The Visual Computer (2022) 38:1027–1050
https://doi.org/10.1007/s00371-021-02066-w

ORIGINAL ARTICLE

Color image encryption scheme based on fractional Hartley transform and chaotic substitution–permutation

Gurpreet Kaur[1] · **Rekha Agarwal**[2] · **Vinod Patidar**[3]

Accepted: 6 January 2021 / Published online: 22 January 2021

Abstract
We propose a novel opto-digital method of color image encryption which utilizes compound chaotic mappings, the reality preserving fractional Hartley transformation and piecewise linear chaotic map for substitution, optical processing and permutation of image pixels, respectively. The image to be encrypted initially undergoes a chaos-based substitution in the spatial domain through the compound chaotic maps followed by a transformation to the combined time–frequency domain using the fractional Hartley transform. A reality preserving version of the fractional Hartley transform is used to eliminate the complexity associated with transform coefficients. Optical transformation of the image, in the fractional Hartley domain, is followed by a permutation through piecewise linear chaotic maps. Due to the intertwined application of optical transformation and chaos-based substitution and permutation processes, the proposed image encryption scheme possesses higher security. The input parameters (initial conditions, control parameters, and number of iterations) of chaotic maps along with fractional orders of the fractional Hartley transform collectively form the secret keys for encryption/decryption. The proposed scheme is a lossless and symmetric encryption scheme. The level of security provided in terms of high sensitivity to keys, resistivity to brute-force attack, classical attacks, differential attacks, entropy attack, noise and occlusion attack along with the elimination of complex coefficients proves its better efficacy as compared to other similar state-of-the-art schemes.

Keywords Color image encryption · Fractional Hartley transform · Chaos · Substitution · Permutation

1 Introduction

Digital information has evolved through decades with extensive growth in its capabilities. In particular, the past 10 years have seen a massive increase in usage of digital data accompanied with day-to-day advancing electronic devices such as smartphones, robotic devices, electronic readers, etc. Such devices ascertain fast processing, immense data storage and computational capabilities. The security concern related to data dissemination, especially images and videos, is still an active area of research. As compared to advancements in technology, most of the security measures such as encryption schemes are based on methodologies that were followed 10 years ago. The classical methods that include data encryption standards (DES), advanced encryption standards (AES), blowfish, etc. are not suitable for bulk data [1, 2] such as image and video. This prompted researchers to come up with some alternative methods for bulk data encryption rather than relying on pure number theory.

For image encryption, there are numerous methods proposed in the literature that include dynamical chaos-based ciphers [3–5] and their hybridization with finite state machine [6], with optimized S-Box generation [7], cascade coupling [8, 9], higher dimensional chaos with DNA [10], parallel with compressive sensing [11]. On the other hand, optical transforms-based image encryption is an active area of research due to the inherent property of high speed and massive parallelism. The transform orders that provide an extra degree of freedom to the encryption scheme serve as secret keys. The transform-based image encryption is inspired from the classical double random phase encoding scheme (DRPE) [12–14] which is implemented with an optical setup comprising of lenses, spatial light modulators

✉ Gurpreet Kaur
gurpreet.preeti.82@gmail.com

[1] USICT, Guru Gobind Singh Indraprastha University, Dwarka, New Delhi 110078, India

[2] Department of ECE, Amity School of Engineering and Technology, New Delhi 110061, India

[3] Department of Physics, Sir Padampat Singhania University, Bhatewar, Udaipur, Rajasthan 313601, India

(SLM) and charged coupled devices (CCD). Most commonly used optical image encryption schemes include Fractional Fourier transform (FrFT) [15–18], Fresnel transform [19, 20], Gyrator transform [21, 22], Mellin transform [23, 24], Hartley transform [25–27], etc.

According to a recent survey reported by Ghadirili et al. [28], 32.03% of total published works on image encryption are based on chaos and only 8.65% are based on transform domain-based encryption schemes. Although the optical transform-based algorithms offer high speed, parallel data processing and thus for image encryption, provide greater flexibility for manipulating parameters such as wavelength, polarization, amplitude or phase but still their usage in practical implementation is less preferred owing to drawback related to complex domain outcome and smaller keyspace. Various researches on cryptanalysis have shown that these algorithms are vulnerable to chosen-plaintext attack (CPA), known-plaintext attack (KPA) and some heuristic attacks [29–31]. Chen et al. [29] suggested that a larger keyspace is required to avoid blind decryption. The reuse of keys should also be avoided [31] following a one-time pad approach.

As mentioned by Ghadirili et al. [28], chaos-based image encryption is preferred owing to its inherent characteristics of high sensitivity to seed values, randomness and ergodicity. The chaotic maps are broadly classified as 1D or higher dimensional maps, whereas 1D maps are simple in hardware implementation but due to certain flaws such as the existence of blank windows in bifurcations, smaller keyspace, etc., lead to their vulnerability to potential attacks [5, 32]. On the other hand, higher dimensional chaotic maps are complex and have larger keyspace but are not cost-effective in hardware implementation [33, 34]. Hybridization of chaotic maps is looked upon as one of the solutions to overcome these limitations [28, 35]. Working toward hybridization, there are number of schemes recently proposed [27, 36–39] that combine chaos with transform domain encryption. Such schemes are based on combination of chaos-dependent permutation along with a particular transform for making the image unintelligible where the order of their application may vary. Either permutation is followed by transform or permutation is performed in the spatial domain prior to transform. However, such schemes are unable to provide enough security although their immunity to noise and data occlusion attacks is fairly good [39, 40]. Moreover, many such schemes fail to provide testimony against most of the classical attacks and differential attacks [29, 30, 41, 42]. Some of the most recently proposed schemes [18, 22, 26, 40, 43–46] lack such analysis.

Keeping into consideration all above-stated limitations in the transform and chaos-based encryption schemes, we propose a novel opto-digital method of color image encryption in which the image to be encrypted is initially processed nonlinearly in the spatial domain with the help of a compound chaotic mapping followed by a reality preserving 2D fractional Hartley transform operation to convert the processed image in the optical domain. The transform coefficients obtained are further scrambled with the help of a piecewise linear chaotic map to enhance the security. The input parameters of chaotic maps thus used and the fractional-order of the fractional Hartley transform serve as the secret symmetric keys for encryption/decryption. The performance and security analyses prove that the proposed scheme is robust and efficient for the secure transmission of images. The proposed scheme is highly sensitive to the keys and has a larger keyspace and thus can withstand various cryptanalytic attacks. Its distinct feature of the complete elimination of the complex coefficient terms makes it suitable for real-time image transmission.

This paper is organized as follows: Introduction in Sect. 1 is followed by Sect. 2 that describes the preliminaries such as fractional transform, reality preserving methodology, chaotic maps, compound mapping, etc., used in the proposed image encryption method. Section 3 elaborates the step-by-step procedure used for the proposed image encryption/decryption, and Section 4 gives the results of performance and security analyses of the proposed scheme. A comparative analysis is included in Sect. 5. Finally, the work is concluded in Sect. 6.

2 Preliminaries

2.1 Fractional integral transform

Fractional transforms have found many applications in the field of engineering and science ever since the advent [16, 47, 48] and later for applications in optics [15, 49, 50]. With the evolution of the digital era, the fractional transforms were studied for their digital representations [17, 51, 52]. The ordinary Fourier transform is the generalized form of fractional-order transforms where the transform order is unity. The integer orders when replaced with fractional orders expand the application area of these transforms. Particularly in optical processing, these transforms are useful in digital holography, as means of modeling speckle fields propagating through apertured optical systems, in quantum optics, in optical encryption by means of random phase encoding (DRPE), in wave field theory to describe the reflection of coherent light from a non-uniform surface which is beneficial in meteorology. The basic form of the integral transform is the Fourier transform. Fourier is obtained following integral representations for $f(x)$ and its nth integral as:

$$D^n f(x) = \frac{1}{2\pi}\int_{-\infty}^{\infty} f(\xi)\mathrm{d}\xi \int_{-\infty}^{\infty} t^n \cos\left\{t(x-\xi) + \frac{n\pi}{2}\right\}\mathrm{d}t \tag{1}$$

where ξ depicts the frequency. Replacing 'n' by an arbitrary fractional number 'α' gives the fractional-order equivalent transform of the function $f(x)$. The arbitrary angle α corresponds to the angle of rotation in the time–frequency domain. It is also understood as the Wigner rotation as explained in position–momentum paradigm [15]. The fractional transform integral is said to be in purely time domain for $\alpha = 0$ and in purely frequency domain if $\alpha = 1$. Thus, a fractional order corresponds to the collective time–frequency domain which gives an extra degree of freedom for its application to image encryption. The Fourier transform and Hartley transform are closely related [25, 52] as the eigenvalues of the DFT are also the eigenvalues of the Hartley transform. Thus, a fractional Hartley transform can also be represented by a fractional Fourier transform [5, 7]. Hartley transform of a function $f(x)$ is given by

$$H(\zeta) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} f(x)\mathrm{cas}(\zeta x)\mathrm{d}x \tag{2}$$

where radian frequency variable $\zeta = 2\pi f$ and cas function is defined as $\mathrm{cas}(\zeta x) = \cos(\zeta x) + \sin(\zeta x)$. The fractional Hartley transform of a time-domain signal is defined as:

$$H^{\alpha}\{f(t)\}(\zeta) = \int_{-\infty}^{\infty} f(t) S_{\alpha}(t,\zeta)\mathrm{d}t \tag{3}$$

where the fractional Hartley kernel is defined as:

$$S_{\alpha}(t,\zeta) = \left(\frac{1-j\cot\alpha}{2\pi}\right)^{1/2} e^{\frac{j\zeta^2}{2}\cot\alpha} e^{\frac{jt^2}{2}\cot\alpha} * \frac{1}{2}\left[\left(1-je^{j\alpha}\right)\mathrm{cas}(\csc\alpha\cdot\zeta t) + \left(1+je^{j\alpha}\right)\mathrm{cas}(-\csc\alpha\cdot\zeta t)\right]. \tag{4}$$

In the discrete domain, the eigenvectors of discrete fractional Fourier transform (DFrFT) are also the eigenvectors of discrete fractional Hartley transform (DFrHT). Thus, in terms of the Fourier transform, FrHT for a 2D signal can be represented as:

$$H^{\alpha,\beta}(u,v) = \left(1 - \frac{\exp\left[j\left(\phi_1+\phi_2\right)\right]}{2}\right)F^{\alpha,\beta}(u,v) + \left(1 + \frac{\exp\left[j\left(\phi_1+\phi_2\right)\right]}{2}\right)F^{\alpha,\beta}(-u,-v) \tag{5}$$

where $F^{\alpha,\beta}$ corresponds to the fractional Fourier transform coefficient, $\phi_1 = \frac{\alpha\pi}{2}, \phi_2 = \frac{\beta\pi}{2}, |\phi_1|, |\phi_2| < \pi, (u,v)$ represent the transform domain.

Therefore, fractional Hartley transform is the real part of fractional Fourier transform plus the negative of the imaginary part of the fractional Fourier transform [27]. The DFrHT possesses all the basic properties that are required in a fractional integral transform. The optical realization of fractional Hartley is described in [53]. However, the transform coefficients of a fractional Hartley transform are complex. These complex values need a holographic technique to record two images, one for spectrum and another for phase. This makes the storage and transmission less efficient due to double memory space requirements. Moreover, the computation complexity also increases during inverse operation.

2.2 Reality preserving method

The reality preserving concept was first introduced by Venturini and Duhamel [54] to overcome the complexity issue in the transform domain, where a reality preserving alternative to the complex fractional cosine and sine transforms was proposed. The reality preserving algorithm maintains most of the desired properties of the transform. As the resulting transform can have continuously increasing decorrelation power as the fractional order varies from '0' to '1' with an order of '0' corresponding to no decorrelation and order of '1' corresponding to a base transform with maximum decorrelation. This decorrelation power is used in various signal processing applications. Reality preserving can be employed where an orthogonal reality preserving transform is required and the de-correlating power is to be controlled by some parameter. The steps for deriving a reality preserving equivalent of FrHT are as follows:

Step 1 For a 1D FrHT of length, M: Let $\mathcal{H}_{\dashv,\frac{M}{2}}$ be a complex-valued fractional Hartley transform matrix with size $M/2(M$ is even). The real input signal is represented by $y = \left\{y_0, y_1, y_2, \ldots y_{M-2}, y_{M-1}\right\}^t$ from which a permutation matrix (P) is obtained as, $y' = \left\{y'_0, y'_1, y'_2, \ldots y'_{M-2} y'_{M-1}\right\}^t$ denoted as $y' = Py$,

Step 2 $\hat{y} = \left\{y'_0 + jy_{\frac{M'}{2}} \middle| y'_1 + y'_{\frac{M}{2}+1} \middle| \ldots y'_{\frac{M}{2}-1} + jy'_2 \middle| y' + jy'_{M-1}\middle|\right\}^t$ is the complex vector built from y. Further, a transform output is obtained from this complex vector such that,

$$\hat{z} = FrH^{\dashv}(\hat{y}).$$

Step 3 The Reality preserving equivalent of transform is obtained as $z' = \left\{\left(Re\,\hat{z}\right), \left(Im\,\hat{z}\right)\right\}; z = P^{-1}(z')^t$, t represents transpose. Thus, $z = P^{-1}\mathrm{RPFrHT}_{\dashv} Py$

$$\mathrm{RPFrHT}_{\dashv} = \begin{bmatrix} Re(\mathcal{H}_{\dashv}) & -Im(\mathcal{H}_{\dashv}) \\ Im(\mathcal{H}_{\dashv}) & Re(\mathcal{H}_{\dashv}) \end{bmatrix} \text{is obtained from } \mathcal{H}_{\dashv,M/2} + j\mathcal{H}_{\dashv,M/2}. \tag{6}$$

2.3 Chaotic maps

Dynamical chaos, observed in many nonlinear dynamical systems, is a deterministic, bounded, aperiodic behavior possessing sensitivity on initial conditions/system parameters. Along with the crucial feature of sensitivity on the initial condition, chaotic systems possess many other interesting and universal features like ergodicity, mixing, invariant density measure, positive metric entropy (KS-entropy), etc. These features make them suitable for use in secure communication. During the last two–three decades, the use of chaotic systems has been explored extensively and a well-defined close relationship between chaotic systems and ideal cryptographic systems has emerged [33]. According to Shannon [55], in order to attain a perfect secrecy, a combination of diffusion and confusion is essential in a cryptographic system. For images, which are characterized by the bulk of data, high correlation and redundancies, the chaotic systems have been found most suitable for achieving the desired level of permutation and substitution [4, 34]. In the proposed image encryption, we use chaotic systems as the source for introducing confusion and diffusion in conjunction with the optical process governed by the reality preserving fractional Hartley transform. The purpose of using transform is to bring the data from the spatial domain to the combined time–frequency domain so that the chaos-based analysis may not be feasible for the intruder. In the following paragraph, we briefly describe the chaotic systems being used in the proposed image encryption scheme.

2.3.1 For permutation/scrambling stage: Piecewise linear chaotic map (PWLCM)/Zhao map

The mathematical form of PWLCM [56] used for diffusion in the proposed image encryption scheme is as follows:

$$f(y,\varepsilon)=\begin{cases}\frac{y}{\varepsilon}, & y\in[0,\varepsilon)\\ \frac{y-\varepsilon}{\frac{1}{2}-\varepsilon}, & y\in\left[\varepsilon,\frac{1}{2}\right]\\ F(1-y,\varepsilon), & y\in\left(\frac{1}{2},1\right]\end{cases} \tag{7}$$

where ε $(0<\varepsilon<1/2)$ is the control/system parameter. If $Y\in[0,1]$, it is known as normalized PWLCM. In this paper, we are using a normalized PWLCM [57] that can be expressed using a simple affine transformation:

$$F_{[0,1]}(y)=\frac{F\left(\frac{y-\gamma_1}{\gamma_2-\gamma_1}\right)-\gamma_1}{(\gamma_2-\gamma_1)}:[0,1]\rightarrow[0,1]. \tag{8}$$

2.3.2 For substitution: Compound chaotic maps

Due to some inherent weaknesses in one-dimensional maps for cryptographic applications [41] and to enhance the robustness in the complete parameter range, researchers have used a combination of chaotic systems, i.e., compound chaotic map [3, 8, 58]. In the proposed work, we use a similar nonlinear combination of three seed maps, $F(x_n), G(x_n)$ and $H(x_n)$. A compound chaos is defined by, $x_{n+1}=\left(F\left(G\left(x_n\right)\right)+H\left(x_n\right)\right)\bmod 1$. The mod operation is to ensure that the output sequence is restricted in the range [0, 1]. The combination of the two maps improves the chaotic behavior [8]. Further, the addition of the third map (modulo 1) enhances the mixing and results in enhanced complexity.

In the proposed image encryption scheme, logistic map (L), tent map (T), and sine map (S) are used for compound mapping.

(a) *Logistic map:* It is originally introduced as a demographic model [59] and is mathematically defined as:

$$\begin{aligned}x_{n+1}&=L\left(x_n\right)=\mu x_n\left(1-x_n\right)\\&=4rx_n\left(1-x_n\right),0<x_n<1\end{aligned} \tag{8}$$

where $\mu\in[0,4]$ or $r\in[0,1]$ is the control parameter, also known as the bifurcation parameter. The 1D logistic map is chaotic for its control parameter range as $0.9\le r<1$.

(b) *Tent map:* It is the simplest piecewise linear chaotic map and is a topological conjugate of logistic map [60] defined in the interval [0, 1] and mathematically described as:

$$x_{n+1}=T\left(x_n\right)=\begin{cases}2rx_n, & \text{if } 0\le x_n\le 0.5\\ 2r\left(1-x_n\right), & \text{if } 0.5<x_n\le 1\end{cases} \tag{10}$$

where $0<r\le 1$. The chaotic behavior is observed for $0.61<r<1$

(c) *Sine map:* Sine map is another simplest 1D nonlinear map [32], mathematically described as:

$$x_{n+1}=S\left(x_n\right)=r\sin\left(\pi x_n\right). \tag{11}$$

The chaotic behavior in this map is observed for $r\in[0.87,1]$. It is qualitatively identical to the logistic map as the topological entropy of the sine map is equal to that of the logistic map at $r=1$. Figure 1 illustrates the complete schematics of developing these three compound chaotic maps (CCM), CCM1, CCM2, and CCM3. The mathematical representation of each CCM is given in Table 1.

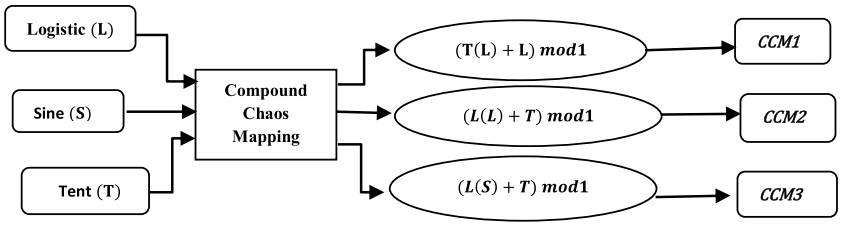

Fig. 1 Generation of compound chaotic maps form basic maps

3 Encryption and decryption procedure

In this section, we describe the processes of encryption and decryption in detail. The proposed encryption process is based on three different stages. A chaos-based substitution/confusion in the spatial domain is the first stage followed by optical processing using reality preserving fractional Hartley transform and finally the third stage of chaos-based diffusion /scrambling in the transform domain. There are a total of 24 keys used in the encryption process that includes nine keys for confusion (first stage), six keys for optical transform and then nine keys for scrambling in the transform domain.

Encryption

3.1 Stage 1: Substitution based on compound chaos (CCM)

The input image 'P' of size $M \times N \times 3$ is decomposed into its red (R), green (G) and blue (B) component images each of size $M \times N$. The first level of encryption is based on compound chaotic maps described in Sect. 2.3.2. For example, the CCM used for the red component $(R)_{M\times N}$ is $(T(L) + L) \bmod 1$ compound chaotic map (CCM1) with parameters $\{c1_0, u1, i1\}$ where $c1_0$ denotes the initial value, $u1$ is the bifurcation parameter and i1 is the number of iterations to be discarded as transient. For CCM1, a chaotic sequence is iterated for $i1 + MN$ different values, i.e., $\{c1_{i1+M\times N}\}$. The initial $i1$ iterations are discarded in order to avoid any computational error and also to increase the security. A similar process is followed for other CCMs. The values of sequence thus obtained are in floating point. These are converted to integer form as:

$$\hat{c} = \left(c_{(1\times M\times N)} \times 10^{14}\right) \bmod 256. \tag{12}$$

The integer sequence is then reshaped to a 2D image of size $M \times N$ and is used for the substitution of each color component of the input image, $P' \in [R, G, B]$ as:

$$S = bitxor\left(\hat{c}_{(M\times N)}, P'_{(M\times N)}\right). \tag{13}$$

3.2 Stage 2: Reality preserving 2D fractional Hartley transform

The outcome from Stage 1 in the spatial domain is then transformed via a fractional Hartley transform with a reality preserving algorithm. The transformation results in the complex coefficients which in optical processing require special holographic techniques for recording. In the digital domain, it becomes difficult to store and transmit the complex coefficients as it leads to increased complexity and memory requirements. To overcome such issues, a reality preserving algorithm [54] is used to obtain transform in the real domain as explained in Sect. 2.2. The substituted outcome of Stage 1 is transformed using the steps explained in Sect. 2.2. It is likely to mention that 1D transformation has to be extended to 2D for image data. The 1D RPFrHT can be easily extended to 2D by cascading two transforms, one along rows of the image and another along with the columns. This requires two different transform orders (α, β) for both

Table 1 Mathematical representation of compound chaotic maps

CCM	Mathematical representation
CCM1 $(T(L) + L) \bmod 1$	$x_{n+1} = \begin{cases} \left(4r\left(4rx_n(1-x_n)\right)\left(1-4rx_n(1-x_n)\right) + (2-2r)x_n\right) \bmod 1 & \text{for } x_n < 0.5 \\ \left(4r\left(4rx_n(1-x_n)\right)\left(1-4rx_n(1-x_n)\right) + (2-2r)(1-x_n)\right) \bmod 1 & \text{else} \end{cases}$
CCM2 $(L(L) + T) \bmod 1$	$x_{n+1} = \begin{cases} \left(4r2rx_n(1-2rx_n) + (4-4r)x_n(1-x_n)\right) \bmod 1 & \text{for } x_n < 0.5 \\ \left(4r2r(1-x_n)\left(1-2r(1-x_n)\right) + (4-4r)x_n(1-x_n)\right) \bmod 1 & \text{else} \end{cases}$
CCM3 $(L(S) + T) \bmod 1$	$x_{n+1} = \begin{cases} \left(r\sin(\pi 2rx_n) + (4-4r)x_n(1-x_n)\right) \bmod 1 & \text{for } x_n < 0.5 \\ \left(r\sin\left(\pi 2r(1-x_n)\right) + (2-2r)(1-x_n)\right) \bmod 1 & \text{else} \end{cases}$

directions. For the sake of brevity, the individual steps of transformation are not again illustrated here. However, to correlate with explanation given in Sect. 2.2, final outcome of 1D RPFrHT for input as substituted image of Stage 1 is represented as:

$$\begin{aligned}\widehat{Z} &= \{Re(FrH^{\alpha}(N)) + j \times Im(FrH^{\alpha}(N))\}\left\{Re\left(\widehat{S}\right) + j \times Im\left(\widehat{S}\right)\right\} \\ \Rightarrow Z &= \begin{bmatrix} Re(FrH^{\alpha}(N))Re\left(\widehat{S}\right) - Im((FrH^{\alpha}(N))Im\left(\widehat{S}\right) \\ Im(FrH^{\alpha}(N))Re\left(\widehat{S}\right) + Re(FrH^{\alpha}(N))Im\left(\widehat{S}\right) \end{bmatrix} \\ &= \begin{bmatrix} Re(FrH^{\alpha}(N)) & -Im(FrH^{\alpha}(N)) \\ Im(FrH^{\alpha}(N)) & Re(FrH^{\alpha}(N)) \end{bmatrix} \begin{bmatrix} Re\left(\widehat{S}\right) \\ Im\left(\widehat{S}\right) \end{bmatrix} \\ &\therefore Z = RPDFrH^{\alpha}T(N) \times S \end{aligned} \tag{14}$$

This 1D RPDFrHT can be extended to 2D by following the same procedure as shown above but in y-direction. For that, each column is treated as a different array and the values are wrapped to half along each column to obtain a matrix of dimensions $M/2 \times N$. The transform order along y-direction, i.e., along each column, is denoted by β. Hence, a 2DRPDFrHT can be described as a cascaded operation of two 1D RPDFrHT's as:

$$\begin{aligned}\text{2DRPFr HT}^{\{\alpha,\beta\}}T\left\{S_{(M,N)}\right\} &= \text{1DRPFrHT}^{(\alpha)}(N) \cdot S_{(M,N)} \\ &\quad \cdot \text{1DRPFrHT}^{(\beta)}(M)\end{aligned} \tag{15}$$

where (M, N) represents the size of the image, (α, β) are the transform orders, $S_{(M,N)}$ is the substituted image of Stage 1. The above-stated procedure is repeated for each color component image with a different set of transform orders.

3.3 Single-bit phase modulation

The transformed image, obtained after reality preserving 2D fractional Hartley transform, in its coefficient has both positive and negative values which are not suitable for optical detection by CCD camera if an optical setup is used. In the digital domain, negative values cannot be realized while storing and retrieving. This issue needs to be handled for the complete recovery of data during the reverse process. A phase modulation method is used with a single bit of the data representing it as either a negative or positive value. This can be termed as a *single-bit phase modulation method*. In this method, we use a variable $P_b(u, v)$ which is assigned a bit '0' for positive value and bit '1' for negative value corresponding to the transform coefficients $h_{(k+1)}(u, v)$:

$$P_b(u, v) = \begin{cases} 1, & \text{if } h_{(k+1)}(u, v) < 0 \\ 0, & \text{otherwise} \end{cases} \tag{16}$$

This single bit value is extracted for each color component and then is concatenated into a single image. This matrix of size $M \times N \times 3$ can be used as a public key as it does not reveal any intuitive information about the encrypted data. Moreover, as it is a single-bit matrix, storage and transmission will not be an issue of concern. During the decryption process, the original transform coefficients are obtained as:

$$h'_{(k+1)}(u, v) = h_{(k+1)}(u, v) \times \left[\exp\left(i\pi P_b(u, v)\right]\right. . \tag{17}$$

3.4 Stage 3: Chaotic scrambling using PWLCM

As explained in Sect. 2.3.1, a PWLCM map is used for generating a chaotic sequence owing to its LE (Lyapunov exponent) being positive over the entire range of its control parameters. Three different PWLCM or W-maps are used each for red, green and blue components of the transform coefficients obtained in Stage 2. For the transform coefficients of size M × N corresponding to each color component, the PWLCM with parameters $\{x_0, u, t\}$ is iterated for $(t + M \times N)$ number of iterations and a sequence of $M \times N$ is generated by discarding first t terms to avoid any computational error of transients.

Step 1 The chaotic sequence generated by each PWLCM can be represented as:

$$P_l = P_{t+1,}P_{t+2}, P_{t+3}, \ldots P_{t+MN-1}, P_{t+MN}. \tag{18}$$

Step 2 The chaotic sequence is then sorted in ascending/descending order into a vector, and the index of the vector is stored as the address into another vector as: $[\text{ind}, P_s] = \text{sort}(P_l)$. This changes the positions of the elements. Record the new index of P_s, i.e., mth element of P_s corresponds to ind{mth} element of P_l.

Step 3 The 2D transform matrix of Stage 2 is reshaped into the 1D sequence of size $MN \times 1$. Vectorization is performed to convert $M \times N$ transform coefficients to a matrix of size $M \times N \times 1$ by extracting the values column by column.

Step 4 Now, the recorded index of the sorted vector ind is used to reorder (permute/scramble) the 1D transform vector as RPFrHT(ind). Finally, this 1D matrix is converted into 2D image format by reconverting it into $M \times N$ vector.

In this stage, the initial value, control parameter and number of iterations to be discarded $\{x_0, u, t\}$ are used as the secret keys. Therefore, there are a total of nine keys for scrambling (three each for R, G and B individually). The scrambled transform coefficients give a final encrypted image which can now be transmitted over a public channel. The complete encryption process is shown in Fig. 2.

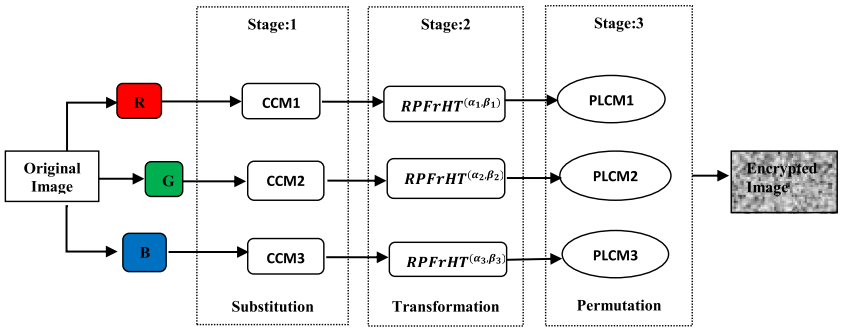

Fig. 2 Encryption process

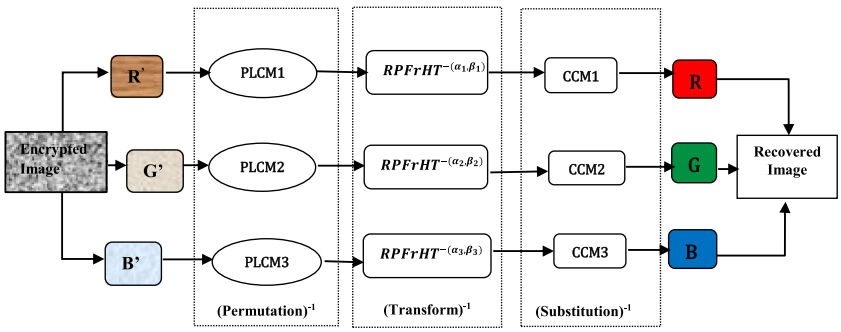

Fig. 3 Decryption process

Decryption

The decryption procedure is illustrated in Fig. 3. Decryption is exactly the reverse of that of encryption. Exactly the same keys (all 24 keys) are required in each stage of decryption to completely recover the original image, thus making it a symmetric key cryptographic process.

The output of Stage 3 of the encryption process which is scrambled transform coefficients is descrambled using the same PWLCM's with parameters $\{x_0, u, t\}$ as used during encryption. The descrambled image components are then inverse transformed with $(\text{RPFrHT})^{-1}$ which is similar to the forward transform with the same transform orders but with negative values (six keys). The next step is the generation of the CCMs with nine keys of Stage 1. The generated CCMs need to be exactly same as used during the forward procedure, for them to be substituted with the inverse transform coefficients to retrieve the original image components.

4 Simulation results

The proposed scheme is realized in MATLAB 9.0, on a personal computer with Intel(R) Core (TM) i5 8250U CPU (3.45 GHz), 8 GB RAM, and 1 TB hard disk capacity. Two standard images (Lena, *Baboon*) taken from the SIPI dataset [61] are considered as test images for visual analysis and statistical analysis. The simulation results for numerical analysis are evaluated for a number of other images taken from the same dataset. The secret keys used in this simulation are randomly generated using a random number generator in MATLAB. The simulations are done with the same set of secret keys throughout this work. The distribution of keys and their corresponding values are given in Table 2.

4.1 Experimental analysis

Figure 4 shows encryption at each stage from left to right. Figure 4a, f shows the original standard color test images (Lena and Baboon). The first stage of encryption is the substitution with compound chaotic maps as described in Sect. 3.1, and the results obtained for this stage using the secret keys (Table 2) for red, green and blue channels, respectively, are shown in Fig. 4b, g. In order to enhance the security, a plain image-dependent session key is generated for each color channel (δ_r, δ_g, δ_b). Also, the session keys are added either to the initial condition or to control parameter alternatively to further create more confusion for any intruder. The next stage is to obtain the reality preserving fractional Hartley transform (RPFrHT) of the image by following the procedure described in Sect. 3.2. The secret keys at the transform stage are basically the pairs of fractional transform orders along the rows and columns of red, green and blue channels, respectively, as shown in Table 2. The resultant transformed images are shown in Fig. 4c, h. The transform output also has certain negative-valued coefficients which are stored in a single-bit phase modulation matrix by storing a bit '0' for positive value and bit '1' for negative value of the coefficients, and the resultant matrix in the form of an image is shown in Fig. 4d,

Table 2 Secret keys in each stage of encryption

Key	Parameter	Value
Stage:1		
(K_1, K_2, K_3)	$[c1_0, u1, i1]$	[0.814723686393179, 0.305791937075619 + δ_r, 1386]
(K_4, K_5, K_6)	$[c2_0, u2, i2]$	[0.313375856139019 + δ_g, 0.426986816293506, 1213]
(K_7, K_8, K_9)	$[c3_0, u3, i3]$	[0.397540404999410 + δ_b, 0.232359246225410, 1432]
Stage:2		
(K_{10}, K_{11})	$[\alpha_1, \beta_1]$	[0.2784, 0.5468]
(K_{12}, K_{13})	$[\alpha_2, \beta_2]$	[0.3648, 0.4575]
(K_{14}, K_{15})	$[\alpha_3, \beta_3]$	[1.1576, 1.4853]
Stage:3		
(K_{16}, K_{17}, K_{18})	$[x_0, u, t]_R$	[0.421761282626275, 0.141886338627215, 1478]
(K_{19}, K_{20}, K_{21})	$[x_0, u, t]_G$	[0.735711678574190, 0.432207329559554, 1321]
(K_{22}, K_{23}, K_{24})	$[x_0, u, t]_B$	[0.733993247757551, 0.555740699156587, 1435]

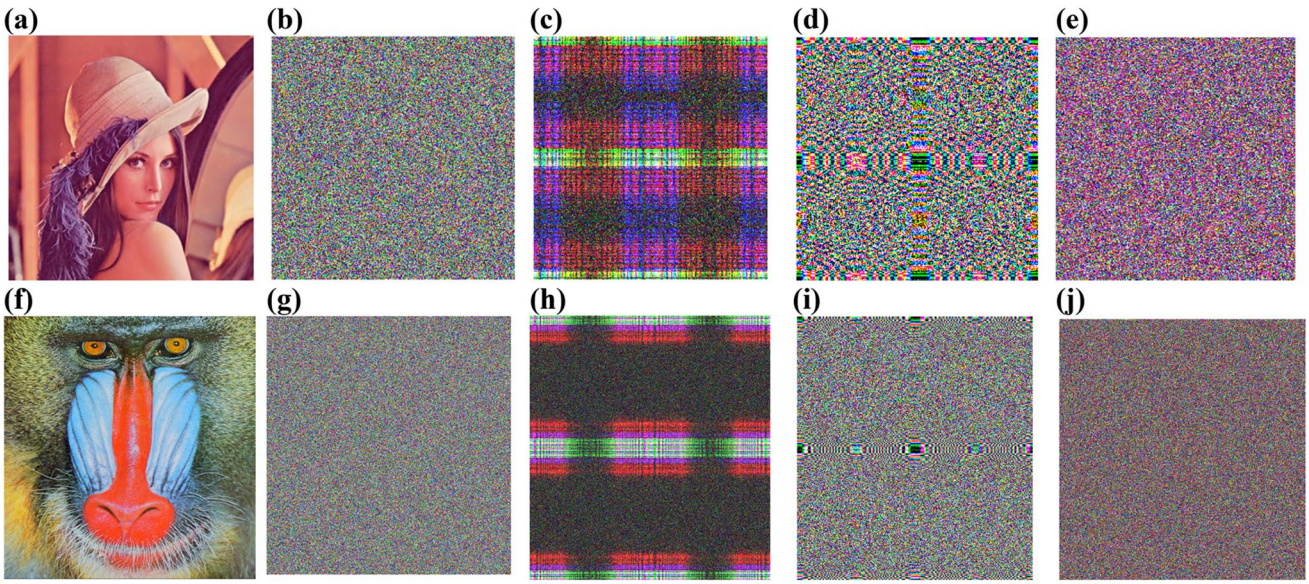

Fig. 4 Perceptual security analysis at each stage of encryption (left to right)

i. It can be seen that transform output has some visual patterns which need to be removed. Therefore, the third and final stage is to permute the transformed image obtained after the second stage with the piecewise linear chaotic map as described in Sect. 3.4. The set of secret keys (Table 2) are used to permute each component image to make it a random noise-like image. The resultant images after the permutation are shown in Fig. 4e, j. This is the final encrypted image that is transmitted over the public channel along with the single-bit phase modulation matrix.

The decryption is exactly the reverse of that of the encryption procedure. If the same sets of keys (as used during encryption) are supplied at all stages of decryption, the original image can be recovered without any loss of data. The complete process of decryption of encrypted images is shown in Fig. 5. Figure 5a, f shows encrypted images of Lena and Baboon, respectively. The encrypted image will be first processed for descrambling/inverse permutation using PWLCM with the same set of secret keys as used for Stage 3 of encryption. The resultant images after the inverse permutation are shown in Fig. 5c, h. This transformed image (which carries the magnitude of transform coefficients) along with the single-bit phase modulation matrix as shown in Fig. 5b, g collectively represents the exact transform coefficients to be processed for the next stage of decryption, i.e., inverse reality preserving Hartley transformation. This combination (images in Fig. 5b, g along with Fig. 5c, h) is processed for inverse RPFrHT with the same pairs of fractional orders as supplied in Stage 2 of the encryption but with negative sign (as explained in Sect. 3). The resultant

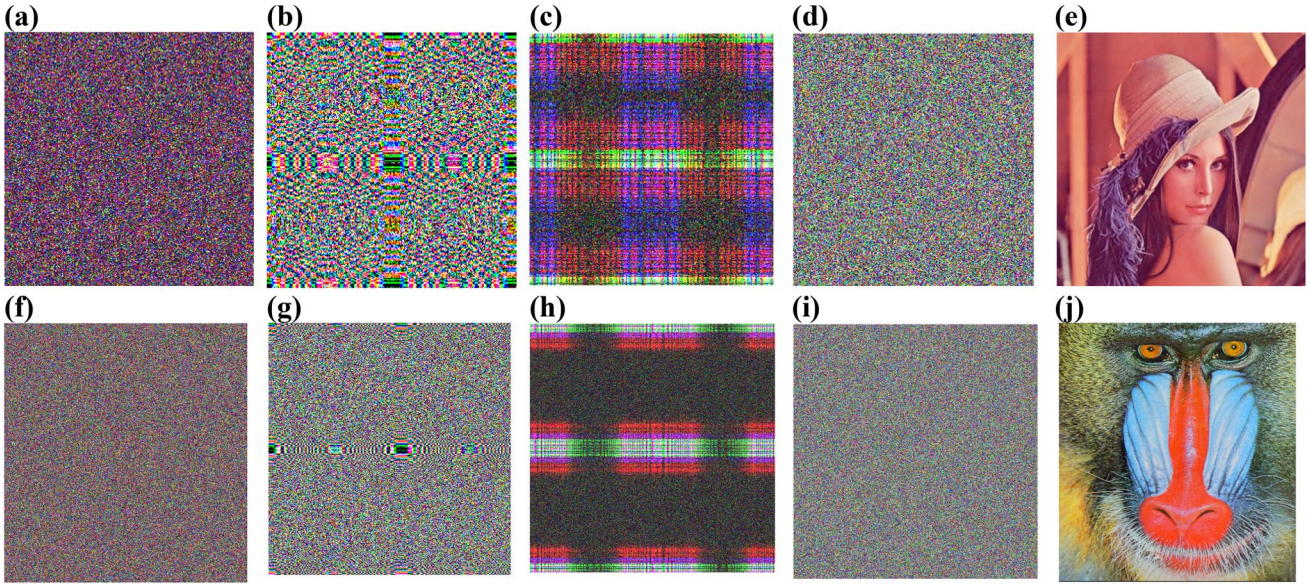

Fig. 5 Illustration of decryption at each stage of recovering the original image (left to right)

images after the inverse transform are shown in Fig. 5d, i. Now the third stage of decryption is executed on the image shown in Fig. 5d, i by following the procedure explained in Sect. 3.1 based on the compound chaotic maps (described in Sect. 2.3.2) and subject to the same set of secret keys for the red, green and blue channels as used in Stage 1 of encryption. The resulting images are the final decrypted/recovered images which are shown in Fig. 5e, j.

We have also experimented with a lot of other images having widely different contents using several combinations of secret keys and analyzed the corresponding encrypted and decrypted images with all intermediated images. We observe that the proposed method completely converts the images into visually obfuscated data and gives a lossless recovery in decryption.

4.2 Security analysis

The major concern of any cryptosystem lies in the level of security it provides. In other words, a good encryption technique should be robust against all sorts of cryptanalytics, statistical and brute-force attacks. In this section, we attempt to provide a complete investigation on the security of the proposed encryption technique.

4.2.1 Brute-force attack

In cryptographic applications, the most important part is the selection of keys. The keyspace should be large enough to counter any brute-force attack. This type of attack is based on exhaustive key searching where the adversary gets capability of recovering the original information by searching all possible keys in the keyspace until a correct key is found. The resistance to brute-force attack is the measure of the keyspace. A larger keyspace ensures better resistance. The keyspace should be $> 2^{120}$ to preclude any eavesdropping [33, 62].

In this scheme, 24 keys are used with different precision levels. There are 12 keys with a precision of 10^{-15}, six keys with the precision of 10^{-4}, six keys with integer values (4 digits). Therefore, the total keyspace can be evaluated as

$$10^{15\times12} \times 10^{4\times6} \times 10^{4\times6} \approx 10^{228},$$

which is sufficiently larger than 2^{120} to resist any brute-force attack.

4.2.2 Perceptual security analysis

Perceptual security analysis determines the measure of dissimilarity between plain and encrypted images.

The utmost requirement of encryption is to make the information unintelligible and obfuscate the pixels in such a way that it appears as random white noise. It is evident from Fig. 4 that the final encrypted images are completely random and thus are visually unrecognizable.

Apart from visual quality, the perceptual security analysis results are numerically represented in terms of certain parameters, viz. peak signal-to-noise ratio (PSNR), mean square error (MSE) and spectral similarity index (SSIM). For a pair of original and encrypted images represented as $o_{i,j}$ and $e_{i,j}$, respectively, these parameters are defined as:

$$\mathrm{PSNR}(o,e) = 10\log_{10}\frac{(L-1)^2}{\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[o_{i,j}-e_{i,j}\right]} \tag{19}$$

$$\mathrm{MSE}(o,e) = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[\left|o_{i,j}-e_{i,j}\right|^2\right] \tag{20}$$

$$\mathrm{SSIM}(o,e) = \frac{(2\mu_o\mu_e + C_1)(2\sigma_{o,e} + C_2)}{(\mu_o^2 + \mu_e^2 + C_1)(\sigma_o^2 + \sigma_e^2 + C_2)} \tag{21}$$

where $[M,N]$ is the image size, L is the highest intensity value (256 for an 8-bit image), $\mu_o, \mu_e, \sigma_o, \sigma_e, \sigma_{oe}$ are mean, variance and covariance of original and encrypted images. C_1, C_2 are constants that are used to stabilize division with a weak denominator.

Mean square error (MSE) is an error metric that allows to compare pixel values of original with that of the encrypted image. Thus, a high value of MSE is desirable during encryption and in the decryption process, MSE should be ideally '0′ for lossless image recovery. PSNR is used as a metric for spectral information measure and is an error metric that is used as quality measure statistics of an image with respect to a reference image. The higher the value of PSNR, the better is its quality. Thus, two similar images will have infinite PSNR. However, a PSNR ≥ 28 is considered satisfactory for a reconstructed image. The purpose of evaluating PSNR is to show that the PSNR of the encrypted image with respect to the original image is very low ($\ll 28$) which indicates a significant difference between the original and encrypted image. However, there is a limitation of just relying on the MSE and PSNR values as these measures utilize only numeric values of pixels and do not consider other factors of the human visual system (HVS). Wang et al. [63] proposed *Structural Similarity Index* (SSIM) as another metric that considers three main biological factors, viz. luminance, contrast and structure comparison between an image and a reference image, and is a method of subjective evaluation for quantifying the visual image quality. SSIM $\in [-1,1]$ with a value of '1' for ideally similar images.

Different images along with test images are simulated for these parameters' evaluation. The simulated results are given in Table 3. As is evident from the results, the PSNR of encrypted images is very low ($\ll 28$) with MSE values ($\cong 10^4$) very high. SSIM of encrypted images is near to 'zero'. All these parameters indicate that the encrypted images have high perceptual security.

During decryption, it is recommended to have decryption error negligibly low [66] for applications such as biometrics and secure military communications. The decryption error of decrypted image, $\mathrm{De}(i,j)$ corresponding to plain image $\mathrm{Pl}(i,j)$ of size $M \times N$ is evaluated [67] as

Table 3 Parameter evaluation for perceptual security analysis

Image	Channel	PSNR	MSE	SSIM
Lena (256×256)	Red	7.6923	1.1062×10^4	0.0103
	Green	8.6871	8.7970×10^3	0.0099
	Blue	8.8999	8.3769×10^3	0.0101
Baboon (512×512)	Red	8.8555	8.4763×10^3	0.0099
	Green	9.0326	8.1250×10^3	0.0089
	Blue	7.8808	1.0593×10^4	0.0080
Balls (256×256)	Red	8.7310	8.7093×10^3	0.0104
	Green	8.0530	1.0181×10^4	0.0106
	Blue	9.1423	7.9223×10^3	0.0094
Peppers (512×512)	Red	9.1118	7.9782×10^3	0.0123
	Green	7.4589	1.1673×10^4	0.0073
	Blue	7.0301	1.2885×10^4	0.0065
House (256×256)	Red	9.5722	7.1756×10^3	0.0105
	Green	8.8021	8.5679×10^3	0.0096
	Blue	8.0486	1.0191×10^4	0.0082
Flowers (256×256)	Red	9.2646	7.7023×10^3	0.0094
	Green	9.6180	7.1004×10^3	0.0095
	Blue	7.3184	1.1883×10^4	0.0100
Jupiter moon (256×256)	Red	5.7259	1.7398×10^4	0.0039
	Green	6.3810	1.4962×10^4	0.0057
	Blue	4.9971	2.0576×10^4	0.0025
Paints (256×256)	Red	8.2937	9.6318×10^3	0.0067
	Green	8.5793	9.0188×10^3	0.0081
	Blue	8.5167	9.1498×10^3	0.0096
Ref. [18]	Red	7.4706	1.1642×10^4	–
	Green	7.6293	1.1224×10^4	–
	Blue	9.1401	7.9264×10^3	–
Ref. [64]		–	$\approx 8 \times 10^3$	–
Ref. [65]	Red	9.2766	–	–
	Green	8.3819	–	–
	Blue	9.2494	–	–

$$\mathrm{DErr} = \left(\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} Q(i,j)\right) \times 100\% \tag{22}$$

$$\text{where } Q(i,j) = \begin{cases} 1, & \mathrm{Pl}(i,j) = \mathrm{De}(i,j) \\ 0, & \text{otherwise} \end{cases}$$

The decryption error of all the images is 'zero' in the proposed scheme. We have also checked the objective metrics for the same to validate our claim. The objective metrics are the same for all test images and are listed in Table 4.

Table 4 Parameters for recovered images

Metric	R	G	B	Ref. [40]	Ref. [65]	Ref. [68]
PSNR	∞	∞	∞	306.586	44.62	41.51
MSE	0	0	0	–	–	–
SSIM	1	1	1	–	–	–

Result is same for all images in the proposed scheme

4.2.3 Statistical analysis

4.2.3.1 Histogram analysis An image histogram depicts the intensity value distribution of image pixels against each gray level. This statistical data can reveal some crucial information for an intruder to decrypt image by analyzing its histogram. Also, this information can be used to mount more statistical attacks. Thus, it becomes necessary to investigate the histograms of the encrypted image. The histogram of an encrypted image should be different from that of the actual image and also independent of the content of the actual image. As shown in Fig. 6, the first and third rows are the RGB channel histograms of plain image Lena and Baboon respectively. The second and fourth rows depict corresponding histograms of encrypted images. It is evident from Fig. 6 that the histograms of the encrypted image are quite different from that of the original image. One more important point worth mentioning here is that the histograms of the final encrypted image are always independent of the original image and hence, do not reveal any information about the original image.

4.2.3.2 Correlation analysis The adjacent pixels in an ordinary image with definite visual content are highly correlated in horizontal, vertical and diagonal directions. A good encryption scheme should be capable to make the correlation sufficiently low in order to resist the statistical attacks. To analyze and compare the correlations of adjacent pixels in the plain and encrypted image, correlation analysis of the proposed scheme is done.

We have randomly selected 100×100 pixels of the red channel from each image. (For brevity, only red channel for both the test images is shown.) Figure 7a–c shows the horizontal, vertical and diagonally shifted pixels of plain image Lena, and Fig. 7d–f shows corresponding correlation plots in encrypted image. Similarly, Fig. 7g–i shows the horizontal, vertical and diagonally shifted pixels of plain image Baboon, and Fig. 7j–l shows corresponding correlation plots in encrypted Baboon. In order to quantify the adjacent pixel correlation in the encrypted image, correlation coefficients are computed through Eq. (23) where x_k and y_k are gray values for *kth* pair of selected adjacent pixels.

$$r_{xy} = \frac{\frac{1}{M}\sum_{k=1}^{M}(x_k - E(x))(y_k - E(y))}{\sqrt{D(x)D(y)}} \tag{23}$$

$$\text{where } D(x) = \frac{1}{M}\sum_{k=1}^{M}(x_k - E(x))^2, \quad D(y) = \frac{1}{M}\sum_{k=1}^{M}(y_k - E(y))^2$$

$$E(x) = \frac{1}{M}\sum_{k=1}^{M} x_k, \quad E(y) = \frac{1}{M}\sum_{k=1}^{M} y_k$$

The correlation analysis is done for all the images in the horizontal, vertical and diagonal directions. We observe that the adjacent pixels are highly correlated in the plain images. However, this correlation is completely removed after the encryption of the images using the proposed image encryption technique. The quantitative results of the correlation coefficients between the horizontally, vertically and diagonally adjacent pixels distributions are given in Table 5 for the encrypted images only (for all three color components). A very low value (≈ 0) of the correlation coefficients for encrypted images proves no correlation and hence resistance to statistical attacks.

4.2.4 Key sensitivity analysis

A cryptosystem is evaluated for its effectiveness in terms of key sensitivity. Therefore, the sensitivity of the keys should be as high as possible. There are two aspects of evaluation for key sensitivity: (1) During encryption, a completely different ciphertext should be generated with a very minute change in key, and (2) During decryption, there should be incorrect recovery (almost a random noise-like) with wrong keys. A key sensitivity parameter (KS) is introduced in [72] which should be ideally 100% for two completely dissimilar images.

However, in practical terms, KS should be as close to 100%. For each key, KS is evaluated in the encryption stage corresponding to each wrong key. For example, the value for the key (K_1) gives ciphered image (C_1), and for altered key with very minute variation (K_1') another ciphered image (C_2) is obtained. Therefore, KS parameter for two ciphered images, C_1 and C_2 is as:

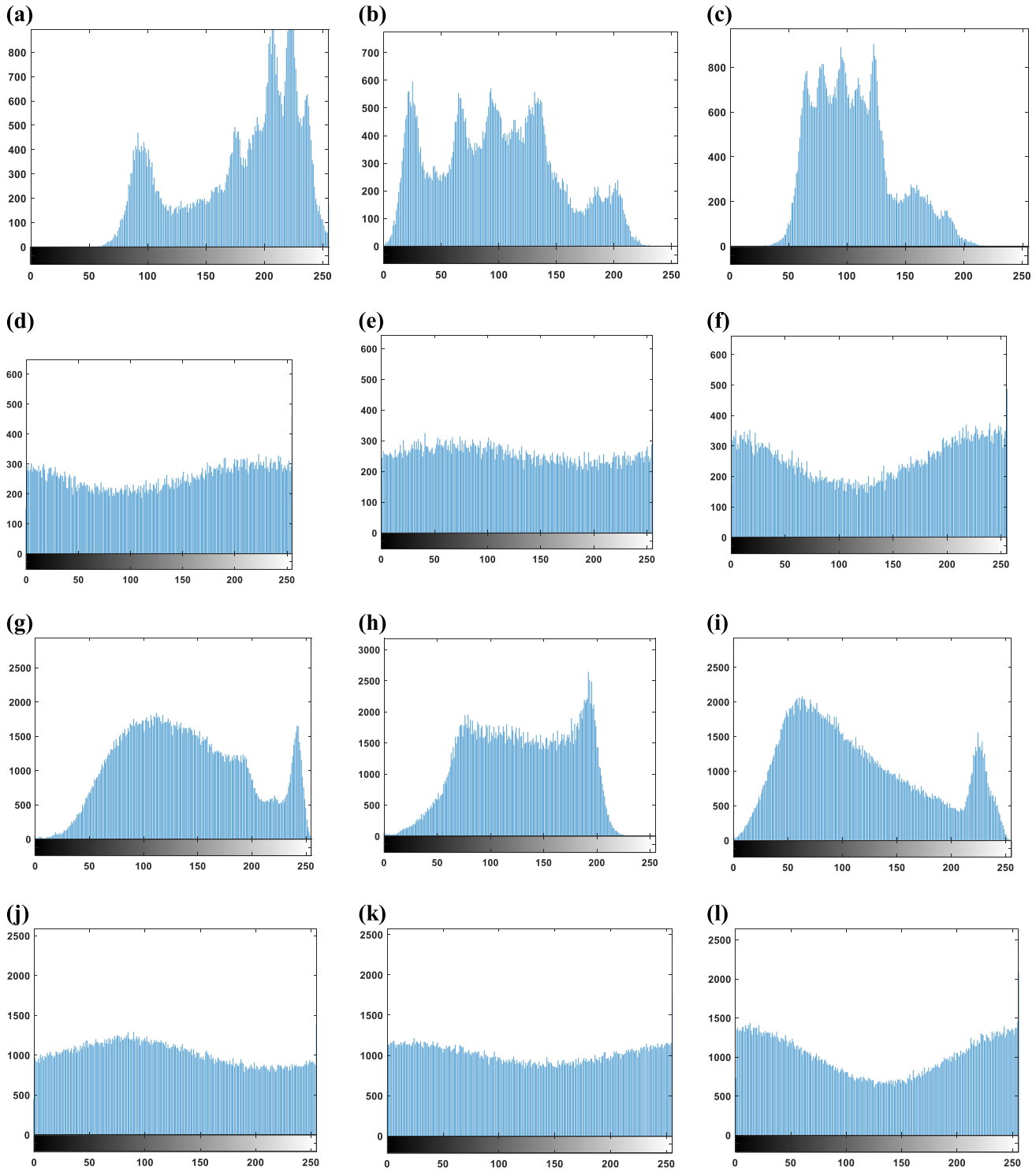

Fig. 6 **a–c** Are RGB histograms of plain image Lena, **d–f** are histograms of Lena in the encrypted domain, **g–i** are RGB histograms of plain image Baboon, **j–l** are histograms (Baboon) in the encrypted domain

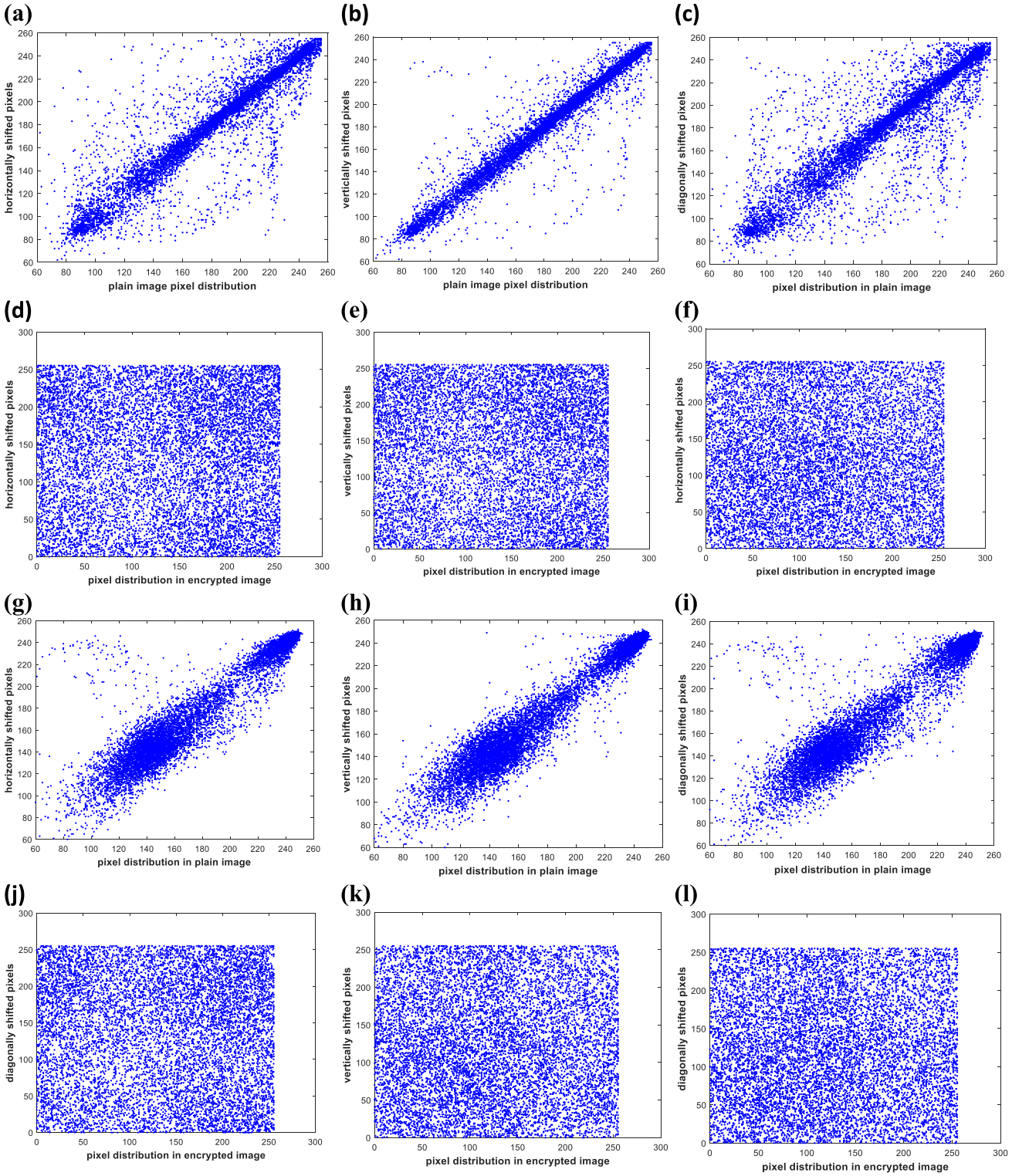

Fig. 7 Correlation analysis: **a–c** are H, V, D correlation plots for plain image Lena, **d–f** are H, V, D correlation plots for corresponding encrypted pixels of image Lena, **g–i** are H, V, D correlation plots for plain image Baboon, **j–l** are H,V,D of encrypted image Baboon

Table 5 Correlation analysis for encrypted images (RGB)

Image	Shift axis	Red channel	Green channel	Blue channel
Lena (256×256)	Horizontal	0.0033	−0.0021	−0.0029
	Vertical	−0.0097	0.0031	0.0022
	Diagonal	−0.0046	−0.0070	-2.9717×10^{-5}
Baboon (512×512)	Horizontal	−0.0029	−0.0034	8.5471×10^{-5}
	Vertical	0.0011	−0.0022	-4.926×10^{-4}
	Diagonal	−0.0041	0.0038	-9.0239×10^{-4}
Balls (256×256)	Horizontal	−0.0062	−0.0035	0.0016
	Vertical	−0.0052	0.0014	−0.0048
	Diagonal	−0.0055	−0.0013	0.0037
Peppers (512×512)	Horizontal	-4.1538×10^{-4}	−0.0015	−0.0033
	Vertical	-2.0646×10^{-5}	0.0043	3.8279×10^{-4}
	Diagonal	−0.0016	-2.8419×10^{-4}	−0.0016
House (256×256)	Horizontal	−0.0021	2.7418×10^{-4}	−0.0021
	Vertical	−0.0041	0.0027	0.0040
	Diagonal	6.6665×10^{-4}	0.0056	−0.0017
Flowers (256×256)	Horizontal	−0.0028	−0.0040	−0.0078
	Vertical	-6.1750×10^{-4}	−0.0069	−0.0055
	Diagonal	−0.0027	−0.0023	0.0023
Jupiter moon (256×256)	Horizontal	0.0027	−0.0050	−0.0043
	Vertical	−0.0017	−0.0023	0.0017
	Diagonal	0.0035	−0.0020	−0.0044
Paints (256×256)	Horizontal	0.0058	−0.0070	-3.9824×10^{-4}
	Vertical	0.0043	0.0048	9.4416×10^{-4}
	Diagonal	−0.0023	-7.2946×10^{-4}	−0.0050
Ref. [18]	–	0.0024	−0.0029	−0.0015
Ref. [67]	–	0.0010	0.0054	0.0056
Ref. [69]	Horizontal	0.0693	0.0693	0.0693
	Vertical	0.0610	0.0610	0.0610
	Diagonal	−0.0242	−0.0242	−0.0242
Ref. [70]	Horizontal	−0.0221	−0.0221	−0.0221
	Vertical	−0.0074	−0.0074	−0.0074
	Diagonal	0.0075	0.0075	0.0075
Ref. [71]	Horizontal	−0.00147	0.00029	0.00262
	Vertical	0.00242	0.00072	−0.00192
	Diagonal	−0.00234	−0.00016	−0.00744

Table 6 Key sensitivity at Stage 1 of encryption

Key	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9
KS (%)	99.59	99.57	99.58	99.60	99.61	99.58	99.62	99.66	99.56

Table 7 Key sensitivity at Stage 2 of encryption

Key	Precision	K_{10}	K_{11}	K_{12}	K_{13}	K_{14}	K_{15}
KS (%)	10^{-2}	99.64	99.59	99.67	99.68	99.60	99.66
	10^{-4}	93.75	92.97	92.76	93.21	92.53	92.55

Table 8 Key sensitivity at Stage 3 of encryption

Key	K_{16}	K_{17}	K_{18}	K_{19}	K_{20}	K_{21}	K_{22}	K_{23}	K_{24}
KS (%)	99.63	99.60	99.61	99.62	99.59	99.61	99.57	99.58	99.62

$$\mathrm{KS} = \frac{1}{M \times N} \sum_{m=1}^{M} \sum_{n=1}^{N} C_1(m,n) \otimes C_2(m,n) \tag{24}$$

where C_1 and C_2 are two different ciphered images with the difference in any one of the keys,

$$C_1(m,n) \otimes C_2(m,n) = \begin{cases} 1, & C_1(m,n) \neq C_2(m,n) \\ 0, & C_1(m,n) = C_2(m,n) \end{cases} \tag{25}$$

The KS value for each key in all three stages of encryption is evaluated (for image Lena) as shown in Tables 6 (for Stage 1), 7 (for Stage 2), 8 (for Stage 3). The KS values are very close to 100% which clearly indicates that key sensitivity is extremely high at the encryption side. It has also

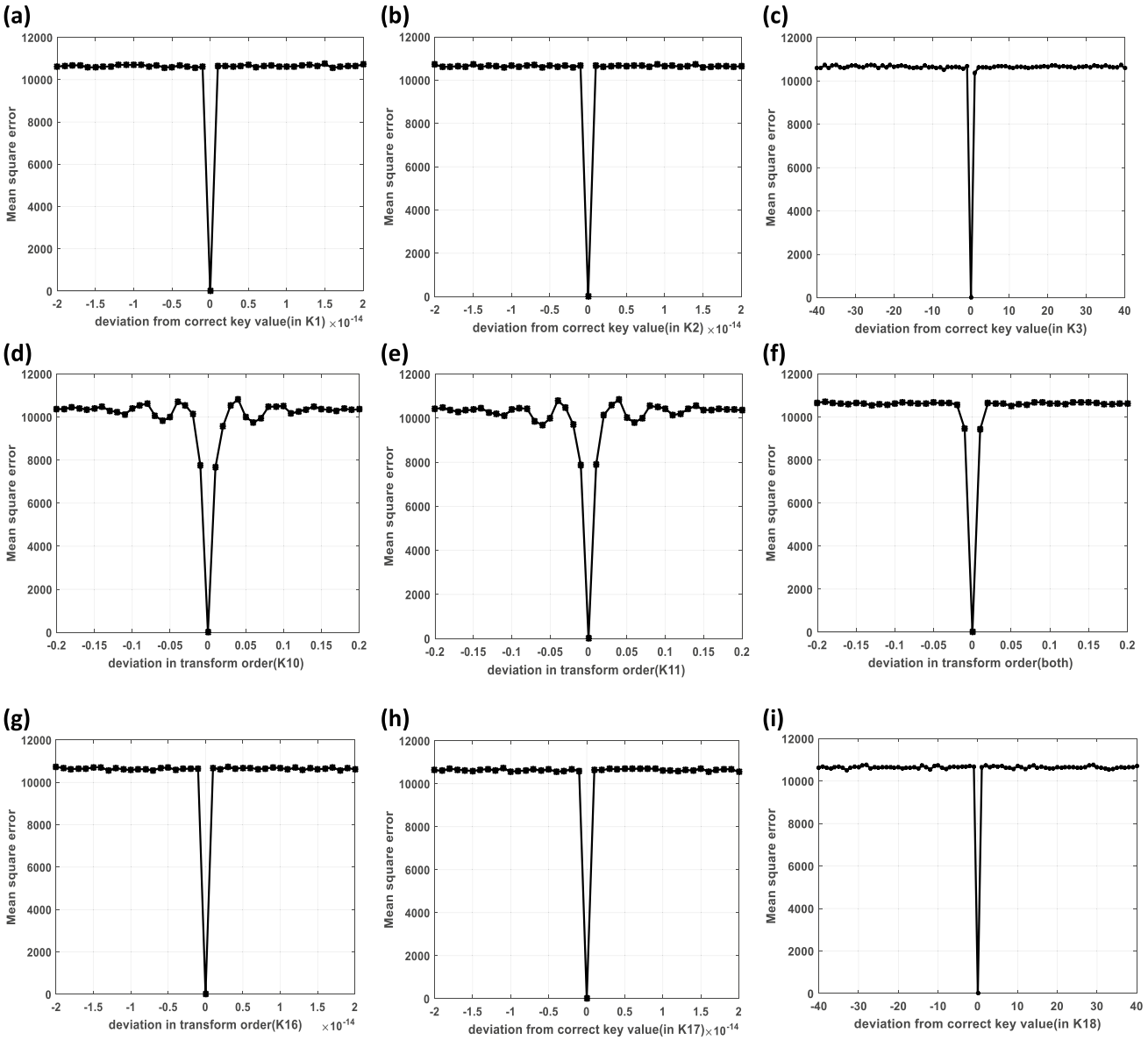

Fig. 8 MSE plots for deviation from correct values **a** for key $K1$, **b** for key $K2$, **c** for key $K3$, **d** for key $K10$, **e** for key $K11$, **f** for deviation in both ($K10$, $K11$) collectively, **g** for key $K16$, **h** for key $K17$, **i** for key K18

been observed that the key sensitivity of Stage 2 (transform stage) is evaluated at different precisions. The KS is a little less when a precision of 10^{-4} is used. This depicts that using only transform for decorrelating the pixels cannot provide optimum security and hence the addition of other security layers is essential.

At decryption, key sensitivity is measured in terms of MSE plots corresponding to deviation in each key over a range in close proximity. For this, each key value is little deviated by infinitesimally small values and the decrypted image is evaluated for its MSE with reference to the original image. It is observed while simulation that the recovery with each wrong key gives a completely random image. For avoiding any redundancy in results, the MSE plots for wrong keys are generated corresponding to each stage for the Red channel only (K_1–K_3: Stage 1,K_{10}–K_{11}: Stage 2, K_{16}–K_{18}: Stage 3). The reader may refer to Table 2 for the description of keys.

The MSE plots depict high sensitivity as there is an error of order of 10^4 with a deviation of as minute as an order of 10^{-15} in the key values for chaotic maps (keys K_1–K_3) as shown in Fig. 8a–c. For MSE plots of keys at stage 2, the values are deviated by 10^{-4} in transform order along x-direction (K_{10}) in Fig. 8d, along y-direction (K_{11}) in Fig. 8e and collectively for both (K_{10},K_{11}) in Fig. 8f . For MSE plots corresponding to keys at stage 3, deviation in key values (K_{16}, K_{17}, K_{18}) of an order of 10^{-15} is plotted and shown in Fig. 8g–i, respectively. It is observed that MSE plots of other channels are similar.

4.2.5 Information entropy analysis

Entropy refers to the measure of amount of information in any signal. For image, the amount of information entropy/Shannon entropy depends on the probability of occurrence of particular pixel intensity in the histogram. For a flat image, entropy is *zero* and for an encrypted image, its entropy is defined as the amount of uncertainty associated with the random image. The random variable can be a quantitative measure of any one of the pixel entities such as color, luminance, saturation, etc. Entropy is thus a statistical measure of randomness. For an image R with pixel values r_i, its entropy is explicitly defined as:

$$H(R) = -\sum_{i=1}^{M} p(r_i)\log_b p(r_i), \tag{26}$$

where p is the probability of occurrence of r_ith pixel; b is the base of log which can be e, 10 or 2. In an image with maximum n bits, $M = 2^n$, $b = 2$.

Recently, another measure for image randomness is introduced [73] which is coined as *local entropy measure*. It is based on Shannon entropy measure over local image pixels. Local entropy measure is able to overcome certain weaknesses of Shannon entropy measure. Some of proved weaknesses in [73] are unfair randomness comparisons for images of variant sizes, failure to distinguish image randomness before and after shuffling, inaccurate values in the case of synthesized images, etc.

Local entropy is the mean entropy of several nonoverlapping image blocks that are randomly selected from the source image. In order to differentiate from local entropy, Shannon entropy is termed as global entropy. Local entropy is evaluated over a certain number of nonoverlapping blocks (k) of image pixels (T_B), therefore termed as (k, T_B)-local entropy as:

Table 9 Entropy analysis for global (Shannon) and local entropy

Test image	Global entropy			Local entropy, $k = 30$, $T_B^{L=256} = 1936$		
	Red	Green	Blue	Red	Green	Blue
Lena	7.9837	7.9916	7.9550	7.8795	7.8889	7.8527
Baboon	7.9865	7.9918	7.9557	7.9615	7.9665	7.9306
Balls	7.9846	7.9919	7.9555	7.8834	7.8866	7.8534
Peppers	7.9679	7.9913	7.9565	7.9437	7.9669	7.9318
House	7.9857	7.9905	7.9550	7.8820	7.8851	7.8533
Flowers	7.9842	7.9914	7.9557	7.8819	7.8892	7.8521
Jupiter moon	7.9834	7.9917	7.9567	7.8794	7.8911	7.8534
Paint colors	7.9843	7.9915	7.9569	7.8820	7.8883	7.8541
Ref. [18]	7.3894	7.5280	7.5131	–	–	–
Ref. [74]	7.9938	7.9938	7.9938	–	–	–
Ref. [65]	7.7771	7.7190	7.7150	–	–	–
Ref. [75]	7.9901	7.9898	7.9899	–	–	–
Ref. [70]	7.8892	7.8892	7.8892	–	–	–

Comparison w.r.t. Lena image

$$\overline{H_{(k,T_B)}(S)} = \sum_{i=1}^{k} \frac{H(S_i)}{k} \tag{27}$$

where S_i are randomly selected nonoverlapping image blocks as S_1, S_2, S_3 … S_k and T_B are the number of pixels in each block, S_k. For image intensity level, $L=2$ (binary image), $T_B^{L=2} = 2$. Similarly, for $L=256$ $T_B^{L=256} = 1936$ and the total number of nonoverlapping blocks should not be less than 30 ($k \geq 30$).

The entropy analysis results of a few test plain images and their corresponding encrypted images are given in Table 9. The values of information entropy for the encrypted images are almost converging to a value of 7.9999, i.e., the highest possible value of information entropy for an 8-bit random image. The local entropy values are also evaluated, and it is observed that local entropy is close to global entropy. This ensures that the proposed scheme gives randomness in encrypted domain indicating a negligible information leakage and thus is secure against entropy attack.

4.2.6 Differential attack analysis

A differential attack is successful when an intruder is able to retrieve some clue about secret keys by slightly changing the plain image and comparing it with the encrypted image. In order to ensure robustness to such attack, it is required that a minute change in the plain image should be able to generate a huge difference in encrypted image. In other words, the diffusion of the system should be able to spread the difference over the entire image. There are two indicators that are used to quantify robustness to differential attack, NPCR (number of pixel change rate) and UACI (unified average change in intensity) [76, 77]. For a plain image with width W and height H,, let there be two ciphertexts generated (C_1, C_2) corresponding to the plain image and another with altered value at pixel location (i, j). These measures are mathematically defined as:

$$\text{NPCR} = \left(\frac{1}{WH}\right) \sum_{i=1}^{W} \sum_{j=1}^{H} D(i,j) \times 100\% \tag{28}$$

$$\text{where } D(i,j) = \begin{cases} 1, & C_1(i,j) \neq C_2(i,j) \\ 0, & \text{otherwise} \end{cases}$$

$$\text{UACI} = \frac{1}{WH}\left[\sum_{i=1}^{W} \sum_{j=1}^{H} \left|\frac{C_1(i,j) - C_2(i,j)}{L-1}\right|\right] \times 100\% \tag{29}$$

where $L=256$ for an 8-bit image. For a 256 Gy-level image encryption, the expected value of NPCR is 99.6094%, whereas that of UACI is 33.4635%. In the proposed scheme, we have modified a randomly selected pixel location (126, 137) for evaluating these parameters. The corresponding NPCR, UACI values are given in Table 10.

4.2.7 Classical attack analysis

There are four types of such attacks that include *ciphertext only attack* where it is assumed that the adversary has access to few ciphertext only [42], *plaintext attack* where it is assumed to have access to set of plaintext only, *known-plaintext attack* where knowledge of a set of plaintexts and corresponding ciphertext is available to the adversary and fourth is a *chosen-plaintext attack* where it is assumed that the adversary has access to set of plaintexts to be encrypted to obtain ciphertexts. As known ciphertext attack provides more information to an adversary, it is believed that if a ciphertext can resist a chosen ciphertext attack, it can also resist other types of attacks [78]. The proposed scheme is

Table 10 Differential attack analysis

Test images	NPCR (%)			UACI (%)		
	Red	Green	Blue	Red	Green	Blue
Lena	99.5605	99.5651	99.6613	34.7023	32.4410	34.4960
Baboon	99.5972	99.5827	99.6357	33.0327	33.8374	34.4669
Balls	99.6201	99.5590	99.5972	34.2801	31.9508	33.7173
Peppers	98.9708	99.5544	99.5770	31.2086	34.1040	34.4196
House	99.5728	99.5514	99.6140	34.4071	32.1189	34.3282
Flowers	99.6140	99.5743	99.5987	34.5727	34.2000	33.3969
Jupiter moon	99.6201	99.5621	99.5987	34.7109	32.5353	33.0210
Paint colors	99.6033	99.5895	99.5773	34.5705	33.2692	34.0478
Ref. [65]	99.7300	99.7300	99.7300	0	0	0
Ref. [68]	99.5600	99.5600	99.5600	31.1700	31.1700	31.1700
Ref. [69]	99.5697	99.5544	99.5789	33.4100	33.4549	33.4409
Ref. [70]	99.8953	99.8953	99.8953	33.7869	33.7869	33.7869
Ref. [71]	99.9900	99.9919	99.9980	33.3403	32.9525	33.3036

Comparison w.r.t. Lena image

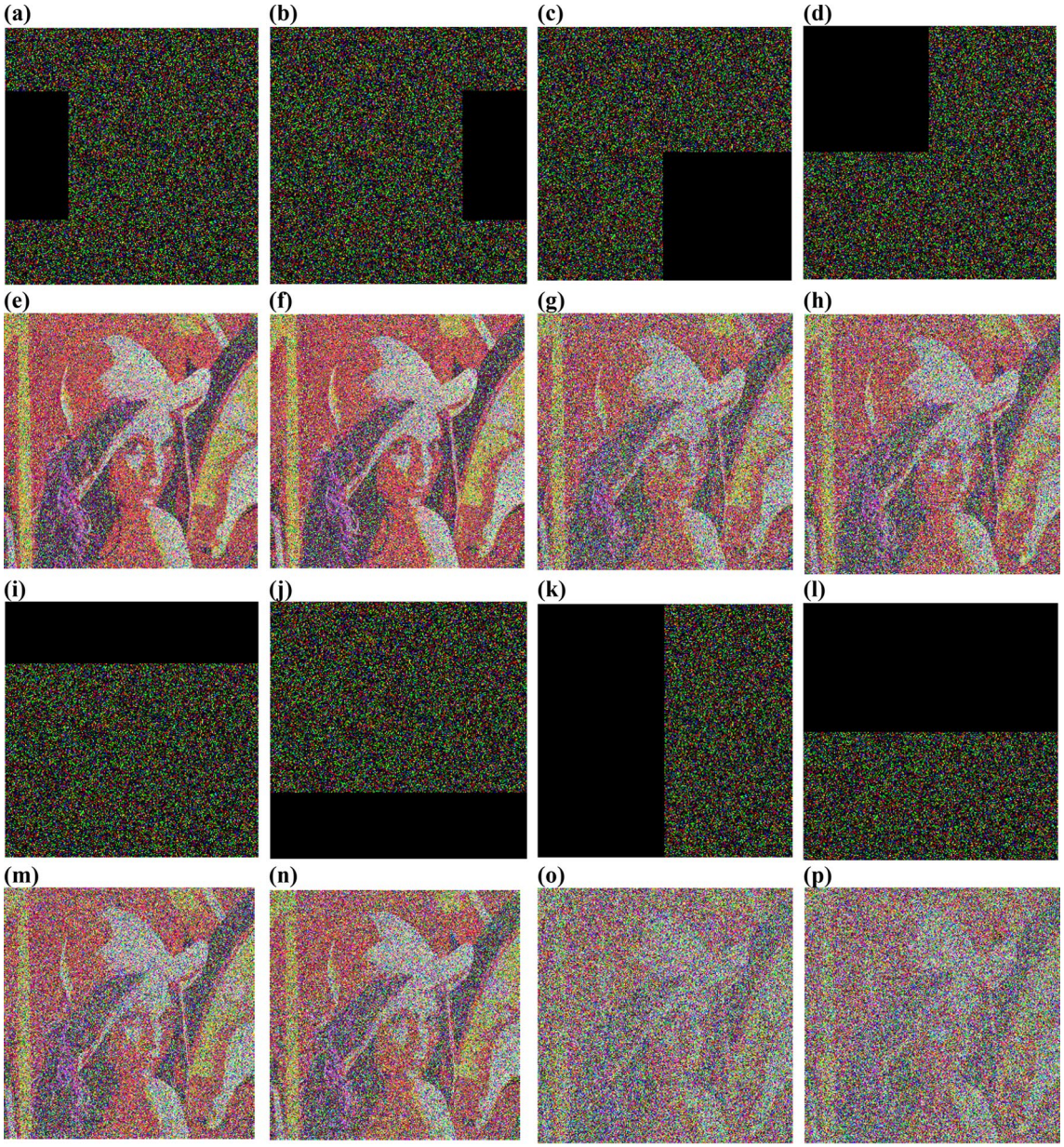

Fig. 9 Data occlusion attack analysis. The first and third rows show the encrypted images cropped from different locations, and second and fourth rows show the corresponding decrypted images with different visual clarity

Table 11 Averaged parameter values

Data occluded (%)	PSNR	MSE	SSIM
50	9.3565	7.35×10^3	0.0994
25	10.5519	5.75×10^3	0.2179
12.5	11.8733	5.00×10^3	0.2766

designed such that it is highly sensitive to keys. Moreover, the ciphertext is dependent on plaintexts as the initial conditions of the chaotic maps that are used in Stage 1 of encryption strongly depend on the plain input. Therefore, a unique ciphertext is generated corresponding to each plaintext. Hence, the proposed scheme is robust to the chosen ciphertext attack.

4.2.8 Data occlusion attack

There is a possibility of data loss while communicating images over heavy traffic channels or due to insecure channels. An effective encryption scheme should be able to recover the image even after occlusion attack if the data are uniformly diffused over the entire image. Post-processing techniques can be further used to recover the losses. To check the tolerance of the proposed scheme, encrypted data are subjected to varying amounts of data loss and corresponding decrypted images are checked for perceptual security. In Fig. 9, the first and third rows depict cropping in encrypted data (Lena image), whereas in the second and fourth rows corresponding decrypted images are shown. It is observed that image contour is still recoverable with up to 50% of data loss. The average values for data loss up to 12.5%, 25% and 50% are recorded in Table 11. The numerical values clearly indicate that the proposed scheme can resist data loss for recovery of the image which can be further improved by applying data post-processing techniques.

4.3 Noise attack analysis

Robustness against noise is an important index to check for the encryption scheme as distortion, degradation and corrupted data (coding error) are common in communication channels. The proposed scheme is checked for the addition of Gaussian noise with zero mean and varying variances to get data corresponding to different SNR (signal-to-noise ratio) between noisy and noise-free encrypted images. This can be mathematically explained as:

$$I_e' = I_e(1 + \sigma G)$$

where I_e' is noisy image I_e is the encrypted image, G represents the Gaussian noise with σ as its standard deviation. Figure 10 shows decrypted images when the encrypted images are distorted with different noise levels. The noise levels are quantified according to the SNR of noisy image with reference to encrypted image. MSE values are plotted for different SNR values. The plot clearly shows that error is proportional to the amount of noise in the encrypted domain.

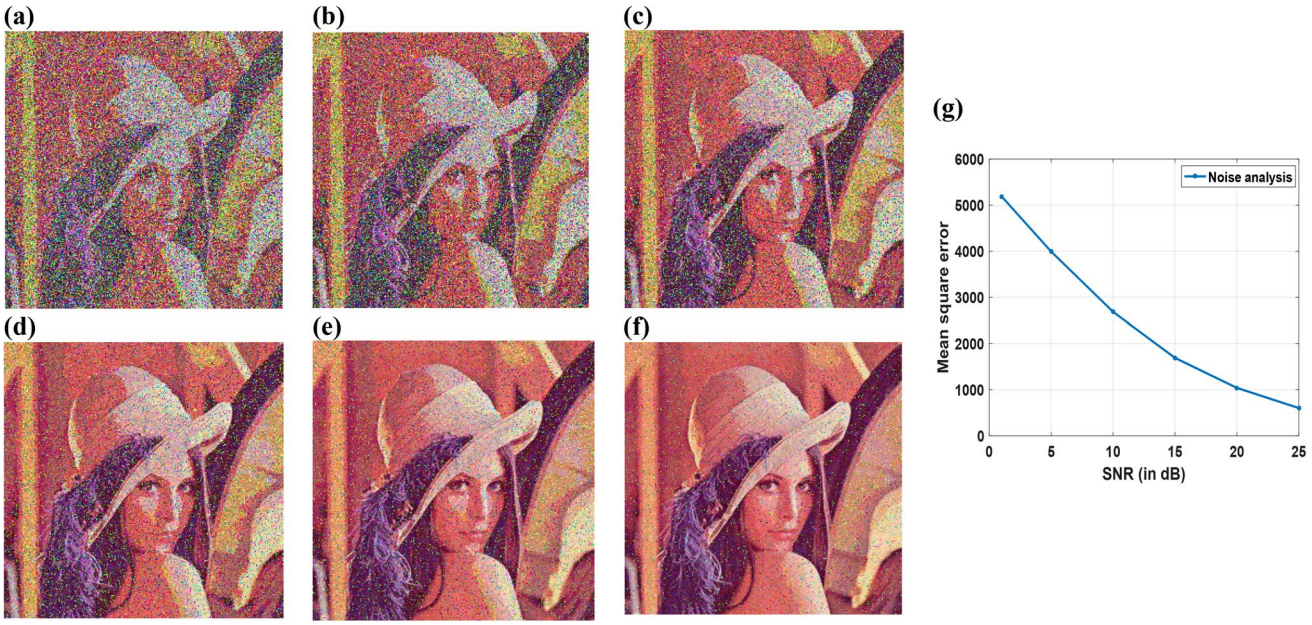

Fig. 10 Noise attack analysis. **a–f** are decrypted images with SNR of 1 dB, 5 dB, 10 dB, 15 dB, 20 dB and 25 dB, respectively. **g** is the corresponding plot of SNR vs. mean square error in decrypted image

Table 12 Time analysis for the encryption algorithm (time in s)

Image size	Our algorithm		Ref. [40]	Ref. [79]		
	Encryption	Decryption	Encryption	Encryption		
				DFrHT	MPFrHT-I	MPFrHT-II
256×256	0.49436	0.34984	0.601	4.1964	4.2432	1.8876
512×512	1.3408	1.0158	–	71.417	71.027	8.4616

Table 13 Comparative for keyspace analysis

Algorithm	Ref. [67]	Ref. [83]	Ref. [84]	Ref. [85]	Ref. [86]	Ref. [71]	Proposed
Keyspace	$2^{250} \approx 10^{75}$	4.2×10^{59}	10^{90}	$2^{129} \approx 10^{39}$	10^{165}	10^{98}	$10^{228} \approx 2^{757}$

Table 14 Comparison of averaged correlation coefficients

Algorithm	Horizontal	Vertical	Diagonal
Ref. [18]	0.0023	–	–
Ref. [67]	0.0010	0.0054	0.0056
Ref. [83]	0.0033	0.0027	0.0043
Ref. [84]	0.0014	0.0029	0.0038
Ref. [85]	0.0040	0.0011	0.0008
Ref. [71]	0.0015	0.0017	0.0033
Ref. [65]	0.0207	–	–
Ref. [79]	0.00063	–	–
Ref. [69]	0.0693	0.0610	0.0242
Proposed	0.0028	0.0050	0.0039

It is evident from Fig. 10 that image contour is detectable with as low as SNR of 1 dB, thereby giving testimony to the fact that the proposed scheme performs fair enough in a noisy environment and thus can resist noise attack.

4.3.1 Speed analysis

The run time of an encryption algorithm is an important issue for real-time applications. Optical transforms have an inherent property of fast and parallel processing. This is due to the optical setup that comprises SLM (for processing complex coefficients) and CCD (for storage). However, in the digital domain, the run time of an algorithm depends on the complexity associated with it. Therefore, a compromise between speed and complexity is highly desirable. The proposed scheme has multiple security layers for attaining substitution, transformation and permutation. The average encryption and decryption times are recorded in Table 12. It is likely to mention that run time can be further improved by optimization methods.

5 Comparative analysis

This section gives a brief summary on various comparisons of the proposed scheme with other similar state-of-the-art schemes. Firstly, by using a reality preserving algorithm [54], the complex computation is eliminated completely which is inherited in all DRPE and other optical transform domain-based encryption schemes [19, 21, 31, 36, 80, 81]. Another limitation in such similar schemes is the shorter key space, thereby leading to possibility of brute-force attack [28, 29, 82]. Table 13 lists some of the recent schemes with their key space for comparison with that of the proposed scheme.

On the bases of histogram analysis, the histogram in the encrypted domain with the proposed scheme is nearly uniform as compared to other similar schemes with optical transform domain [18, 19, 23, 40, 45, 64, 87]. The uniform histogram gives higher security against entropy attacks. A comparison of entropy values for RGB of image Lena is listed in Table 9.

Any encryption algorithm can be characterized by its decorrelating ability. For a comparison on this, Table 14 lists some of the recent published works in terms of their averaged correlation coefficients (with reference to Lena image).

Another important parameter for comparison is the decrypted image quality. To check, we have evaluated decryption error (DErr) as explained at the end of Sect. 4.2.2. DErr is 'zero' for all test images which clearly depicts that proposed scheme is lossless unlike some other recent schemes that are either fixed/single transform order-based [23, 40, 46, 65, 67, 86, 88] or others that are based on multiple parameters [43, 64, 74, 79, 89]. The PSNR of the decrypted image with reference to the original image (Lena image) is listed in Table 4. The proposed scheme is also robust to differential attacks as is evident from the analysis for NPCR and UACI values (Table 10).

6 Conclusion

Recently, many researchers have come up with image encryption schemes based on the optical transform domain. To overcome the limitations of shorter keyspace with the only transform-based approach, researchers have intertwined chaos and fractional transform domain in some way or other to get the benefit of both. Most of the schemes are focused on decorrelation based on fractional transform and chaos-based scrambling with different orders of their operation to improve security and also to enlarge the keyspace. However, these schemes fail to provide enough security due to certain limitations of the transform domain. The proposed scheme is based on three security layers with compound chaos-based substitution followed by decorrelation of pixels with a reality preserving fractional Hartley transform and another chaos-based permutation, thereby facilitating a lossless recovery at decryption. The proposed scheme is a novel method that not only enlarges the keyspace but also provides better robustness to most of the possible attacks. Security analysis and

comparative analysis collectively give testimony to the efficacy of the scheme.

References

1. Chen, G., Mao, Y., Chui, C.K.: A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons Fractals **21**(3), 749–761 (2004). https://doi.org/10.1016/j.chaos.2003.12.022
2. Chiaraluce, F., Ciccarelli, L., Gambi, E., Pierleoni, P., Reginelli, M.: A new chaotic algorithm for video encryption. IEEE Trans. Consum. Electron. **48**(4), 838–844 (2002). https://doi.org/10.1109/TCE.2003.1196410
3. Behnia, S., Akhshani, A., Mahmodi, H., Akhavan, A.: A novel algorithm for image encryption based on mixture of chaotic maps. Chaos Solitons Fractals **35**(2), 408–419 (2008). https://doi.org/10.1016/j.chaos.2006.05.011
4. Patidar, V., Pareek, N.K., Purohit, G., Sud, K.K.: A robust and secure chaotic standard map based pseudorandom permutation–substitution scheme for image encryption. Opt. Commun. **284**(19), 4331–4339 (2011). https://doi.org/10.1016/j.optcom.2011.05.028
5. Arroyo, D., Rhouma, R., Alvarez, G., Li, S., Fernandez, V.: On the security of a new image encryption scheme based on chaotic map lattices. Chaos Interdiscip. J. Nonlinear Sci. **18**(3), 033112 (2008). https://doi.org/10.1063/1.2959102
6. Alawida, M., Teh, J.S., Samsudin, A.: An image encryption scheme based on hybridizing digital chaos and finite state machine. Signal Process. **164**, 249–266 (2019). https://doi.org/10.1016/j.sigpro.2019.06.013
7. Alzaidi, A.A., Ahmad, M., Doja, M.N., Al Solami, E., Beg, M.S.: A new 1D chaotic map and β-Hill climbing for generating substitution-boxes. IEEE Access **6**, 55405–55418 (2018). https://doi.org/10.1109/ACCESS.2018.2871557
8. Zhou, Y., Hua, Z., Pun, C.M., Chen, C.P.: Cascade chaotic system with applications. IEEE Trans. Cybern. **45**(9), 2001–2012 (2015). https://doi.org/10.1109/ACCESS.2018.2871557
9. Lan, R., He, J., Wang, S., Gu, T., Luo, X.: Integrated chaotic systems for image encryption. Signal Process. **147**, 133–145 (2018). https://doi.org/10.1016/j.sigpro.2018.01.026
10. Zhang, Y.Q., Wang, X.Y., Liu, J., Chi, Z.L.: An image encryption scheme based on the MLNCML system using DNA sequences. Opt. Lasers Eng. **82**, 95–103 (2016). https://doi.org/10.1016/j.optlaseng.2016.02.002
11. Chai, X., Gan, Z., Chen, Y., Zhang, Y.: A visually secure image encryption scheme based on compressive sensing. Signal Process. **134**, 35–51 (2017). https://doi.org/10.1016/j.sigpro.2016.11.016
12. Refreiger, P., Javidi, B.: Optical image encryption based on input plane and Fourier plane random encoding. Opt. Lett. **20**(7), 767–769 (1995). https://doi.org/10.1364/OL.20.000767
13. Unnikrishnan, G., Singh, K.: Double random fractional Fourier domain encoding for optical security. Opt. Eng. **39**(11), 2853–2860 (2000). https://doi.org/10.1117/1.1313498
14. Wang, Q., Guo, Q., Lei, L., Zhou, J.: Iterative partial phase encoding based on joint fractional Fourier transform correlator adopting phase-shifting digital holography. Opt. Commun. **313**, 1–8 (2014). https://doi.org/10.1016/j.optcom.2013.09.058
15. Mendlovic, D., Ozaktas, H.M.: Fractional Fourier transforms and their optical implementation: I. JOSA **10**(9), 1875–1881 (1993). https://doi.org/10.1364/JOSAA.10.001875
16. Namias, V.: The fractional order fourier transform and its application to quantum mechanics. IMA J. Appl. Math. **25**(3), 241–265 (1980). https://doi.org/10.1093/imamat/25.3.241
17. Ozaktas, H.M., Arikan, O., Kutay, M.A., Bozdagt, G.: Digital computation of the fractional Fourier transform. IEEE Trans. Signal Process. **44**(9), 2141–2150 (1996). https://doi.org/10.1109/78.536672
18. Mishra, D.C., Sharma, R.K., Suman, S., Prasad, A.: Multi-layer security of color image based on chaotic system combined with RP2DFRFT and Arnold transform. J. Inf. Secur. Appl. **37**, 65–90 (2017). https://doi.org/10.1016/j.jisa.2017.09.006
19. Hwang, H.: Optical color image encryption based on the wavelength multiplexing using cascaded phase-only masks in Fresnel transform domain. Opt. Commun. **285**(5), 567–573 (2012). https://doi.org/10.1016/j.optcom.2011.11.007
20. Wang, Y., Quan, C., Tay, C.J.: Optical color image encryption without information disclosure using phase-truncated Fresnel transform and a random amplitude mask. Opt. Commun. **344**, 147–155 (2015). https://doi.org/10.1016/j.optcom.2015.01.045
21. 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. Opt. Lasers Eng. **75**, 17–26 (2015). https://doi.org/10.1016/j.optlaseng.2015.06.005
22. Abuturab, M.: Securing color image using discrete cosine transform in gyrator transform domain structured-phase encoding. Opt. Lasers Eng. **50**(10), 1383–1390 (2012). https://doi.org/10.1016/j.optlaseng.2012.04.011
23. Zhou, N., Wang, Y., Gong, L.: Novel optical image encryption scheme based on fractional Mellin transform. Opt. Commun. **284**(13), 3234–3242 (2011). https://doi.org/10.1016/j.optcom.2011.02.065
24. Vashisth, S., Singh, H., Yadav, A.K., Singh, K.: Image encryption using fractional Mellin transform, structured phase filters, and phase retrieval. Optik **125**(18), 5309–5315 (2014). https://doi.org/10.1007/978-981-13-1642-5_29
25. Bracewell, R.N.: Aspects of the Hartley transform. Proc. IEEE **82**(3), 381–387 (1994). https://doi.org/10.1109/5.272142
26. Liu, Z., Zhang, Y., Liu, W., Meng, F., Wu, Q., Liu, S.: Optical color image hiding scheme based on chaotic mapping and Hartley transform. Opt. Lasers Eng. **51**(8), 967–972 (2013). https://doi.org/10.1016/j.optlaseng.2013.02.015
27. Singh, N., Sinha, A.: Optical image encryption using improper Hartley transforms and chaos. Optik **121**(10), 918–925 (2010). https://doi.org/10.1016/j.ijleo.2008.09.049
28. Ghadirli, H.M., Nodehi, A., Enayatifar, R.: An overview of encryption algorithms in color images. Signal Process. **164**, 163–185 (2019). https://doi.org/10.1016/j.sigpro.2019.06.010
29. Chen, J., Bao, N., Li, J., Zhu, Z.L., Zhang, L.Y.: Cryptanalysis of optical ciphers integrating double random phase encoding with permutation. IEEE Access **5**, 16124–16129 (2017). https://doi.org/10.1109/ACCESS.2017.2735420
30. Singh, P., Yadav, A.K., Singh, K.: Known-Plaintext attack on cryptosystem based on fractional hartley transform using particle swarm optimization algorithm. In: Engineering Vibration, Communication and Information Processing, Singapore, pp. 317–327 (2019). https://doi.org/10.1007/978-981-13-1642-5_29
31. Kumar, P., Joseph, J. and Singh, K.: Double random phase encoding based optical encryption systems using some linear canonical transforms: weaknesses and countermeasures. In: Linear Canonical Transforms, pp. 367–396. Springer, New York (2016). https://doi.org/10.1007/978-1-4939-3028-9_13
32. Kathleen, T., Tim, D. and James, A.: Chaos: an introduction to dynamical systems. Physics Today, vol. 50, pp. 67–68. Publisher: Springer-Verlag, New York (1997). ISBN 3-540-78036-x
33. Alvarez, G., Li, S.: Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurc. Chaos **16**(8), 2129–2151 (2006). https://doi.org/10.1142/S0218127406015970

34. Huang, C.K., Nien, H.H.: Multi chaotic systems based pixel shuffle for image encryption. Opt. Commun. **282**(11), 2123–2127 (2009). https://doi.org/10.1016/j.optcom.2009.02.044
35. Teh, J.S., Alawida, M., Sii, Y.C.: Implementation and practical problems of chaos-based cryptography revisited. J. Inf. Secur. Appl. **50**, 102421 (2020). https://doi.org/10.1016/j.jisa.2019.102421
36. Zhang, Y., Xiao, D.: Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform. Opt. Lasers Eng. **51**(4), 472–480 (2013). https://doi.org/10.1016/j.optlaseng.2012.11.001
37. Li, H., Wang, Y.: Double-image encryption based on discrete fractional random transform and chaotic maps. Opt. Lasers Eng. **49**(7), 753–757 (2011). https://doi.org/10.1016/j.optlaseng.2011.03.017
38. Singh, N., Sinha, A.: Gyrator transform-based optical image encryption, using chaos. Opt. Lasers Eng. **47**(5), 539–546 (2009). https://doi.org/10.1016/j.optlaseng.2008.10.013
39. Wu, J., Guo, F., Liang, Y., Zhou, N.: Triple color images encryption algorithm based on scrambling and the reality-preserving fractional discrete cosine transform. Optik **125**(16), 4474–4479 (2014). https://doi.org/10.1016/j.ijleo.2014.02.026
40. Singh, P., Yadav, A.K., Singh, K.: Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition. Opt. Lasers Eng. **91**, 187–195 (2017). https://doi.org/10.1016/j.optlaseng.2016.11.022
41. Li, C., Li, S., Asim, M., Nunez, J., Alvarez, G., Chen, G.: On the security defects ofan image encryption scheme. Image Vis. Comput. **27**(9), 1371–1381 (2009). https://doi.org/10.1016/j.imavis.2008.12.008
42. Chang, X., Yan, A., Zhang, H.: Ciphertext-only attack on optical scanning cryptography. Opt. Lasers Eng. **126**, 105901 (2020). https://doi.org/10.1016/j.optlaseng.2019.105901
43. Lang, J.: Image encryption based on the reality-preserving multiple-parameter fractional Fourier transform and chaos permutation. Opt. Lasers Eng. **50**(7), 929–937 (2012). https://doi.org/10.1016/j.optlaseng.2012.02.012
44. Sui, L., Duan, K., Liang, J., Zhang, Z., Meng, H.: Asymmetric multiple-image encryption based on coupled logistic maps in fractional Fourier transform domain. Opt. Lasers Eng. **62**, 139–152 (2014). https://doi.org/10.1016/j.optlaseng.2014.06.003
45. Ran, Q., Yuan, L., Zhao, T.: Image encryption based on nonseparable fractional Fourier transform and chaotic map. Opt. Commun. **348**, 43–49 (2015). https://doi.org/10.1016/j.optcom.2015.03.016
46. Kaur, G., Agarwal, R., Patidar, V.: Multiple image encryption with fractional Hartley transform and robust chaotic mapping. In: 6th International Conference on Signal Processing and Integrated Networks (SPIN), pp. 399–403. IEEE (2019). https://doi.org/10.1109/SPIN.2019.8711777
47. McBride, A.C., Kerr, F.H.: On Namias's fractional Fourier transforms. IMA J. Appl. Math. **39**(2), 159–175 (1987). https://doi.org/10.1093/imamat/39.2.159
48. Condon, E.: Theories of optical rotatory power. Rev. Mod. Phys. **9**(4), 432 (1937). https://doi.org/10.1103/RevModPhys.9.432
49. Ozaktas, H.M., Mendlovic, D.: Fractional Fourier transforms and their optical implementation II. JOSA A **10**(12), 2522–2531 (1993). https://doi.org/10.1364/JOSAA.10.002522
50. Almeida, L.B.: The fractional Fourier transform and time-frequency representations. IEEE Trans. Signal Process. **42**(11), 3084–3091 (1994). https://doi.org/10.1109/78.330368
51. Pei, S.C., Tseng, C.C., Yeh, M.H., Shyu, J.J.: Discrete fractional Hartley and Fourier transforms. IEEE Trans. Circuits Syst. II Analog Digit. Signal Process. **45**(6), 665–675 (1998). https://doi.org/10.1109/82.686685
52. Pei, S.C., Ding, J.J.: Fractional cosine, sine, and Hartley transforms. IEEE Trans. Signal Process. **50**(7), 1661–1680 (2002). https://doi.org/10.1109/TSP.2002.1011207
53. Zhao, D., Li, X., Chen, L.: Optical image encryption with redefined fractional Hartley transform. Opt. Commun. **281**(21), 5326–5329 (2008). https://doi.org/10.1016/j.optcom.2008.07.049
54. Venturini, I., Duhamel, P.: Reality preserving fractional transforms [signal processing applications]. In: Acoustics, Speech, and Signal Processing 5(V-205), France (2004). https://doi.org/10.1109/ICASSP.2004.1327083
55. Shannon, C.E.: Communication theory of secrecy systems. Bell Syst. Tech. J. **28**(4), 656–715 (1949). https://doi.org/10.1002/j.1538-7305.1949.tb00928.x
56. Zhou, L.H., Feng, Z.J.: A new idea of using one-dimensional PWL map in digital secure communications-dual-resolution approach. IEEE Trans. Circuits Syst. II Analog Digit. Signal Process. **47**(10), 1107–1111 (2000). https://doi.org/10.1109/82.877154
57. Li, S., Chen, G., Mou, X.: On the dynamical degradation of digital piecewise linear chaotic maps. Int. J. Bifurc. Chaos **15**(10), 3119–3151 (2005). https://doi.org/10.1142/S0218127405014052
58. Zhou, Y., Bao, L., Chen, C.P.: A new 1D chaotic system for image encryption. Signal Process. **97**, 172–182 (2014). https://doi.org/10.1016/j.sigpro.2013.10.034
59. May, R.M.: Simple mathematical models with very complicated dynamic. Nature **261**(5560), 459 (1976)
60. Al-Shameri, W.F.H., Mahiub, M.A.: Some dynamical properties of the family of tent maps. Int. J. Math. Anal. **7**(29), 1433–1449 (2013). https://doi.org/10.12988/ijma.2013.3361
61. Weber, A.G.: The USC-SIPI image database version 5. USC-SIPI Report, 315(1) (1997)
62. Talhaoui, M.Z., Wang, X., Talhaoui, A.: A new one-dimensional chaotic map and its application in a novel permutation-less image encryption scheme. Vis. Comput. (2020). https://doi.org/10.1007/s00371-020-01936-z
63. Wang, Z., Bovik, A.C., Sheikh, H.R., Simoncelli, E.P.: Image quality assessment: from error visibility to structural similarity. IEEE Trans. Image Process. **13**(4), 600–612 (2004). https://doi.org/10.1109/TIP.2003.819861
64. Azoug, S.E., Bouguezel, S.: A non-linear preprocessing for optodigital image encryption using multiple-parameter discrete fractional Fourier transform. Opt. Commun. **359**, 85–94 (2016). https://doi.org/10.1016/j.optcom.2015.09.054
65. Faragallah, O.S., Alzain, M.A., El-Sayed, H.S., Al-Amri, J.F., El-Shafai, W., Afifi, A., Naeem, E.A., Soh, B.: Block-based optical color image encryption based on double random phase encoding. IEEE Access **7**, 4184–4194 (2019). https://doi.org/10.1109/ACCESS.2018.2879857
66. Murillo-Escobar, M.A., Cruz-Hernández, C., Abundiz-Pérez, F., López-Gutiérrez, R.M., Del Campo, O.A.: A RGB image encryption algorithm based on total plain image characteristics and chaos. Signal Process. **109**, 119–131 (2015). https://doi.org/10.1016/j.sigpro.2014.10.033
67. Souyah, A., Faraoun, K.M.: An image encryption scheme combining chaos-memory cellular automata and weighted histogram. Nonlinear Dyn. **86**(1), 639–653 (2016). https://doi.org/10.1007/s11071-016-2912-0
68. Jain, R., Sharma, J.B.: Symmetric color image encryption algorithm using fractional DRPM and chaotic baker map. In: IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT) (2016). https://doi.org/10.1109/RTEICT.2016.7808152
69. Farah, M.B., Guesmi, R., Kachouri, A., Samet, M.: A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation. Opt. Laser Technol. **121**, 105777 (2020). https://doi.org/10.1016/j.optlastec.2019.105777

70. Li, G.: Double chaotic image encryption algorithm based on optimal sequence solution and fractional transform. Vis. Comput. **35**(9), 1267–1277 (2019). https://doi.org/10.1007/s00371-018-1574-y
71. Kang, X., Ming, A., Tao, R.: Reality-preserving multiple parameter discrete fractional angular transform and its application to color image encryption. IEEE Trans. Circuits Syst. Video Technol. **29**(6), 1595–1607 (2018). https://doi.org/10.1109/TCSVT.2018.2851983
72. Lian, S.: Multimedia content encryption: techniques and applications. Auerbach Publication, Taylor & Francis Group (2008). ISBN-13: 978-1-4200-6527-5
73. Wu, Y., Zhou, Y., Saveriades, G., Agaian, S., Noonan, J.P., Natarajan, P.: Local Shannon entropy measure with statistical tests for image randomness. Inf. Sci. **222**, 323–342 (2013). https://doi.org/10.1016/j.ins.2012.07.049
74. Kaur, G., Agarwal, R., Patidar, V.: Chaos based multiple order optical transform for 2D image encryption. Eng. Sci. Technol. Int. J. **23**(5), 998–1014 (2020). https://doi.org/10.1016/j.jestch.2020.02.007
75. Liu, H., Kadir, A.: Asymmetric color image encryption scheme using 2D discrete-time map. Signal Process. **113**, 104–112 (2015). https://doi.org/10.1016/j.aeue.2014.02.002
76. Wu, Y., Noonan, J.P., Agaian, S.: NPCR and UACI randomness tests for image encryption. Cyber J. Multidiscip. J. Sci. Technol. J. Sel. Areas Telecommun. (JSAT) **1**(2), 31–38 (2011)
77. Tong, X.J., Zhang, M., Wang, Z., Liu, Y., Xu, H., Ma, J.: A fast encryption algorithm of color image based on four-dimensional chaotic system. J. Vis. Commun. Image Represent. **33**, 219–234 (2015). https://doi.org/10.1016/j.jvcir.2015.09.014
78. Wang, X.Y., Li, P., Zhang, Y.Q., Liu, L.Y., Zhang, H., Wang, X.: A novel color image encryption scheme using DNA permutation based on the Lorenz system. Multimed. Tools Appl. **77**(5), 6243–6265 (2018). https://doi.org/10.1007/s11042-017-4534-z
79. Kang, X., Tao, R., Zhang, F.: Multiple-parameter discrete fractional transform and its applications. IEEE Trans. Signal Process. **64**(13), 3402–3417 (2016). https://doi.org/10.1109/TSP.2016.2544740
80. Liu, Z., Xu, L., Lin, C., Dai, J., Liu, S.: Image encryption scheme by using iterative random phase encoding in gyrator transform domains. Opt. Lasers Eng. **49**(4), 542–546 (2011). https://doi.org/10.1016/j.optlaseng.2010.12.005
81. Zhou, N., Li, H., Wang, D., Pan, S., Zhou, Z.: Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform. Opt. Commun. **343**, 10–21 (2015). https://doi.org/10.1016/j.optcom.2014.12.084
82. Ran, Q., Zhang, H., Zhang, J., Tan, L., Ma, J.: Deficiencies of the cryptography based on multiple-parameter fractional Fourier transform. Opt. Lett. **34**(11), 1729–1731 (2009). https://doi.org/10.1364/OL.34.001729
83. Liu, H., Kadir, A., Niu, Y.: Chaos-based color image block encryption scheme using S-box. AEU-Int. J. Electron. Commun. **68**(7), 676–686 (2014). https://doi.org/10.1016/j.sigpro.2015.01.016
84. Wu, X., Kan, H., Kurths, J.: A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps. Appl. Soft Comput. **37**, 24–39 (2015). https://doi.org/10.1016/j.asoc.2015.08.008
85. Enayatifar, R., Sadaei, H.J., Abdullah, A.H., Lee, M., Isnin, I.F.: A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata. Opt. Lasers Eng. **71**, 33–41 (2015). https://doi.org/10.1016/j.optlaseng.2015.03.007
86. Hu, G., Kang, X., Guo, Z., Luo, X.: A novel image encryption scheme based on hidden random disturbance and feistel RPMPFrHT network. In: Chinese Conference on Image and Graphics Technologies. Springer, Singapore (2018). https://doi.org/10.1007/978-981-13-1702-6_25
87. Hennelly, B., Sheridan, J.T.: Optical image encryption by random shifting in fractional Fourier domains. Opt. Lett. **28**(4), 269–271 (2003). https://doi.org/10.1364/OL.28.000269
88. Sui, L., Gao, B.: Single-channel color image encryption based on iterative fractional Fourier transform and chaos. Opt. Laser Technol. **48**, 117–127 (2013). https://doi.org/10.1016/j.optlastec.2012.10.016
89. Shan, M., Chang, J., Zhong, Z., Hao, B.: Double image encryption based on discrete multiple-parameter fractional Fourier transform and chaotic maps. Opt. Commun. **285**(21–22), 4227–4234 (2012). https://doi.org/10.1016/j.optcom.2012.06.023

Gurpreet Kaur obtained her Master of Technology in Signal and Image processing from Guru Gobind Singh Indraprastha University, New Delhi. Currently, she is pursuing her Ph.D. at University School of Information, Communication and Technology, Guru Gobind Singh Indraprastha University, New Delhi, India. She has more than 11 years of teaching experience. Her research interests are signal and image processing, fractional transforms and their application in encryption and watermarking, chaos theory and image encryption.

Rekha Agarwal received the B.Eng. (Electronics and Communication) from Madhav Institute of Technology and Science, Jiwaji University, Gwalior, M.P., India, M.Eng. (Communications) from Malaviya National Institute of Technology, Jaipur, Rajasthan, and Ph.D. From Guru Gobind Singh Indraprastha University, New Delhi, India. At present, she is working as Professor, Department of ECE at Amity School of Engg. and Tech., New Delhi. Her research interest lies in the area of wireless communications, coding techniques, antenna arrays, etc.

Vinod Patidar is working as Professor and Head of Physics at Sir Padampat Singhania University (SPSU), Udaipur, India, since September 01, 2015. He is also Dean Research of the University. Prior to his present position, he has served as Associate Dean Research (October 2018–January 2019), Associate Professor & Head (2011–2015) and Assistant Professor (2008–2011) at SPSU, Senior Lecturer (2007–2008) and Lecturer (2005–2007) in the Department of Physics, Banasthali University, Banasthali, India. He has about 20 years of research and teaching experience. He received his M.Sc. (Physics) degree with the University Gold Medal in 1999 and completed the Doctoral Research (Ph.D.) in the field of Nonlinear Dynamics with a National Level Fellowship (JRF & SRF-UGC) in 2004 from M. L. S. University, Udaipur, India. He has published one research monograph and more than 70 research papers in various refereed international/national journals and conference proceedings. He has been the reviewer of research articles submitted to 30 international journals. His present research interests include bifurcation & chaos in classical systems, control & synchronization of chaos, dynamical behavior of q-deformed nonlinear dynamical systems, applications of chaotic dynamical systems in the development of secure cryptosystems & their crypt-analysis and theoretical studies of electron atom/ion collisions.