*Optica Applicata, Vol. LIV, No. 4, 2024*
DOI: 10.37190/oa/194974

# Non-linear cryptosystem utilizing biological mutation operation in the two-dimensional non-separable linear canonical transform domain

Bhavana Sharma[1], Hukum Singh[2,*], Pankaj Rakheja[1], Mehak Khurana[3]

[1] Department of Computer Science & Engineering, The NorthCap University, Gurugram, India 122017

[2] Department of Applied Sciences, The NorthCap University, Gurugram, India 122017

[3] Department of Information Technology, Ahlia University, Manama, Bahrain

[*] Corresponding author email: hukumsingh@ncuindia.edu

This paper introduces a novel image encryption algorithm in the 2D-NSCT domain, employing a 4D hyperchaotic mapping, DNA coding with biological mutation, and the phase truncation and Fourier transfrom (PTFT) operation. Unlike existing DNA-based encryption methods that heavily rely on the XOR operator, our proposed scheme integrates a biological mutation operator to enhance the security of the encryption process. The performance and effectiveness of our cryptosystem are thoroughly evaluated through comprehensive experiments and analysis on various grayscale images, including *Cameraman*, *Peppers*, and *Baboon* images. Simulation results are presented in this paper to demonstrate the performance of the proposed encryption algorithm. Notably, our algorithm exhibits high sensitivity to encryption parameters, and the utilization of DNA coding and PTFT adds an extra layer of security to the image encryption algorithm. To assess the resilience of our proposed algorithm, we conducted thorough simulations and subjected it to various challenges, including statistical attacks, noise attacks, occlusion attacks, classical cryptographic attacks, and special iterative attacks for asymmetric schemes, and along with brute-force attacks. The results validate the resilience of our proposed scheme and showcase its ability to withstand existing cryptographic attacks. Moreover, a comparative analysis was conducted to evaluate the performance of our proposed scheme against existing encryption algorithms of similar nature. The outcomes of this study clearly demonstrate that our encryption algorithm surpasses these existing schemes in terms of effectiveness and resilience against cryptographic attacks, affirming its superiority.

Keywords: PSNR, MSE, 2D-NSLCT, Matric, cryptographic attacks.

## 1. Introduction

In the present era of digital advancements, safeguarding the security of communication and image data has become paramount. With the continuous evolution of technology, the strategies employed to ensure secure transmission and storage of data have also progressed. Consequently, protecting data from unauthorized access by hackers has emerged as a significant apprehension. Images and videos often serve as repositories for crucial information, intensifying the importance of image security. Traditional techniques such as picture encryption and watermarking play crucial roles in fortifying the security of images. Various conventional digital methods for encrypting images, such a, data encryption standard (DES), advance encryption standard (AES) and many others, have been proposed in past, but these are computationally intensive, have cumbersome key management, inadequate key length and susceptible to attacks. In response to these challenges, researchers have proposed alternative methods for picture encryption, including optical image encryption. Optical image encryption offers several advantages such as parallel processing, simplified calculations, reduced power consumption, and the utilization of multivariate encryption parameters. These properties enhance the efficiency and effectiveness of encrypting images optically. The pioneering work in optical image encryption, known as double random phase encoding (DRPE), was first introduced by Refregier and Javidi in 1995. Optical encryption techniques for grayscale images have been successfully achieved using the Fourier domain, specifically in the context of double random phase encoding (DRPE). Javidi *et al.* made significant advancements in enhancing the security of DRPE in 1997, 1999, and 2000 [1-4]. Building upon DRPE, various optical image encryption algorithms have been proposed in alternative domains. In 2006, Peng *et al.* revealed vulnerabilities to known plaintext attacks in the DRPE [4-6]. Subsequently, Unnikrishnan *et al.* introduced the concept of DRPE in the fractional Fourier domain [7]. This paved the way for the development of image encryption algorithms based on double random phase encoding in different transforms domain, including Fresnel, fractional Fourier, Gyrator, fractional Mellin transform, and fractional Hartley domain [8-14].

To further enhance the security of image encryption techniques, chaotic maps have been used as they exhibit characteristics such as sensitivity to initial parameters, unpredictability, and ergodicity. The picture scrambling technique is effective in minimizing the correlation between neighboring pixels, and chaotic systems have proven to be valuable in achieving this. Numerous researchers have employed chaotic maps in their image encryption schemes for making it more robust and secure [11,15-20]. Various types of chaotic systems [21], 2D logistic maps [22], chaotic Baker map [23,24], and fractional Fourier transform [25], have been utilized by researchers for this purpose. Implementing chaotic systems not only increases the uncertainty in the resulting ciphertext picture but also expands the key space, enhancing the overall security of the encryption process.

Later in order to resolve issues of key management, the researcher proposed switch to asymmetric cryptosystems, where different encryption and decryption keys were utilized. Several techniques commonly used in optical image encryption include equal modulus decomposition (EMD), random modulus decomposition (RMD), unequal modulus decomposition (UMD), phase truncation and phase reservation. Subsequent investigations revealed vulnerabilities in equal modulus decomposition (EMD), random modulus decomposition (RMD), and unequal modulus decomposition (UMD) techniques, proving them susceptible to various types of attacks [26,27].

DNA, short for deoxyribonucleic acid, is a biological molecule that carries the genetic information of all living organisms. DNA encryption exhibits unique qualities, including low power consumption, vast storage capacity, and the ability for parallel processing. These distinctive attributes of DNA have captured the attention and interest of cryptographers, who recognize its potential for advancing the field of encryption [28]. In 1999, CLELLAND *et al.* introduced a method for concealing information in DNA microdots [29], marking a significant advancement in the realm of cryptography. This approach opened new possibilities in the field. In 2010, ZHANG *et al.* developed an image encryption technique that utilized DNA and a chaotic map [30]. In this approach, DNA addition was utilized for diffusion while a chaotic map was employed for permutation. Following that, numerous image encryption algorithms were proposed, incorporating DNA and permutation techniques such as chaos, hyper chaos, wavelets, and entropy [31-34]. It has also been demonstrated that DNA-based picture cryptosystems are subject to cryptographic attacks [21-24].

In order to bolster security measures, double and multilayer image encryption techniques have been adopted. Various approaches have been developed for double image encryption, including methods based on random phase encoding in fractional Fourier transform [25] and two-coupled logistic maps in discrete multiple parameter fractional angular transform [35], Arnold transform and discrete fractional angular transform [36], and phase retrieval algorithm with 2D non-separable linear canonical transform [37]. These techniques aim to fortify the encryption process by incorporating multiple layers and diverse transformations, providing added layers of complexity and security to the encryption of images.

In the proposed mechanism, the above analysis has been used and 4D hyperchaotic mapping, DNA encoding, bio-inspired mutations operations, phase truncated Fourier transform in 2D-NSLCT transform domain have been utilized. This scheme is designed with an asymmetric nature, effectively addressing key management concerns. The manuscript is structured into different sections. Section 2 provides an overview of the techniques utilized, such as DNA encoding and decoding rules, biological mutation operations, 2D non-separable linear canonical transform, 4D hyperchaotic system, and phase truncation and reservation operations, with detailed mathematical explanations. The encryption and decryption procedures are discussed in Section 3. Section 4 presents simulation and result analysis for the proposed scheme. In Section 5 statistical analyses comprising of information entropy, histogram and 3D plot analysis and correlation distribution analysis have been carried out. The robustness of the proposed scheme against various attacks and key sensitivity analysis are investigated and explored in Section 6. Finally, Section 7 concludes the manuscript by summarizing the overall work accomplished.

## 2. Overview

### 2.1. Deoxyribonucleic acid

DNA, short for Deoxyribonucleic acid, is a crucial molecule present in the cells of all living organisms. It serves as the carrier of genetic information, passing it down from one generation to the next. The structure of DNA is composed of a double helix, with four nucleotides, namely Adenine (A), Guanine (G), Cytosine (C), and Thymine (T), forming the building blocks. These nucleotides exhibit a specific pattern of base pairing: A always bonds with T, and C always bonds with G. This base pairing can be likened to the complementary nature of binary digits (0 s and 1s) used in computer programming. In fact, the four nucleotides in DNA can be represented using binary digits according to specific rules outlined in Table 1.

Table 1 [38] outlines a set of guidelines for converting binary digits (0 and 1) into their corresponding DNA sequences. These guidelines enable the translation of binary sequences into DNA sequences. For example, according to rule 1, a binary sequence of 01 corresponds to the DNA sequence G. Similarly, applying rule 5 translates a binary sequence of 1011 into the DNA sequence AC. Rule 8 allows the conversion of 0010 into CT in DNA. These conversion rules are universally applicable to any binary sequence and are presented comprehensively in Table 1, including their respective DNA sequences.

Conversely, by referring to the decoding rule outlined in Table 1, DNA sequences can be translated back into binary numbers. For instance, utilizing rule 1, a DNA sequence of G can be converted into the binary sequence 01. Similarly, applying rule 5 translates a DNA sequence of AC into the binary sequence 1011. By following rule 8, a DNA sequence of CT can be converted into the binary sequence 0010. The instructions provided in Table 1 can be used to convert other DNA sequences into their corresponding binary numbers as well.

### 2.2. Biological mutation operations

Mutations are errors that occur during the process of cell division and DNA replication. These mistakes, known as mutation operations, can cause alterations in the order of

Table 1. DNA encoding and decoding rules [38].

| | 00 | 10 | 01 | 11 |
|---|---|---|---|---|
| Rule 1 | A | C | G | T |
| Rule 2 | A | G | C | T |
| Rule 3 | T | G | C | A |
| Rule 4 | T | C | G | A |
| Rule 5 | G | A | T | C |
| Rule 6 | G | T | A | C |
| Rule 7 | C | A | T | G |
| Rule 8 | C | T | A | G |

genetic information. In biological cells, mutations can have significant effects. This research explores various types of mutations, including duplication, insertion, deletion, and substitution. Deletion involves the removal of one or more DNA bases, leading to a change in the reading frame and resulting in a completely new DNA base sequence. On the contrary, insertion involves the addition of one or more DNA bases, which modifies the DNA sequence and leads to a frame shift mutation. Substitution, on the other hand, occurs when one or more DNA bases are replaced with different bases, resulting in a point mutation. Additionally, duplication refers to the replication of one or more DNA bases within the sequence. To demonstrate the impact of mutations, we applied the DNA encoding and decoding rules outlined in Table 1 to a grayscale image pixel with an arbitrary value of 197. On applying DNA encoding rule 1 DNA sequence obtained is TAGG. Now on applying DNA deletion, insertion, substitution, and duplication techniques the sequence obtained is TAG, TAGGC, TGAG and TGAGG, respectively. On decoding the above sequences, the decimal values attained are 49, 790, 209 and 837 individually.

## 2.3. 2D non-separable linear canonical transform

The two-dimensional non-separable linear canonical transform (2D NS-LCT) is an integral transform with enhanced capabilities. It introduces four additional cross-parameters that establish connections between the two dimensions, effectively expanding the number of free parameters to ten. The continuous form of the 2D NS-LCT [37,39,40] for a signal $f(x, y)$ is mathematically defined by

$$\begin{aligned} F(x', y') &= L_{\mathrm{M}}\{f(x, y)\}(x', y') \\ &= \frac{1}{\sqrt{j\det(B)}} \iint_{-\infty}^{\infty} \exp\left(\frac{j\pi(k_1 x'^2 + k_2 x'y' + k_3 y'^2)}{\det(B)}\right) \\ &\quad \times \exp\left(\frac{j2\pi\left[(-b_{22}x' + b_{12}y')x + (b_{21}x' - b_{11}y')y\right]}{\det(B)}\right) \\ &\quad \times \exp\left(\frac{j\pi(p_1 x^2 + p_2 xy + p_3 y^2)}{\det(B)}\right) f(x, y)\,\mathrm{d}x\,\mathrm{d}y \end{aligned} \tag{1}$$

where

$$k_1 = d_{11}b_{22} - d_{12}b_{21} \tag{2a}$$

$$k_2 = 2(-d_{11}b_{22} + d_{12}b_{11}) \tag{2b}$$

$$k_3 = -d_{21}b_{12} + d_{22}b_{11} \tag{2c}$$

$$p_1 = a_{11}b_{22} - a_{21}b_{12} \tag{2d}$$

$$p_2 = 2(a_{12}b_{22} - a_{22}b_{12}) \tag{2e}$$

$$p_3 = -a_{12}b_{21} + a_{22}b_{11} \tag{2f}$$

The system's transform matrix can be expressed as

$$M = \begin{bmatrix} a_{11} & a_{21} & b_{11} & b_{21} \\ a_{21} & a_{22} & b_{21} & b_{22} \\ c_{11} & c_{21} & d_{11} & d_{21} \\ c_{21} & c_{22} & d_{21} & d_{22} \end{bmatrix} \tag{3}$$

$$M = \begin{bmatrix} A & B \\ B & D \end{bmatrix} \tag{4}$$

The transform matrix of the system is given by the equation, where $A$, $B$, $C$ and $D$ are $2 \times 2$ submatrices, and the determinant of $B \neq 0$. The matrix $M$ consists of 16 parameters as shown in equation (3), and these parameters need to fulfil certain constraints:

$$\begin{array}{lcl} AB^{\mathrm{T}} = BA^{\mathrm{T}} & & A^{\mathrm{T}}C = C^{\mathrm{T}}A \\ CD^{\mathrm{T}} = DC^{\mathrm{T}} & \text{or} & B^{\mathrm{T}}D = D^{\mathrm{T}}B \\ AD^{\mathrm{T}} - BC^{\mathrm{T}} = 1 & & A^{\mathrm{T}}D - C^{\mathrm{T}}B = 1 \end{array} \tag{5}$$

The identity matrix $I$ represents a $2 \times 2$ matrix with ones on the diagonal and zeros elsewhere. By imposing these constraints or equations, the number of independent variables is reduced to ten [39,41-44]. The inverse of the 2D-NSLCT of $F(x', y')$ can be attained by

$$f(x, y) = L_{M^{-1}}\{F(x', y')\}(x, y) \tag{6}$$

Here $x'$ and $y'$ are coordinates in 2D-NSLCT domain and

$$M^{-1} = \left[D^{\mathrm{T}} \quad -B^{\mathrm{T}}; -C^{\mathrm{T}} \quad A^{\mathrm{T}}\right] \tag{7}$$

## 2.4. 4D hyper chaotic system

The encryption scheme proposed in this study utilizes the hyperchaotic Lü system [43,45] to generate a keystream sequence for permutation [35]. The behaviour of the 4D chaotic framework can be effectively described by the following equation

$$\left.\begin{aligned}\frac{\mathrm{d}x}{\mathrm{d}t} &= a(y-x)+u\\ \frac{\mathrm{d}y}{\mathrm{d}t} &= -xz+cy\\ \frac{\mathrm{d}z}{\mathrm{d}t} &= xy-bz\\ \frac{\mathrm{d}u}{\mathrm{d}t} &= xz+du\end{aligned}\right\} \tag{8}$$

In the system [45], the constants $a$, $b$ and $c$ represent specific parameters, while $d$ serves as the control parameter. When $a = 36$, $b = 3$, $c = 20$, and $-0.35 < d \leq 1.30$, the Lü system exhibits a hyperchaotic behaviour. The initial values $(x, y, z, u)$ of the system uniquely determine its chaotic trajectory. Thus, these initial values are employed as the secret key to generate the permutation sequence.

To scramble the pixels of the input image, the permutation sequence generated by the 4D hyperchaotic system is utilized. The permutation process involves the following steps.

Step 1: The pixels of the input image, with dimensions $H \times W$, are arranged in a one -dimensional array 1Darray = $\{p_0,\ p_1,\ \ldots, p_{M\times N-1}\}$ following the order from left to right and top to bottom.

Step 2: A hyperchaotic sequence of length $\mathrm{Len}_{\mathrm{per}}$ = length(1Darray) – 1 is generated by iterating the hyperchaotic system (8).

Step 3: To mitigate the detrimental effects of transient behaviour, the 4D hyperchaotic system is pre-iterated $N_1$ (a constant) time. The fourth-order Runge–Kutta method [46] can be employed to numerically solve the system using a step size of $h_\mathrm{s} = 0.005$, as depicted below:

$$\left.\begin{aligned}x_{n+1} &= x_n + \frac{h_\mathrm{s}}{6} \times (K_1 + 2K_2 + 2K_3 + K_4)\\ y_{n+1} &= y_n + \frac{h_\mathrm{s}}{6} \times (L_1 + 2L_2 + 2L_3 + L_4)\\ z_{n+1} &= z_n + \frac{h_\mathrm{s}}{6} \times (M_1 + 2M_2 + 2M_3 + M_4)\\ u_{n+1} &= u_n + \frac{h_\mathrm{s}}{6} \times (N_1 + 2N_2 + 2N_3 + N_4)\end{aligned}\right\} \tag{9}$$

where,

$$K_1 = a(y_n - x_n) + u_n$$

$$L_1 = -x_n z_n + c y_n$$

$$M_1 = x_n y_n - b z_n$$

$$N_1 = x_n z_n + d u_n$$

$$K_j = a \times \left[\left(y_n + \frac{h_s \times L_{j-1}}{2}\right) - \left(x_n + \frac{h_s \times K_{j-1}}{2}\right)\right] + \left(u_n + \frac{h_s \times N_{j-1}}{2}\right)$$

$$L_j = -\left(x_n + \frac{h_s \times K_{j-1}}{2}\right)\left(z_n + \frac{h_s \times M_{j-1}}{2}\right) + c \times \left(y_n + \frac{h_s \times L_{j-1}}{2}\right)$$

$$M_j = \left(x_n + \frac{h_s \times K_{j-1}}{2}\right)\left(y_n + \frac{h_s \times L_{j-1}}{2}\right) - b \times \left(z_n + \frac{h_s \times M_{j-1}}{2}\right)$$

$$N_j = \left(x_n + \frac{h_s \times K_{j-1}}{2}\right)\left(z_n + \frac{h_s \times M_{j-1}}{2}\right) + d \times \left(u_n + \frac{h_s \times N_{j-1}}{2}\right)$$

with $j = 2, 3$, and

$$K_j = a \times \left[(y_n + h_s L_{j-1}) - (x_n + h_s K_{j-1})\right] + (u_n + h_s N_{j-1})$$

$$L_j = -(x_n + h_s K_{j-1})(z_n + h_s M_{j-1}) + c \times (y_n + h_s L_{j-1})$$

$$M_j = -(x_n + h_s K_{j-1})(y_n + h_s L_{j-1}) - b \times (z_n + h_s M_{j-1})$$

$$N_j = -(x_n + h_s K_{j-1})(z_n + h_s M_{j-1}) + d \times (u_n + h_s N_{j-1})$$

with $j = 4$.

Step 4: The chaotic sequence derived from Step 3 is converted into a row matrix and arranged in ascending order to extract the permutation keystream.

Step 5: Using the sorted sequence obtained in Step 4, the pixels, or elements of the original image (1D array) are adjusted accordingly.

Step 6: The rearranged 1D array from Step 5 is reshaped into a matrix with dimensions $H \times W$, resulting in the final scrambled image.

## 2.5. Phase truncation and phase reservation in 2D-NSLCT

The phase truncated Fourier transform (PTFT) technique in 2D non-separable linear canonical transform involves the following steps.

Step 1: The input image $I$ is combined with RPM1 and saved as $I_1$. This can be represented mathematically using following equation:

$$I_1 = I \cdot \text{RPM1} \tag{10}$$

where $\text{RPM1} = \exp(2\pi i \times m(x, y))$ and $m(x, y)$ is a random matrix that has the same size as the input image.

Step 2: It involves performing the 2D non-separable linear canonical transform on the bonded image $I_1$ obtained from Step 1.

$$I_2 = \text{2D-NSLCT}(I_1) \tag{11}$$

Step 3: The PTFT principle is applied to separate the phase reserved part, which is the angle of $I_2$, denoted as Private Key 1 (PR1) and the phase truncated part of $I_2$, which is the absolute value of $I_2$, denoted as $\text{abs}(I_2)$. This step is mathematically represented as follows:

$$\text{PR1} = \text{angle}(I_2) \tag{12}$$

$$I_3 = \text{abs}(I_2) \tag{13}$$

Step 4: $I_3$ is bonded with a random phase mask (RPM2), followed by performing an inverse 2D-NSLCT on the result and storing it as $I_4$. The mathematical representation of this process is presented in following equation:

$$I_4 = \text{2D-NSLCT}^{-1}(I_3 \cdot \text{RPM2}) \tag{14}$$

where RPM2 is defined as $\exp(2\pi i \times n(x, y))$, where $n(x, y)$ is a random matrix with the same size as the input image.

Step 5: It involves storing the phase reserved part of $I_4$ as a private key (PR2) and the phase truncated part of $I_4$ (*i.e.*, $\text{abs}(I_4)$) as the ciphertext. This can be represented mathematically by the following equations:

$$\text{PR2} = \text{angle}(I_4) \tag{15}$$

$$C = \text{abs}(I_4) \tag{16}$$

The process of PTFT in the 2D non-separable linear canonical transform is illustrated in Fig. 1. To decrypt the encrypted image, the same steps as the encryption process are followed but in reverse order.

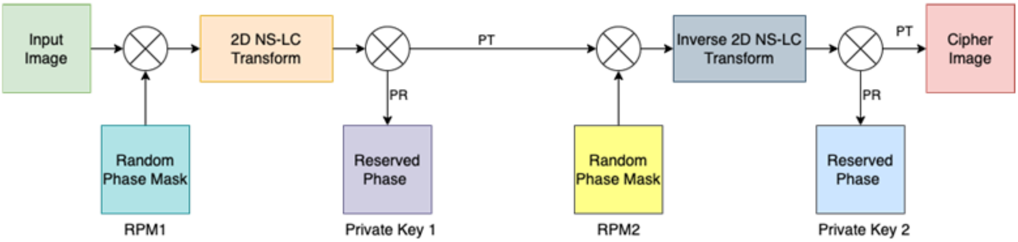

Fig. 1. Schematic depiction of the encryption procedure of PTFT in 2D-NS LCT domain.

## 3. Proposed cryptosystem

The proposed algorithm consists of three distinct stages for encryption. Initially, the input image undergoes a permutation process. Subsequently, DNA-based diffusion is employed, followed by the application of phase truncation and phase reservation (PTFT) in the 2D-NSLCT domain.

### 3.1. Encryption process

Step 1: An input image of size $m \times n$ is taken and transformed into a vector of size $(1, m \times n)$, and the outcome is saved as $E_1$.

Step 2: A chaotic 4D-hyperchaotic map is applied on $E_1$ for obtaining scrambled image $I_{sc}$.

Step 3: In the diffusion process, the first 8 pixels of scrambled image are subjected to 8 DNA encoding rules as defined in Table 1 and so on. Here $r$ demonstrates rule number and varies from 1 to 8.

$$E_2 = \text{DNAencoding}(I_{sc}, \text{rule}(r)) \tag{17}$$

Step 4: Apply the bio-inspired mutation operation on $E_2$ as discussed in Subsection 2.2 and store the resulting value as $E_3$.

Step 5: $E_3$ is obtained using the corresponding DNA decoding rule, as specified in Table 1.

$$E_4 = \text{DNAencoding}(E_3, \text{rule}(r)) \tag{18}$$

Step 6: Convert $E_4$ rom 8-bit binary to decimal. Reshape the resulting decimal value to match the size of the input image, which is $m \times n$ and PTFT in applied in 2D-NSLCT domain, following the procedure outlined in Subsection 2.5 PTFT operation yields two private keys, denoted as PR1 and PR2 and ciphertext $C$.

The complete encryption process of the proposed algorithm is schematically described in Fig. 2.

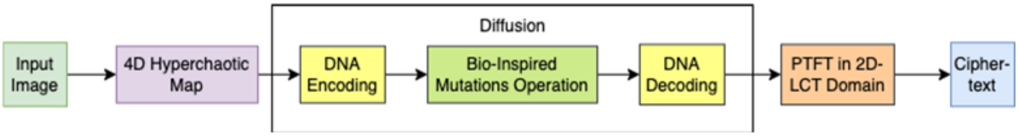

Fig. 2. Schematic representation of the encryption process of proposed algorithm.

### 3.2. Decryption process

Step 1: Ciphertext (C) obtained is bonded with the private key (PR2) and result is stored as $D_1$.

$$D_1 = C \cdot \exp(i \cdot \text{PR2}) \tag{19}$$

Step 2: 2D-NSLCT Transform is performed on $D_1$ and obtained result is bonded with the private key (PR1) and result is stored as $D_2$.

$$D_2 = \text{2D-NSLCT}(D_1) \cdot \exp(i \cdot \text{PR1}) \tag{20}$$

Step 3: Apply DNA encoding on $D_2$ after taking inverse 2D-NSLCT and result is stored as $D_3$.

$$D_3 = \text{DNAencoding}(\text{2D-NSLCT}^{-1}(D_2), \text{rule}(r)) \tag{21}$$

Step 4: Utilize the inverse of the bio-inspired mutation operation employed in the encryption process and store the resulting value as $D_4$.

Step 5: Now vector $D_4$ is decoded using the DNA decoding rule defined in Table 1.

$$D_5 = \text{DNAdecoding}(D_4, \text{rule}(r)) \tag{22}$$

where rule($r$) is DNA decoding rule defined in Table 1.

Step 6: Now to get final decrypted image $I_r$ apply inverse hyperchaotic map on $D_5$.

The complete decryption process of the proposed algorithm is schematically described by Fig. 3.

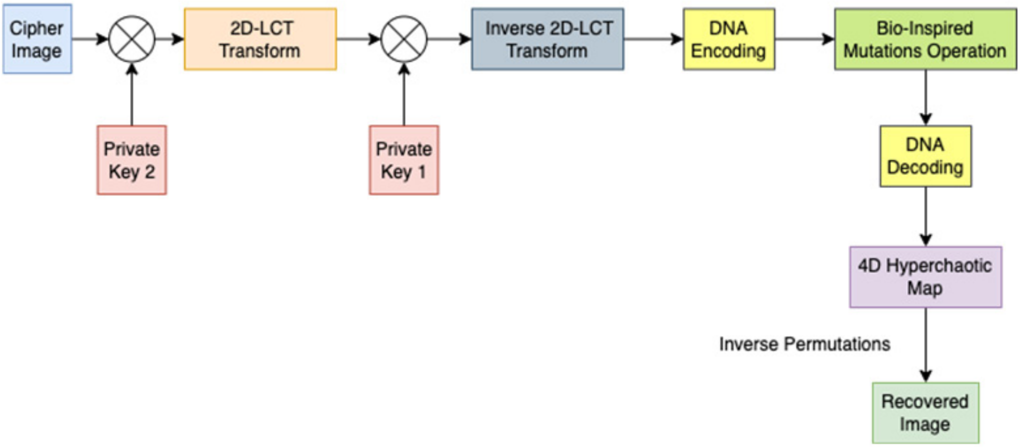

Fig. 3. Schematic representation of the decryption process of proposed algorithm.

The proposed scheme utilizes DNA encoding and DNA decoding, biologically inspired mutations, 4D hyperchaotic system and PTFT technique in 2D-NSLCT domain. RPM1 and RPM2 act as public keys whereas elements of matrix $M$ of 2D-NSLCT, PR1, PR2, 4D hyperchaotic initial conditions and parameters serve as private keys for the designed mechanism. So, the proposed scheme is asymmetric in nature and use of PTFT makes it non-linear too.

To achieve the optical realization of 2D-NSLCT [37], a configuration involving two cylinder-shaped lenses (L1 and L2) positioned non-orthogonally can be utilized. This

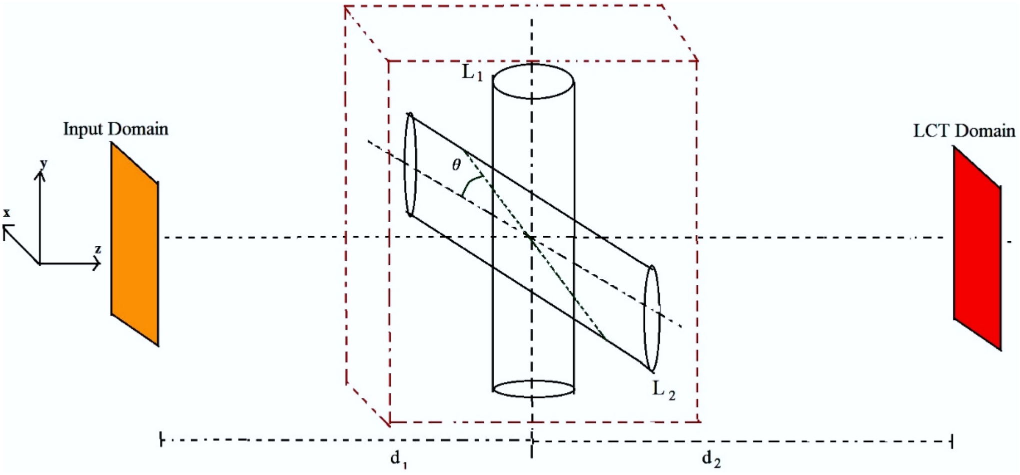

Fig. 4. Optical realization of 2D-NSLCT [37].

setup is depicted in Fig. 4, where the lenses L1 and L2 have focal lengths $f_1$ and $f_2$, respectively. They are positioned perpendicular to the optical axis ($z$-axis) and parallel to the input and output planes. Specifically, L1 is aligned along the $y$-axis, while L2 is inclined at an angle $h$ relative to the $x$-axis around the optical axis, as demonstrated in Fig. 4.

Figure 5 illustrates a potential optical configuration for decrypting the encrypted image. In this setup, the system is illuminated with coherent light. The communication between a personal computer (PC) and the optical system is facilitated by a spatial light modulator (SLM) and a charge-coupled device (CCD). The ciphertext C is combined with the private key PR2 using the spatial light modulator (SLM). The resulting output is then transformed into the 2D-NSLCT domain using the optical setup described in

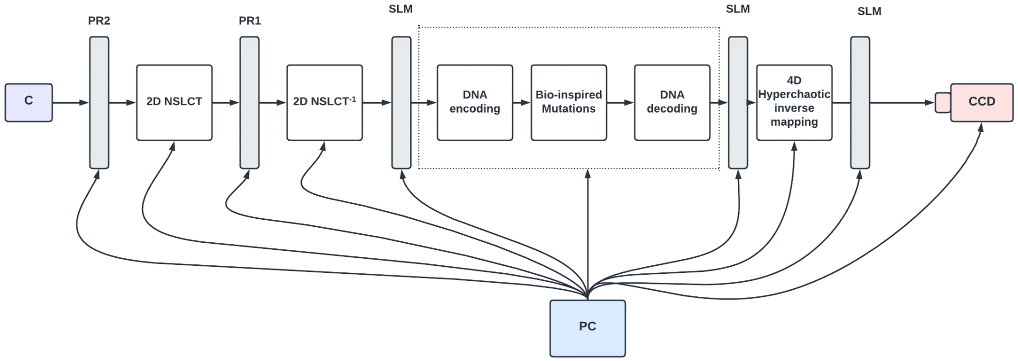

Fig. 5. The decryption process in the optoelectronic setup (proposed) involves the utilization of several components: PC (personal computer), SLM (spatial light modulator) and CCD (charged-coupled device).

Fig. 5. Afterwards, the private key PR1 is applied, and the intermediate image undergoes an inverse 2D-NSLCT transform. The resultant image is captured by the SLM and further processed by a personal computer (PC). The processes of DNA encoding, bio-inspired mutations, and DNA decoding are handled by the PC. Subsequently, the output obtained is descrambled using an inverse hyperchaotic system. The final decrypted output is captured by a charged-coupled device (CCD) and stored in the PC.

## 4. Simulation and result analysis

In order to validate and verify the proposed mechanism, numerical simulations have been carried out in MATLAB on Intel(R) Core (TM) i7-7700HQ CPU @ 2.80GHz with 16 GB RAM. Input grayscale image of *Cameraman*, *Baboon*, and *Peppers* of dimensions $256 \times 256$ are used. The values of 4D hyperchaotic parameters $a$, $b$, $c$, $d$, and $h$; and initial values $(x, y, z, u)$ of the system taken are 36, 3, 20, 1.1, 0.005, 4.1437594350718, 5.3052357062825, 26.36372354340482 and –28.5802537020945, respectively. The 2D-NSLCT matrix $M$ employed in the proposed mechanism is

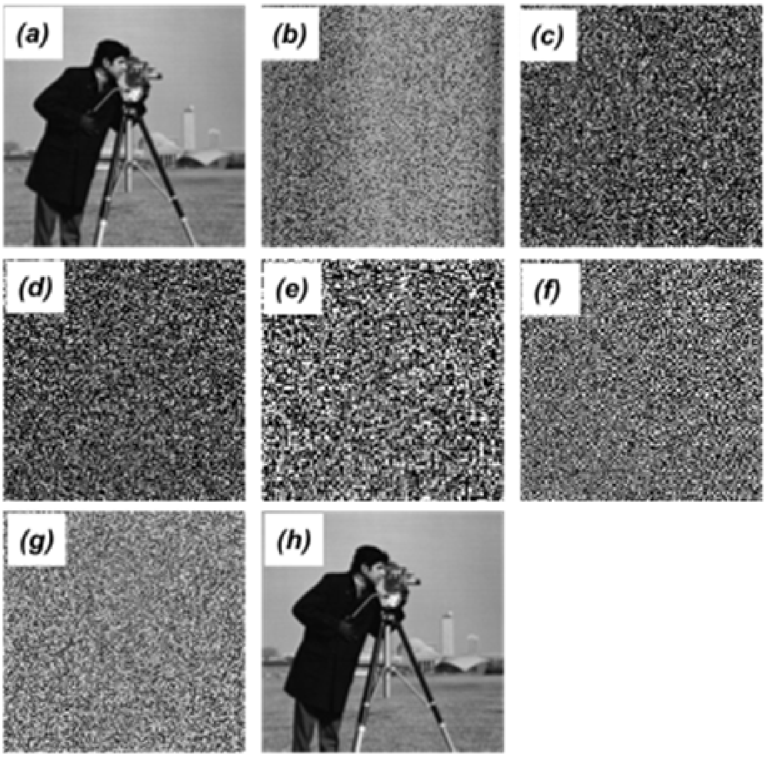

Fig. 6. (a) Original image, (b) scrambled image, (c) RPM1, (d) RPM2, (e) Private Key 1, (f) Private Key 2, (g) encrypted image, and (h) decrypted image.

$$M = \begin{bmatrix} 8 & 9 & 1 & 0.5 \\ 10 & -3 & 0.5 & 0.5 \\ 122 & -58 & 5 & 6 \\ -26 & 164 & 7 & 0 \end{bmatrix} \tag{23}$$

Scheme validation results are shown in Fig. 6: (a) original image, (b) scrambled image, (c) RPM1, (d) RPM2, (e) Private Key 1, (f) Private Key 2, (g) encrypted image and (h) decrypted image, respectively. This obviously shows efficacy and robustness of the proposed mechanism as encrypted image is random and decrypted image exactly resembles original image. CC between original image and encrypted and decrypted images is −0.0012 and 1, respectively. Whereas MSE and PSNR between original and decrypted images are 0 and infinity, respectively.

## 5. Statistical analysis

The statistical analysis of the proposed scheme involved several key components, including information entropy, histogram analysis, and 3D plots. These analyses were conducted on the input images, encrypted image, and decrypted images to gain insights into the scheme's performance and characteristics. To assess the performance of the proposed scheme, evaluation parameters such as correlation coefficient (CC), mean squared error (MSE) and peak signal noise ratio (PSNR) have been taken. These parameters were calculated using standard methodologies.

$$\mathrm{CC} = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W}\left|\left[I(i,j) - \overline{I(i,j)}\right]\left[I_{\mathrm{d}}(i,j) - \overline{I_{\mathrm{d}}(i,j)}\right]\right|}{\sqrt{\sum_{i=1}^{H}\sum_{j=1}^{W}\left[I(i,j) - \overline{I(i,j)}\right]^2}\sqrt{\sum_{i=1}^{H}\sum_{j=1}^{W}\left[I_{\mathrm{d}}(i,j) - \overline{I_{\mathrm{d}}(i,j)}\right]^2}} \tag{24}$$

$$\mathrm{MSE}(I(i,j),\, I_{\mathrm{d}}(i,j)) = \frac{1}{H \times W}\sum_{i=1}^{H}\sum_{j=1}^{W}\left[I(i,j) - I_{\mathrm{d}}(i,j)\right]^2 \tag{25}$$

$$\mathrm{PSNR} = 10 \times \log_{10}\left(\frac{255^2}{\mathrm{MSE}}\right) \tag{26}$$

Let us denote the input image as $I(i,j)$ and the decrypted image as $I_{\mathrm{d}}\underline{(i,j)}$, both with dimensions $H \times W$. The average value of the input image, denoted as $\overline{I(i,j)}$, can be calculated using the equation given below:

$$\overline{I(i,j)} = \frac{1}{H \times W}\sum_{i=1}^{H}\sum_{j=1}^{W} I(i,j) \tag{27}$$

Similarly, the mean of the decrypted image, denoted as $I_{\mathrm{d}}(i,j)$ can be obtained using a similar approach.

## 5.1. Information entropy

Information entropy [47,48] is a statistical measure used to quantify the level of unpredictability in an image, thereby providing an indication of image quality. The information entropy $H(m)$ for a given source m is calculated using the following equation:

$$H(m) = \sum_{k=1}^{256} P(m_k) \log_2 \frac{1}{P(m_k)} \tag{28}$$

Here, $P(m_k)$ represents the likelihood of occurrence of $m_k$. In the case of grayscale images, the estimated entropy falls within the range of 0 to 8. For instance, the grayscale images *Cameraman*, *Baboon* and *Peppers* exhibit entropy estimates of 7.0097, 7.6058 and 7.3011, respectively. However, the encrypted images demonstrate an entropy of 7.9956, 7.9954 and 7.9954, respectively.

## 5.2. Histogram and 3D plots

The effectiveness of the proposed picture encryption technique is further examined through histogram analysis and three-dimensional plots. They can assess robustness

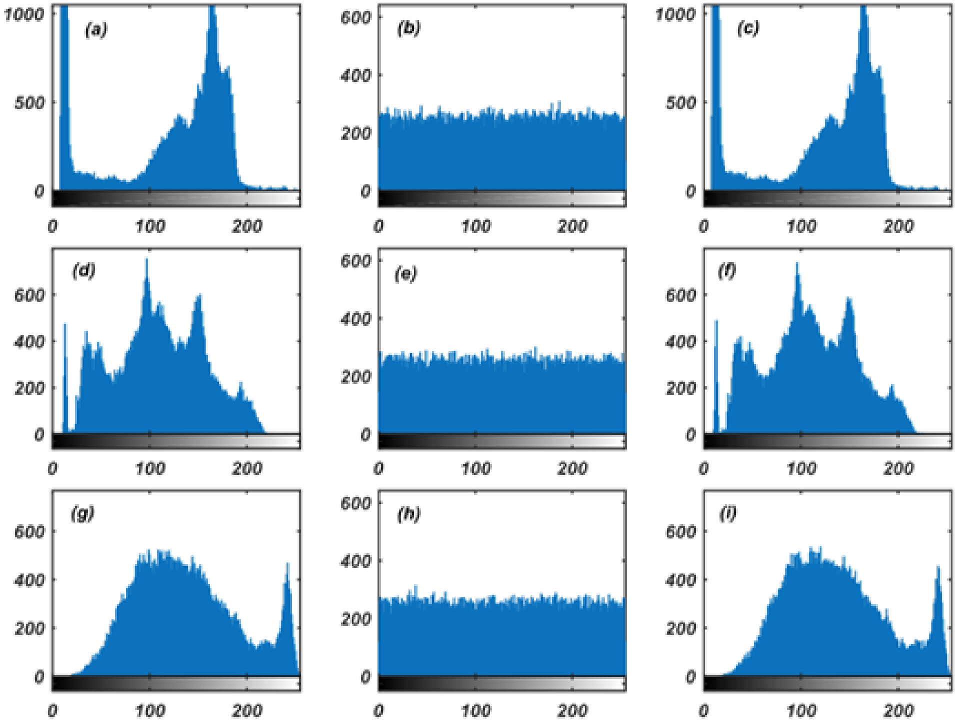

Fig. 7. Histogram analysis of original image, encrypted image, and decrypted image: (a-c) *Cameraman*, (d-f ) *Barbara* and (g-i) *Baboon*, respectively.

and efficiency of the proposed mechanism. A reliable encryption algorithm should exhibit distinct histograms between the plaintext and ciphertext images, while the histograms of the plaintext and recovered images should be similar.

Figures 7(a),(d),(g) show the histograms of the plaintext images for *Cameraman*, *Barbara*, and *Baboon*, respectively. The corresponding histogram plots of the ciphertext and recovered images can be seen in Figs. 7(b),(e),(h) and Figs. 7(c),(f),(i), respectively. It is evident from Fig. 10 that the histogram plots of the plaintext and ciphertext differ significantly, while the histogram plots of the plaintext and recovered images are similar. This observation confirms that the histogram plot of the ciphertext does not reveal any information about the original image since it does not provide insights into the pixel positions.

In addition to histograms, 3-D plots offer valuable insights into both pixel values and their positions. When evaluating the robustness of a cryptosystem, it is important to examine the 3-D plots of the plaintext and ciphertext. Ideally, these plots should exhibit distinct characteristics. Conversely, the 3-D plots of the plaintext and recovered images should demonstrate similarities, indicating successful decryption. Figures 8(a),(d),(g) and Figs. 8(b),(e),(h) depict the 3-D plots of the plaintext and ciphertext im-

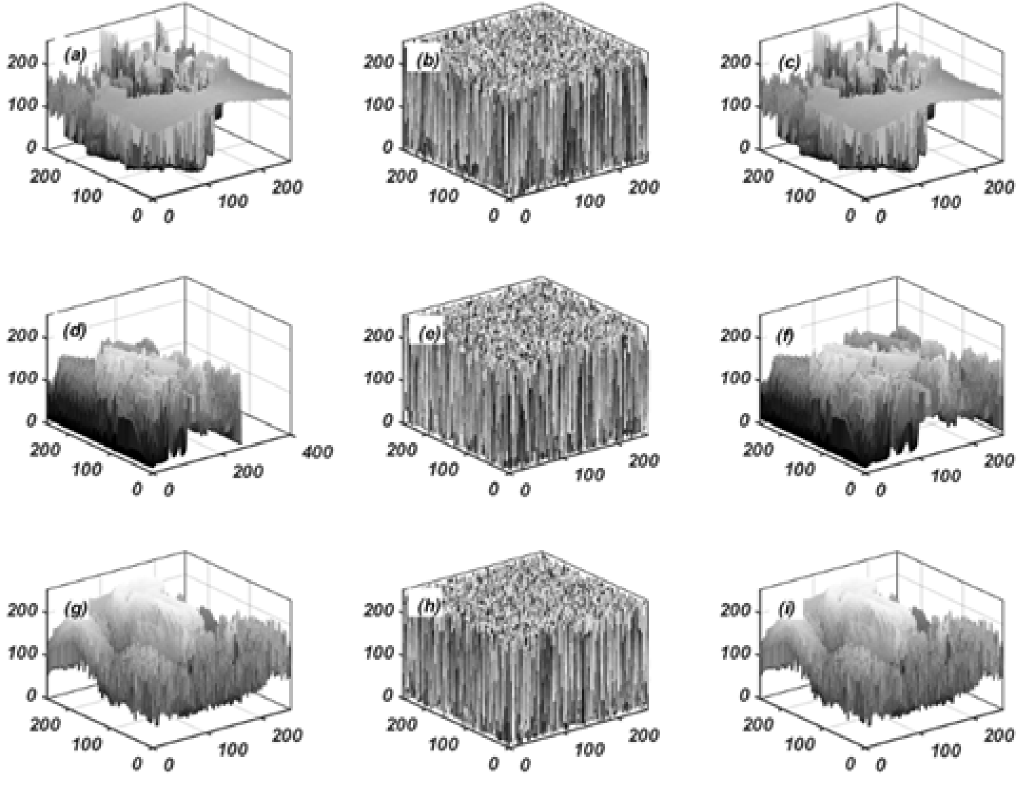

Fig. 8. Original image, encrypted image, and decrypted image: (a-c) *Cameraman*, (d-f) *Barbara*, and (g-i) *Baboon*, respectively.

ages for *Cameraman*, *Barbara*, and *Baboon*, respectively. Figure 8 confirms that the 3-D plots of the ciphertext do not provide any valuable information about the plaintext. Furthermore, Figs. 8(c),(f),(i) present the corresponding 3-D plots of the recovered images, indicating that the 3-D plots of the plaintext and ciphertext images are identical. Therefore, the analysis of histograms and 3-D plots demonstrates that the ciphertext produced by the proposed cryptosystem does not disclose any information about the original plaintext and remains consistent across different types of images.

## 5.3. Pixel correlation distribution analysis

To demonstrate the robustness of the proposed mechanism, correlation distribution analysis is also conducted. Specifically, 1000 pairs of adjacent pixels are randomly selected from input and encrypted images in horizontal, diagonal, and vertical directions. The correlation distributions were plotted and analyzed.

From Figs. 9(a),(c),(e), it is evident that input image exhibits a strong degree of correlation among adjacent pixels in all directions. However, Figs. 9(b),(d),(f) clearly

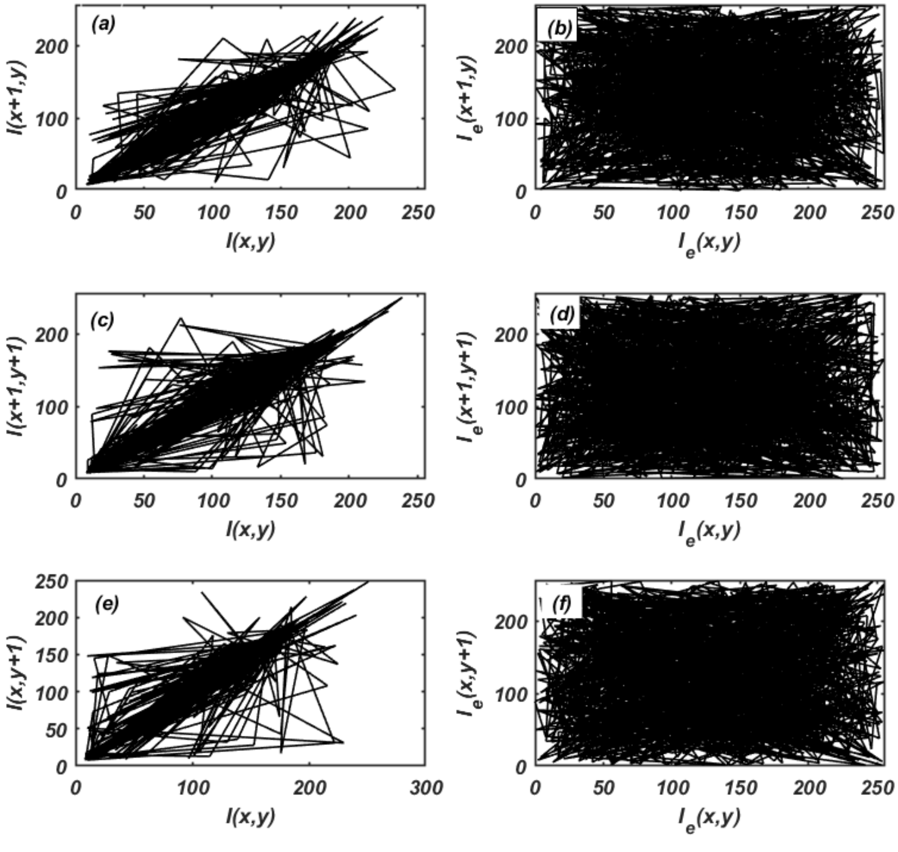

Fig. 9. Correlation distribution analysis: original image and encrypted image horizontal, diagonal, and vertical adjacent pixel distribution, respectively.

illustrates the extremely poor correlation between adjacent pixels in the encrypted image across all three directions. Furthermore, the pixels in the encrypted image not only exhibit poor correlation but are also randomly dispersed.

## 6. Attack analysis and key sensitivity analysis

To validate and verify the performance of the proposed mechanism it has been investigated and examined against various attacks like noise attack, occlusion attack and special attack. Further to explore robustness of the scheme, its sensitivity to various keys and parameters have also been analyzed

### 6.1. Noise attack analysis

Noise may creep in any communication channel and adversely affect the quality of the data traversing through it [48-53]. Considering this fact, the proposed system is analyzed against noise attack to assess the robustness of scheme against such assaults. Ciphertext image $C$ is contaminated with Gaussian random noise $G$ of strength $K$ with

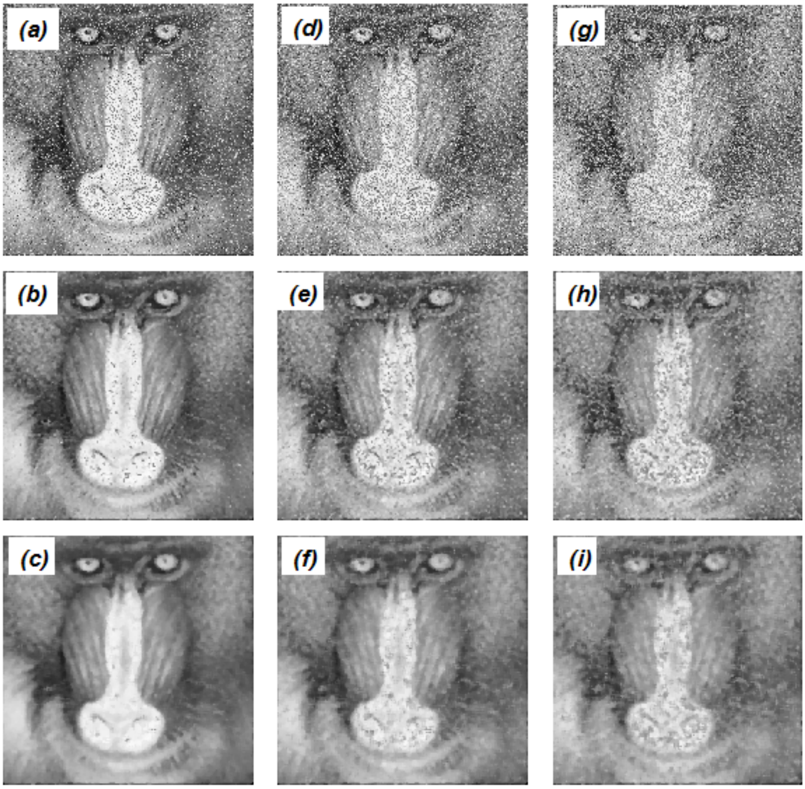

Fig. 10. Noise attack results: decrypted image, 3 × 3 median filtered result and 5 × 5 median filtered result for sigma = 1, 3 and 5, respectively.

Table 2. CC values of decrypted images, 3 × 3 median filtered result and 5 × 5 median filtered result for sigma = 1, 3 and 5, respectively.

| | Sigma = 1 | Sigma = 3 | Sigma = 5 |
|---|---|---|---|
| CC1 | 0.7578 | 0.6271 | 0.5347 |
| CC2 | 0.9480 | 0.8876 | 0.8284 |
| CC3 | 0.9437 | 0.9148 | 0.8792 |

zero mean and unity standard deviation. Corrupted ciphertext image is represented by $C'$ and computed using equation below:

$$C' = C + 0.01 \times kG \tag{29}$$

Figure 10 displays noise attack results on *Baboon* image, where (a)–(c) displays decrypted images with noise strength 1, output obtained after applying to median filter of 3 × 3 size and output obtained after applying to median filter of 5 × 5 size, respectively. Similar results for noise strength 3 and 5 are illustrated in (d)–(f) and (g)–(i), respectively. These results clearly demonstrate the effectiveness of the proposed scheme in handling noise attacks. The application of the median filter technique improves the quality of the decrypted images, as evidenced by the CC analysis conducted in Table 2. The analysis reveals that when $k = 1$, the output obtained after applying the 3 × 3 median filter exhibits a better resemblance or similarity to the original image. On the other hand, for $k = 3$ and $k = 5$, the output obtained after applying the 5 × 5 median filter shows a better resemblance or similarity to the original image. In conclusion, the proposed scheme demonstrates effective resistance against noise attacks, primarily due to the incorporation of the median filter technique.

## 6.2. Occlusion attack analysis

An occlusion attack involves intentionally obscuring or blocking certain parts or regions of an image or dataset. This manipulation can take the form of objects, patterns, or textures that cover or partially obstruct specific areas of interest within the data. The proposed scheme has been evaluated against occlusion attack to assess the resilience and effectiveness of the system when processing and analysing images with obscured or occluded regions. Figure 11 demonstrates occlusion attack analysis where (a)–(d) displays occlusion results with 12.5%, 25%, 37.5% and 50% occlusion of *Peppers* image whereas (e)–(h) and (i)–(l) illustrates results obtained after applying median filter of size 3 × 3 and 5 × 5, respectively. It is quite evident from the visual results obtained that median filtering enhances the quality of images decrypted up to 50% occlusion later the quality degrades. The same is proved by Fig. 12 which shows CC plot against percentage of occlusion. The plot reveals that for occlusion levels below 10% median filter of size 3 × 3 performs well. However, for occlusion levels ranging from 10% to 50% median filter of dimension 5 × 5 yields better results. Conversely, for occlusion levels exceeding 50%, median filtering becomes ineffective. In conclusion, the proposed scheme demonstrates a certain degree of resistance against occlusion attacks, thanks

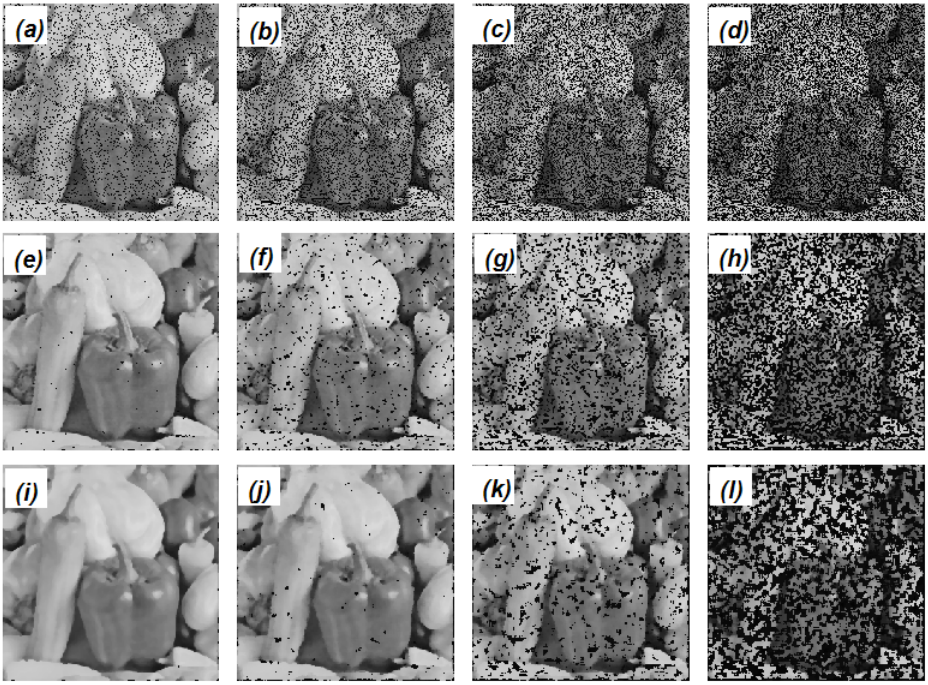

Fig. 11. Occlusion attack analysis: (a-d) Occlusion results with 12.5%, 25%, 37.5% and 50% occlusion of *Peppers* image whereas (e-h) and (i-l) shows results obtained after applying median filter of size 3 × 3 and 5 × 5, respectively.

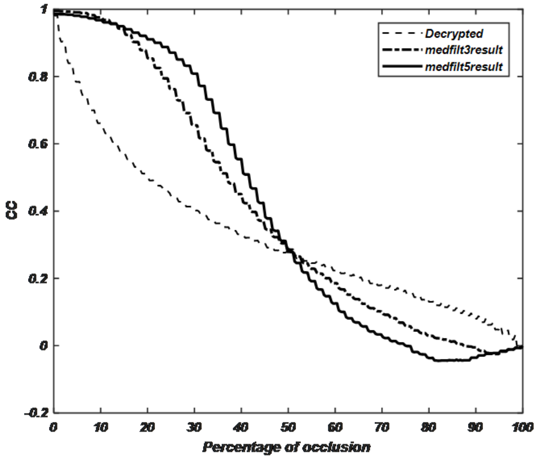

Fig. 12. CC plot against percentage of occlusion for decrypted image, results obtained after applying median filter of size 3 × 3 and 5 × 5, respectively.

to the utilization of median filtering. However, the effectiveness of the scheme varies depending on the occlusion percentage and the size of the median filter.

### 6.3. Special attack analysis

The proposed cryptosystem exhibits an asymmetric nature, wherein the private keys are dependent on the plaintext. If attackers manage to acquire the keys for a specific plaintext through a chosen plaintext attack, they will be unable to utilize those same keys for other plaintexts due to the inherent property of key variation in an asymmetric cryptosystem. Consequently, the chosen plaintext attack and known plaintext attack are rendered ineffective against the proposed cryptosystem.

In a specific iterative attack scenario, the attacker possesses a substantial amount of information regarding the cryptosystem, encompassing the public key, ciphertext, and all private keys except one. Employing a specialized iterative attack algorithm, the attacker employs an iterative approach to recover the plaintext [26]. PTFT alone is vulnerable to special attack so additional parameters and keys of 4D hyperchaotic parameters and initial conditions, 2D-NSLCT and biological mutation operations make the proposed scheme insusceptible to special attacks. So, in order to resist special attacks other keys and parameters play a vital role. Section 6.4 below clearly reflects the sensitivity of the proposed mechanism to these keys and parameters. So, it can be said that even if any parameter or key is not known then attacker will not be able to recover the original images as proved.

### 6.4. Key sensitivity analysis

The proposed scheme's sensitivity to various keys and parameters has been carried out to show robustness and efficacy of the scheme. To assess the sensitivity of the scheme against different keys, decryption experiments were conducted using incorrect values for various keys, namely PR2, RPM2, and PR1, as depicted in Fig. 13. The obtained results clearly demonstrate the high sensitivity of the proposed mechanism to these key variations.

Decryption experiments were conducted to evaluate the impact of incorrect values for hyperchaotic parameters and initial conditions. The results of these decryption attempts are presented in Fig. 14. The results obtained from the decryption process do not provide any insight into the original image, thereby illustrating the sensitivity of the proposed mechanism to changes in hyperchaotic parameters and initial conditions.

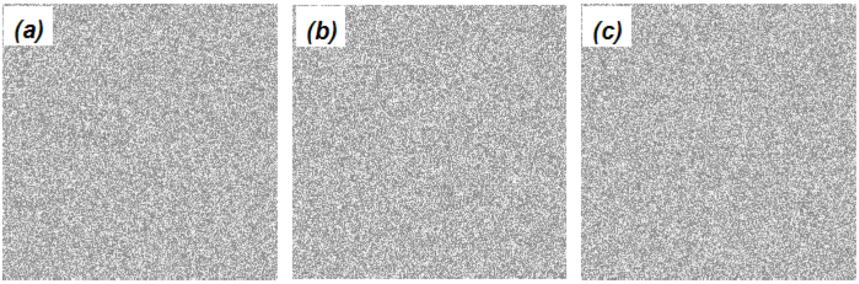

Fig. 13. Decryption with wrong (a) Private Key 2, (b) RPM2, and (c) Private Key 1.

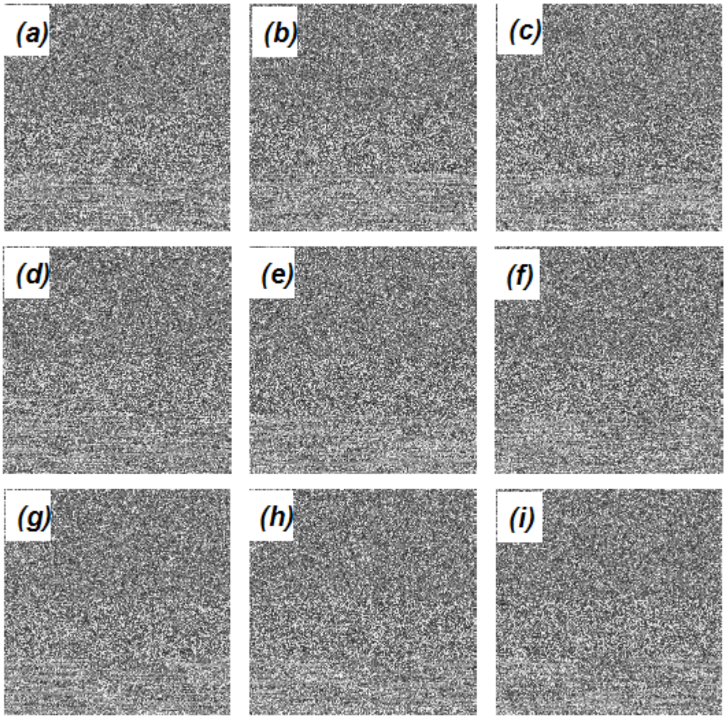

Fig. 14. Decryption with incorrect values of hyperchaotic parameters and initial conditions: (a) $a = 36.1$; (b) $b = 3.1$; (c) $c = 20.1$; (d) $d = 1.11$; (e) $h = 0.0051$; (f) $x(1) = 4.1437594350717$; (g) $y(1) =$ $= 5.3052357062824$; (h) $z(1) = 26.36372354340481$, and (i) $u(1) = –28.5802537020944$.

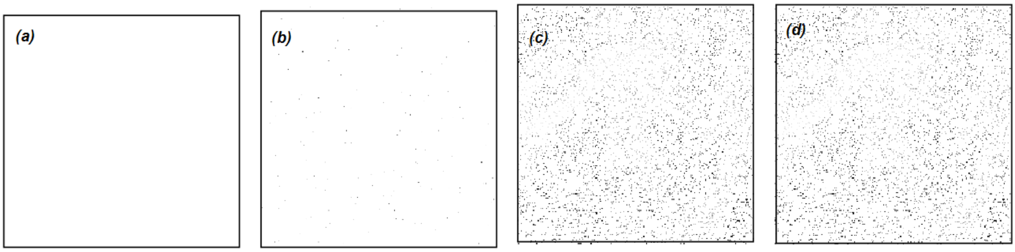

Fig. 15. Decrypted image $I_{\mathrm{dec}}(x)$ on taking (a) $b_{11} = 1.0005$ instead of 1; (b) $b_{12} = 0.50001$ instead of 0.5; (c) $b_{21} = 0.50001$ instead of 0.5 and (d) $b_{22} = 0.50001$ instead of 0.5, respectively.

Figure 15 exhibits the decrypted image when erroneous values are used for the elements of matrix M. Specifically, (a) $b_{11} = 1.0005$ instead of 1; (b) $b_{12} = 0.50001$ instead of 0.5; (c) $b_{21} = 0.50001$ instead of 0.5 and (d) $b_{22} = 0.50001$ instead of 0.5, respectively. This observation provides compelling evidence for the sensitivity of the proposed encryption scheme to the elements of matrix M. It is evident that successful decryption of the images cannot be achieved without precise knowledge of these parameters.

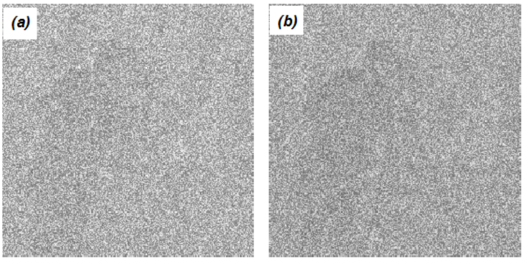

Fig. 16. Decrypted image $I_{\text{dec}}(x)$ on making wrong biological mutations of (a) substitution and (b) deletion.

The process of biological mutations has the potential to provide an additional layer of defence. For further information on the various mutation operations, please refer to Section 2.2. The conclusions that an eavesdropper obtains from a mutation process that is different from the one that is used in encryption will be an incorrect interpretation [38]. Figure 16 illustrates decryption results for wrong biological mutations of: substitution and deletion, respectively. And results obtained does not convey any information about the input plaintext image taken. Thus, these biological mutations play a significant role in securing the scheme.

The decryption results demonstrate the sensitivity of the proposed scheme to different keys and parameters. Therefore, it can be concluded that to successfully decrypt the encrypted image, it is essential to have knowledge of every parameter and key.

## 7. Conclusion

This paper presents a novel approach to asymmetric optical cryptosystems using a 4D hyperchaotic system combined with DNA encoding and bio-inspired mutation operations in the 2D-NSLCT transform domain. The 4D hyperchaotic system is utilized to generate a permutation sequence for pixel scrambling of the input image. Chaotic parameters and initial conditions enhance the key space too. The 2D-NSLCT parameters serve as additional keys to resist brute-force attacks. The proposed method utilizes PTFT operations twice to generate ciphertext which generates two private keys. The validity of the proposed system has been confirmed through MATLAB simulations, demonstrating excellent performance against occlusion, noise, classical cryptographic and specific attacks. Moreover, this paper introduces a new research direction by utilizing 2D-NSLCT instead of conventional transforms. The results indicate that the scheme offers improved security compared to existing schemes in terms of visual detectability, entropy, key space, and attack analysis. Additionally, the proposed method offers advantages in terms of key management and the nonlinear characteristics of asymmetric optical cryptosystems.

### Ethical approval

Manuscript has not been published elsewhere and that it has not been submitted simultaneously for publication elsewhere.

**Conflicts of interest**

The authors declare that they have no conflicts of interest.

**Data availability**

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

**Acknowledgement**

The authors gratefully acknowledge the support from the Anusandhan National Research Foundation (ANRF), Science & Engineering Research Board (SERB) Core Research Grant (CRG) scheme, Govt. of India, grant No. CRG/2023/005504-G.

## References

[1] JAVIDI B., SERGENT A., ZHANG G., GUIBERT L., *Fault tolerance properties of a double phase encoding encryption technique*, Optical Engineering **36**(4), 1997: 992-998. https://doi.org/10.1117/1.601144

[2] JAVIDI B., NOMURA T., *Securing information by use of digital holography*, Optics Letters **25**(1), 2000: 28-30. https://doi.org/10.1364/OL.25.000028

[3] KISHK S., JAVIDI B., *Information hiding technique with double phase encoding*, Applied Optics **41**(26), 2002: 5462-5470. https://doi.org/10.1364/AO.41.005462

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

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

[6] PENG X., ZHANG P., WEI H., YU B., *Known-plaintext attack on optical encryption based on double random phase keys*, Optics Letters **31**(8), 2006: 1044-1046. https://doi.org/10.1364/OL.31.001044

[7] UNNIKRISHNAN G., JOSEPH J., SINGH K., *Optical encryption by double-random phase encoding in the fractional Fourier domain*, Optics Letters **25**(12), 2000: 887-889. https://doi.org/10.1364/OL.25.000887

[8] SINGH P., YADAV A.K., SINGH K., *Known-plaintext attack on cryptosystem based on fractional Hartley transform using particle swarm optimization algorithm*, [In] Ray K., Sharan S.N., Rawat S., Jain S.K., Srivastava S., Bandyopadhyay A., [Eds.] *Engineering Vibration, Communication and Information Processing*, Lecture Notes in Electrical Engineering, Vol. 478, Singapore, Springer, 2019: 317-327. https://doi.org/10.1007/978-981-13-1642-5_29

[9] YADAV A.K., SINGH P., SINGH K., *Cryptosystem based on devil's vortex Fresnel lens in the fractional Hartley domain*, Journal of Optics **47**, 2018: 208-219. https://doi.org/10.1007/s12596-017-0435-9

[10] CHEN H., ZHU L., LIU Z., TANOUGAST C., LIU F., BLONDEL W., *Optical single-channel color image asymmetric cryptosystem based on hyperchaotic system and random modulus decomposition in Gyrator domains*, Optics and Lasers in Engineering **124**, 2020: 105809. https://doi.org/10.1016/j.optlaseng.2019.105809

[11] KUMAR R., QUAN C., *Optical colour image encryption using spiral phase transform and chaotic pixel scrambling*, Journal of Modern Optics **66**(7), 2019: 776-785. https://doi.org/10.1080/09500340.2019.1572807

[12] KUMAR J., SINGH P., YADAV A.K., KUMAR A., *Asymmetric cryptosystem for phase images in fractional fourier domain using LU-decomposition and Arnold transform*, Procedia Computer Science **132**, 2018: 1570-1577. https://doi.org/10.1016/j.procs.2018.05.121

[13] SINGH P., YADAV A.K., SINGH K., *Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition*, Optics and Lasers in Engineering **91**, 2017: 187 -195. https://doi.org/10.1016/j.optlaseng.2016.11.022

[14] Singh P., Yadav A.K., Singh K., Saini I., *Optical image encryption in the fractional Hartley domain, using Arnold transform and singular value decomposition*, AIP Conference Proceedings **1802**(1), 2017: 020017. https://doi.org/10.1063/1.4973267

[15] Archana, Sachin, Singh P., *Cryptosystem based on triple random phase encoding with chaotic Henon map*, [In] Ray K., Roy K.C., Toshniwal S.K., Sharma H., Bandyopadhyay A. [Eds.], *Proceedings of International Conference on Data Science and Applications*, Lecture Notes in Networks and Systems, Vol. 148, Springer, Singapore, 2021: 73-84. https://doi.org/10.1007/978-981-15-7561-7_5

[16] Elshamy A.M., Rashed A.N.Z., Mohamed A.E.-N.A., Faragalla O.S., Mu Y., Alshebeili S.A., Abd El-Samie F.E., *Optical image encryption based on chaotic Baker map and double random phase encoding*, Journal of Lightwave Technology **31**(15), 2013: 2533-2539. https://doi.org/10.1109/JLT.2013.2267891

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

[18] Sharma B., Singh H., Khurana M., *Image quality enhancement using deep learning based convolution residual networks techniques*, Journal of Information Systems Engineering and Management **10**(40S) 2025: 1246-1266. https://doi.org/10.52783/jisem.v10i40s.7876

[19] Sachin, Archana, Singh P., *Optical image encryption algorithm based on chaotic Tinker Bell map with random phase masks in Fourier domain*, [In] Ray K., Roy K.C., Toshniwal S.K., Sharma H., Bandyopadhyay A. [Eds.], *Proceedings of International Conference on Data Science and Applications*, Lecture Notes in Networks and Systems, Vol. 148, Springer, Singapore, 2021: 249-262. https://doi.org/10.1007/978-981-15-7561-7_20

[20] Sharma N., Saini I., Yadav A., Singh P., *Phase-image encryption based on 3D-Lorenz chaotic system and double random phase encoding*, 3D Research **8**, 2017: 39. https://doi.org/10.1007/s13319-017-0149-4

[21] Chen J., Chen L., Zhou Y., *Cryptanalysis of a DNA-based image encryption scheme*, Information Sciences **520**, 2020: 130-141. https://doi.org/10.1016/j.ins.2020.02.024

[22] Dou Y., Liu X., Fan H., Li M., *Cryptanalysis of a DNA and chaos based image encryption algorithm*, Optik **145**, 2017: 456-464. https://doi.org/10.1016/j.ijleo.2017.08.050

[23] Hermassi H., Belazi A., Rhouma R., Belghith S.M., *Security analysis of an image encryption algorithm based on a DNA addition combining with chaotic maps*, Multimedia Tools and Applications **72**, 2014: 2211-2224. https://doi.org/10.1007/s11042-013-1533-6

[24] Su X., Li W., Hu H., *Cryptanalysis of a chaos-based image encryption scheme combining DNA coding and entropy*, Multimedia Tools and Applications **76**, 2017: 14021-14033. https://doi.org/10.1007/s11042-016-3800-9

[25] Tao R., Xin Y., Wang Y., *Double image encryption based on random phase encoding in the fractional Fourier domain*, Optics Express **15**(24), 2007: 16067-16079. https://doi.org/10.1364/OE.15.016067

[26] Archana, Sachin, Singh P., *Cascaded unequal modulus decomposition in Fresnel domain based cryptosystem to enhance the image security*, Optics and Lasers in Engineering **137**, 2021: 106399. https://doi.org/10.1016/j.optlaseng.2020.106399

[27] Wu J., Liu W., Liu Z., Liu S., *Cryptanalysis of an "asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition"*, Applied Optics **54**(30), 2015: 8921-8924. https://doi.org/10.1364/AO.54.008921

[28] Akkasaligar P.T., Biradar S., *Selective medical image encryption using DNA cryptography*, Information Security Journal: A Global Perspective **29**(2), 2020: 91-101. https://doi.org/10.1080/19393555.2020.1718248

[29] Clelland C.T., Risca V., Bancroft C., *Hiding messages in DNA microdots*, Nature **399**, 1999: 533-534. https://doi.org/10.1038/21092

[30] Zhang Q., Guo L., Wei X., *Image encryption using DNA addition combining with chaotic maps*, Mathematical and Computer Modelling **52**(11-12), 2010: 2028-2035. https://doi.org/10.1016/j.mcm.2010.06.005

[31] Diaconu A.-V., *Circular inter–intra pixels bit-level permutation and chaos-based image encryption*, Information Sciences **355-356**, 2016: 314-327. https://doi.org/10.1016/j.ins.2015.10.027

[32] El-Khamy S.E., Mohamed A.G., *An efficient DNA-inspired image encryption algorithm based on hyper-chaotic maps and wavelet fusion*, Multimedia Tools and Applications **80**, 2021: 23319-23335. https://doi.org/10.1007/s11042-021-10527-6

[33] Jain A., Rajpal N., *A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps*, Multimedia Tools and Applications **75**, 2016: 5455-5472. https://doi.org/10.1007/s11042-015-2515-7

[34] Zhen P., Zhao G., Min L., Jin X., *Chaos-based image encryption scheme combining DNA coding and entropy*, Multimedia Tools and Applications **75**, 2016: 6303-6319. https://doi.org/10.1007/s11042-015-2573-x

[35] Fu C., Zhang G., Zhu M., Chen Z., Lei W., *A new chaos-based color image encryption scheme with an efficient substitution keystream generation strategy*, Security and Communication Networks, Vol. 2018, 2018: 2708532. https://doi.org/10.1155/2018/2708532

[36] Liu Z., Gong M., Dou Y., Liu F., Lin S., Ahmad M.A., Dai J., Liu S., *Double image encryption by using Arnold transform and discrete fractional angular transform*, Optics and Lasers in Engineering **50**(2), 2012: 248-255. https://doi.org/10.1016/j.optlaseng.2011.08.006

[37] Kumar R., Sheridan J.T., Bhaduri B., *Nonlinear double image encryption using 2D non-separable linear canonical transform and phase retrieval algorithm*, Optics & Laser Technology **107**, 2018: 353-360. https://doi.org/10.1016/j.optlastec.2018.06.014

[38] Sachin, Singh P., *Asymmetric cryptosystem based on biological mutation operation in chirp-Z domain*, Multimedia Tools and Applications **82**, 2023: 42439-42463. https://doi.org/10.1007/s11042-023-15190-7

[39] Ding J.-J., Pei S.-C., *Eigenfunctions and self-imaging phenomena of the two-dimensional nonseparable linear canonical transform*, Journal of the Optical Society of America A **28**(2), 2011: 82-95. https://doi.org/10.1364/JOSAA.28.000082

[40] Zhao L., Healy J.J., Sheridan J.T., *Sampling of the two dimensional non-separable linear canonical transform*. Proceedings of the SPIE, Vol. 9131, Optical Modelling and Design III, 2014: 913112. https://doi.org/10.1117/12.2052549

[41] Koç A., Ozaktas H.M., Hesselink L., *Fast and accurate computation of two-dimensional non-separable quadratic-phase integrals*, Journal of the Optical Society of America A **27**(6), 2010: 1288 -1302. https://doi.org/10.1364/JOSAA.27.001288

[42] Zhao L., Healy J.J., Sheridan J.T., *Unitary discrete linear canonical transform: Analysis and application*, Applied Optics **52**(7), 2013: C30-C36. https://doi.org/10.1364/AO.52.000C30

[43] Ding J.-J., Pei S.-C., Liu C.-L., *Improved implementation algorithms of the two-dimensional nonseparable linear canonical transform*, Journal of the Optical Society of America A **29**(8), 2012: 1615-1624. https://doi.org/10.1364/JOSAA.29.001615

[44] Alieva T., Bastiaans M.J., *Alternative representation of the linear canonical integral transform*, Optics Letters **30**(24), 2005: 3302-3304. https://doi.org/10.1364/OL.30.003302

[45] Chen A., Lu J., Lü J., Yu S., *Generating hyperchaotic Lü attractor via state feedback control*, Physica A: Statistical Mechanics and its Applications **364**, 2006: 103-110. https://doi.org/10.1016/j.physa.2005.09.039

[46] Butcher J., *The Numerical Analysis of Ordinary Differential Equations: Runge–Kutta and General Linear Methods*, John Wiley & Sons, 1987.

[47] Lai C.S., Tao Y., Xu F., Ng W.W.Y., Jia Y., Yuan H., Huang C., Lai L.L., Xu Z., Locatelli G., *A robust correlation analysis framework for imbalanced and dichotomous data with uncertainty*, Information Sciences **470**, 2019: 58-77. https://doi.org/10.1016/j.ins.2018.08.017

[48] LYDA R., HAMROCK J., *Using entropy analysis to find encrypted and packed malware*, IEEE Security & Privacy **5**(2), 2007: 40-45. https://doi.org/10.1109/MSP.2007.48

[49] YADAV P.L., SINGH H., *Security enrichment of optical image cryptosystem based on superposition technique using fractional Hartley and gyrator transform domains deploying equal modulus decomposition*, Optical and Quantum Electronics **51**, 2019: 140. https://doi.org/10.1007/s11082-019-1854-4

[50] MAAN P., SINGH H., KUMARI A.C., *Optical asymmetric cryptosystem based on Kronecker product, hybrid phase mask and optical vortex phase masks in the phase truncated hybrid transform domain*, 3D Research **10**, 2019: 8. https://doi.org/10.1007/s13319-019-0218-y

[51] KHURANA M., SINGH H., *Asymmetric optical image triple masking encryption based on gyrator and Fresnel transforms to remove Silhouette problem*, 3D Research **9**, 2018: 38. https://doi.org/10.1007/s13319-018-0190-y

[52] SINGH H., YADAV P., *An optical vortex-based asymmetric cryptosystem using QZ modulation for the double image encryption in the gyrator transform*, Iran Journal of Computer Science **7**, 2024: 829 -842. https://doi.org/10.1007/s42044-024-00196-7

[53] SINGH H., GAUR K.S., THAKRAN S., SINGH K., *An asymmetric phase image encryption technique using Arnold transform, singular value decomposition, Hessenberg decomposition, and fractional Hartley transform*, Applied Physics B **130**, 2024: 186. https://doi.org/10.1007/s00340-024-08312-y

*Received September 13, 2024*
*in revised form October 20, 2024*