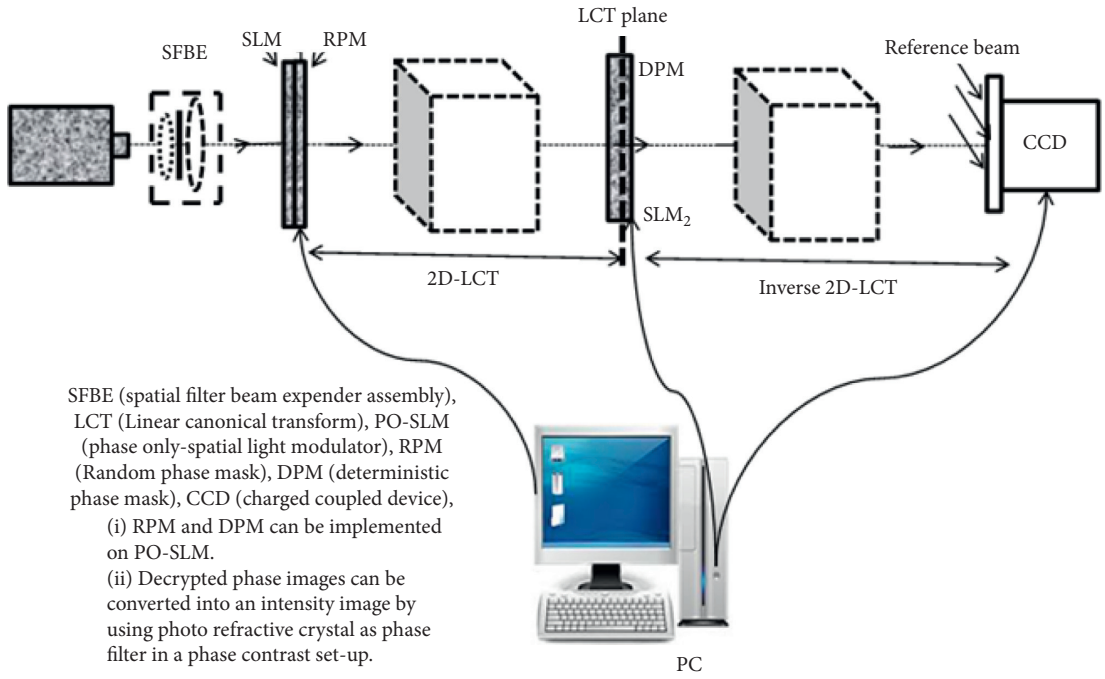

Figure 5: Proposed optoelectronic encryption setup.

4. Simulation Results and Discussion

4.1. Encryption and Decryption Results. A series of computer simulations were performed using MATLAB (version R2020a) software to verify the efficiency of the proposed approach. The size of all the plain text images and target images selected were 256×256. In this scheme, two grayscale images tree and baboon Figures 6(a) and 6(b) of size 256×256 pixels have been considered. The LCT parameters are considered in the present scheme are $\alpha_1 = 0.3, \beta_1 = 0.5, \gamma_1 = 0.7$ and $\alpha_2 = 0.5, \beta_2 = 0.7, \gamma_2 = 0.9$. For simplicity, you can use these values and other integer values. Figures 6(c) and 6(d) show the grayscale encrypted image of the grayscale used in the scheme. Using the correct LCT sequence and keys, the original images are, respectively, reflected in Figures 6(e) and 6(f).

4.2. Performance Analysis. In this section, mean squared error (MSE) and a peak signal-noise ratio (PSNR) are used as the convergence criterion in the iterative process. If f_i and f_i' denotes input and the decrypted image, then MSE is calculated as follows:

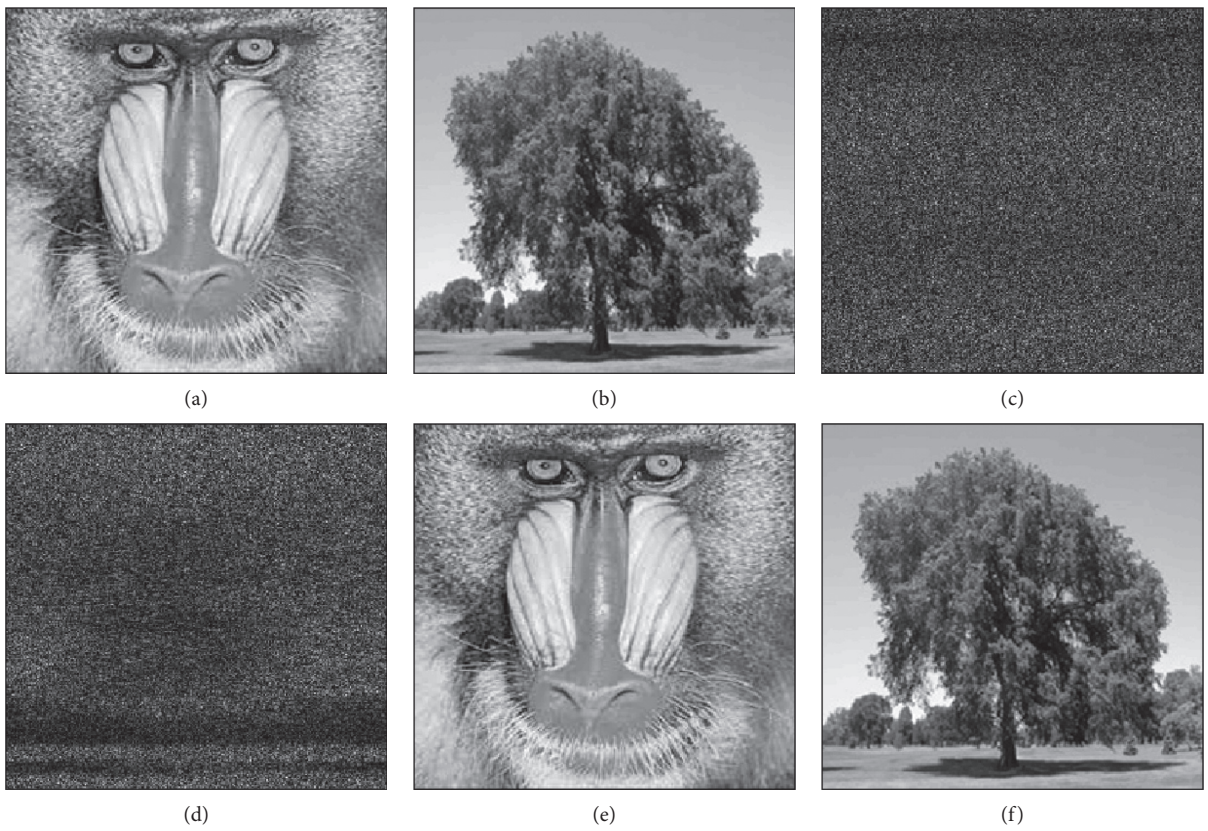

Figure 6: (a, b) Input images of 256×256 pixels; (c, d) encrypted images; (e, f) decrypted images.

$$\text{MSE} = \left(\frac{\sum_{i=1}^{L} \left| f_i - f_i' \right|^2}{L} \right). \tag{16}$$

In equation (16), L is the sum of pixels and denotes the size of the image. The suggested strategy is very safe because all the values of DPM must be reasonably when arranging for accurate image conversion. In case any of the esteem is inaccurately chosen automatically, there is an error in MSE; hence, decrypted image is not getting. The MSE for the tree and baboon pictures is as follows: 7.7485×10^{-25} and 2.5223×10^{-25}. The minimum value of MSE demonstrates a superior likeness to the tried image.

PSNR measures the modification between the input image f_i and f_i' is decoded image and its equation can be written as follows:

$$\text{PSNR} = 10 \times \log \left\{ \frac{L^2}{\text{MSE}} \right\}. \tag{17}$$

The numerical esteem of PSNR obtained for our suggested algorithm for the tree and baboon image is 92.42 dB and 91.48 dB, respectively.

4.3. Relative Error (RE). The relative error is computed between plain image and decoding image using mathematical expression represented in the following equation:

$$\text{RE} = \sum_{x=1}^{L} \sum_{y=1}^{L} \frac{\left| f_i(x, y) - f_i'(x, y) \right|^2}{\sum_{x=1}^{L} \sum_{y=1}^{L} f_i(x, y)^2}. \tag{18}$$

Among them, $f_i(x, y)$ and $f_i'(x, y)$, respectively, represented the input, decrypted picture. The RE values of the algorithm used for tree and baboon images are 0.0054 and 0.0049, respectively. It can be seen from these data that it reflects that the image is obtained faithfully.

4.4. Key Sensitivity Analysis. Image encryption technique is sensitive to the initial values of the secret key. To obtain a sensitivity analysis of the image encryption technique, take incorrect parameters. The correct parameters are $\alpha_1 = 0.3, \beta_1 = 0.5, \gamma_1 = 0.7$ and $\alpha_2 = 0.5, \beta_2 = 0.7, \gamma_2 = 0.9$ as the orders of LCT. The responsiveness of the architecture has also been substantiated against each individual parameter. The retrieved images for erroneous values are shown in Figure 7 for the various variable of and phase masks. Figures 7(a)–7(f) correspond to an image of a tree decrypted with incorrect values. Figures 7(a) and 7(b) are decrypted image tree and baboon by using incorrect two LCT orders; Figure 7(c) and 7(d) are decrypted image using another two-wrong parameter of LCT, and Figures 7(e) and 7(f) with wrong values of DPM and RPM. Figure 8(a) is an MSE plot with the first LCT order $\alpha_1 = 0.5$, while Figure 8(b) is another graph of MSE with iteration number for the second LCT.

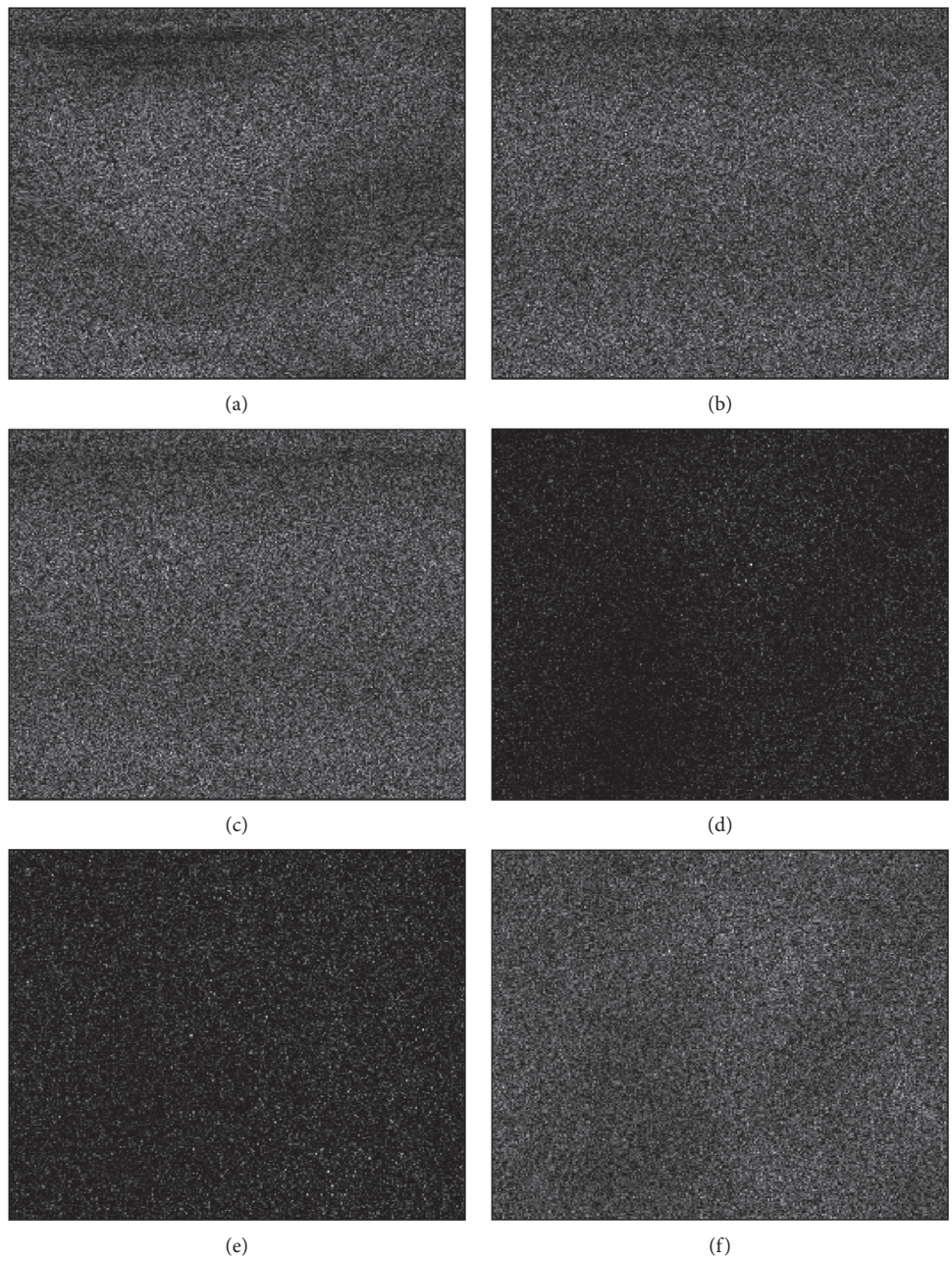

Figure 7: (a, b) Retrieved images of tree, baboon for wrong two LCT orders; (c, d) decrypted images using another two-wrong parameter; (e, f) wrong values of DPM and RPM.

Figure 8(c) is another plot MSE with LCT order $\beta 2 = 0.6$ The graphs clearly reflect that the scheme is highly sensitive to the LCT order.

4.5. Correlation Coefficient (CC) Analysis. In this section, the correlation coefficient (CC) of two adjacent pixels in the original image and its encrypted image is examined. The CC is calculated by the following relations:

$$\mathrm{CC} = \frac{\sum_{i=1}^{N} (x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\left(\sum_{i=1}^{N} (x_i - \overline{x})^2\right)\left(\sum_{i=1}^{N} (y_i - \overline{y})^2\right)}}, \tag{19}$$

where $\overline{x} = 1/N \sum_{i=1}^{N} x_i$ and $\overline{y} = 1/N \sum_{i=1}^{N} y_i$. An illegitimate user cannot obtain any valid information from this statistical data. Plots of correlation distribution for randomly chosen 15,000-pixel pairs Figures 9(a), 9(d), 9(g), 9(j), and 9(m) show the input images; Figures 9(b), 9(e), 9(h), 9(k), and 9(n) show correlation distribution of input images; Figures 9(c), 9(f), 9(i), 9(l), and 9(o) correlation distribution of encrypted images, respectively. The correlation graphics of input images are different, but the correlation plots of encrypted images are similar, so based on the encryption images, it is difficult for the hacker to identify the correct image. Table 1 shows the values of horizontal,

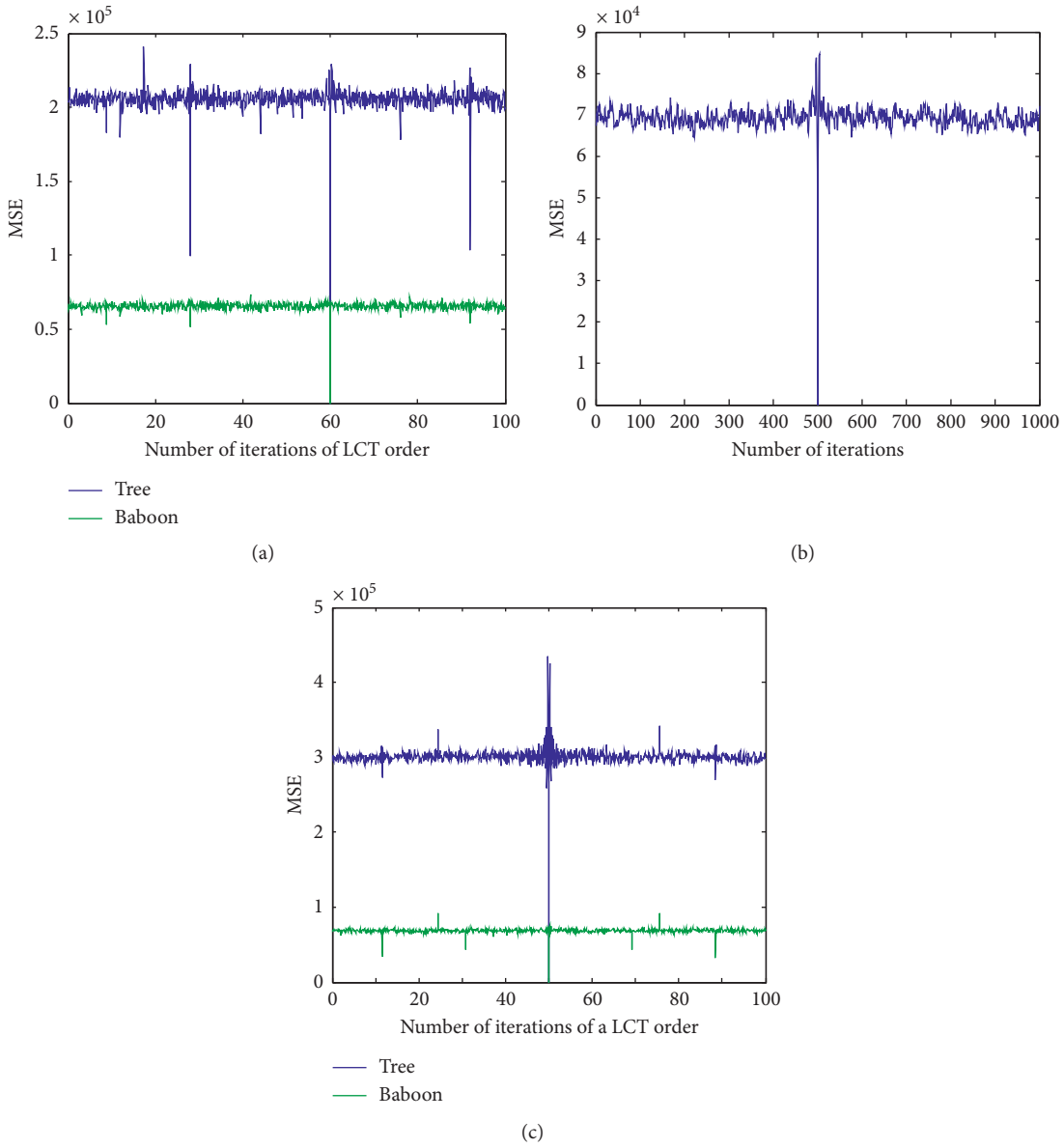

Figure 8: (a) MSE plots and the number of iterations of first LCT order; (b) MSE plot against the number of iterations for single image; (c) MSE plot and the number of iterations of second LCT order.

diagonal, and vertical pixels of input and encrypted images (Figure 9).

4.6. Statistical Analysis. To demonstrate the ability to resist statistical attacks of the proposed image encryption algorithm, different kinds of statistical analysis methods are being utilized.

4.6.1. Histogram Analysis. In order to obtain an effective and safe optical image encryption scheme, it should be able to encrypt different input images into an encryption form with similar histograms. The histograms of the tree, baboon, and their corresponding encrypted images are shown in Figures 10(a)–10(d). We can see from the histograms point of view input images are completely different, but the histograms of the encrypted images are indistinguishable, so it is difficult for an attacker to identify the correct picture.

4.6.2. Entropy Analysis. Entropy (H) can be represented as follows:

$$H = -\sum_{i=1}^{M} p_i \log 2p_i, \tag{20}$$

The chi-square value is calculated by the following equation [74–76]:

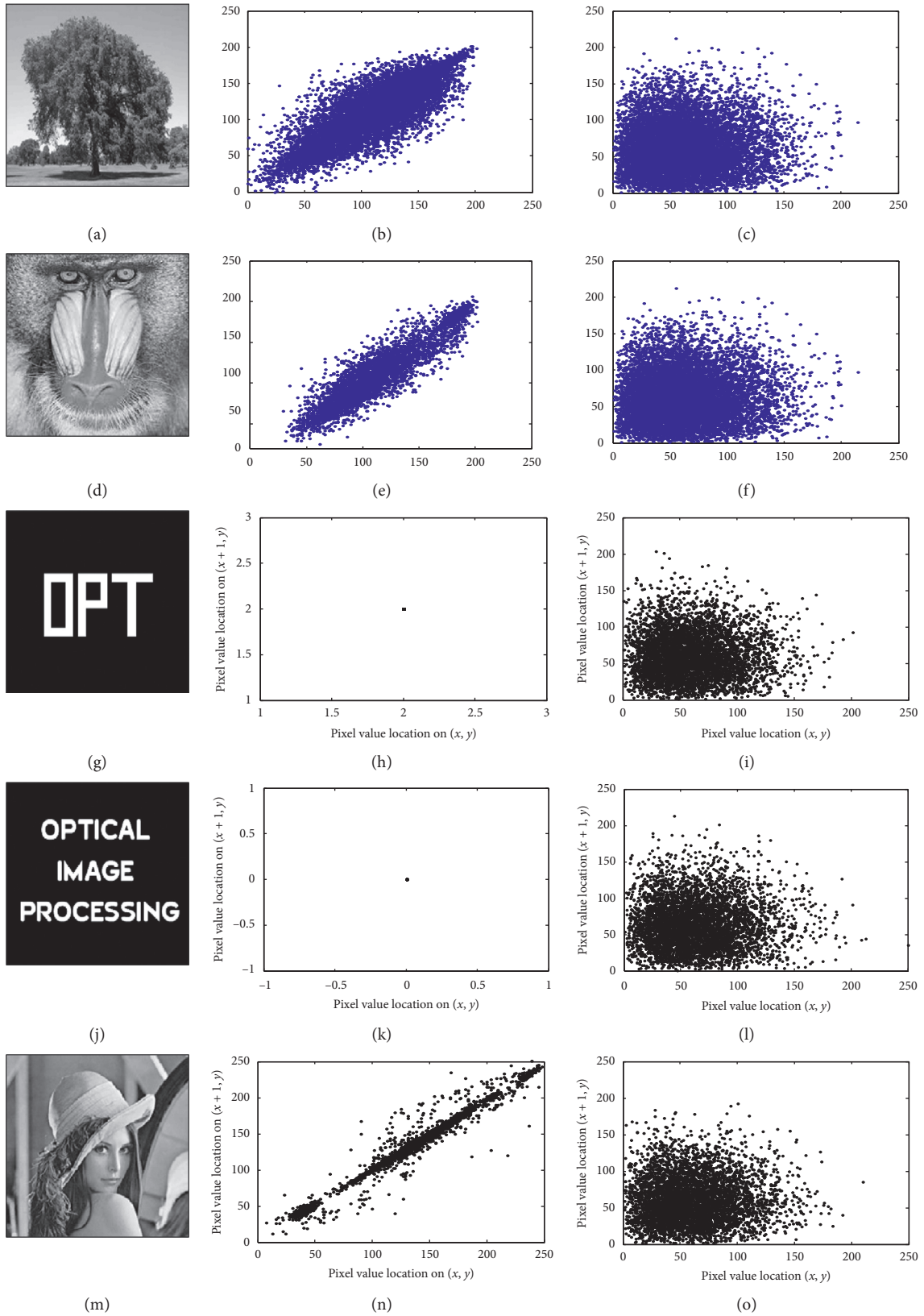

Figure 9: Plots of correlation distribution for randomly chosen 15,000-pixel pairs; (a, d, g, j, m) of input images; (b, e, h, k, n) correlation distribution of input images; (c, f, i, l, o) correlation distribution of encrypted images.

Table 1: Calculation of CC value along horizontal, diagonal, and vertical of original and cipher images.

Image	Original image			Cipher image		
	Horizontal	Diagonal	Vertical	Horizontal	Diagonal	Vertical
Lena	0.9562	0.9509	0.9817	0.0093	0.0121	0.0086
Baboon	0.9077	0.7566	0.8179	0.0077	0.0092	0.0157
OPT	0.9497	0.9354	0.9695	0.0106	0.0020	0.0092
Optical image processing	0.8994	0.8586	0.9465	0.0006	0.0038	0.0048

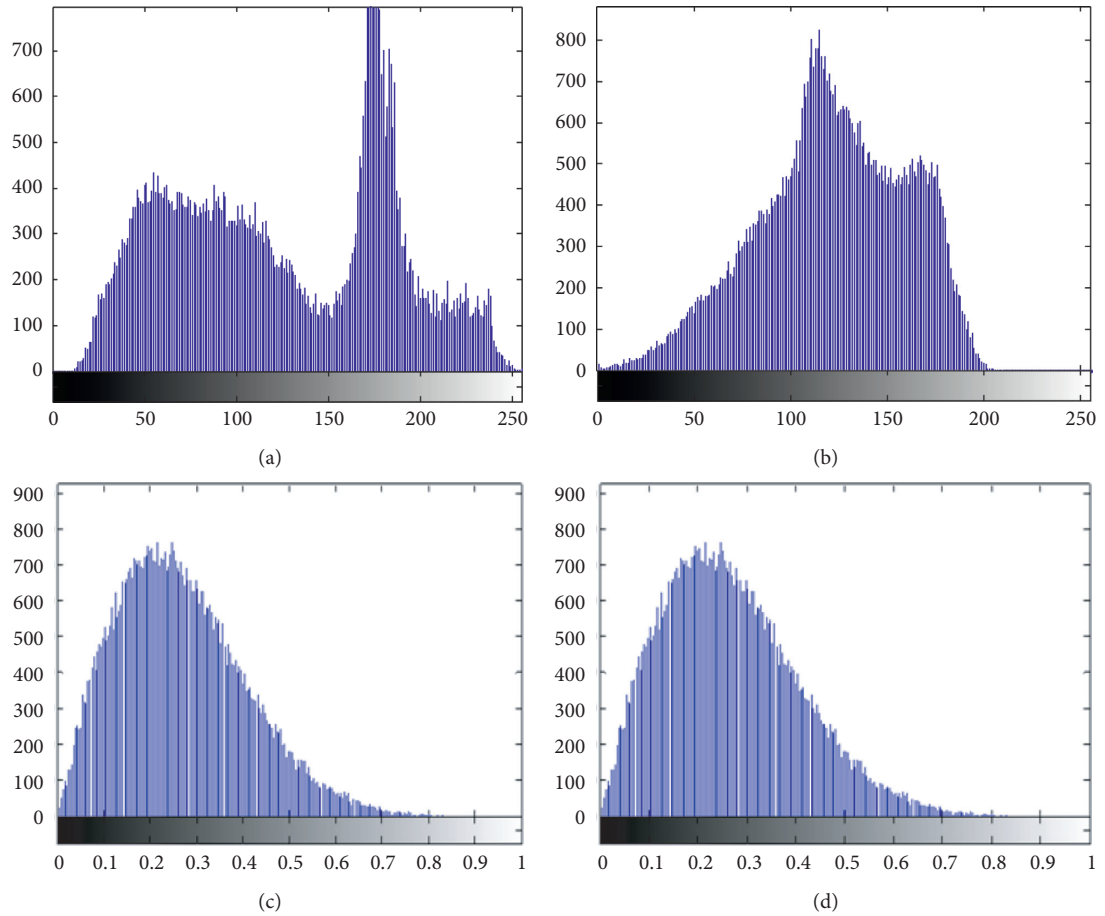

Figure 10: Histogram plots (a) of an input tree and (b) input image of a baboon; (c, d) encrypted images of tree and baboon.

$$\chi^2_{\text{test}} = \sum_{i=0}^{255} \frac{\text{obs}_i - \exp_i}{\exp_i}, \tag{22}$$

where *pi* represents the probability. The ideal entropy is 8. The entropies obtained from the cipher image of the baboon, tree, optical image processing, OPT, and Lena images using the proposed algorithm are nearly standard entropy, respectively. These values are near the ideal value, then the loss is insignificant, and the suggested algorithm is strongly against the entropy attack. Table 2 shows entropies of input, encrypted and decrypted, respectively.

Variance is the quantitative measure of histogram analysis. In addition, histogram variances are mainly used to quantitatively examine the uniformity of an image. Lower variance means higher uniformity of an image, alternatively the better security of the particular algorithm. The mathematical expression for calculating the variance is as follows [74–76]:

$$\text{Variance}(I) = \frac{1}{k^2} \sum_{i=0}^{k} \sum_{j=0}^{k} \frac{\left(I_i - I_j\right)^2}{2}, \tag{21}$$

where k is the number of grayscale values, I_i and I_j are the number of pixels for a particular grayscale values i and, j, respectively, and I is the vector of all I_i's and I_j's . Variance results are tabulated in Table 3.

The result shows our encryption scheme is better and more efficient, giving better results than others.

The chi-square test is the degree of deviation between the actual observation value and the theoretical inference value

Table 2: The entropy calculations of grayscale and text images.

S. No	Image	Type/size	Entropy of input image	Entropy of encrypted image	Entropy of decrypted image
1	Baboon	JEPG/256	7.0587	8.000	5.3239
2	Tree	JEPG/256	6.9181	8.000	6.2558
3	Optical image processing	JEPG/256	6.7272	7.647	6.7272
4	OPT	JEPG/256	0	7.627	0
5	Lena	JEPG/256	7.9216	7.8350	7.9216

Table 3: Histogram variance results of 5 images using the proposed cryptosystem.

S. No	Image	Variance of original image	Variance of encrypted image	Ref. [77]	Ref. [78]	Ref. [79]
1.	Lena	38842.58	245.0547	244.31	276.39	260.70
2.	Tree	161272.20	233.272	—	—	—
3.	Optical image processing	21762.61	222.02	—	—	—
4.	OPT	31541.41	230.593	—	—	—
5.	Baboon	628013.38	228.59	—	—	—

of the statistical sample. The larger the chi-square value, the less conformable and on the contrary, the more it is consistent. If the two values are completely equal, the chi-square value is 0, indicating that the theoretical value is completely consistent.where obs_i is the observed frequency of i, and $\exp_i$ is the expected frequency of i. The expected frequency $\exp_i$ is as follows:

$$\exp_i = \frac{M \times N}{256}, \tag{23}$$

where $M \times N$ is the size of images.

Table 4 lists the test results for encrypted images. According to the chi-square distribution, $\chi^2_{255;0:\,05} = 293{:}\ 247$ and $\chi^2_{255;0:\,01} = 310{:}\ 457$**;** from this, we can see that for the 1% and 5% significant level, accept the hypothesis, so we can confirm that the pixel distribution is uniform.

Table 4: Results of the χ^2_{test}.

S. No	Images	χ^2_{test}	Result
1	Lena (512×512)	232.1440	Accept
2	Baboon (512×512)	230.1243	Accept
3	Tree (512×512)	234.2467	Accept
4	OPT (512×512)	231.1053	Accept

4.7. Attack Analysis

4.7.1. Robustness Method Against Pixels Cropped. In an occlusion attack, some parts of the encrypted image are blocked, which will cause the encrypted image to be blurred. This leads to blurred decrypted images depending on the size of the blocked parts. Different cases have been evaluated by taking the different sizes of the filter in the encrypted image. When the encrypted image is occluded or blocked, it impacts the quality of the recovered images. The occlusion is considered by changing the encrypted image by 10%, 25%, 50%, and 75%. As the occlusion percentage increases, the quality of the restored image gradually decreases. But still, the recovered images are visible till 25%. Figure 11(a) is 10% encrypted image; Figure 11(b) is occluded 25%. Similarly, 50% is occluded in Figure 11(c), 75% in Figure 11(d), and their corresponding effect is reflected in Figures 11(e) and 11(f); the MSE and CC plot with the occluded area. A larger value of MSE states a larger loss of information and degraded condition of recovered images.

4.7.2. Noise Attack Analysis. The encrypted image on the stage of image processing and image transmission is susceptible to different kinds of noise. These noises have a great influence on the quality of the decryption images. In this work, we have added Gaussian noise to the encoded image. The noise interferes with the ciphered images by relation [80–82].

$$\mu'(\rho, \sigma) = \mu(u, v) + kG, \tag{24}$$

where $\mu(u, v)$ is encrypted picture and $\mu'(\rho, \sigma)$ is the noised image, k is a constant factor and G is Gaussian noise with 0 and 1 standard deviation. Figures 12(a)–12(h) show the recovered images from the encrypted data distorted by Gaussian noise with standard deviations of 0.02. Figure 13 shows the plot of MSE with noise factor (k).

4.7.3. Classical Attack Analysis. The security of a cryptographic system depends on its resistance to four basic attacks. These basic attacks are cipher text only attack, known plain text attack, chosen plain text attack, and chosen cipher text attack. Among them, chosen plain text attack is the most powerful attack. If a cryptosystem is secure against this attack, it is secure against the other three attacks. The proposed scheme has eight keys; one from a deterministic phase mask, one from RPM, and six from linear canonical transform parameters, and the scheme is highly sensitive to all these parameters. If a small change is made in these parameters, the results would be completely different. So, the proposed scheme is secure enough against chosen plain text

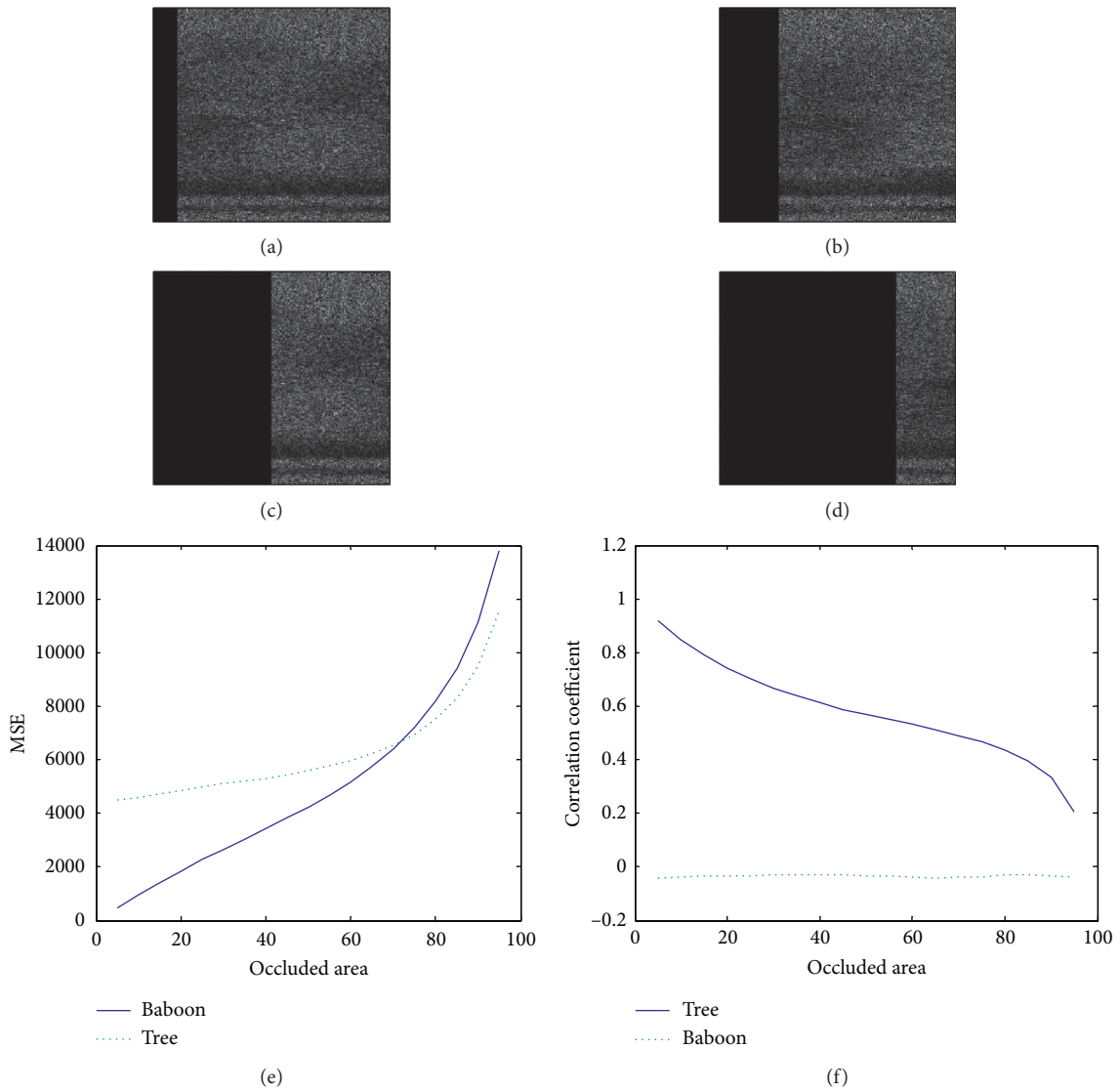

Figure 11: Occlusion results to the grayscale images of varying degrees of occlusion. (a) For 10% occlusion of the encrypted image. (b) For 25% occlusion of the encrypted image. (c) For 50% occlusion of the encrypted image. (d) For 75% occlusion of the encrypted image; (e) MSE plot with the percentage of the occluded area; (f) CC plot with the percentage of occluded area.

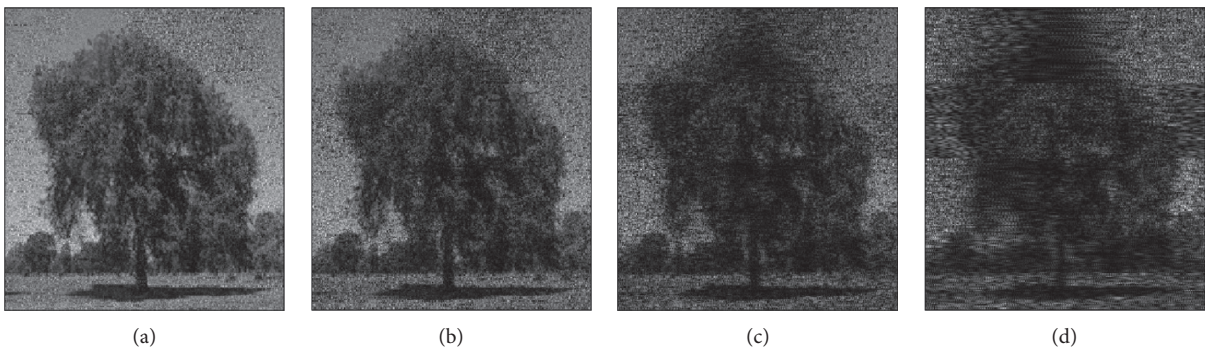

Figure 12: Retrieved image for (a) $k = 0.1$; (b) $k = 0.5$; (c) $k = 1$; (d) $k = 2$.

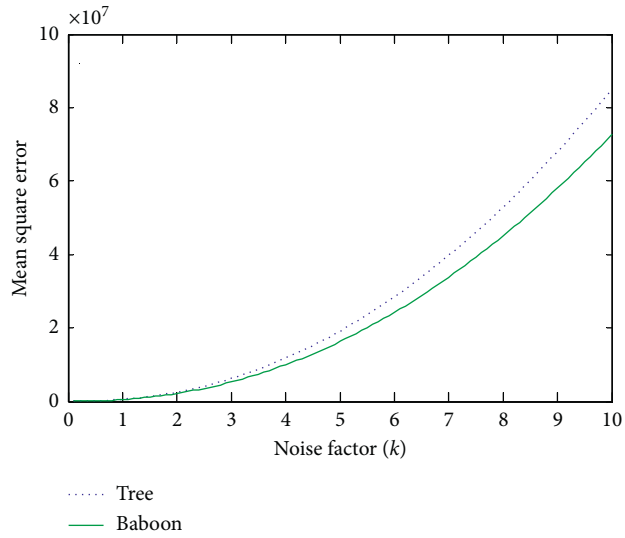

Figure 13: MSE plot of images tree and baboon with varying noise factor k.

attacks and hence against other classical attacks too. The analysis proves that the presented system is resistant to several attacks which threaten the authenticity of any cryptosystem. Hence it is a much more secure and powerful yet simple cryptosystem.

In CPA, the attacker has the plain image and scheme. With respect to these, he will try the cipher image. Normally, DRPE is highly vulnerable to CPA. If an attacker chooses the Dirac delta function, which is shown in the below equation:

$$\delta(x, y) = \begin{cases} 1, & x = 0 \text{ and } y = 0, \\ 0, & \text{otherwise.} \end{cases} \tag{25}$$

Dirac delta function is to be considered a single nonzero pixel at the centre of the image and all the other values are zero. In order to perform chosen plaintext analysis, created Dirac delta function is considered as plain image and cipher image calculation is given in the equation.

$$\text{DRPE}_{\text{cpa}} = \left\{\text{LCT}^{\beta}\left(\text{LCT}^{\alpha}[\delta(x, y). * \text{DPM}(x, y). * \text{RPM}(x, y)]\right\}. \tag{26}$$

From the above equation, the second secret key is easily obtained by drpe_{cpa}. Figure 14 shows the CPA analysis of the DRPE system.

4.7.4. Speed Performance Analysis. The speed of the scheme measures the performance and the time taken by the scheme for the execution. It is important that the encryption and decryption schemes are fast enough to meet real time requirements. The scheme needs to be faster to reach the level of real time applications. The scheme has been tested against the speed by executing the scheme on a personal computer with configuration Intel (R) Core (TM) i3-2328 CPU @ 2.20 GHz–2.71 GHz, 2 GB RAM running Windows 10 on MATLAB R2020a 5 (9.6..0.1174912) 64 bit (win64), LM: 40664749. The total time taken for both encryption and decryption is 0.66 s. This time is due to the introduction of DPM. After introducing the DPM, the time taken is still very small and proves the scheme to be fast and efficient.

4.7.5. Quantitative Comparison Analysis. The proposed scheme is quantitatively compared with various recent schemes in terms of entropy, execution time, and key space. Table 4 gives the key space, time execution, and entropy of cipher text of various schemes. As can be seen from Table 4, the proposed scheme has the least execution time of 1.515843 seconds with a key space of RPM, DPM, and 6 keys. The cipher-text entropy value is 7.261, which indicates the randomness in the encrypted image. All these parameters demonstrate the strength and quality of the proposed encryption scheme. Table 5 reflected the quantitative comparative analysis of the proposed scheme and earlier reported schemes.

5. Differential Attack Analysis

The Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI): Let encrypted images before and after one pixel change in the image be $E_1(x, y)$ or $E_2(x, y)$. The NPCR and UACI are given as follows [76]:

$$\text{NPCR} = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\frac{D(x, y)}{M \times N} \times 100\%,$$

$$\text{UACI} = \frac{1}{M \times N}\left(\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\frac{\left|E_1(x, y) - E_2(x, y)\right|}{255}\right) \times 100\%, \tag{27}$$

where $D(x, y)$ is a two-dimensional array having the same size as images $E_1(x, y)$ or $E_2(x, y)$ and M and N are the width and height of the image. The matrix $D(x, y)$ is defined by $E_1(x, y)$ and $E_2(x, y)$; if $E_1(x, y) \neq E_2(x, y)$, then

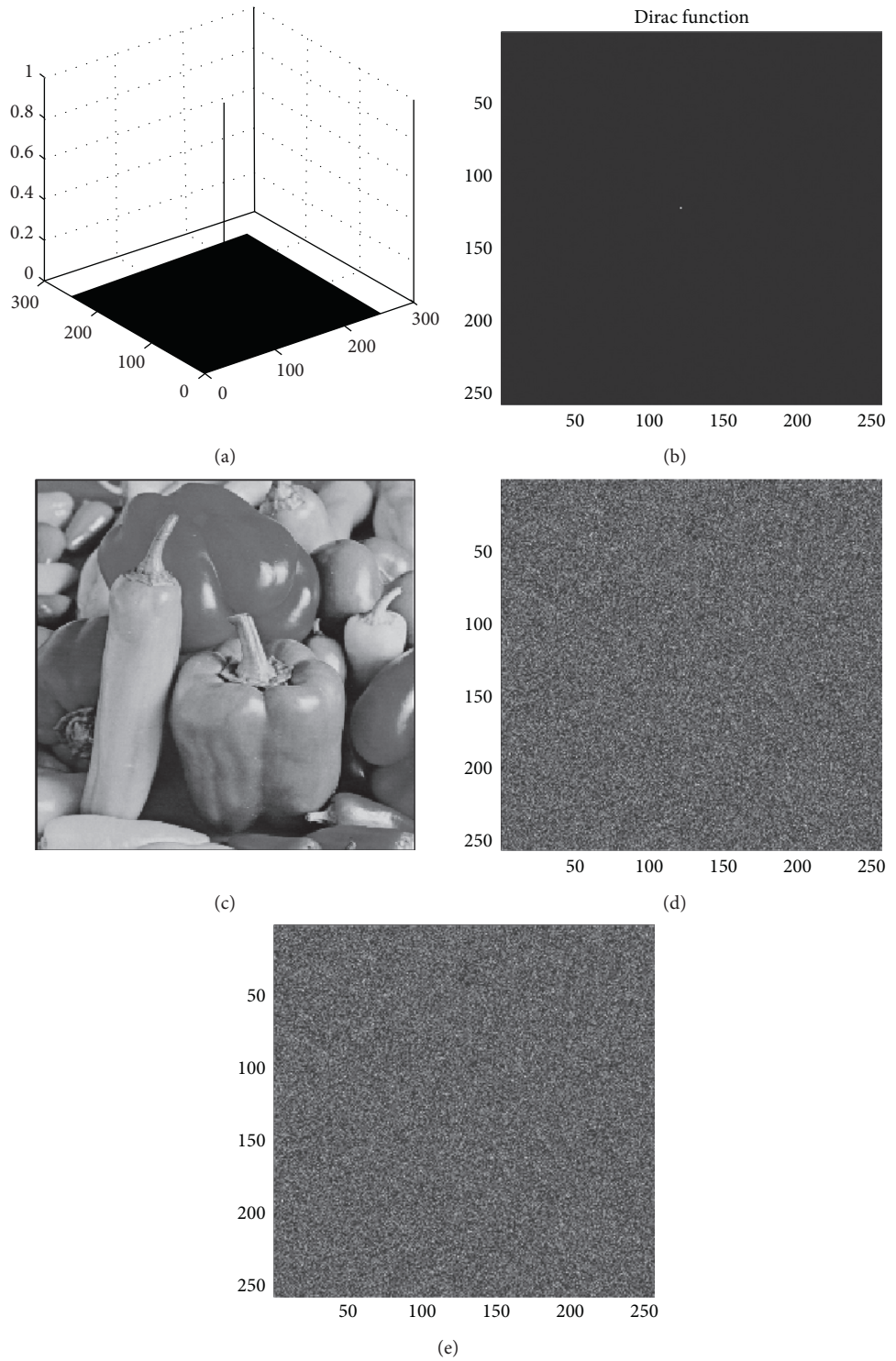

Figure 14: (a) 3D plot of Dirac delta function; (b) Dirac delta function; (c) decrypted image of DRPE with CPA; (d) DRPE encrypted image with CPA; (e) encrypted image with DPM phase key.

Table 5: Quantitative comparison analysis.

Parameters	Ref [36]	Ref. [25]	Ref. [83]	Ref. [84]	Present scheme
Element in key space	9	6 (RPM + SPM)	6	6	DPM + RPM+6 (LCT order)
Entropy of the encrypted image	7.452	7.841	7.530	7.991	7.942
Execution time	3.80553 s	2.8371 s	—	—	1.515843 s

$D(x, y) = 1$; otherwise $D(x, y) = 0$. The ideal values of NPCR and UACI are 99.61% and 33.46%, respectively. The NPCR and UACI between $E_1(x, y)$ and $E_2(x, y)$ are computed as 97.49% and 31.20%. The calculated values of NPCR and UACI are close to the ideal values. It means that the algorithm can resist differential cryptanalysis.

6. Conclusion

In this contribution, it demonstrates that the simulation LCT encrypting system is capable of information security with noise-free recovery. The experimental results show that the linear canonical transform order can be considered as an extra security key. It is found that a small variation in order will lead to a large change in CC, MSE, and PSNR values. The use of DPM increases the key space also as extra security of the scheme. The proposed scheme is asymmetric and also uses the SVD operation that increases the security of the algorithm. The scheme is tested for various attacks such as occlusion and noise and it was found the scheme is not vulnerable. Numerical simulations are performed to demonstrate the feasibility and validity of this method. Key sensitivity has been analyzed by MSE curves under different decryption keys. Several possible attacks such as KPA and CPA have been considered and results demonstrate that the proposed encryption system has higher security.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

The authors wish to thank the management of The NorthCap University, Gurugram, India, for their encouragement in supporting various research facilities.

References

[1] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Letters*, vol. 20, no. 7, pp. 767–769, 1995.

[2] O. Matoba, T. Nomura, E. Perez-Cabre, M. S. Millan, and B. Javidi, "Optical techniques for information security," *Proceedings of the IEEE*, vol. 97, no. 6, pp. 1128–1148, 2009.

[3] A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," *Advances in Optics and Photonics*, vol. 1, no. 3, pp. 589–636, 2009.

[4] M. S. Millan, Perez-Cabre, G. Cristobal, P. Schelkens, and H. Thienpont, *Optical Data Encryption, Optical and Digital Image Processing: Fundamentals and Applications*, pp. 739–747, Wiley, Hoboken, NJ, USA, 2011.

[5] B. Javidi, A. Carnicer, M. Yamaguchi et al., "Roadmap on optical security," *Journal of Optics*, vol. 18, pp. 1–39, 2016.

[6] A. K. Yadav, S. Vashisth, H. Singh, and K. Singh, "Optical cryptography and watermarking using some Fractional canonical transforms, and structured masks," in *Proceedings of the First International conference, IEM Optronix 2014*, pp. 25-26, Kolkata, India, June 2015.

[7] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," *Optics Letters*, vol. 25, no. 12, pp. 887–889, 2000.

[8] M. Dahiya, S. Sukhija, and H. Singh, "Image encryption using Quad masks in fractional Fourier domain and case study," in *Proceedings of the IEEE, International Advance Computing Conference*, pp. 1048–1053, Gurgaon, India, February 2014.

[9] H. Singh, "Optical cryptosystem of color images using random phase masks in the fractional wavelet transform domain," in *Proceeding of International Conference on Condensed Matter and Applied Physics AIP Conference Proceedings*, pp. 020063–20071/4, Bikaner, India, May 2016.

[10] H. Singh, "Optical cryptosystem of color images based on fractional-, wavelet transform domains using random phase masks," *Indian Journal of Science and Technology*, vol. 9S, no. 1, pp. 1–15, 2016.

[11] P. Maan and H. Singh, "Non-Linear cryptosystem for image encryption using radial Hilbert mask in fractional Fourier transform domain," *3D Research*, vol. 9, p. 53, 2018.

[12] S. Yadav and H. Singh, "Asymmetric cryptosystem based on fractional Fourier transform domain using triple random phase masks," in *Proceedings of the 2nd International Conference on Communication and Computing Systems*, pp. 105–111, Gurgaon, India, December 2019.

[13] G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," *Optics Letters*, vol. 29, no. 14, pp. 1584–1586, 2004.

[14] H. Singh, A. K. Yadav, S. Vashisth, and K. Singh, "Optical image encryption using devil's vortex toroidal lens in the Fresnel transform domain," *International Journal of Optics*, vol. 2015, pp. 1–13, Article ID 926135, 2015.

[15] H. Singh, "Cryptosystem for securing image encryption using structured phase masks in Fresnel wavelet transform domain," *3D Research*, vol. 7, p. 34, 2016.

[16] N. Zhou, Y. Wang, and L. Gong, "Novel optical image encryption scheme based on fractional Mellin transform," *Optics Communications*, vol. 284, no. 13, pp. 3234–3242, 2011.

[17] S. Vashisth, H. Singh, A. K. Yadav, and K. Singh, "Devil's vortex phase structure as frequency plane mask for image encryption using the fractional Mellin transform," *International Journal of Optics*, vol. 2014, Article ID 728056, 9 pages, 2014.

[18] S. Vashisth, H. Singh, A. K. Yadav, and K. Singh, "Image encryption using fractional Mellin transform, structured phase filters, and phase retrieval," *Optik*, vol. 125, no. 18, pp. 5309–5315, 2014.

[19] H. Singh, "Watermarking image encryption using deterministic phase mask and singular value decomposition in fractional Mellin transform domain," *IET Image Processing*, vol. 12, no. 11, pp. 1994–2001, 2018.

[20] J. A. Rodrigo, T. Alieva, and M. L. Calvo, "Gyrator transform: properties and applications," *Optics Express*, vol. 15, no. 5, pp. 2190–2193, 2007.

[21] H. Singh, A. K. Yadav, S. Vashisth, and K. Singh, "Fully phase image encryption using double random-structured phase masks in gyrator domain," *Applied Optics*, vol. 53, no. 28, pp. 6472–6481, 2014.

[22] H. Singh, A. K. Yadav, S. Vashisth, and K. Singh, "Double phase-image encryption using gyrator transforms, and

structured phase mask in the frequency plane," *Optics and Lasers in Engineering*, vol. 67, pp. 145–156, 2015.

[23] H. Singh, "Hybrid structured phase mask in frequency plane for optical double image encryption in gyrator transform domain," *Journal of Modern Optics*, vol. 65, no. 18, pp. 2065–2078, 2018.

[24] M. Khurana and H. Singh, "Asymmetric optical image triple masking encryption based on gyrator and Fresnel transforms to remove silhouette problem," *3D Research*, vol. 9, p. 38, 2018.

[25] M. Khurana and H. Singh, "A spiral-phase rear mounted triple masking for secure optical image encryption based on gyrator transform," *Recent Patents on Computer Science*, vol. 12, no. 2, pp. 80–94, 2019.

[26] H. Singh, "Devil's vortex Fresnel lens phase masks on an asymmetric cryptosystem based on phase-truncation in gyrator wavelet transform domain," *Optics and Lasers in Engineering*, vol. 81, pp. 125–139, 2016.

[27] I. Mehra, A. Fatima, and N. K. Nishchal, "Gyrator wavelet transform," *IET Image Processing*, vol. 12, no. 3, pp. 432–437, 2017.

[28] Y. Xiao, L. Zhou, and W. Chen, "Secured single-pixel ghost holography," *Optics and Lasers in Engineering*, vol. 128, p. 106045, 2020.

[29] A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," *Optics Letters*, vol. 30, no. 13, pp. 1644–1646, 2005.

[30] X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," *Optics Letters*, vol. 31, no. 8, pp. 1044–1046, 2006.

[31] X. Peng, H. Wei, and P. Zhang, "Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain," *Optics Letters*, vol. 31, no. 22, pp. 3261–3263, 2006.

[32] W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated Fourier transforms," *Optics Letters*, vol. 35, no. 2, pp. 118–120, 2010.

[33] J. Cai, X. Shen, M. Lei, C. Lin, and S. Dou, "Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition," *Optics Letters*, vol. 40, no. 4, pp. 475–8, 2015.

[34] W. Qiu, B.-Z. Li, and X.-W. Li, "Speech recovery based on the linear canonical transform," *Speech Communication*, vol. 55, no. 1, pp. 40–50, 2013.

[35] R. Kumar, J. T. Sheridan, and B. Bhaduri, "Nonlinear double image encryption using 2D non-separable linear canonical transform and phase retrieval algorithm," *Optics and Laser Technology*, vol. 107, pp. 353–360, 2019.

[36] P. Rakheja, R. Vig, and P. Singh, "Double image encryption using 3D Lorenz chaotic system, 2D non-separable linear canonical transform and QR decomposition," *Optical and Quantum Electronics*, vol. 52, p. 103, 2020.

[37] S. K. Rajput and O. Matoba, "Security-enhanced optical voice encryption in various domains and comparative analysis," *Applied Optics*, vol. 58, no. 11, pp. 3013–3022, 2019.

[38] Z. J. Huang, S. Cheng, L. H. Gong, and N. R. Zhou, "Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform," *Optics and Lasers in Engineering*, vol. 124, p. 105821, 2019.

[39] J. J. Healy, "Simulating first order optical systems-algorithms for and composition of discrete linear canonical transforms," *Journal of Optics*, vol. 20, no. 1, Article ID 014008, 2018.

[40] L. Zhao, I. Muniraj, J. J Healy et al., "2D Non-separable Linear Canonical transform (2D-NS-LCT) based cryptography," in *Proceedings of the SPIE 10233, Holography: Advances and Modern Trends V*, vol. 10233, p. 102331B, Prague, Czech Republic, May 2017.

[41] D. Wei, R. Wang, and Y.-M. Li, "Random discrete linear canonical transform," *Journal of the Optical Society of America A*, vol. 33, no. 12, pp. 2470–2476, 2016.

[42] C. Guo, I. Muniraj, and J. T. Sheridan, "Phase-retrieval-based attacks on linear-canonical-transform-based DRPE systems," *Applied Optics*, vol. 55, no. 17, pp. 4720–4728, 2016.

[43] B. M. Hennelly and J. T. Sheridan, "Fast numerical algorithm for the linear canonical transform," *Journal of the Optical Society of America A*, vol. 22, no. 5, pp. 928–937, 2005.

[44] P. Kumar, J. Joseph, and K. Singh, "Double random phase encoding based optical encryption systems using some linear canonical transforms: weaknesses and countermeasures," *Linear Canonical Transforms*, vol. 198, pp. 367–396, 2016.

[45] S.-C. Pei and S.-G. Huang, "Two-dimensional nonseparable discrete linear canonical transform based on CM-CC-CM-CC decomposition," *Journal of the Optical Society of America A*, vol. 33, no. 2, pp. 214–217, 2016.

[46] J. Wu, W. Liu, Z. Liu, and S. Liu, "Correlated-imaging-based chosen plaintext attack on general cryptosystems composed of linear canonical transforms and phase encodings," *Optics Communications*, vol. 338, pp. 164–167, 2015.

[47] L. Zhao, J. J. Healy, and J. T. Sheridan, "Constraints on additivity of the 1D discrete linear canonical transform," *Applied Optics*, vol. 54, no. 33, pp. 9960–9965, 2015.

[48] L. Zhao, J. J. Healy, and J. T. Sheridan, "Unitary discrete linear canonical transform: analysis and application," *Applied Optics*, vol. 52, no. 7, pp. C30–C36, 2013.

[49] L. Zhao, J. J. Healy, and J. T. Sheridan, "Two-dimensional non separable linear canonical Transform: sampling theorem and unitary discretization," *Journal of the Optical Society of America A*, vol. 31, no. 12, pp. 2632–2641, 2014.

[50] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Computers & Mathematics with Applications*, vol. 59, no. 10, pp. 3320–3327, 2010.

[51] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Optics Communications*, vol. 284, no. 16-17, pp. 3895–3903, 2011.

[52] H. Liu, X. Wang, and A. kadir, "Image encryption using DNA complementary rule and chaotic maps," *Applied Soft Computing*, vol. 12, no. 5, pp. 1457–1466, 2012.

[53] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dynamics*, vol. 62, no. 3, pp. 615–621, 2010.

[54] X. Wang, L. Feng, and H. Zhao, "Fast image encryption algorithm based on parallel computing system," *Information Sciences*, vol. 486, pp. 340–358, 2019.

[55] X. Wang and S. Gao, "Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network," *Information Sciences*, vol. 539, pp. 195–214, 2020.

[56] X. Wang and S. Gao, "Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory," *Information Sciences*, vol. 507, pp. 16–36, 2020.

[57] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Processing*, vol. 92, no. 4, pp. 1101–1108, 2012.

[58] Y.-Q. Zhang and X.-Y. Wang, "A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice," *Information Sciences*, vol. 273, pp. 329–351, 2014.

[59] Y.-Q. Zhang and X.-Y. Wang, "A new image encryption algorithm based on non-adjacent coupled map lattices," *Applied Soft Computing*, vol. 26, pp. 10–20, 2015.
[60] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A novel chaotic image encryption scheme using DNA sequence operations," *Optics and Lasers in Engineering*, vol. 73, pp. 53–61, 2015.
[61] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," *Optics and Lasers in Engineering*, vol. 66, pp. 10–18, 2015.
[62] Y. Xian and X. Wang, "Fractal sorting matrix and its application on chaotic image encryption," *Information Sciences*, vol. 547, pp. 1154–1169, 2021.
[63] Li Qi, X. Wang, X. Wang, B. Ma, and Y. Shi, "An encrypted coverless information hiding method based on generative models," *Information Sciences*, vol. 553, pp. 19–30, 2021.
[64] X. Zhang, L. Wang, Y. Wang, Y. Niu, and Y. Li, "An image encryption algorithm based on hyperchaotic system and variable-step Josephus problem," *International Journal of Optics*, vol. 2020, p. 6102824, 2020.
[65] Z. Liu, S. Li, W. Liu, W. Liu, and S. Liu, "Image hiding scheme by use of rotating squared sub-image in the gyrator transform domains," *Optics & Laser Technology*, vol. 45, no. 1, pp. 198–203, 2013.
[66] W. Zamrarni, E. Ahouzi, A. Lizana, J. Campos, and M. J. Yzuel, "Optical image encryption technique based on deterministic phase masks," *Optical Engineering*, vol. 55, no. 10, p. 103108, 2016.
[67] R. Girija and H. Singh, "A cryptosystem based on deterministic phase masks and fractional Fourier transform deploying singular value decomposition," *Optical Quantum Electronics*, vol. 50, p. 210, 2018.
[68] G. Unnikrishnan and K. Singh, "Optical encryption using quadratic phase systems," *Optics Communications*, vol. 193, no. 1-6, pp. 51–67, 2001.
[69] R. Girija and H. Singh, "Triple-level cryptosystem using deterministic masks and modified Gerchberg-Saxton iterative algorithm in fractional Hartley domain by positioning singular value decomposition," *Optik*, vol. 187, pp. 238–257, 2019.
[70] R. Girija and H. Singh, "An Asymmetric cryptosystem based on the random weighted singular value decomposition and fractional Hartley domain," *Multimedia Tools and Applications*, vol. 78, pp. 1–19, 2019.
[71] H. Singh, "Nonlinear optical double image encryption using random vortex in fractional Hartley transform domain," *Optica Applicata*, vol. 47, no. 4, pp. 557-558, 2017.
[72] P. L. Yadav and H. Singh, "Optical double image hiding in the fractional Hartley transform using structured phase filter and Arnold transform," *3D Research*, vol. 9, p. 20, 2018.
[73] M. Khurana and H. Singh, "Spiral-phase masked optical image health care encryption system for medical images based on fast Walsh-Hadamard transform for security enhancement," *International Journal of Healthcare Information Systems and Informatics*, vol. 13, no. 4, pp. 98–117, 2018.
[74] K. A. K. Patro, B. Acharya, and V. Nath, "Secure, lossless, and noise-resistive image encryption using chaos, hyper-chaos, and DNA sequence operation," *IETE Technical Review*, vol. 37, pp. 223–245, 2019.
[75] K. A. K. Patro and B. Acharya, "A novel multi-dimensional multiple image encryption technique," *Multimedia Tools and Applications*, vol. 79, no. 19-20, pp. 12959–12994, 2020.
[76] K. A. K. Patro and B. Acharya, "Secure multi-level permutation operation based multiple colour image encryption," *Journal of Information Security and Applications*, vol. 40, pp. 111–133, 2018.
[77] X. Chai, K. Yang, and Z. Gan, "A new chaos-based image encryption algorithm with dynamic key selection mechanisms," *Multimedia Tools and Applications*, vol. 76, no. 7, pp. 9907–9927, 2017.
[78] C. Zhu, S. Xu, Y. Hu, and K. Sun, "Breaking a novel image encryption scheme based on Brownian motion and PWLCM chaotic system," *Nonlinear Dynamics*, vol. 79, no. 2, pp. 1511–1518, 2014.
[79] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, "An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations," *Signal Processing Image Communication*, vol. 52, pp. 6–19, 2017.
[80] P. Maan and H. Singh, "Optical asymmetric cryptosystem based on kronecker product, hybrid phase and optical vortex phase masks in the phase truncated hybrid transform domain," *3D Research*, vol. 10, p. 8, 2019.
[81] A. K. Yadav, S. Vashisth, H. Singh, and K. Singh, "A phase-image watermarking scheme in gyrator domain using devil's vortex Fresnel lens as a phase mask," *Optics Communications*, vol. 344, pp. 172–180, 2015.
[82] M. Khurana and H. Singh, "An asymmetric image encryption based on phase truncated hybrid transforms," *3D Research*, vol. 8, p. 28, 2017.
[83] L. Sui and B. Gao, "Single-channel color image encryption based on iterative fractional Fourier transform and chaos," *Optics & Laser Technology*, vol. 48, pp. 117–127, 2013.
[84] M. Ge and R. Ye, "A novel image encryption scheme based on 3D bit matrix and chaotic map with Markov properties," *Egyptian Informatics Journal*, vol. 20, no. 1, pp. 45–54, 2019.

Composition Comments

1. At the publication end, the e-mail for the corresponding author will automatically be added. Hence, we ignored the author corrections regarding e-mail of the corresponding author. Hence please check.

2. Please note that as per style, both given names and surnames should be in author name, hence we ignore your comment. Please confirm.

It is very important to confirm the author(s) last and first names in order to be displayed correctly on our website as well as in the indexing databases:

Author 1
Given Names: Anshula
Last Name: Sangwan

Author 2
Given Names: Hukum
Last Name: Singh

It is also very important for each author to provide an ORCID (Open Researcher and Contributor ID). ORCID aims to solve the name ambiguity problem in scholarly communications by creating a registry of persistent unique identifiers for individual researchers.

To register an ORCID, please go to the Account Update page (http://mts.hindawi.com/update/) in our Manuscript Tracking System and after you have logged in click on the ORCID link at the top of the page. This link will take you to the ORCID website where you will be able to create an account for yourself. Once you have done so, your new ORCID will be saved in our Manuscript Tracking System automatically.