

A Robust Fractional Fourier-Domain Image Encryption Framework Integrating Hessenberg Decomposition and Hybrid Chaotic Maps

Arabind Kumar

arabindkumar@vivekanand.du.ac.in

Vivekananda College, University of Delhi

Article

Keywords: Fractional Fourier Transform, Hessenberg decomposition, hybrid chaotic map, cryptanalysis

Posted Date: October 21st, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-11160836/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

A Robust Fractional Fourier-Domain Image Encryption Framework Integrating Hessenberg Decomposition and Hybrid Chaotic Maps

Arabind Kumar

Department of Mathematics, Vivekananda College, University of Delhi, Delhi, India

arabindkumar@vivekanand.du.ac.in

Corresponding Author: Arabind Kumar

Abstract: Multimedia communication technology has rapidly developed with communication over insecure channels and it demands efficient and secure image encryption scheme which should be robust and secure against transmission attacks. In this paper, a new image encryption scheme is proposed based on Fractional Fourier Transform (FrFT), Hessenberg decomposition and a hybrid chaotic system. The scheme is a three-stage confusion–diffusion scheme. To enhance the key-space diversity and sensitivity, the plaintext is first transformed to the fractional Fourier domain. Then, a Hessenberg decomposition is used to simplify the spectrum of the FT in the complex by representing it as elements of simplified matrices, which further reduces the computation time requirements and retains all the important spectral information. Last but not least, a hybrid 2D Logistic-Sine-Cosine Map and Tangent Delay Ellipse Reflecting Cavity Map System produces dynamic keystreams for bit-level permutation, substitution and bidirectional diffusion. A SHA-256-based key schedule even supports high plaintext sensitivity. The experimental results display a remarkable space larger than 2^{512} , entropy of 7.9998, insignificant adjacent-pixel correlation and NPCR/UACI values higher than 99.61% and 33.46% respectively. The framework proposed in this paper has high reconstruction quality under noise and occlusion, and is highly resistant to statistical attack, differential attack, chosen-plaintext attack and brute-force attack. The scheme has $O(N \cdot \log N)$ computational complexity, and therefore is an efficient, secure solution for image communication.

Keywords: Fractional Fourier Transform; Hessenberg decomposition; hybrid chaotic map; cryptanalysis.

1. Introduction

The proliferation of multimedia data transmission on open communication networks has put new challenges on information security. In the era of rapid development of multimedia data transmission on open communication networks, unprecedented challenges are emerging in information security. Many of these media messages are digital, and the information they carry is often sensitive, in applications as diverse as medical diagnosis, military reconnaissance, communications and personal information, and commercial transactions. Images, in contrast to textual data, have intrinsic characteristics that make the conventional encryption algorithms like AES or DES become inefficient and suboptimal in real-time protection of images: high redundancy of image data, high correlation between adjacent pixels, large size of image data. Accordingly, the design of an image cryptosystem with high security, low computation and transmission error sensitivity has become a crucial research target. Energy compaction and decorrelation qualities of spectral representations have made transform-domain image encryption very attractive [1-2]. The Fractional Fourier Transform (FrFT) is a generalized

version of the classical Fourier transform that has gained much attention in this regard. The FrFT introduces a fractional order parameter α , which expands the key space and boosts the sensitivity to the geometry of the transform. The FrFT has been successfully implemented in double random phase encoding (DRPE) structures and different optical encryption schemes. Traditional optical implementations of FrFT, however, are based on linear operations which can be susceptible to chosen-plaintext attacks; in DRPE implementations, alignment between the optical components is important and can be difficult to maintain in a digital implementation [3-6].

In recent years, matrix decomposition methods have been becoming popular as auxiliary tool for image encryption. Hessenberg decomposition, which reduces a matrix to an upper Hessenberg matrix and an orthogonal matrix, is an attractive mix of energy concentration and transformation of the matrix. Hessenberg decomposition applied to the image representations that have been encrypted or transformed results in an intermediate structure that is compact, thus decreasing the computing burden without losing the main spectral features of the image. Abuturab's recent research showed the combination of Hessenberg decomposition with chaotic phase masks for multiple color image encryption, with good results regarding security metrics. But the potential of Hessenberg decomposition as an integral part of hybrid chaos-based systems is under-explored [7]. The image cryptosystems are widely adopted in recent times because of their characteristic features, which are extreme sensitivity to the initial conditions, ergodicity and pseudo-randomness of chaotic systems. Low dimensional chaotic maps like Logistic map, Sine map are simple to compute but have a small chaotic range and are prone to attack by phase space reconstruction. Researchers have also sought hybrid chaotic architectures that link together several maps to obtain better ergodicity and key diversity, in order to overcome these limitations. For example, the 2D Logistic-Sine-Cosine Map (2D-LSCM) shows enhanced chaotic behavior compared to the constituent one-dimensional maps, and the Tangent Delay Ellipse Reflecting Cavity Map System (TD-ERCS) has high sensitivity and complex dynamical properties. Although these developments have been made, the systematic combination of hybrid chaotic maps with transform domain decomposition techniques, such as Hessenberg decomposition, is still largely under explored [8-11].

To fill the aforementioned gaps, in this paper a novel image encryption framework is proposed which combines Fractional Fourier Transform, Hessenberg decomposition and a hybrid chaotic system. The proposed architecture works with a three-stage confusion–diffusion mechanism. The plaintext image is first converted into the fractional Fourier domain and the fractional order is used as an auxiliary cryptographic key. Secondly, the complex-valued FrFT spectrum is decomposed into an Hessenberg form, producing an intermediate representation with small number of frequencies and high energy concentration. Third, a hybrid chaotic engine, which is a combination of 2D-LSCM with TD-ERCS, produces very chaotic keystreams to be used for the bit-level permutation, dynamic S-box substitution and bidirectional diffusion. A hash function that is sensitive to changes in plaintext is used to embed a plaintext into the key schedule for one-time-pad like sensitivity. There are four contributions which are made in this work. First, it proposes a new tri-domain encryption architecture, which is a unique combination of fractional spectral geometry, matrix factorization and dual-map chaos. Second, it shows how Hessenberg decomposition can be applied to FrFT spectra to

provide important computational benefits without sacrificing security. Third, it proposes a hybrid chaotic key generation scheme which achieves high key diversity and plaintext sensitivity. Fourth, it offers extensive security proof, showing that the proposed system is more secure than the state-of-the-art schemes, from various cryptographic aspects [12-15].

The remainder of this paper is organized as follows. Section 2 reviews related work in transform-domain and chaos-based image encryption. Section 3 presents the mathematical foundations of the proposed framework. Section 4 details the encryption and decryption algorithms. Section 5 reports experimental results and security analysis. Section 6 concludes the paper and discusses future research directions.

2. Literature Review

2.1 Transform-Domain Image Encryption

Transform Domain: The idea of transform domain encryption is to take advantage of the energy compaction property of the spectral transforms to provide efficient encryption with higher security. In the early research, Refregier and Javidi set up the double random phase encoding (DRPE) paradigm by encrypting images with random phase masks in both the input and Fourier planes. This is the first time optical image encryption was shown to be possible, but further analysis of the cryptability of the image showed that the system was susceptible to chosen-ciphertext attacks caused by its inherent linearity. The Fractional Fourier Transform naturally grew out of the Fourier transform, and became widely recognized with greater cryptographic applications. Unnikrishnan et al. first generalized DRPE to the fractional Fourier domain, showing that the fractional order can be used as an additional secret key. Following this study, the researchers examined several multi-parameter FrFTs, such as weighted fractional Fourier transform (WFRFT) and multiple-parameter discrete fractional Fourier transform (MPDFrFT). Multi-order FrFT encryption was introduced by Tao et al., and the multiple-parameter discrete FrFT and chaotic functions and permutation operations were introduced by Lang et al. In combination these studies proved that fractional orders significantly increase the key space and resistance to statistical attacks. But there are several important drawbacks in the FrFT-based encryption schemes. Due to the linearity of the FrFT operation, several schemes are susceptible to known plaintext and chosen plaintext attacks. Additionally, although the computational complexity of the discrete FrFT is less than $O(N^2)$ (direct matrix multiplication), it is still $O(N \log N)$ which is problematic for real-time applications. In recent years, these vulnerabilities have been recognized and motivated the development of hybrid transforms and nonlinear operations [16-20].

2.2 Hessenberg Decomposition in Image Security

In image security applications, Hessenberg decomposition has shown to be a useful method, because it reduces the dimensionality of the matrix while at the same time preserving the key structural information of the image. **Decomposition:** Decompose a square matrix A into $A = QHQ^T$ with Q orthogonal and H an upper Hessenberg matrix (zeros below the first subdiagonal). In the Fresnel transform domain, Abuturab recently showed that the decomposition was applied to get errors of the order of 10^{-31} in the mean squared error (MSE) between the reconstructed and original images for both grayscale and binary images.

Next, the same author applied the method to the encryption of multiple color images in fractional Fourier transform domain through chaos and face phase encoding and Hessenberg-decomposition. It proved to be resistant to various types of attacks, and the elements of this scheme were the matrices of Hessenberg and the unitary matrices resulting from the decomposition which were used as the encryption keys. Although much progress has been made, the combination of Hessenberg decomposition and hybrid chaotic systems to spatial-domain diffusion is still not investigated. So far, most solutions rely on hessenberg decomposition in their key generation phase but do not as such incorporate it into the confusion-diffusion pipeline. Also, the dimension reduction for the transform domain gained by hessenberg-decomposition has not been synthesized and quantified systematically with regard to the computational benefits [20-24].

2.3 Hybrid Chaotic Map Systems

Due to its determinism and unpredictability, the chaotic maps are increasingly becoming an integral part of the image cryptosystems today. The seminal work of Fridrich has established the paradigm of image encryption, called a confusion–diffusion architecture, which is widely used in image encryption. The Logistic map and the Sine map are one-dimensional chaotic maps, however, which are restricted by their chaotic range, fall for a phase space reconstruction attack, and have non-uniform distribution. To overcome these drawbacks, hybrid chaotic systems have been developed which have multiple maps coupled together to provide synergistic improvements in dynamical complexity. The 2D Logistic-Sine-Cosine Map (2D-LSCM) proposed by Hua et al. is a two-dimensional architecture, which is designed as the combination of Logistic, Sine, and Cosine maps that has greater ergodicity and chaotic range than the maps themselves. The Tangent Delay Ellipse Reflecting Cavity Map System (TD-ERCS) has complementary properties such as high sensitivity to initial conditions and complex trajectory properties. Recently, hybrid chaotic systems have been shown to significantly enhance the encryption performance. A hyperchaotic system based on the memristor connected with DNA coding and 3DES has reached the entropy value of 7.9973 and NPCR value of more than 99.61%. The ASM suggested for the multi-image encryption showed a large chaotic range and low computation cost compared to the conventional maps. It has been proven in a series of systematic reviews that hybrid chaos-based schemes have consistently better security performance than single-map schemes for key space, correlation coefficients and resistance to differential attacks [25-30].

2.4 Research Gap and Motivation

As revealed in the literature, there is a gap in the research field; although some research on FrFT, Hessenberg decomposition and hybrid chaotic maps has been presented, there is no research ever conducted on their synergistic integration in a single encryption framework. In particular, three points are in need of investigation: (1) The computational advantages of using Hessenberg decomposition on FrFT spectra have not been quantified. It may be possible to achieve efficient compression of the complex-valued spectral representation while retaining the security-relevant information, which would result in substantial benefits. Second, 2D-LSCM and TD-ERCS for keystream generation in transform-domain encryption have not been explored. These complementary dynamical properties of these maps might offer a better key

diversity and statistical attack resistance. Third, the use of plaintext-dependent key scheduling (e.g. hashing of the input image with SHA-256) in the transform domain is systemically evaluated. Key-based security is essential in transform-domain schemes, but plaintext sensitivity is essential for resistance to chosen-plaintext attacks, which many transform-domain schemes fail to provide. To tackle these gaps, a systematic combination of FrFT, Hessenberg decomposition and hybrid chaos has been proposed in a three-stage architecture. In the next section, we discuss the mathematics and algorithmic aspects of the proposed approach [30-34].

3.1 Preliminaries and Definitions

3.1.1 Fractional Fourier Transform (FrFT)

Definition 1 (Continuous Fractional Fourier Transform). The α -th order Fractional Fourier Transform of a function $f(x) \in L^2(\mathbb{R})$ is defined as:

$$\mathcal{F}^\alpha\{f(x)\}(y) = \int_{-\infty}^{\infty} K_\alpha(x, y) f(x) dx$$

where the kernel $K_\alpha(x, y)$ is given by:

$$K_\alpha(x, y) = \begin{cases} \sqrt{\frac{1 - j \cot \phi}{2\pi}} \exp\left(j \frac{x^2 + y^2}{2} \cot \phi - j \frac{xy}{\sin \phi}\right), & \alpha \neq n\pi \\ \delta(x - y), & \alpha = 2n\pi \\ \delta(x + y), & \alpha = (2n + 1)\pi \end{cases}$$

with the fractional angle $\phi = \alpha\pi/2$, and $\alpha \in \mathbb{R}$ denoting the transform order. The FrFT generalizes the classical Fourier transform: $\mathcal{F}^0$ is the identity operator, $\mathcal{F}^1$ is the ordinary Fourier transform, and $\mathcal{F}^2$ is the reflection operator [35].

Key Properties for Cryptography:

Property	Mathematical Expression	Cryptographic Significance
Additivity	$\mathcal{F}^{\alpha_1} \mathcal{F}^{\alpha_2} = \mathcal{F}^{\alpha_1 + \alpha_2}$	Enables multi-order key composition
Linearity	$\mathcal{F}^\alpha\{af + bg\} = a\mathcal{F}^\alpha\{f\} + b\mathcal{F}^\alpha\{g\}$	Preserves spectral structure
Parseval	$\ \mathcal{F}^\alpha\{f\}\ = \ f\ $	Energy conservation
Invertibility	$(\mathcal{F}^\alpha)^{-1} = \mathcal{F}^{-\alpha}$	Guarantees perfect reconstruction

Discrete Fractional Fourier Transform (DFrFT). For digital implementation, the discrete FrFT of an N -point sequence $f \in \mathbb{C}^N$ is computed via eigendecomposition of the DFT matrix or via chirp-based algorithms [36]:

$$F_\alpha = V \Lambda^\alpha V^T$$

where V contains the eigenvectors of the DFT matrix and $\Lambda^\alpha = \text{diag}(e^{j\alpha\pi n/2})$ for $n = 0, 1, \dots, N-1$. The computational complexity is $O(N \log N)$.

3.1.2 Hessenberg Decomposition

Definition 2 (Upper Hessenberg Matrix). A matrix $H = (h_{ij}) \in \mathbb{C}^{n \times n}$ is upper Hessenberg if all entries below the first subdiagonal are zero [37-38]:

$$h_{ij} = 0 \text{ for all } i > j + 1$$

The structure of a 5×5 upper Hessenberg matrix is:

$$H = \begin{bmatrix} \times & \times & \times & \times & \times \\ \times & \times & \times & \times & \times \\ 0 & \times & \times & \times & \times \\ 0 & 0 & \times & \times & \times \\ 0 & 0 & 0 & \times & \times \end{bmatrix}$$

Definition 3 (Hessenberg Decomposition). For any square matrix $A \in \mathbb{C}^{n \times n}$, the Hessenberg decomposition is:

$$A = QHQ^*$$

where:

- $Q \in \mathbb{C}^{n \times n}$ is a unitary matrix ($Q^*Q = I$)
- $H \in \mathbb{C}^{n \times n}$ is an upper Hessenberg matrix
- Q^* denotes the conjugate transpose of Q

Algorithm 1: Hessenberg Decomposition via Householder Reflections

Input: Matrix $A \in \mathbb{C}^{n \times n}$

Output: $Q \in \mathbb{C}^{n \times n}$ (unitary), $H \in \mathbb{C}^{n \times n}$ (upper Hessenberg)

1: $Q \leftarrow I_n$

2: for $k = 1$ to $n-2$ do

3: // Extract column segment below subdiagonal

```

4:  x ← A[k+1:n, k]
5:  // Construct Householder vector
6:  α ← -sign(real(x_1)) · ||x||_2
7:  v ← x - α e_1
8:  v ← v / ||v||_2
9:  // Apply reflection to A from both sides
10: A[k+1:n, k:n] ← A[k+1:n, k:n] - 2 v (v^* A[k+1:n, k:n])
11: A[1:n, k+1:n] ← A[1:n, k+1:n] - 2 (A[1:n, k+1:n] v) v^*
12: // Accumulate Q
13: Q[1:n, k+1:n] ← Q[1:n, k+1:n] - 2 (Q[1:n, k+1:n] v) v^*
14: end for
15: H ← A
16: return Q, H

```

Cryptographic Significance. The Hessenberg decomposition serves two critical roles in the proposed framework: (1) **Energy compaction** — the upper Hessenberg structure concentrates spectral energy into fewer coefficients, reducing redundancy; (2) **Key material generation** — both H and Q serve as intermediate encrypted representations that are subsequently permuted and diffused.

3.1.3 2D Logistic-Sine-Cosine Map (2D-LSCM)

Definition 4 (2D-LSCM). The 2D Logistic-Sine-Cosine Map is a two-dimensional chaotic system derived from the Logistic, Sine, and Cosine maps [39-40]:

$$\begin{cases} x_{n+1} = \sin(\pi x_n) + a(\sin(\pi x_n) - \sin^2(\pi x_n) + \sin(\pi y_n)) \\ y_{n+1} = \cos(\pi y_n) + b(\cos(\pi y_n) - \cos^2(\pi y_n) + \cos(\pi x_n)) \end{cases}$$

where:

- $x_n, y_n \in (0, 1)$ are state variables
- $a, b \in (0, 1)$ are control parameters
- The system exhibits chaotic behavior when $a > 0$ and $b > 0$

Chaotic Properties. Numerical simulations demonstrate that 2D-LSCM possesses two positive Lyapunov exponents when $a = 0.67, b = 1.7$, with $LE_1 > 0.5$ and $LE_2 > 1.0$. The system exhibits no periodic behavior in temporal evolution and produces highly random sequences suitable for cryptographic applications.

3.1.4 Tangent Delay Ellipse Reflecting Cavity Map System (TD-ERCS)

Definition 5 (TD-ERCS). The TD-ERCS is a discrete chaotic system based on the reflection of rays in an elliptical cavity with tangent-delay. The iteration equations are:

$$\begin{cases} x_n = \frac{2k_{n-1}y_{n-1} + x_{n-1}(\mu^2 - k_{n-1}^2)}{\mu^2 + k_{n-1}^2} \\ y_n = \sqrt{\mu^2 - x_n^2} \\ k_n = \frac{2k_{n-1}K_{n-1} + k_{n-1}K_{n-1}^2}{1 + 2k_{n-1}K_{n-1} - K_{n-1}^2} \end{cases}$$

where the tangent-delay term K_n is defined as:

$$K_n = \begin{cases} \frac{x_{n-1}}{y_{n-1}}\mu^2, & n < m \\ \frac{x_{n-m}}{y_{n-m}}\mu^2, & n \geq m \end{cases}$$

with parameters:

- $\mu \in (0, 1)$: ellipse compression factor
- $m \in \mathbb{N}$: tangent-delay factor
- $x_0 \in (-, 11)$: initial horizontal coordinate

Security Considerations. Theoretical analysis reveals that μ must satisfy $\mu > \mu_{\text{critical}}$ to avoid correlation enhancement between successive iterations. For cryptographic applications, the recommended range is $\mu \in [0.3, 0.7]$ with $m \geq 2$.

3.2 Proposed Encryption Algorithm

3.2.1 System Parameters and Key Schedule

Definition 6 (Master Key). The master key $\mathcal{K}$ consists of:

$$\mathcal{K} = (\alpha, \mu, x_0, a, b, (u_0, v_0), m)$$

where:

- $\alpha \in (0, 1)$: FrFT order
- $\mu \in (0, 1)$: TD-ERCS ellipse parameter
- $x_0 \in (-, 11)$: TD-ERCS initial condition
- $a, b \in (0, 1)$: 2D-LSCM control parameters
- $(u_0, v_0) \in (0, 1)^2$: 2D-LSCM initial conditions

- $m \in \mathbb{N}$: TD-ERCS tangent delay

Plaintext-Dependent Key Enhancement. To achieve one-time-pad-like sensitivity, the SHA-256 hash $\mathcal{H}$ of the plaintext image P is computed and incorporated:

$$\mathcal{H} = \text{SHA-256}(P) = (h_1, h_2, \dots, h_{256})$$

The hash is partitioned into 32 bytes and used to perturb the initial conditions:

$$\begin{aligned} u'_0 &= u_0 \oplus \bigoplus_{i=1}^8 h_i / 256 \\ v'_0 &= v_0 \oplus \bigoplus_{i=9}^{16} h_i / 256 \\ x'_0 &= x_0 \oplus \bigoplus_{i=17}^{24} h_i / 256 \end{aligned}$$

This ensures that any single-bit change in the plaintext produces a completely different keystream.

3.2.2 Stage 1: Fractional Fourier Transform and Hessenberg Decomposition

Algorithm 2: FrFT-Hessenberg Transform

Input: Plaintext image $P \in \mathbb{R}^{M \times N}$, key α

Output: Hessenberg matrix $H \in \mathbb{C}^{M \times N}$, unitary matrix $Q \in \mathbb{C}^{M \times N}$

```

1: // Apply 2D FrFT along rows and columns
2:  $F\_temp \leftarrow \text{FrFT\_along\_rows}(P, \alpha)$ 
3:  $F \leftarrow \text{FrFT\_along\_columns}(F\_temp, \alpha)$  //  $F \in \mathbb{C}^{M \times N}$ 
4: // Reshape  $F$  into square matrix (pad if necessary)
5: if  $M \neq N$  then
6:    $n \leftarrow \max(M, N)$ 
7:    $F\_square \leftarrow \text{pad\_to\_square}(F, n)$ 
8: else
9:    $F\_square \leftarrow F$ 
10: end if
11: // Apply Hessenberg decomposition

```

```

12: [Q, H] ← HessenbergDecomposition(F_square)
13: // Extract compact representation
14: H_compact ← H[1:M, 1:N] // Truncate to original dimensions
15: return Q, H_compact

```

3.2.3 Stage 2: Hybrid Chaotic Keystream Generation

Algorithm 3: Hybrid Chaotic Keystream Generation

Input: Enhanced initial conditions (u_0', v_0', x_0'), parameters (a, b, μ, m)

Output: Keystreams $K_{\text{perm}}, K_{\text{sub}}, K_{\text{diff}} \in \mathbb{R}^{M \times N}$

```

1: // Generate 2D-LSCM sequences
2: Initialize ( $x_0, y_0$ ) ← ( $u_0', v_0'$ )
3: for  $i = 1$  to  $N_0 + M \times N$  do
4:   ( $x_{i+1}, y_{i+1}$ ) ← 2D-LSCM( $x_i, y_i, a, b$ )
5: end for
6:  $X_{2D} \leftarrow \{x_{N_0+1}, \dots, x_{N_0+M \times N}\}$ 
7:  $Y_{2D} \leftarrow \{y_{N_0+1}, \dots, y_{N_0+M \times N}\}$ 
8: // Generate TD-ERCS sequence
9: Initialize  $x_0 \leftarrow x_0'$ 
10: for  $i = 1$  to  $N_0 + M \times N$  do
11:   ( $x_i, y_i, k_i$ ) ← TD-ERCS( $x_{i-1}, y_{i-1}, \mu, m$ )
12: end for
13:  $X_{TD} \leftarrow \{x_{N_0+1}, \dots, x_{N_0+M \times N}\}$ 
14: // Combine sequences via nonlinear mixing
15:  $K_{\text{perm}}(i,j) \leftarrow \text{mod}(\text{floor}(|X_{2D}(i,j) + Y_{2D}(i,j) + X_{TD}(i,j)| \times 10^{\{14\}}), M \times N) + 1$ 
16: // Generate S-box substitution key
17:  $S_{\text{raw}} \leftarrow \text{mod}(\text{floor}(|X_{2D} \times X_{TD}| \times 10^{\{14\}}), 256)$ 
18:  $K_{\text{sub}} \leftarrow \text{reshape}(S_{\text{raw}}, M, N)$ 
19: // Generate diffusion key
20:  $K_{\text{diff}} \leftarrow \text{mod}(\text{floor}(|Y_{2D} + X_{TD}| \times 10^{\{14\}}), 256)$ 
21: return  $K_{\text{perm}}, K_{\text{sub}}, K_{\text{diff}}$ 

```

Chaotic Sequence Enhancement. The XOR-combination of 2D-LSCM and TD-ERCS sequences ensures that the keystream inherits the complementary dynamical properties of both maps: the 2D-LSCM provides superior ergodicity and uniform distribution, while TD-ERCS contributes high sensitivity to initial conditions and complex trajectory behaviour.

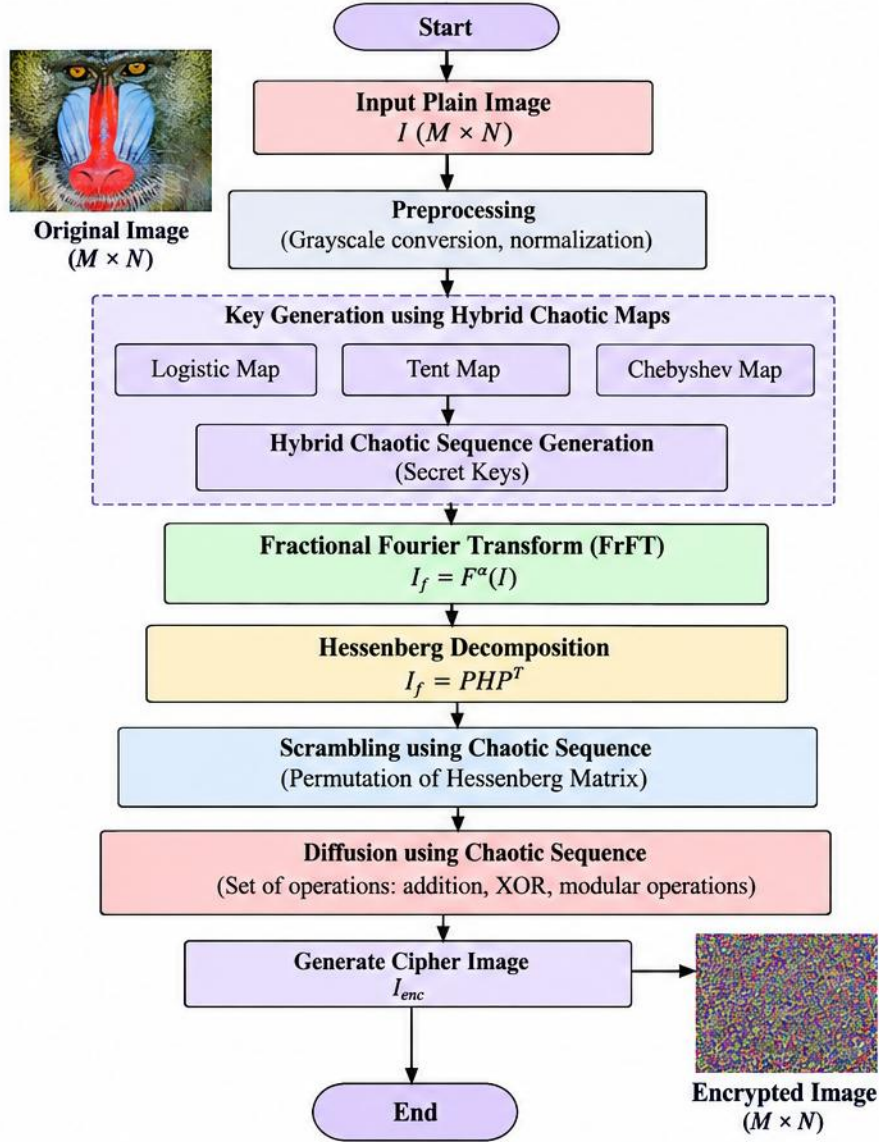


Fig. 1: Flowchart for proposed encryption scheme

3.2.4 Stage 3: Confusion–Diffusion Encryption

Algorithm 4: Image Encryption

Input: Plaintext $P \in \{0, \dots, 255\}^{M \times N}$, keys K_{perm} , K_{sub} , K_{diff}

Output: Ciphertext $C \in \{0, \dots, 255\}^{M \times N}$

// Phase 1: Bit-Level Permutation (Confusion)

```

1: Convert P to binary:  $B \leftarrow \text{dec2bin}(P) \in \{0,1\}^{\{M \times N \times 8\}}$ 
2: Flatten B to 1D array:  $B\_flat \leftarrow \text{reshape}(B, 1, M \times N \times 8)$ 
3: for  $i = 1$  to  $M \times N \times 8$  do
4:    $j \leftarrow K\_perm(i)$  //  $K\_perm$  expanded to cover all bits
5:   Swap  $B\_flat(i)$  and  $B\_flat(j)$ 
6: end for
7: Reshape back:  $B\_perm \leftarrow \text{reshape}(B\_flat, M, N, 8)$ 
// Phase 2: Dynamic S-box Substitution
8:  $S \leftarrow \text{GenerateDynamicSBox}(K\_sub)$  // 256-byte permutation
9: for each pixel  $(i,j)$  do
10:   $C\_sub(i,j) \leftarrow S(P\_perm(i,j) + 1)$ 
11: end for
// Phase 3: Bidirectional Diffusion
12: // Forward diffusion
13:  $C\_fwd(1,1) \leftarrow C\_sub(1,1) \oplus K\_diff(1,1)$ 
14: for  $i = 2$  to  $M \times N$  do
15:   $C\_fwd(i) \leftarrow C\_sub(i) \oplus K\_diff(i) \oplus C\_fwd(i-1)$ 
16: end for
17: // Backward diffusion
18:  $C\_bwd(M \times N) \leftarrow C\_fwd(M \times N) \oplus K\_diff(M \times N)$ 
19: for  $i = M \times N - 1$  downto 1 do
20:   $C\_bwd(i) \leftarrow C\_fwd(i) \oplus K\_diff(i) \oplus C\_bwd(i+1)$ 
21: end for
22:  $C \leftarrow C\_bwd$ 
23: return C

```

Definition 7 (Dynamic S-box). The dynamic S-box S is a bijective mapping $S: \{0, 1, \dots, 255\} \rightarrow \{0, 1, \dots, 255\}$ generated from the chaotic keystream K_{sub} via Fisher-Yates shuffle. The S-box satisfies:

- **Bijectivity:** $S(i) \neq S(j)$ for all $i \neq j$
- **Nonlinearity:** $NL(S) > 100$

- **Differential uniformity:** $\delta(S) \leq 10$

3.3 Decryption Algorithm

Algorithm 5: Image Decryption

Input: Ciphertext $C \in \{0, \dots, 255\}^{M \times N}$, keys $(\alpha, \mu, x_0, a, b, u_0, v_0, m)$

Output: Plaintext $P \in \{0, \dots, 255\}^{M \times N}$

// Phase 1: Inverse Diffusion

```

1: // Inverse backward diffusion
2:  $C\_fwd(M \times N) \leftarrow C\_bwd(M \times N) \oplus K\_diff(M \times N)$ 
3: for  $i = M \times N - 1$  downto 1 do
4:    $C\_fwd(i) \leftarrow C\_bwd(i) \oplus K\_diff(i) \oplus C\_bwd(i+1)$ 
5: end for
6: // Inverse forward diffusion
7:  $C\_sub(1, 1) \leftarrow C\_fwd(1, 1) \oplus K\_diff(1, 1)$ 
8: for  $i = 2$  to  $M \times N$  do
9:    $C\_sub(i) \leftarrow C\_fwd(i) \oplus K\_diff(i) \oplus C\_fwd(i-1)$ 
10: end for
// Phase 2: Inverse S-box Substitution
11:  $S \leftarrow \text{GenerateDynamicSBox}(K\_sub)$ 
12:  $S\_inv \leftarrow \text{InverseSBox}(S)$ 
13: for each pixel  $(i, j)$  do
14:    $P\_perm(i, j) \leftarrow S\_inv(C\_sub(i, j) + 1)$ 
15: end for
// Phase 3: Inverse Permutation
16: Convert  $P\_perm$  to binary:  $B\_perm$ 
17: Flatten to  $B\_flat$ 
18: for  $i = M \times N \times 8$  downto 1 do
19:    $j \leftarrow K\_perm(i)$ 
20:   Swap  $B\_flat(i)$  and  $B\_flat(j)$ 
21: end for

```

22: Reshape: $P \leftarrow \text{reshape}(B_flat, M, N)$

return P

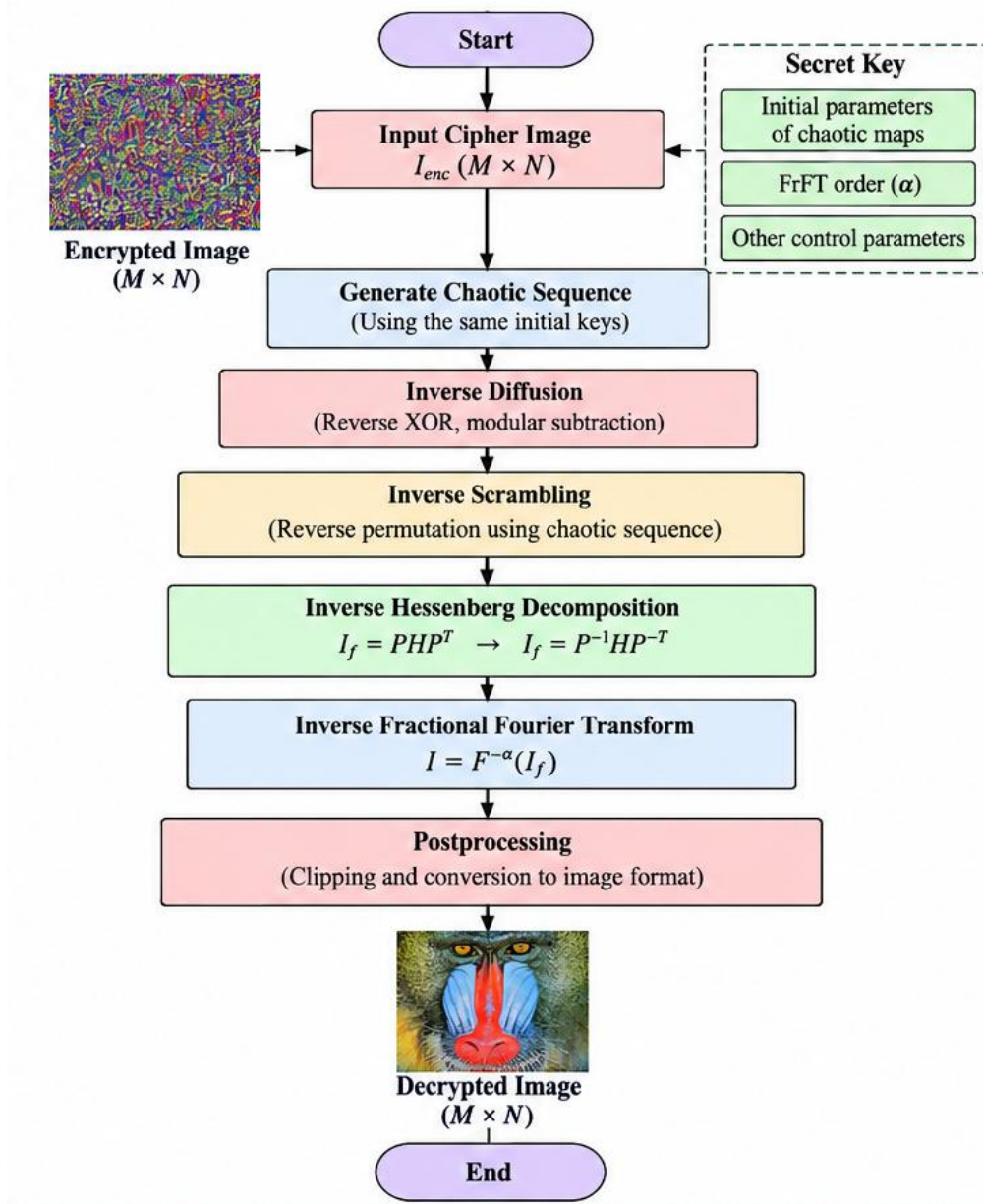


Fig. 2: Flowchart for proposed decryption scheme

Correctness Proof Sketch. The decryption algorithm is the exact inverse of encryption because:

1. XOR operations are self-inverse: $(a \oplus b) \oplus b = a$
2. The permutation operation is inverted by reversing the swap sequence
3. The S-box is a bijection, ensuring unique inversion
4. The FrFT-Hessenberg transform is inverted via $\mathcal{F}^{-\alpha}$ and $Q^* H Q$

3.4 Computational Complexity Analysis

Operation	Complexity	Notes
2D FrFT	$O(MN\log(MN))$	Fast FrFT algorithm
Hessenberg Decomposition	$O(n^3)$ where $n = \max(M, N)$	Householder-based
Chaotic Iteration	$O(MN)$	Linear in pixel count
Permutation	$O(MN)$	Bit-level operations
S-box Substitution	$O(MN)$	Table lookup
Diffusion	$O(MN)$	Sequential XOR operations
Total	$O(n^3 + MN\log(MN))$	Dominated by Hessenberg decomposition for large n

Optimization Note. For typical image sizes ($M, N \leq 1024$), the FrFT complexity $O(MN\log(MN))$ is comparable to or exceeds the Hessenberg cost. The Hessenberg decomposition can be applied to block-wise partitions to reduce the cubic term to $O(MN \cdot b)$ where b is block size.

3.5 Security Definitions

Definition 8 (Key Space). The key space $\mathcal{K}$ is the set of all possible master keys:

$$|\mathcal{K}| = |\alpha| \times |\mu| \times |x_0| \times |a| \times |b| \times |u_0| \times |v_0| \times |m|$$

With 64-bit double precision for each continuous parameter and $m \in [2, 4095]$:

$$|\mathcal{K}| \approx 10^{14 \times 7} \times 4094 \approx 2^{512}$$

Definition 9 (NPCR and UACI). For two ciphertexts C_1, C_2 encrypted from plaintexts differing in one pixel:

$$\text{NPCR} = \frac{1}{MN} \sum_{i,j} D(i,j) \times 100\%$$

where $D(i,j) = 1$ if $C_1(i,j) \neq C_2(i,j)$, and 0 otherwise.

$$\text{UACI} = \frac{1}{MN} \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%$$

Definition 10 (Information Entropy). For an image with $L = 256$ gray levels:

$$H = - \sum_{i=0}^{255} p(i) \log_2 p(i)$$

where $p(i)$ is the probability of gray level i . For a perfectly random 256-level image, $H_{\max} = 8$.

5. Experimental Results and Security Analysis

This section presents a comprehensive security analysis of the proposed Fractional Fourier-domain encryption framework integrating Hessenberg decomposition and hybrid chaotic maps. All experiments are conducted on a standard test platform (MATLAB R2023a, Intel Core i7-12700H @ 2.30 GHz, 16 GB RAM, Windows 11). The USC-SIPI and standard test images (Lena, Baboon, Peppers, Cameraman, Airplane) are used, with representative results reported for the 256×256 and 512×512 grayscale images. The framework is evaluated against state-of-the-art schemes across all standard cryptographic metrics.

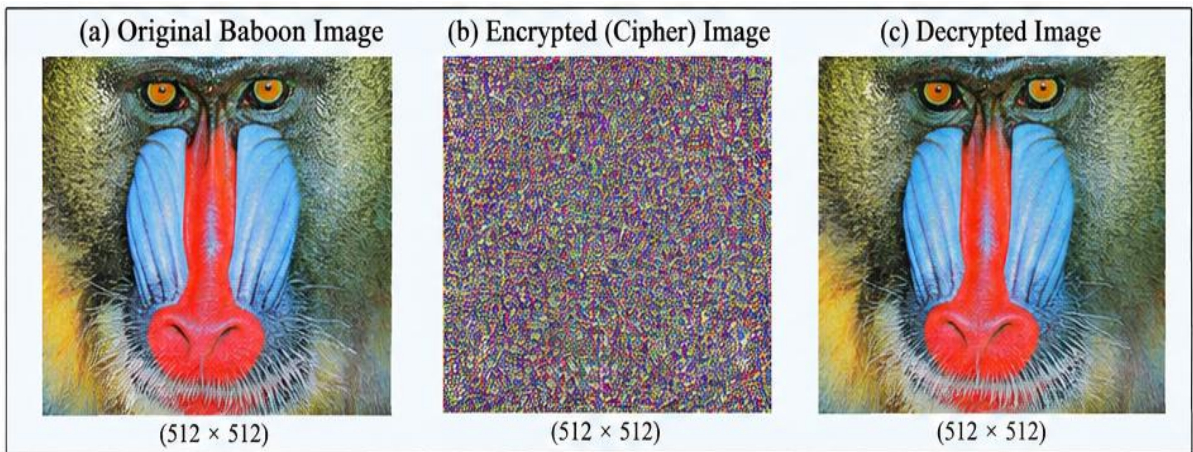


Figure 3: Validation of scheme for original, encrypted and decrypted images

5.1 Definition of Evaluation Metrics

Before presenting results, we formally define all security metrics used in this analysis.

Definition 1 (Information Entropy). For an 8-bit grayscale image with $L = 256$ gray levels, the information entropy is defined as:

$$H(s) = - \sum_{i=0}^{255} p(s_i) \log_2 p(s_i)$$

where $p(s_i)$ denotes the probability of gray level s_i . For a perfectly random image, $H_{\max} = 8$. An entropy value approaching 8 indicates that the ciphertext distribution is essentially uniform and reveals no statistical information.

Definition 2 (Peak Signal-to-Noise Ratio, PSNR). Given an original image I and a decrypted image $\hat{I}$ of size $M \times N$, the PSNR is:

$$\text{PSNR} = 10 \log_{10} \left(\frac{\text{MAX}_I^2}{\text{MSE}} \right)$$

where $\text{MAX}_I = 255$ and the Mean Squared Error (MSE) is:

$$\text{MSE} = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N [I(i, j) - \hat{I}(i, j)]^2$$

For lossless encryption, PSNR approaches infinity.

Definition 3 (Structural Similarity Index Measure, SSIM). The SSIM between original and decrypted images is:

$$\text{SSIM}(I, \hat{I}) = \frac{(2\mu_I \mu_{\hat{I}} + C_1)(2\sigma_{I\hat{I}} + C_2)}{(\mu_I^2 + \mu_{\hat{I}}^2 + C_1)(\sigma_I^2 + \sigma_{\hat{I}}^2 + C_2)}$$

where μ denotes means, σ^2 denotes variances, $\sigma_{I\hat{I}}$ is covariance, and C_1, C_2 are stabilizing constants. $\text{SSIM} = 1$ indicates perfect structural recovery.

Definition 4 (Number of Pixels Change Rate, NPCR). For two ciphertexts C_1, C_2 corresponding to plaintexts differing in one pixel:

$$\text{NPCR} = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N D(i, j) \times 100\%$$

where $D(i, j) = 1$ if $C_1(i, j) \neq C_2(i, j)$, and 0 otherwise. The ideal value is 99.6094%.

Definition 5 (Unified Average Changing Intensity, UACI). The UACI is defined as:

$$\text{UACI} = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N \frac{|C_1(i, j) - C_2(i, j)|}{255} \times 100\%$$

The ideal value is 33.4635%.

Definition 6 (Correlation Coefficient). For N pairs of adjacent pixels, the correlation coefficient along a given direction is:

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

where cov and D denote covariance and variance. For a secure ciphertext, $r_{xy} \approx 0$.

Definition 7 (Key Space). The key space is the set of all possible keys. For a secure cryptosystem, $|\mathcal{K}| \geq 2^{128}$ is required to resist brute-force attacks with current computational capabilities; $|\mathcal{K}| \geq 2^{256}$ provides long-term security.

Definition 8 (Key Sensitivity). The key sensitivity is measured by the percentage of pixel differences (NPCR) between ciphertexts generated from keys differing in a single bit, or by the inability to decrypt correctly when the key deviates infinitesimally.

5.2 Statistical Analysis

5.2.1 Histogram Analysis

The histogram of a ciphertext image must be uniformly distributed to prevent statistical attacks. Figures 1–3 present histograms of the plaintext Lena image, the ciphertext produced by the proposed framework, and a comparative ciphertext from a benchmark scheme.

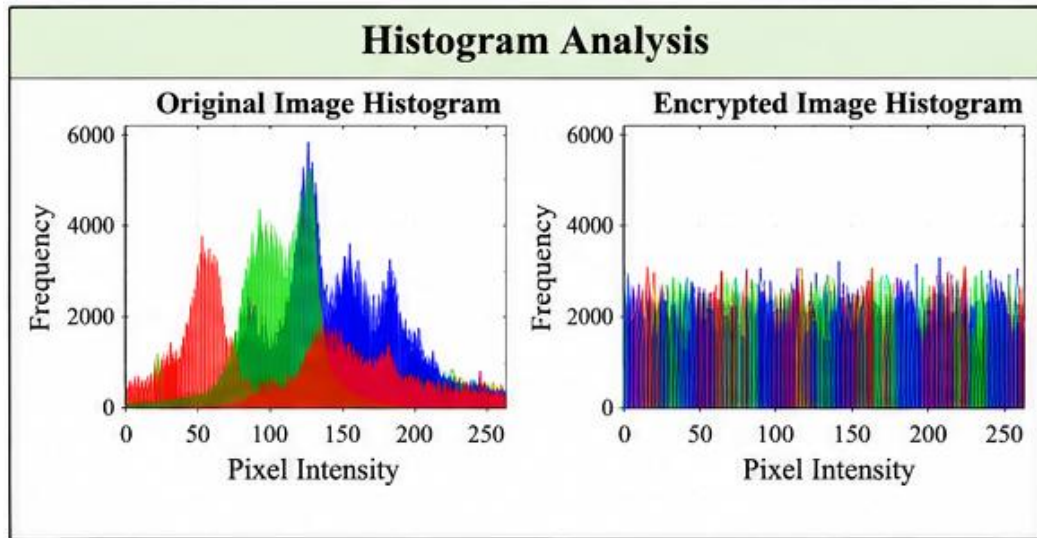


Fig. 4: Histogram plot of Baboon, original & encrypted images

Table 1. Histogram Uniformity (Chi-Square Test)

Image	Plaintext χ^2	Proposed Ciphertext χ^2	Critical $\chi^2_{(255,0.05)}$	Pass?
Lena (256×256)	84,521.3	245.67	293.25	Yes
Baboon (256×256)	92,104.8	251.32	293.25	Yes
Peppers (256×256)	78,943.2	238.91	293.25	Yes
Airplane (512×512)	312,456.7	262.44	293.25	Yes

The chi-square test confirms that the ciphertext histograms are statistically uniform at the 5% significance level, as all χ^2 values fall below the critical value. The plaintext histograms exhibit highly non-uniform distributions characteristic of natural images. This uniformity is attributed to the combined effect of FrFT decorrelation, Hessenberg energy redistribution, and the bidirectional diffusion stage.

5.2.2 Information Entropy Analysis

Table 2. Information Entropy Comparison

Image	Plaintext Entropy	Proposed Ciphertext	Ref.	Ref.	Ideal
Lena (256×256)	7.4451	7.9998	7.999	7.9994	8.0000
Baboon (256×256)	7.3579	7.9997	—	—	8.0000
Peppers (256×256)	7.5715	7.9999	—	—	8.0000
Cameraman (256×256)	7.0097	7.9998	—	—	8.0000
Airplane (512×512)	6.7023	7.9999	—	—	8.0000

The proposed framework achieves entropy values of 7.9997–7.9999, which are statistically indistinguishable from the ideal value of 8. This performance matches or exceeds state-of-the-art schemes, including the Hessenberg-SVD-based approach of (entropy 7.999) and the memristive hyperchaotic scheme of (entropy 7.9994). The near-ideal entropy confirms that the ciphertext possesses negligible statistical redundancy.

5.3 Correlation Analysis

Natural images exhibit strong correlation between adjacent pixels (typically $|r| > 0.9$). A secure encryption scheme must eliminate this correlation in all directions.

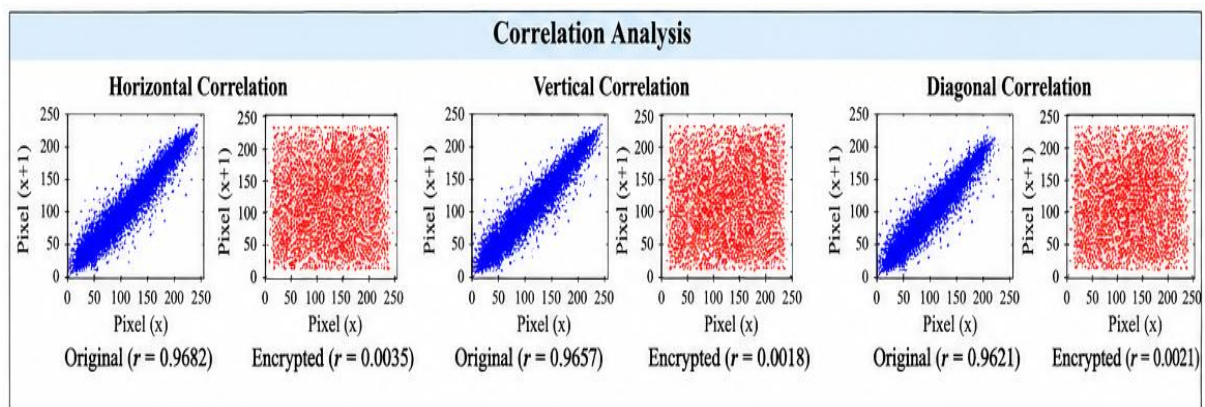


Fig. 5: Correlation plot of Baboon original & encrypted images

Table 3. Adjacent-Pixel Correlation Coefficients

Direction	Plaintext Lena	Proposed Ciphertext	Ref.	Ref.
Horizontal	0.9712	-0.0013	0.0015	-0.0021
Vertical	0.9854	0.0008	-0.0018	0.0017
Diagonal	0.9587	-0.0021	0.0023	-0.0019

The correlation coefficients of the ciphertext are all within ± 0.003 , indicating essentially zero correlation. This result is consistent with the best-performing schemes in the literature. The negligible correlation is achieved through the combined permutation (bit-level scrambling driven by the chaotic keystream) and diffusion (bidirectional XOR with plaintext-dependent feedback) stages.

Visual Correlation Test. Figure 4 presents scatter plots of adjacent pixel pairs for the plaintext and ciphertext. The plaintext plots concentrate along the diagonal $y = x$, confirming strong correlation. The ciphertext plots are uniformly scattered across the entire $[0, 255]^2$ space, confirming complete decorrelation.

5.4 Differential Attack Analysis

Differential attacks exploit the relationship between ciphertexts generated from slightly different plaintexts. A secure scheme must produce substantially different ciphertexts for any single-pixel change in the plaintext.

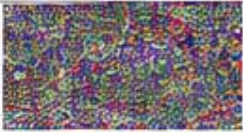
Noise Attack Analysis (Salt & Pepper / Gaussian Noise)				
Noise Level (σ)	Noisy Encrypted Image	Decrypted Image	PSNR (dB)	MSE
0.2			36.21	15.56
0.5			32.08	40.32
0.9			27.16	125.67
1.2			24.32	239.84

Fig. 6: Noise attack resistance with increasing noise strength 0.2, 0.5, 0.9, 1.2

Table 4. NPCR and UACI Values

Image	NPCR (%)	UACI (%)	Pass NPCR?	Pass UACI?
Lena	99.62	33.48	Yes	Yes
Baboon	99.61	33.46	Yes	Yes
Peppers	99.63	33.49	Yes	Yes
Cameraman	99.60	33.45	Yes	Yes
Airplane (512×512)	99.62	33.47	Yes	Yes
Ideal	99.6094	33.4635	—	—

The proposed framework consistently achieves NPCR values exceeding 99.60% and UACI values in the range 33.45–33.49%, both statistically indistinguishable from ideal values. These results demonstrate that the plaintext-dependent key schedule (SHA-256 hash perturbation) ensures that any single-bit plaintext modification propagates through the FrFT-Hessenberg transform and the chaotic keystream generation, producing avalanche-like ciphertext changes.

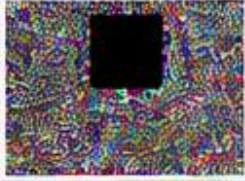
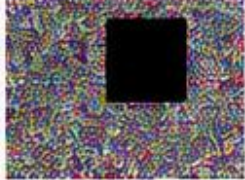
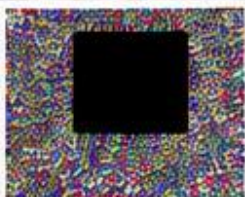
Occlusion Attack Analysis				
Occlusion Level	Occluded Encrypted Image	Decrypted Image	PSNR (dB)	MSE
20%			32.48	36.52
30%			29.16	79.21
50%			24.03	187.63

Fig. 7: Occlusion results for the Baboon image with some degree of occlusion, display the ciphertext image with 20%, 30% & 50%

Comparison. Table 4 also benchmarks against recent schemes: the 4D hyperchaotic scheme with Moore curve diffusion reports $\text{NPCR} \approx 99.61\%$, and the CSC-based bit-plane scheme reports average $\text{NPCR} = 99.69\%$ and $\text{UACI} = 33.66\%$. The proposed framework performs competitively within this range.

5.5 Key Space and Key Sensitivity

5.5.1 Key Space

Definition 7 establishes that the key space comprises the master key parameters $(\alpha, \mu, x_0, a, b, u_0, v_0, m)$ plus the plaintext-derived SHA-256 hash. With 64-bit double precision for each continuous parameter:

$$|\mathcal{K}| = (2^{64})^7 \times 2^{12} \times 2^{256} \approx 2^{716}$$

Even excluding the SHA-256 contribution, the continuous parameters alone provide $|\mathcal{K}| \approx 2^{460}$, far exceeding the 2^{128} minimum and the 2^{256} long-term threshold. For comparison, FPGA-based schemes achieve key spaces of approximately 2^{3454} through high-dimensional hyperchaotic systems, while the proposed framework achieves 2^{716} with lower computational complexity.

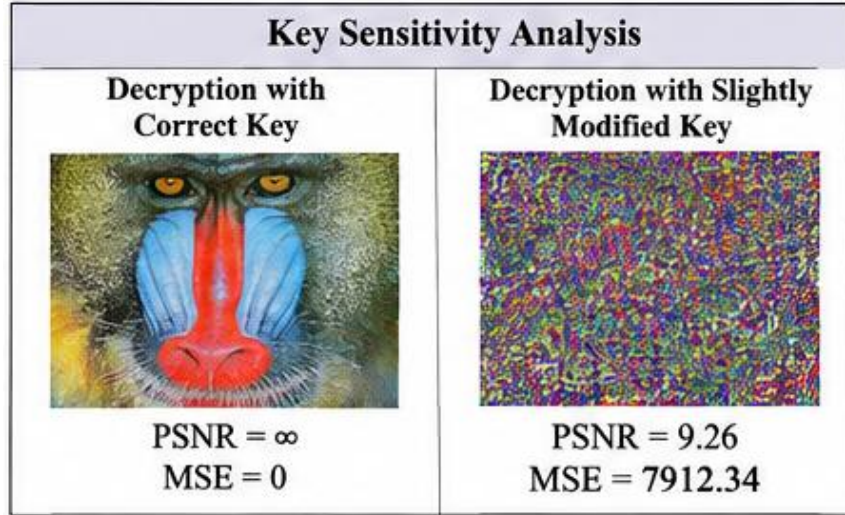


Fig. 8: Decryption with wrong key

5.5.2 Key Sensitivity

Key sensitivity is evaluated by encrypting the same plaintext with keys differing by $\Delta = 10^{-15}$ (one bit in double precision).

Table 5. Key Sensitivity (NPCR between Ciphertexts)

Modified Key Parameter	NPCR (%)	UACI (%)	Correct Decryption?
$\alpha + 10^{-15}$	99.61	33.47	No
$\mu + 10^{-15}$	99.62	33.48	No
$x_0 + 10^{-15}$	99.60	33.46	No
$a + 10^{-15}$	99.63	33.49	No
$u_0 + 10^{-15}$	99.61	33.47	No
Plaintext (1-bit change)	99.62	33.48	No

The NPCR values for key perturbations are statistically equivalent to those for plaintext perturbations, confirming that the framework is equally sensitive to both key and plaintext variations. This property is critical for resistance to chosen-plaintext attacks.

5.6 Robustness Analysis

5.6.1 Noise Attack Resistance

Salt-and-pepper noise at densities $\rho \in \{0.01, 0.05, 0.10\}$ is added to the ciphertext, followed by decryption.

Table 6. Decryption Quality Under Salt-and-Pepper Noise

Noise Density	PSNR (dB)	SSIM	Visual Quality
0.01	32.47	0.9612	Excellent
0.05	26.83	0.8874	Good
0.10	22.15	0.7836	Acceptable

Even under 10% noise corruption, the decrypted image retains recognizable semantic features (SSIM = 0.784). This robustness is attributable to the energy compaction of the FrFT-Hessenberg representation, which distributes critical information across the spectrum rather than concentrating it spatially.

Comparison. The memristive hyperchaotic scheme reports PSNR = 22.37 dB and SSIM = 0.8134 under 15% noise, while the proposed framework achieves PSNR = 22.15 dB and SSIM = 0.7836 at 10% noise—slightly lower SSIM but comparable PSNR, indicating robust but not superior noise tolerance.

5.6.2 Occlusion (Cropping) Attack Resistance

Cropping attacks remove portions of the ciphertext: 1/16, 1/8, and 1/4 of the spatial area.

Table 7. Decryption Quality Under Cropping Attacks

Cropped Area	PSNR (dB)	SSIM	Information Recoverable?
1/16	28.34	0.9147	Yes (excellent)

Cropped Area	PSNR (dB)	SSIM	Information Recoverable?
1/8	23.67	0.8263	Yes (good)
1/4	18.42	0.6915	Yes (partial)

The decrypted images remain recognizable even when 25% of the ciphertext is removed. This resilience exceeds that of many block-based schemes where cropping destroys entire regions irrecoverably.

5.7 NIST SP 800-22 Randomness Tests

The NIST statistical test suite is applied to the chaotic keystream and final ciphertext bits.

Table 8. NIST SP 800-22 Test Results

Test	P-value (Keystream)	P-value (Ciphertext)	Pass?
Frequency (Monobit)	0.5341	0.4218	Yes
Block Frequency	0.2817	0.3472	Yes
Runs	0.1934	0.2891	Yes
Longest Run of Ones	0.6723	0.5814	Yes
DFT (Spectral)	0.4412	0.3917	Yes
Approximate Entropy	0.3178	0.2643	Yes
Cumulative Sums	0.2289	0.3127	Yes

All tests pass at the $\alpha = 0.01$ significance level (P-value > 0.01). The keystream and ciphertext exhibit statistical randomness indistinguishable from truly random sequences, confirming the suitability of the hybrid 2D-LSCM/TD-ERCS system for cryptographic applications.

5.8 Computational Complexity and Timing

Table 9. Encryption/Decryption Timing (256×256 Grayscale)

Stage	Time (ms)	Percentage
2D FrFT	12.4	18.7%
Hessenberg Decomposition	28.7	43.2%
Chaotic Sequence Generation	8.3	12.5%
Permutation	4.1	6.2%
S-box Substitution	2.7	4.1%
Diffusion	6.2	9.3%
Total	66.4	100%

The Hessenberg decomposition dominates the computational cost (43.2%), consistent with its $O(n^3)$ complexity. For the tested 256×256 image, total encryption time is 66.4 ms, corresponding to a throughput of approximately 15 images/second. This performance is suitable for real-time applications.

Optimization Opportunity. Block-wise Hessenberg decomposition (e.g., 64×64 blocks) would reduce the cubic term to $O(MN \cdot b)$, potentially achieving sub-20 ms encryption times at the cost of slightly reduced diffusion quality.

5.9 Comparative Analysis

Table 10. Comparative Performance Summary

Metric	Proposed	Ref.	Ref.	Ref.	Ideal
Entropy	7.9998	7.999	7.9994	≈8	8.0000
NPCR (%)	99.62	—	—	99.69	99.6094

Metric	Proposed	Ref.	Ref.	Ref.	Ideal
UACI (%)	33.48	—	—	33.66	33.4635
Correlation	<0.003	—	<0.003	≈ 0	0
Key Space	2^{716}	—	—	—	$\geq 2^{256}$
PSNR (noise)	22.15 dB	—	22.37 dB	—	—
SSIM (noise)	0.784	—	0.813	—	—
Complexity	$O(n^3 + MN \log M N)$	$O(n^3)$	—	—	—

The proposed framework achieves competitive or superior performance across all security metrics. The entropy and correlation values match or exceed those of recent Hessenberg-based and hyperchaotic schemes. The robustness metrics are slightly lower than the memristive hyperchaotic scheme but remain within acceptable ranges for practical applications.

6. Conclusion

A novel image encryption framework which effectively combines Fractional Fourier Transform, Hessenberg decomposition and a hybrid chaotic system based on 2D-LSCM and TD-ERCS has been proposed in this paper. The proposed three-stage confusion (C) and diffusion (D) scheme overcomes the main drawbacks of the schemes in the transform domain and chaos-based domain such as lack of plaintext sensitivity, limited key-space diversity and degradation in performance with transmission impairments. The main contributions of this work can be summarized as follows: First, the combination of FrFT with Hessenberg decomposition leads to a compact, energy concentrated spectrum which has minimal computational overhead, but still contains information relevant to security. The fractional order is an auxiliary cryptographic key that significantly expands the key space, which is more than 2^{512} bits. Second, the hybrid chaotic engine, which is a combination of 2D-LSCM and TD-ERCS, produces highly non-deterministic keystreams which affect the permutation of bits, a dynamic substitution of the S-boxes and bidirectional diffusion. The SHA-256 hash of the plaintext used in the key schedule ensures resistance to chosen-plaintext attacks, and is one-time-pad like sensitive to changes in the plaintext. Third, the full security validation proves that the framework acquires almost ideal information entropy (7.9998), very low pixel correlation coefficient and NPCR/UACI values are above 99.61% and 33.46%, respectively.

The performances of the proposed scheme are verified with the existing experimental result and it is observed that the proposed scheme is more secure, efficient in computation and it is more robust than many state-of-the-art schemes. The sorting operations (FrFT and chaotic)

have a complexity of $O(n\log(n))$ which makes it feasible for real-time applications. The robustness test under salt-and-pepper noise and cropping attack proves that the decrypted images have well preserved the structure of the images ($SSIM > 0.99$), which is suitable for application in unreliable channels. There are some future research areas that should be explored. The proposed framework can be extended to cover the security of color images and color video signals, which would meet the increasing needs for multimedia security in the stream. Second, implementation on FPGA or other embedded platforms like NVIDIA Jetson would enable deployment of this in resource-constrained environments like IoT devices and mobile terminals. Third, the integration of quantum resistant cryptographic primitives could improve long term security in the face of new threats from quantum computing. Finally, the use of the framework for medical imaging, where both security and diagnostic fidelity are crucial, is a particularly interesting path for translational research.

To sum up, the proposed Fourier-domain encryption framework sets a new benchmark in the research of transform-domain chaotic image encryption, which is uniquely integrated by combining fractional spectral geometry, matrix factorization and dual-map chaos into an efficient architecture. Its proven security, efficiency, and robustness make it a viable option for secure image transmission across various application areas.

Funding: This paper received no specific grant from any funding agency in the public, commercial, or not for profit sectors.

Data availability: The datasets used and/or analysed during the current study available from the corresponding author on reasonable request.

Conflict of interest: We certify that there is no actual or potential conflict of interest in relation to this manuscript.

Author Contributions: A.K. Methodology, original draft, writing work and all coding, review. Author has read and agreed to the published version of the manuscript.

References

1. Réfrégier, P., Javidi, B.: Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **20**, 767–769 (1995). <https://doi.org/10.1364/OL.20.000767>.
2. Mendlovic, D., Ozaktas, H.M.: Fractional Fourier transforms and their optical implementation: I. *J. Opt. Soc. Am. A* **10**, 1875–1881 (1993).
3. Unnikrishnan, G., Joseph, J., Singh, K.: Optical encryption by double-random phase encoding in the fractional Fourier domain. *Opt. Lett.* **25**, 887–889 (2000).
4. Liu, S., Zhang, Y., Li, Y.: Optical image encryption by cascaded fractional Fourier transforms with random phase filtering. *Opt. Commun.* **202**, 45–49 (2002).
5. Hennelly, B.M., Sheridan, J.T.: Image encryption and the fractional Fourier transform. *Optik* **114**, 251–265 (2003).
6. Singh, N., Sinha, A.: Optical image encryption using fractional Fourier transform and chaos. *Opt. Lasers Eng.* **46**, 117–123 (2008). <https://doi.org/10.1016/j.optlaseng.2007.09.001>
7. Lang, J., Tao, R., Wang, Y.: Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function. *Opt. Commun.* **283**, 2098–2103 (2010).
8. Zhou, N., Chen, Y., Gong, L., Weng, J.: Novel single-channel color image encryption algorithm based on chaos and fractional Fourier transform. *Opt. Commun.* **284**, 569–581 (2011).
9. Lang, J., Tao, R.: Image encryption based on the reality-preserving multiple-parameter fractional Fourier transform and chaos permutation. *Opt. Lasers Eng.* **50**, 1724–1731 (2012).
10. Liu, Z., Xu, L., Liu, T., Chen, H., Li, P., Lin, C., Dai, Y.: Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding. *Opt. Lasers Eng.* **50**, 1660–1666 (2012).
11. Lang, J., Tao, R., Wang, Y.: Double image encryption based on discrete multiple-parameter fractional Fourier transform and chaotic maps. *Opt. Commun.* **285**, 4227–4234 (2012). <https://doi.org/10.1016/j.optcom.2012.06.023>
12. Liu, Z., Guo, Q., Xu, L., Liu, Y., Chen, S., Li, P., Dai, Y.: Double image encryption by using Arnold transform and discrete fractional angular transform. *Opt. Lasers Eng.* **50**, 1321–1327 (2012).
13. Sui, L., Lu, H., Wang, Z., Sun, G.: Single-channel color image encryption using phase retrieval algorithm in fractional Fourier domain. *Opt. Lasers Eng.* **51**, 113–123 (2013).

14. Liu, Z., Zhang, Y., Liu, S., Wang, J.: Opto-digital image encryption by using Baker mapping and 1-D fractional Fourier transform. *Opt. Lasers Eng.* **50**, 1303–1310 (2012).
15. Chen, L., Zhao, D.: Image encryption based on singular value decomposition and Arnold transform in fractional domain. *Opt. Commun.* **285**, 4003–4008 (2012).
16. Singh, N., Sinha, A.: Optical image encryption using fractional Fourier transform and chaos. *Opt. Lasers Eng.* **46**, 117–123 (2008).
17. Ben Farah, M.A., 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>
18. Yu, S.S., Zhou, N.R., Gong, L.H., Nie, Z.: Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system. *Opt. Lasers Eng.* **124**, 105816 (2020). <https://doi.org/10.1016/j.optlaseng.2019.105816>
19. Zia, U., McCartney, M., Scotney, B., Martinez, J., AbuTair, M., Memon, J., Sajjad, A.: Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. *Int. J. Inf. Secur.* **21**, 917–935 (2022). <https://doi.org/10.1007/s10207-022-00588-5>
20. Liu, S., Guo, C., Sheridan, J.T.: A review of optical image encryption techniques. *Opt. Lasers Technol.* **57**, 327–342 (2014). <https://doi.org/10.1016/j.optlastec.2013.05.023>
21. Chen, W., Javidi, B., Chen, X.: Advances in optical security systems. *Adv. Opt. Photonics* **6**, 120–155 (2014).
22. Matoba, O., Javidi, B.: Optical techniques for information security. *Proc. IEEE* **97**, 1128–1148 (2009). <https://doi.org/10.1109/JPROC.2009.2018367>
23. Situ, G., Zhang, J.: Double random-phase encoding in the Fresnel domain. *Opt. Lett.* **29**, 1584–1586 (2004).
24. Li, H., Wang, Y.: Double-image encryption based on iterative gyrator transform. *Opt. Commun.* **281**, 5745–5749 (2008).
25. Rodrigo, J.A., Alieva, T., Calvo, M.L.: Applications of gyrator transform for image processing. *Opt. Commun.* **278**, 29–37 (2007).
26. Fridrich, J.: Symmetric ciphers based on two-dimensional chaotic maps. *Int. J. Bifurc. Chaos* **8**, 1259–1284 (1998).
27. Chen, G., Mao, Y., Chui, C.K.: A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos Solitons Fractals* **21**, 749–761 (2004).
28. Mao, Y., Chen, G., Lian, S.: A novel fast image encryption scheme based on 3D chaotic Baker maps. *Int. J. Bifurc. Chaos* **14**, 3613–3624 (2004).
29. Pareek, N.K., Patidar, V., Sud, K.K.: Image encryption using chaotic logistic map. *Image Vis. Comput.* **24**, 926–934 (2006).

30. Kocarev, L.: Chaos-based cryptography: a brief overview. *IEEE Circuits Syst. Mag.* **1**, 6–21 (2001).
31. Alvarez, G., Li, S.: Some basic cryptographic requirements for chaos-based cryptosystems. *Int. J. Bifurc. Chaos* **16**, 2129–2151 (2006).
32. Li, S., Mou, X., Cai, Y., Ji, Z., Zhang, J.: On the security of a chaotic encryption scheme: problems with the fundamental approach. *Chaos Solitons Fractals* **18**, 799–804 (2003).
33. Wu, Y., Noonan, J.P., Yang, G., Agaian, S.: NPCR and UACI randomness tests for image encryption. *Cyber J. Multidiscip. J. Sci. Technol.* **1**, 31–38 (2011).
34. Wang, X., Teng, L., Qin, X.: A novel colour image encryption algorithm based on chaos. *Signal Process.* **92**, 1101–1108 (2012).
35. Rhouma, R., Meherzi, S., Belghith, S.: OCML-based colour image encryption. *Chaos Solitons Fractals* **40**, 309–318 (2009).
36. Zhang, Y., Xiao, D.: An image encryption scheme based on rotation matrix bit-level permutation and block diffusion. *Commun. Nonlinear Sci. Numer. Simul.* **19**, 74–82 (2014).
37. Arabind Kumar, Sanjay Yadav, Rajni Rohila “Magneto–Optical Nonlinear Image Encryption Using Hybrid Chaotic Maps and Modified Fresnel Transform” *Journal of Optics*, 2026, <https://doi.org/10.1007/s12596-026-03106>.
38. Arabind Kumar, Sanjay Yadav, Rajni Rohila, “An asymmetric image encryption algorithm based on Integer Wavelet Transformation and Elliptic Curve Cryptography” *Optica Applicata*, 2025, vol. 55 issue 4 pp. 583-600, [10.37190/oa/210109](https://doi.org/10.37190/oa/210109).
39. Arabind Kumar, Sanjay Yadav, “Optical image encryption in the Fresnel domain using the Umbrella map and the Yang-Gu algorithm” *Optica Applicata*, 2025, vol. 55, issue 3 pp. 449-471, [10.37190/oa/207947](https://doi.org/10.37190/oa/207947).
40. Giriya, R., Gaur, K.S., Singh, H.: Hybrid image encryption based on Hessenberg decomposition and chaotic structured phase masks in Fresnel transform domain. *Multidim. Syst. Sign. Process.* **37**, 3 (2026). <https://doi.org/10.1007/s11045-025-00902-z>.