International Journal of Safety and Security Engineering
Vol. 16, No. 3, March, 2026, pp. 591-602
Journal homepage: http://iieta.org/journals/ijsse

Integrated Framework Design of Hybrid Security Approach to Safeguard High-Dimensional Data Transmission

Mona[1,2*], B. G. Prasad[1]

[1] Department of Computer Science and Engineering, Dayananda Sagar College of Engineering, Visvesvaraya Technological University, Belagavi 590018, India
[2] BNM Institute of Technology (BNMIT), Visvesvaraya Technological University, Belagavi 590018, India

Corresponding Author Email: mshirs123@gmail.com

https://doi.org/10.18280/ijsse.160312

Received: 8 January 2026
Revised: 25 February 2026
Accepted: 21 March 2026
Available online: 31 March 2026

Keywords:
high-dimensional data encryption, chaos-based security, logistic map, bio-inspired optimization, entropy analysis, correlation mapping, secure image transmission

ABSTRACT

This paper proposes a chaos-based hybrid encryption scheme for secure transmission of high-dimensional image data. The approach combines a lightweight logistic-map-based chaotic sequence generator, bit-wise transformation of quadrant-wise, and a bio-inspired optimization approach. First, pseudo-random permutations and multiple chaotic sequences are generated with the help of a user-defined secret key to use them in partition-wise encryption. Then, quadrant-based transformation and entropy-based recombination are used to improve diffusion and decrease pixel correlation. Lastly, a bio-inspired optimization algorithm identifies the best encryption configuration by minimizing the correlation coefficients. The results of the experiments have shown that the proposed scheme has high security performance, whereby the entropy values are close to the ideal level (8 for grayscale images), adjacent pixel correlation is highly reduced, and key sensitivity is high. The comparative analysis shows that the approach is better in security and computing efficiency compared to the current techniques, therefore making the method appropriate to large-scale, high-dimensional image transmission in bandwidth-limited settings.

1. INTRODUCTION

In recent times, the transmission of high-dimensional data (HDD), especially images, has increased exponentially, as users frequently upload high-resolution images on social media such as Facebook, Instagram, etc. The high-dimensional images often contain complex pixel distributions, while being large in size and rich with sensitive information [1]. The characteristics of HDD images also include color richness, high spatial resolution, while an exponential rise in the number of pixels per frame could be seen. It also consists of a multi-layered structure, whereas adjacent pixels in high-dimensional images exhibit high correlation, which leads to spatial redundancy [2]. These high-dimensional images basically demand efficient and secure transmission in bandwidth-intensive networks. HDD images from drones and satellites are also used in land mapping, agriculture and disaster response, in which they require high-fidelity data transmission for accurate analysis [2, 3]. In the context of healthcare imaging, HDD images could also support in remote diagnostics thereby require high resolution image sharing with security, confidentiality and integrity [4]. In the recent times training models on large RGB datasets (e.g. ImageNet, COCO, etc.) require moving of vast amount of HDD image data across the networks and cloud serves whereas HDD images from smart cameras in smart cities or security systems are constantly transmitted and stored, demanding both high throughput and data confidentiality. The challenge arises as these images are inherently high-dimensional due to their multi-channel structure and pixel depth. Also, these data types are typically characterized by high spatial resolution, multiband frequencies and large-storage requirements which makes them vulnerable targets for unauthorized access, interception and cryptanalysis [5]. Standard cryptographic schemes like Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) offer strong security assurances and are also used to offer general-purpose data encryption. But applied to the high-dimensional image data directly, some practical limitations can occur, such as computational cost, large latency with large scale data, and lack of inherent optimization of image-specific properties, such as strong spatial correlation, and redundancy. There is therefore increased interest in developing image encryption schemes that are designed to be able to encrypt high-dimensional large-scale data, in an efficient manner, and still maintain strong security properties. Chaos-based and hybrid approaches have therefore been given consideration in this regard since they offer high sensitivity, randomness and efficiency [6, 7]. However, due to the unique characteristics of image data—such as high pixel correlation, redundancy, and large data volume—standard cryptographic schemes may exhibit limitations in efficiency or diffusion when applied directly. Therefore, these techniques often lack adaptability to the HDD structures which also affects their suitability for real-

time and bandwidth intensive environments [8, 9]. Also, one of the major drawbacks of RSA and AES based recent advancements of encryption is these methods do not cope well with spectral or inter-channel redundancies which result in not only increased transmission loads but also introduces potential weakness exploitable through statistical and differential attacks [10, 11]. Also, these methods often fail to account for intrinsic data redundancies and inter-pixel correlations, resulting in inefficient bandwidth utilization and vulnerability to various forms of cryptanalytic attacks. Furthermore, the inherent pixel correlations in HDD images also aggravate the risk of potential information exploitation by adversaries and leakage, if not effectively diffused during the encryption process [12, 13]. Deep learning (DL) based encryption models have recently become popular as promising alternatives to these approaches. However, DL based encryption models highly rely on large-scale and exhaustive training that increases the cost of computing power. Also, DL models such as CNNs, RNNs, Transformers, etc. often suffers from poor generalization, overfitting issues and problems of computational demands and also exhibit vulnerability to the various adversarial attacks [14]. The problem of poor generalization implies here that DL models often memorize the training data instead of learning generalized encryption schemes, therefore while they applied over HDD images from unseen distributions, their performance can degrade significantly [14]. Also, it has been observed that DL models could be vulnerable to various attacks as small adversarial perturbations in high-dimensional images can mislead the DL-based encryption models, causing incorrect or failed decryption. Most of the DL-based encryption approaches lacks theoretical cryptographic proofs or entropy-based validations whereas their black-box nature also makes it hard to quantitatively assess the security strength [15, 16]. However, chaos-based models offer various cryptographic indicators such as key sensitivity, entropy and correlation disruption, offering a more interpretable and mathematically provable framework [17]. However, existing chaos-based encryption strategies also could suffer from residual correlation among pixels especially in high-dimensional RGB images which could reduce the encryption strength. Existing classical chaos-based encryption models also suffers from low-key space dimensionality making them more vulnerable to brute-force attacks. On the hand many chaos-based encryption strategies are computationally expensive and not optimized for processing large images which negatively influence encryption/decryption delays and make them less-suitable for bandwidth-intensive applications such as social media or satellite imaging. Many chaos-based systems are empirically tested but not evaluated under formal security analysis. Therefore, their impact against modern cryptanalytic techniques such as chosen-plaintext or known plaintext attacks remains questionable [18, 19]. Therefore, the concern among research community continues to rise to ensure efficient, secure and reliable transmission of HDD over exposed medium like radio-channels.

The proposed study therefore, addresses the above challenges in the existing system and further introduces improvised chaos-based hybrid security framework that offers lightweight, robust and highly sensitive encryption for HDD image transmission. It employs a light-weight logistic-map based chaotic sequence generation which is guided by user-defined confidential key attributes to introduce unpredictable and sensitive key streams. The hybrid security approach also further enables a quadrant-wise portioning operation to process the image in quadrants (I1 to I4). Here each partition is encrypted considering uniquely initialized chaotic sequence. The encrypted segments are then combined through bio-inspired spatial optimization while evaluating quadrant reordering strategies based on entropy and correlation metrics, thereby maximizing the confusion and diffusion properties. This optimization strategy here helps towards optimizing the entropy and pixel correlation which are essential to ensure better image security. Here the scope of optimization arises as it is valuable for high-dimensional images where uniform security metrics across various channels are computationally hard to maintain. In summary, the proposed work basically offers a Two-Layer Security Approach, where in Layer-1 inclusion of Logistic Chaotic Map (LCM) enables faster, lightweight encryption strategy for high-speed and high-volume processing. In Layer-2, optimization-driven refinement further enhances the protection of high-dimensional image data against statistical and differential attacks while disrupting pixel correlations and enhancing entropy. To evaluate the performance of the proposed encryption, the study considers extensive simulation with respect to several key metrics that include Shannon entropy, horizontal/vertical/diagonal correlation coefficients and key sensitivity. Experimental outcome shows that the hybrid security approach offers high entropy values approaching ideal randomness and low correlation between adjacent pixels post-encryption and strong resistance against key-related brute force and statistical attacks. Extensive simulation outcome also shows that the approach offers a stable and computationally efficient encryption solution for secure voluminous data transmission, making it suitable for applications in secure remote sensing, telemedicine, and defense-grade multimedia communication.

The key contributions of the proposed study are as follows:

- The proposed hybrid chaos-based encryption modeling has exploited multiple self-reliantly seeded chaotic maps. This approach ensured strong pixel-level confusion and diffusion in Layer-1. Unlike, traditional chaos-based strategies the proposed work effectively deals with precision instability and limited key-space problems.
- The approach of computing enables parallelism which ensures secure handling of HDD image without compromising with the processing bottlenecks. In Layer-2, the security approach applies a novel optimization strategy that helps determining the encrypted quadrant configuration with lowest spatial correlation. In each stage of Layer-2 processing the outcome obtained from previous iteration is optimized so that the best encrypted HDD image could be produced with highest entropy and the lowest correlation coefficient among adjacent pixels.
- Unlike existing DL-based encryption modeling, which evaluates black-box models the proposed system offers encryption strength viz. various measurable parameters such as entropy, correlation coefficients, key-sensitivity and encryption time.
- Unlike AES, RSA and DL models, the proposed hybrid security offers light-weight and scalable encryption which reduces the computational and memory burden.
- The proposed security strategy also keeps first five unencrypted pixels preserved to support the integrity checks and structure retention which could be useful for

synchronization in streaming environments.

- Unlike existing system, the proposed work disrupts the inter-pixel correlations and ensures high key sensitivity, therefore the system becomes robust against various forms of attacks such as brute-force, differential and statistical attacks.

Integration of these enhancements in the proposed security approach offers robust, efficient and secure solution for HDD image transmission and also strikes the trade-off between security strength, computational efficiency and adaptability for high-dimensional image transmission. The reduction in computational burden and maximized encryption strength makes it ideal for high-speed and secure image transmission especially in environments like social media.

The remainder of the paper is structured as follows: Section 2 presents the discussion on related works in the domain of high-dimensional image encryption, while highlighting both strength and limitations of the existing methods. Section 3 further talks about the research problem, and Section 4 outlines the detailed research method of the proposed hybrid security approach. In Section 5, the simulation outcomes are analysed under different parametric conditions and it also offers discussion on security strength and validation of the proposed approach. Finally, the conclusion and future research directions are discussed in Section 6.

2. RELATED WORK

In recent years, there has been a surge in studies focusing on secure HDD transmission, especially with chaos and DL-based encryption models. The authors in study [20] presented DeepKeyGen: GAN-based key generation for high-dimensional images. The authors focused on secure key generation along with high-dimensional image encryption. The approach offers high security and adaptive key generation but suffers from high computational cost and limited interoperability problem. Another approach of DeepEDN is introduced by the authors in the study [21] for IoMT high-dimensional image encryption. The approach even though offers high level security and ROI mining but found resource intensive and its black-box nature makes it hard to quantitatively assess the security strength. The authors in study [22] introduced a DNA-based color image encryption with convolutional autoencoder. The strategy offers efficient encryption of large-sized color images and also ensures dimensionality reduction with high reconstruction accuracy. However, suffers from potential information loss and complex DNA operations. The authors performed analysis of chaos-based image encryption methods where the presented work evaluated various chaos-based encryption techniques.

The study offers comprehensive analysis while identifying the strengths but lacks practical implementation details. The authors in study [23] presented enhanced chaos in Duffing map for asymmetric encryption to address the problem of multi-stability in chaotic systems. The presented work offers improved chaos and effective encryption but complexity in implementation arises. A Chaos-based image encryption with random number embedding and DNA level permutation is introduced by the authors in study [24]. In this approach enhanced security is ensured through randomness and DNA techniques. The experimental outcome shows that the approach offers strong diffusion and confusion properties while suffers from increased computational load. The authors in study [25] presented high-dimensional image encryption using DNA complementary rule and chaotic maps where the authors have combined DNA computing with chaos for encryption. The outcome of the study offers high key sensitivity which it also obtains good statistical properties. However, the approach suffers from complexity in DNA encoding/decoding. Fast image encryption using lifting scheme and chaos is presented in the study [26] where the speed optimization problem is resolved for high-dimensional image encryption. Even though the authors claim that the presented approach offers high speed and optimal security metrics but a potential trade-off between speed and security is not addressed properly. Table 1 shows a comparison of AES with other techniques in terms of implementation cost, entropy and correlation.

Table 1. Comparison of Advanced Encryption Standard (AES), chaos-based and hybrid image encryption methodology in terms of computational speed, cost of implementation and statistical security measures (entropy and correlation coefficient)

Method Type	Speed	Implementation Cost	Entropy	Correlation	Remarks
AES (Baseline) [7]	Moderate–Low (for large images)	High	High (~7.9)	Low	Strong security but high computational cost for real-time image encryption
Chaos-based [27]	High	Low–Moderate	High (~7.8–7.99)	Very Low	Efficient for images due to randomness and sensitivity to initial conditions
Hybrid (Chaos + AES / others) [28]	High	Moderate	Very High (~7.997)	Minimal	Combines cryptographic strength with efficiency and improved security metrics
Hybrid (Chaos-based models) [29]	High	Moderate	High (~7.9)	Very Low	Achieves better trade-off between speed and statistical security

3. RESEARCH PROBLEM

Researchers have explored various pitfalls in traditional security strategies that are tailored and instrumental in the encrypted domain for secure HDD transmission in bandwidth-intensive applications. The primary challenge arises in dealing with high computational complexity associated with recent improvised AES and RSA strategies, as they involve complex mathematical operations leading to increased computational overhead when applied to HDD. HDD images often consist of redundant entities across different spectral bands or layers. Traditional encryption models do not consider this redundancy, leading to inefficient data handling and increased transmission bandwidth, which is not suitable and encouraged in bandwidth-intensive applications. It has also been observed that traditional approaches fail to support scalable encryption modeling for secure HDD transmission, making them unsuitable for high-speed communication networks. Also,

traditional encryption-based modeling's are vulnerable to different forms of cryptanalysis where the attackers exploit correlation between pixels in HDD images and reduce the security strength.

It has been also observed that existing DL-based encryption models has emerged as promising approach to secure HDD transmission but comes with several pitfalls such as security vulnerabilities to adversarial attacks where small perturbations in the input can cause incorrect decryption. It is also observed that security of neural networks is often based on empirical results rather than rigorous theoretical proofs and claims. The neural networks have tendency to memorize the training data rather than learning generalized encryption patterns and this can lead to poor generalization and making the encryption ineffective for diverse datasets. The challenges in DL encryptions also include high computational and energy costs, slow encryption, decryption speeds along with scalability problems with large-scale datasets.

Thus, the problem is that implemented encryption methods of HDD usually possess high computational complexity, low scalability, and possible susceptibility to attacks, which makes them inefficient in transmitting data safely in applications that require a large bandwidth. techniques for HDD suffer from high computational complexity and poor scalability.

4. PROPOSED DESIGN METHODOLOGY

The proposed work introduces a novel computational model that combines bio-inspired algorithmic strategy with chaotic systems to protect HDD transmission within an encrypted domain. The proposed work also aims to offer simple, optimized operation that significantly improves the performance of encryption modelling in HDD and protects the confidentiality and integrity of the HDD from a security point of view during transmission in bandwidth-intensive applications.

4.1 High-dimensional image data pre-processing for encrypted domain

The proposed work considers a high-dimensional image data I_{HDD} for transmission and applies pre-processing operation over the $I_{HDD} \in \mathbb{R}^{m\times n\times 3}$ / $\mathbb{R}^{m\times n}$. The pre-processing operation in the encrypted module locates the image data I_{HDD} and further performs a mapping operation on I_{HDD} in the form of $\mathfrak{f}_{map}: \mathcal{F} \rightarrow \mathbb{R}^{m\times n\times 3}$ / $\mathbb{R}^{m\times n}$ where $\mathcal{F}$ belongs to the set of valid high-dimensional image file locations. The mapping function generates $\mathbb{R}^{m\times n\times 3}$ / $\mathbb{R}^{m\times n}$in the form of numerical matrix of pixel attributes. The pre-processing operation in the proposed security framework also checks the dimensionality of the $I_{HDD} \in \mathbb{R}^{m\times n\times 3}$ and convert it into $I_{HDD} \in \mathbb{R}^{m\times n}$. This computing step basically reduces dimensionality while preserving the luminance that is critical for computational efficiency. The proposed hybrid security approach also exploits correlation estimation across spatial domains of the image data $I_{HDD} \in \mathbb{R}^{m\times n}$. For any pixel $p(x,y) \in I_{HDD} \in \mathbb{R}^{m\times n}$, three correlation types are computed to estimate the local spatial dependency.

4.2 Correlation analysis before high-dimensional data encryption

Natural high-dimensional image data often exhibit high spatial correlation among complex neighbouring pixels (horizontal, vertical, diagonal). This reflect a highly structured and predictable pixel layout which is vulnerable to various forms of statistical attacks. The prime objective of the proposed security strategy is to eliminate such predictability. It has to be noted that high residual correlation in the encrypted high-dimensional image can be exploited by statistical attacks which further reveals the structure or patterns of the original image. Therefore, the need arises to validate encryption system's resilience to statistical analysis. In the first computing step the proposed system applies a functional module of $\mathfrak{f}_{HC}(x)$ that enables estimation of correlation among horizontal pixel entities in $p_h(x,y) \in I_{HDD} \in \mathbb{R}^{m\times n}$. Let $I_{HDD} \in \mathbb{R}^{m\times n}$ is an image matrix from HDD, where m refers to the number of rows and n refers to the number of columns. The horizontal pixel pairs in $I_{HDD} \in \mathbb{R}^{m\times n}$ defined as $\{(x_h, y_h)\}$ where $x_h = I_{HDD}(\mathrm{i},\mathrm{j})$ and $y_h = I_{HDD}(\mathrm{i},\mathrm{j}+1)$. Here $i: \forall i = 1 \rightarrow m$-1 and $j: \forall j = 1 \rightarrow n$-1. The proposed method reduces the computational load in the execution by introducing an empirical constant value of h. The analytical modeling for the estimation of horizontal correlation initially computes the mean values of x_h and y_h in the form of E_x and E_y and further estimate the variance considering the following mathematical modeling.

$$\mathrm{D_x} = {}^{1}\!/_{\mathrm{n}} \textstyle\sum_{\mathrm{h=1}}^{\mathrm{n}} (\mathrm{x_h} - \mathrm{E_x})^2, \quad \mathrm{D_y} = {}^{1}\!/_{\mathrm{n}} \sum_{\mathrm{h=1}}^{\mathrm{n}} (\mathrm{y_h} - \mathrm{E_y})^2 \tag{1}$$

Further, the computing operation also considers estimating the covariance $\mathrm{cov_{xy}}$ which is also computed considering the following mathematical operation.

$$\mathrm{cov_{xy}} = {}^{1}\!/_{\mathrm{n}} \sum_{\mathrm{h=1}}^{\mathrm{n}} (\mathrm{x_h} - \mathrm{E_x})(\mathrm{y_h} - \mathrm{E_y}) \tag{2}$$

Finally, the horizontal correlation coefficient is estimated as follows:

$$\mathrm{r_{xy}^{H}} = {}^{|\mathrm{cov_{xy}}|}\!/_{\sqrt{\mathrm{D_x, D_y}}} \tag{3}$$

Here in the proposed security strategy Pearson correlation coefficient is applied over horizontal adjacent pixels that measures how similar neighbouring pixel values are across the rows of the HDD. The goal of encryption is to retain low redundancy so that $r_{xy}^{(\mathrm{encrypted})} \approx 0$.

Similarly, the security approach also considers estimating the correlation between vertical pixel pairs $\{(x_v, y_v)\}$ in $I_{HDD} \in \mathbb{R}^{m\times n}$. Here $x_v = I_{HDD}(i,j)$ and $y_v = I_{HDD}(\mathrm{i}+1,\mathrm{j})$. Further considering the Pearson correlation coefficient estimation the statistical similarity between vertically adjacent pixels is measured in the form of r_{xy}^{V}. The process also further computes the correlation between diagonally adjacent pixels where $x_d = I_{HDD}(i,j)$ and $y_d = I_{HDD}(\mathrm{i}+1,\mathrm{j}+1)$. The diagonal correlation r_{xy}^{D} verifies how pixel intensity is related along diagonal paths. Similar to vertical and horizontal correlation, high values indicate structural regularity, while low values signify high confusion after encryption, which corresponds to optimal security. Like, vertical/horizontal correlation here, the high values imply structural regularity,

whereas low values indicate post-encryption high confusion and optimal security. The proposed security module further computes the global correlation measures, which consider the average of three directions as follows:

$$r_x' = {}^1\!/_3\,(r_{xy}^H + r_{xy}^V + r_{xy}^D) \quad (4)$$

This provides an average estimation of pixel dependency that also implies how redundant or predictable the data is before applying the proposed encryption strategy. Here the quantitative measure of pixel dependencies offers a baseline prior to applying the chaos-based encryption modeling.

4.3 Partitioning operation in the context of high-dimensional data security

This partitioning operation is also a pre-processing operation prior to encryption. It helps in enabling parallel encryption, and also localizes correlation analysis which supports modular encryption architecture in hybrid secure schemes. The proposed security model considers $I_{HDD} \in \mathbb{R}^{m\times n}$ and further split the data into four different quadrants, considering the midpoints of $m_2 = \lfloor {}^m\!/_2 \rfloor$ and $n_2 = \lfloor {}^n\!/_2 \rfloor$. It computes the top-left partition in the form of $I_1 = I_{HDD} \in \mathbb{R}^{m\times n}(1 \to m_2, 1 \to n_2)$, top-right partition in the form of $I_2 = I_{HDD} \in \mathbb{R}^{m\times n}(1 \to m_2, n_2 + 1 \to n)$. Further, it also computes the bottom-left partition in the form of $I_3 = I_{HDD} \in \mathbb{R}^{m\times n}(m_2 + 1 \to m, 1 \to n_2)$ and the bottom-right partition of $I_4 = I_{HDD} \in \mathbb{R}^{m\times n}(m_2 + 1 \to m, n_2 + 1 \to n)$. The operation results are further visualized as $\bigcup_{i=1}^4 I \in \mathbb{R}^{m_2\times n_2}$.

4.4 Chaos seed initialization for high-dimensional data

The security modeling further enables a chaotic system parameter initialization mechanism, which is customized considering the pixel attributes from the partitioned image data quadrants. Let each partition in $\bigcup_{i=1}^k I$ where $k = 1\to4$ is of $m_k \times n_k$ size. Here, the approach considers the first 5 grayscale pixel intensity values p_i from partition I_k to derive the chaotic seed. The computation modeling in this phase consists of three core stages, which are binary representation computation, decimal conversion and normalization operations. Here each pixel $p_i \in [0,255]$ is further represented in an 8-bit binary representation as $B_i \in \{0,1\}^8$. Further, the process stacks them into a form of binary stream of length 40 as $B_k \in \{0,1\}^{40}$. Further, the process computes a 40-bit decimal number in the form of U_k which is computed considering the following Eq. (5):

$$U_k = \sum_{i=1}^{40} B_k^{(i)}.\,2^{40\text{-}i} \quad (5)$$

Here $B_k^{(i)} \in \{0,1\}$ refers to the i^{th} bit in the 40-bit stream for the partition k. Further, the normalization operation takes place over U_k that generates $U0_k$. This computing step in the proposed security approach plays a crucial role in securing the HDD transmission for several key reasons, including:

- Deriving initial chaotic seed values directly from image pixel intensities, the encryption operation becomes data-dependent.
- Even a small variation in the high-dimensional image alters the chaotic seed computation that generates completely different encrypted outputs.

This strategy also enhances the sensitivity and unpredictability in encrypted mechanism. That means this step transform static image features into highly sensitive and unpredictable control parameters for chaos-based encryption modeling. It also helps coupling the data and encryption key that ensures high security, strong diffusion and robustness against various forms of statistical attacks.

4.5 Customized chaotic functional design in hybrid security strategy

In this step, the proposed security framework also computes the chaotic sequence, which makes use of a confidential key attribute($K \in \mathbb{R}$). The chaotic charting and encryption module in this proposed security strategy utilizes the strength factors of logistic maps and bitwise XOR operations to secure the high-dimensional image data. The process considers a partitioned data sequence in the form of $I_1.I_2, I_3, I_4 \in \mathbb{R}^{m\times n}$. Further, it exploits the logistic map to generate the Chaotic sequence. The secret key $K \in \mathbb{R}$ seed the pseudorandom number generator, and further it generates permutation vector P_{vec}^K that shuffle the pixel indices.

4.6 Chaotic sequence generation in hybrid security approach

The popularity of chaotic systems arises due to their potential deterministic, complex and pseudo-random behaviour. Here deterministic implies that the system follows precise mathematical rules without any randomness. Also, here pseudo-random behaviour exhibits that the output appears random and unpredictable especially over time, even though it's fully determined by initial conditions. The characteristic-deterministic yet unpredictable makes chaotic systems suitable for HDD encryption especially images with complex pixel distributions. Chaos functions like logistic maps are also known for their sensitivity to initial conditions and pseudo-randomness which also helps in high-dimensional image data encryption. The Chaotic function in the design and modeling of the proposed security framework follows logistic map and is defined as follows:

$$x_{n+1} = r x_n (1 - x_n) \quad (6)$$

Here $x_n \in (0,1)$ is considered a state at the iteration of n. $r \in \sigma, k$ refers to the factor that controls the behaviour of the function. The function is considered chaotic if $r > \sigma$. Here x_0 is the initial condition in the Chaotic functional system. In the proposed security framework for each quadrant, the logistic map enables the generation of a chaotic sequence which can be computed considering the following Eq. (7).

$$x_n = r x_{n-1} \cdot (1 - x_{n-1}) \text{ where } 0<x_0<1,\ r = 4 \quad (7)$$

Here x_0 refers to the initial value, r is a control parameter and the sequence is generated up to $N = n_r * n_c$ values. Here n_r refers to m and n_c refers to n in reference to the above computing stages. The above function is computed for 1 to ($n_r * n_c$-1) values.

Further, the computation generates a chaotic sequence in the form of $\{x_n\}_{n=1}^N$. Further outcome of the key-based permutation vector P_{vec}^K is used to perform the index-based permutation and extraction as shown in the following Eq. (8).

$$E^{(k)} = x_n{}^{(k)}(P_{vec}^{K})_{1\to n_r * n_c} \quad (8)$$

Here the chaotic sequence is re-ordered with respect to the permutation vector representation. Further the proposed work performs dimension normalization for data matrix $T \in \mathbb{R}^{4\times N}$ where all encrypted vectors $E^{(k)}$ are further appended. Here the approach applies matrix formation via zero-padding shorter rows during the appending operations. The computation of $T \in \mathbb{R}^{4\times N}$ is performed considering the following mathematical expression. Let $E^{(k)} \in \mathbb{R}^{m}$ then

$$T_{(i,:)} = \begin{cases} E^{(k)}, & len(T) = M \\ [E^{(k)}, 0 \ldots .0], & M < N \\ truncate\ or\ adjust, & M > N \end{cases} \quad (9)$$

Here M is the length of chaotic vector $E^{(k)}$ for each quadrant and n refers to the target row width considering the max of $E^{(k)}$ lengths. The value of length of $M = {n_r * n_c}/{4}$. The computation also helps in generating the chaotic encrypted keys in this security approach. The process also performs chaotic sequence re-ordering for the ease of computation. The following Figure 1 shows the computational steps involved in generating the chaotic sequence of HDD.

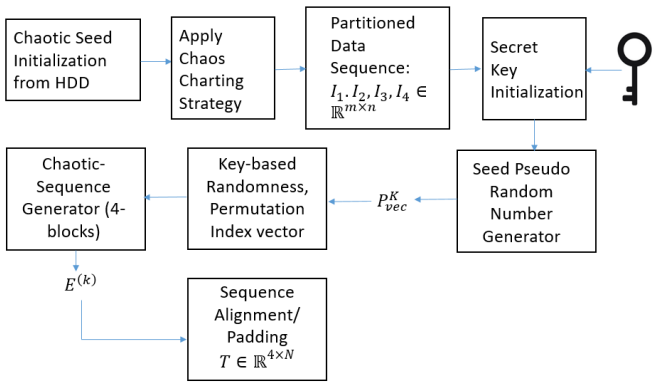


Figure 1. Chaotic sequence generation in hybrid security approach

4.7 Chaos-based encryption mechanism

It is further used to form the encryption key stream. Here, each partition uses a different seed, such as $x_n^{(1)}$ uses U_{01} for I_1, $x_n^{(2)}$ uses U_{02} for I_2, $x_n^{(3)}$ uses U_{03} for I_3 and $x_n^{(4)}$ uses U_{04} for I_4. Further, the proposed work considers the pixel shuffling operation via the permutation index. It computes a permutation vector $P_{vec} \in \mathbb{Z}^{n_r,n_c}$. This vector further helps permute the indices for each partition's chaotic sequence and generates $\mathrm{X}^{\mathrm{perm}}$. The computation process also enables sequence normalization, which scales the chaotic sequence of HDD to the grayscale range. Finally, an encryption mask is generated in the form of $E_{mask} \in \mathbb{Z}^{n_r,n_c}$. Further, each individual partition of $I^{(i)} \in \mathbb{Z}^{n_r,n_c}$ for $\bigcup_{i=1}^{4} I \in \mathbb{R}^{m_2\times n_2}$ is encrypted considering the chaotic XOR operations, block diffusion $\Phi(.)$ using forward chaining for each $I_E^{(i)}$ and global diffusion $\Psi(.)$, as shown in the following Eq. (10) and (11) respectively.

$$I_E^{(i)} = \Phi\left(I^{(i)} \oplus mod\left(\lfloor X(IX) \times 10^{14} \rfloor, 256\right)\right) \quad (10)$$

$$I_E = \Psi\left(\bigcup_{i=1}^{4} I_E^{(i)}\right) \quad (11)$$

As in the proposed security approach pseudo-random generator ($\varepsilon_G(K)$) outcome is seeded with $K \in \mathbb{R}$. Therefore, any adversaries' not having $K \in \mathbb{R}$ unable to reproduce the same permutation or encryption sequence. Therefore, while combined with chaotic maps, $\varepsilon_G(K)$ provides unpredictability and also strengthen the encryption process. Here in $I_E^{(i)}$ the first five pixels are typically preserved as header for the purpose of synchronization. Finally, the proposed computational approach reconstructs the full encrypted HDD $I_E^{(i)}$ considering four different encrypted quadrants which is shown as follows:

$$I_E^{(i)} = \begin{bmatrix} I_E^{(1)} & I_E^{(2)} \\ I_E^{(3)} & I_E^{(4)} \end{bmatrix} \quad (12)$$

In the proposed system, zero-padding plays a key role in matrix formation and positively influences the encryption modeling. Existing chaos-based encryption schemes typically represent data as one-dimensional vectors. In contrast, the proposed security modeling applies encryption operation like bitxor where the need for matching the shape of the original high-dimensional image blocks arise. To meet this requirement, a matrix reshaping operation is employed. When the chaotic sequence, after permutation and quantization, does not match the size of the image blocks, zero-padding resolves the dimensional inconsistency. Furthermore, zero-padding ensures that:

- All encrypted blocks have a uniform size;
- They can be correctly placed back into the global image matrix $I_E^{(i)}$.

This approach also helps eliminating the indexing errors and support smoother reconstruction of encrypted high-dimensional image in the proposed system. The analytical design of the chaotic-based encryption algorithm is shown as below:

Algorithm: Chaotic-Based Encryption

Input: $K \in \mathbb{R}$ // Secret Key Attribute, $I_1.I_2,I_3,I_4 \in \mathbb{R}^{m\times n}$, $\varepsilon_G(K)$

Output: $I_E^{(i)}$

Begin

1. Initialize $I_1.I_2,I_3,I_4 \in \mathbb{R}^{m\times n}$, $K \in \mathbb{R}$
2. Sub-images $\bigcup_{i=1}^{4} I \in \mathbb{R}^{m_2\times n_2}$
3. For $1\rightarrow (n_r * n_c\text{-}1)$
4. Apply logistic-map for Chaotic sequence generation

$$x_n = r x_{n-1} \cdot (1 - x_{n-1}) \text{ where } 0 < \boldsymbol{x_0} < 1, r = 4$$

5. End
6. P_{vec}^{K} of integers from $1 \rightarrow (n_r * n_c)$ generated by $\varepsilon_G(K)$ seeded by K // $\mathrm{X}^{\mathrm{perm}}$
7. Initial seed values for chaotic sequence

$$U_{0i} \in (0,1) \text{ for } x_n \text{ for } i\text{th partition } (i = 1 \rightarrow 4)$$

8. Apply index-based permutation and extraction

$$E^{(k)} = x_n{}^{(k)}(P_{vec}^{K})_{1\to n_r * n_c}$$

9. Normalize and scale the chaotic sequence and generate $T \in \mathbb{R}^{4\times N}$
10. Apply Encryption Transformation

$$I_E^{(i)} = \Phi\left(I^{(i)} \oplus mod\left(\lfloor X(IX) \times 10^{14} \rfloor, 256\right)\right), \forall I^{(i)} \in \mathbb{Z}^{n_r,n_c} \text{ for } \bigcup_{i=1}^{4} I \in \mathbb{R}^{m_2 \times n_2}$$

Followed by

$$I_E = \Psi\left(\bigcup_{i=1}^{4} I_E^{(i)}\right)$$

11. Concatenation operation of Quadrants

$$I_E^{(i)} = \begin{bmatrix} I_E^{(1)} & I_E^{(2)} \\ I_E^{(3)} & I_E^{(4)} \end{bmatrix}$$

End

The proposed hybrid security strategy also synergizes a bio-inspired algorithmic modeling with the above customized encryption module which is basically a chaos-based encryption system. It also helps forming a hybrid approach that addresses the growing security needs of bandwidth-intensive applications. The security framework- applies a custom chaos-based encryption strategy as high-dimensional images benefit from light-weight chaotic-encryption methods owing to their larger size and need for fast processing. The proposed work also further integrates a novel bio-inspired strategy for effectively tuning the encryption parameters that also reduces computational burden to a longer run. The encrypted data chunks are considered an initial population and evolve them towards optimized outcome to enable adaptive security enhancement.

4.8 Bio-inspired optimization integration

The proposed security framework further considers $I_E^{(i)} \in \mathbb{R}^{n_r,n_c}$ and further also applies image partitioning operation and split the encrypted image into equal-sized quadrants. It is represented as follows:

$$I_E^{(i)} = \begin{bmatrix} q_1 & q_2 \\ q_3 & q_4 \end{bmatrix}, q_i \in \mathbb{R}^{n_r/2 \times n_c/2} \quad (13)$$

The approach further applies a partition recombination modeling, which is also referred to as a bio-inspired shuffling strategy that generates four different recombinations of quadrants in the form of $\bigcup_{i=1}^{4} S_i \in \mathbb{R}^{n_r/2 \times n_c/2}$. Here for each configuration of S_i, the system further computes correlation estimation in the form of $r_{xy}^H, r_{xy}^V, r_{xy}^D$ and also further estimates the average correlation R_x' for each shuffled image matrix. The system also formulates optimization criteria to obtain the G_{opt} that is represented as follows:

$$G_{opt} = \arg\min_i \; R_x'(i) \;, \forall i \in 1 \rightarrow 4 \quad (14)$$

The security approach further computes the information entropy, considering a customized function of $f(H)$ for the considered high-dimensional image data. The computation is carried out considering the following mathematical operation.

$$f(H)_{I_E^{(i)}} = -\sum_{i=0}^{255} p_i \log_2 p_i \quad (15)$$

where, p_i refers to the probability of gray-level i in the image of $I_E^{(i)}$. Further the shuffled image obtained from G_{opt} is used as cipher image. The proposed strategy aims to optimize the process while striving to achieve lower correlation values. Here, low correlation via G_{opt} implies better encryption. Also, the entropy estimation here measures the unpredictability, where the study maximizes the function $f(H)_{I_E^{(i)}}$ to generate a stronger cipher prior to network transmission. Here the index of the optimal pattern i is stored in the last pixel of $I_E(n_r, n_c) = i$. Further, the system communicates the optimized encrypted HDD to the receiver side via bandwidth-friendly transmission. In the proposed hybrid security framework, the optimization policy is integrated with the chaos-based encryption strategy to optimize the encrypted images and further it helps in determining the one with the highest entropy and lowest adjacent pixel correlation as the final cipher image. Here the proposed work employs a genetic algorithm (GA) that refines the encrypted images while considering the following key aspects:

- Fitness Evaluation: This criterion is assessed considering entropy and pixel correlation metrics.
- Selection and Crossover: The approach combines high fitness images to produce new generations.
- Termination: The process continues until the improvements plateau and till it ensures optimal encryption quality.

4.9 Hybrid security decryption approach

In the decryption pipeline of the proposed work, the study considers the encrypted high-dimensional image data of $I_E^{(i)}$ and further applies the bio-inspired optimization to re-order $q_i \in \mathbb{R}^{n_r/2 \times n_c/2}$. It also further applies the complementary (2×2) portioning operation and further computes the chaotic initialized seed value. Further, considering the secret key entity of $K \in \mathbb{R}$ seeds from the authorized user side, the system applies a chaotic charting strategy to re-generate the $T \in \mathbb{R}^{4 \times N}$ which further undergoes the decryption operation to reconstruct the original image. The evaluation metrics used in the proposed security approach consider entropy analysis, correlation mapping and confidential key-sensitivity, which are further assessed in the next segment of the study.

5. RESULTS AND DISCUSSION

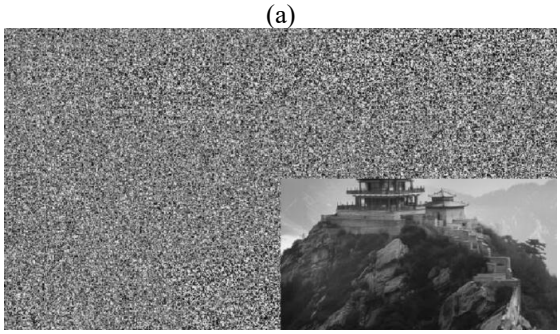
This section evaluates the performance of the proposed chaos-based image encryption strategy with quadrant-wise optimization on high-dimensional grayscale images. Here, the security analysis is performed considering the evaluation metrics such as entropy, correlation coefficient, and key sensitivity to assess the strength of confusion and diffusion in the cipher domain. Specifically, the same set of benchmark images (e.g., Lena and Peppers) was used for all methods without any variation in preprocessing. All images were converted to grayscale and resized (if required) using the same procedure.

The evaluation metrics, including entropy, correlation coefficients, Number of Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI), and encryption time, were computed using uniform mathematical definitions across all methods. To ensure a fair and consistent comparison, all evaluated encryption methods, including the proposed approach, AES, and other referenced techniques, were tested

under identical experimental conditions.

The experimental evaluation used MATLAB 2015a on a system with an Intel Core i5 processor, 8 GB RAM, and Windows OS. The Mersenne Twister RNG rng(K, 'twister') was used for permutation generation. Chaotic sequences were generated using the logistic map with r = 4. Image-dependent initial conditions were used to enhance security with high-dimensional grayscale images of variable sizes of 512 × 512 (i.e., standard test size) and 1024 × 1024 (high-dimensional, high-quality visual data). The visualization of the proposed method results is depicted in Figure 2, where Figure 2(a) is the original high-dimensional grayscale input image and Figure 2(b) is the generated encrypted image using the hybrid chaos-based encryption technique. The encrypted output is highly distorted in appearance and loses structural information, which suggests that it is more randomized and that the original image characteristics will be well concealed.

(a)



(b)

Figure 2. (a) Input high-dimensional image, (b) hybrid chaos-based encryption outcome

5.1 Entropy analysis

The entropy analysis that measures randomness in the encrypted images is close to the ideal entropy of 8 for grayscale images. It has to be noted that for four different high-dimensional test images, the proposed system accomplishes entropy values between ~7.9732–~7.9993, which signifies that since the high-dimensional grayscale images are structurally high-dimensional, the values indicate significant randomness and unpredictability post-encryption within the evaluated channel or layer. The consistent outcome of entropy also demonstrates that the encrypted outputs are highly disordered, which minimizes the predictability that could be exploited by the attackers. The consistency in entropy outcome also suggests that the hybrid encryption model performs uniformly well across different input types of high-dimensional image data. However, the proposed hybrid chaos-based encryption accomplishes a highest entropy of ~7.999, which is very close to the ideal case and also indicates high resistance against entropy-based attacks.

It is important to note that the proposed hybrid chaos-based encryption has a maximum entropy of about 7.999 which is very close to the ideal entropy of 8, hence showing high resistance to entropy-based attacks.

Table 2. Analysis of entropy in hybrid chaos encryption modeling

High-Dimensional Test Images	Entropy Values
Image-1 	7.9993
Image-2 	7.9968
Image-3 	7.9981
Image-4 	7.9992
Image-5 	7.9736
Image-6 	7.9732

The entropy estimation outcome for each high-dimensional test data is shown in Table 2. The consistently high entropy values (~7.99) imply increased randomness in information content post encryption. This confirms the effectiveness of the proposed encryption framework in enhancing data confidentiality. The extensive analysis also considered comparing the outcome of the proposed hybrid chaos-based encryption strategy with other recent popular image

encryption strategies, such as the approaches of Natiq et al. [23], Huang and Zhou [24], and AES [9]. For fair comparison purposes, the proposed work considered images of Lena and Peppers with complex pixel distributions. Figure 3 shows the comparison of Entropy among different approaches as an evaluation metric.

Figure 3 illustrates the entropy values obtained for two different grayscale images when the image encryption is performed considering Natiq et al. [23], Huang and Zhou [24] and AES [9] strategies along with our approach. Here, the highest entropy value for proposed chaos-encryption modeling is obtained ~7.9736 for Lena image and ~7.9732 for Peppers, which are comparable and superior when compared with other approaches. Here, the high entropy indicates greater randomness and better resistance to statistical attacks. It can also be seen that for both approaches, the highest entropy value in the proposed system closely approaches the ideal value of 8. This clearly demonstrates the superiority of the proposed encryption policy over the traditional approaches, as it maximizes the information uncertainty of the high-dimensional encrypted images. The high entropy also implies structural randomness in the encrypted high-dimensional image that can defend against several common cryptographic, statistical and image-specific attacks, such as histogram analysis, correlation checks, and other statistical tools cannot easily reveal the patterns or keys. It has to be noted that attackers can't easily predict how the cipher image varies based on plain text variations. In the proposed approach, the use of chaotic maps provides a large key space of $> 2^{128,}$ which makes the exhaustive key search infeasible and prohibits brute-force attacks. High entropy also implies that attackers cannot reverse engineer or simulate the encryption process. The proposed chaos-based encryption model also successfully defends against chosen-plaintext and ciphertext-only attacks.

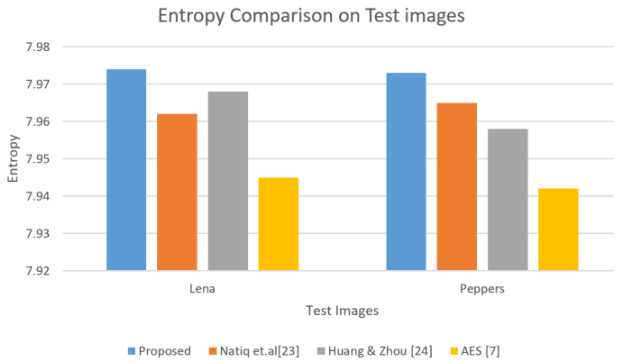


Figure 3. Analysis of entropy for different approaches

5.2 Correlation coefficient analysis

The key metrics for performance analysis also consider the assessment of the correlation coefficient to verify the outcome of the proposed hybrid security strategy. Table 3 shows the outcome of the initial correlation of pixels and the correlation of pixels after performing the optimized and chaos-based encryption modeling. The interpretation of the quantitative outcome from Table 3 shows a sharp drop in correlation after performing the proposed encryption strategy for all the high-dimensional test images. This clearly indicates a strong disruption of pixel relationships. The interpretation of the outcome shows that original images have high correlations (~0.506—~0.999).

However, in the proposed system, the values are minimized to ~0, which implies strong pixel decorrelation, high randomness and also near-complete elimination of spatial patterns, which further reduces the predictability. The security analysis shows that if attackers typically attempt to analyse the pixel intensity distributions and correlations, then low correlation makes it nearly impossible to extract statistical patterns from an encrypted high-dimensional image. Hence, the proposed model is robust against statistical attacks. Also, it minimizes the risk of Chosen-Plaintext Attacks (CPA) during the transmission along with Known-Plain Text Attacks (KPA). It can also defend against differential attacks, as small pixel changes do not produce predictable ciphertext changes due to low correlation. Hence, attackers cannot model or reverse engineer the encryption. The high de-correlation, combined with other metrics like high entropy and key sensitivity, significantly increases the key-space and complicates the brute-force analysis. Figure 4 exhibits the visual outcome of initial correlation, post-encryption correlation and entropy values obtained from the proposed approach.

Table 3. Analysis of correlation of pixels in hybrid chaos encryption modeling

High-Dimensional Test Images	Initial Correlation of Pixels	Correlation After Hybrid Encryption
High-Dimensional Test Image-1	0.50662	0.013761
High-Dimensional Test Image-2	0.96457	0.011257
High-Dimensional Test Image-3	0.96203	0.0034626
High-Dimensional Test Image-4	0.99962	0.0096526

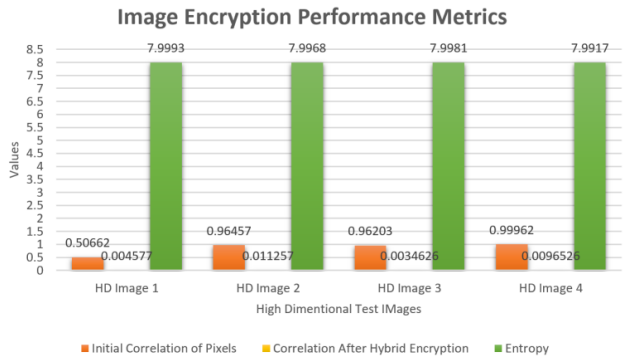


Figure 4. Analysis of correlation coefficients for different approaches

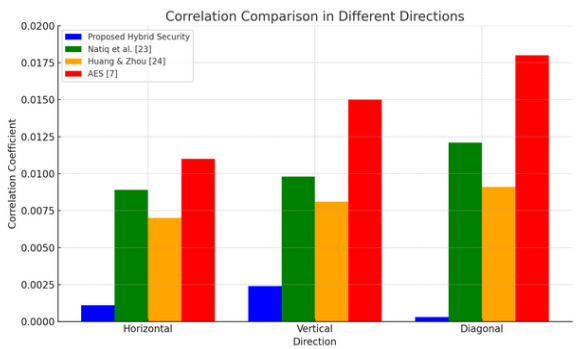


Figure 5. Analysis of average correlation coefficients

The extensive analysis of correlation is also performed considering a comparative study for other related approaches, such as Natiq et al. [23] and Huang and Zhou [24] and AES [9] for Lena and Pepper images, which is shown in Figure 5.

Analysis of the correlation coefficient shows that the proposed hybrid security method achieves the lowest correlation coefficients in all directions compared with other popular baseline approaches. Here, the low correlation among adjacent pixels of encrypted images implies strong decorrelation, which is crucial for resisting different forms of statistical and structural attacks. The proposed method disrupts the pixel relationship more effectively, making it harder for attackers to extract any visual or statistical patterns. Therefore, the results confirm that the proposed approach provides stronger encryption with higher randomness and unpredictability. The derived values for chaotic seed initialization are provided in Table 4.

Table 4. Derived values for chaotic seed initialization

Derived Values for Chaotic Seed Initialization	$U0_1$	$U0_2$	$U0_3$	$U0_4$
High-Dimensional Test Image-1	0.069957	0.11443	0.96973	0.86130
High-Dimensional Test Image-2	0.000661	0.65755	0.05586	0.66233
High-Dimensional Test Image-3	1.000000	0.90628	1.000000	0.24461
High-Dimensional Test Image-4	0.902460	0.27419	0.93824	0.99902

The security analysis also shows that minor changes in the key lead to significantly different encrypted high-dimensional images, which clearly confirms that the proposed hybrid security approach can significantly resist brute-force attacks.

5.3 Encryption time analysis

The study also further assessed the encryption time in seconds for all the approaches and validated the effectiveness of the proposed chaos-based encryption strategy towards striking the balance between security and computational complexity.

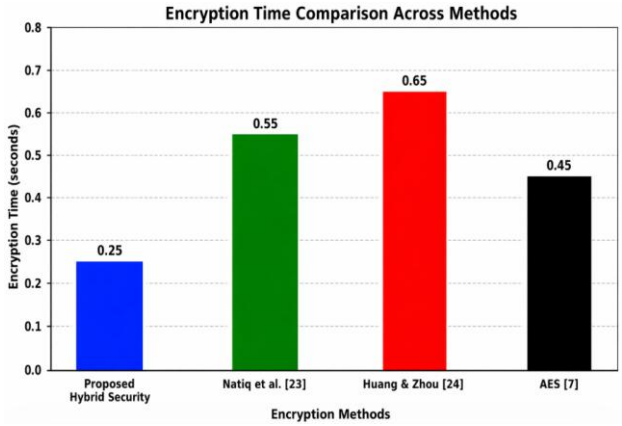
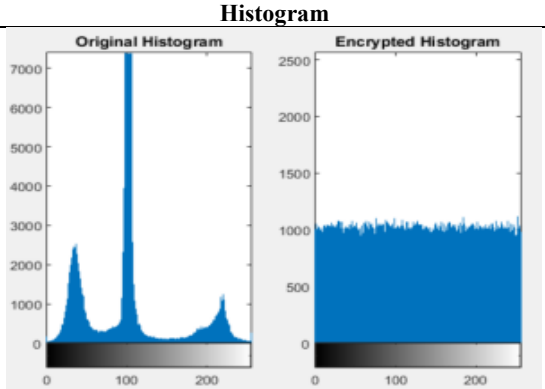
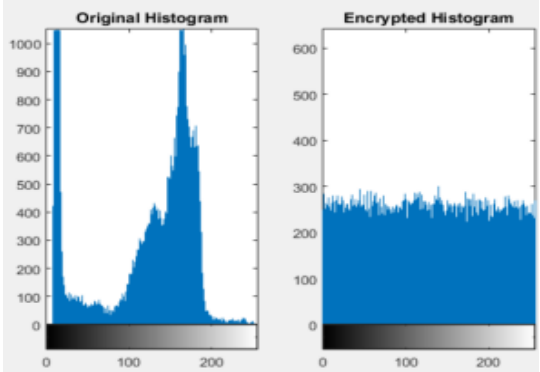
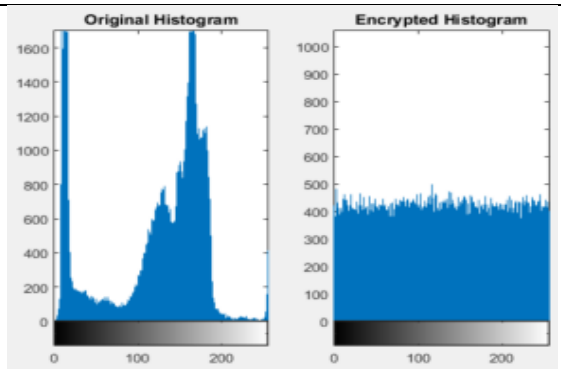
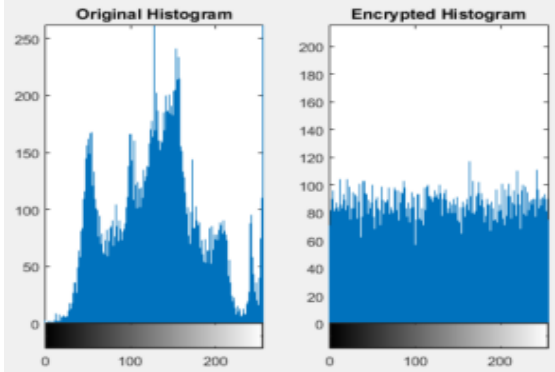


Figure 6. Analysis of encryption time (secs)

The proposed hybrid method is the fastest among all tested approaches, completing encryption in 0.25 seconds (Figure 6). It incorporates a bio-inspired optimization policy and achieves a high entropy value, indicating considerable resistance against various attacks. In comparison, the methods of Natiq et al. [23] and Huang and Zhou [24] pose slower encryption due to complex operations like double parity and hyper-chaotic scrambling. The proposed method is also approximately 44% faster than the standard AES algorithm, indicating strong computational efficiency.

Table 5. Security analysis histogram, NPCR and UACI

Test Image	Histogram	NPCR (%)	UACI (%)
1		99.6155	33.4304
2		99.5895	33.0991

3		99.6101	33.4538
4		99.5937	33.6427

Note: NPCR = Number of Pixel Change Rate, UACI = Unified Average Changing Intensity

5.4 Security analysis

The strength of the proposed encryption algorithm is also assessed through key cryptographic metrics, including histogram analysis, NPCR, and UACI, as shown in Table 5. Together, these measures confirm the algorithm's robustness against both statistical and differential attacks. As seen from the histogram analysis, the encrypted image has a uniform and flat distribution following encryption, that is, the histogram is homogeneous and flattened, lacking any discernible patterns or structures. In summary, statistical attacks are successfully thwarted. Pixel values seem arbitrary and erratic. NPCR, which measures how much an encrypted image changes when one pixel in input changes, is seen close to 99%, which is achieved using Strong chaining diffusion on each quadrant and also Global diffusion. Also, UACI, which measures the intensity difference between two encrypted images, is 33%, which is good and is achieved by the chaotic technique and diffusion chaining.

6. CONCLUSION

This paper presents a robust hybrid encryption framework that combines chaos-based modeling with bio-inspired quadrant transformation for securing high-dimensional image data, particularly suited for bandwidth-intensive applications. The proposed method was assessed using key evaluation metrics such as entropy, correlation coefficients, and key sensitivity and NPCR, UACI, or histogram tests. The proposed encryption scheme achieved entropy values close to the ideal value of 8, indicating strong randomness and resistance to entropy-based attacks. Compared to conventional AES and existing chaos-based encryption techniques, this shows a notable entropy improvement of 0.6% to 0.75%, which is significant for ensuring data unpredictability in cryptographic systems. This method significantly reduced horizontal, vertical, and diagonal pixel correlations, bringing them close to zero and improving resistance to statistical analysis. This translates to an average correlation disruption improvement of over 58% compared to traditional methods, highlighting its strong effectiveness against statistical and cryptanalytic attacks. Future work will focus on enhancing adaptability, supporting multi-modal data, and enabling lightweight, real-time deployment across resource-constrained and scalable platforms.

REFERENCES

[1] Nayak, S.R., Mishra, J., Khandual, A., Palai, G. (2018). Fractal dimension of RGB color images. Optik, 162: 196-205. https://doi.org/10.1016/j.ijleo.2018.02.066

[2] Kior, A., Yudina, L., Zolin, Y., Sukhov, V., Sukhova, E. (2024). RGB imaging as a tool for remote sensing of characteristics of terrestrial plants: A review. Plants, 13(9): 1262. https://doi.org/10.3390/plants13091262

[3] Feng, H., Tao, H., Li, Z., Yang, G., Zhao, C. (2022). Comparison of UAV RGB imagery and hyperspectral remote-sensing data for monitoring winter wheat growth. Remote Sensing, 14(15): 3811. https://doi.org/10.3390/rs14153811

[4] El-Shafai, W., Hemdan, E.E.D. (2023). Robust and efficient multi-level security framework for color medical images in telehealthcare services. Journal of Ambient Intelligence and Humanized Computing, 14(4): 3675-3690. https://doi.org/10.1007/s12652-021-03494-1

[5] Sulaiman, H.O. (2022). An enhanced Rivest-Shamir-Adleman algorithm image security using residue number system. Master's thesis, Kwara State University, Nigeria. https://doi.org/10.14710/jtsiskom.2021.14038

[6] Zia, U., McCartney, M., Scotney, B., Martinez, J., AbuTair, M., Memon, J., Sajjad, A. (2022). Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains.

International Journal of Information Security, 21(4): 917-935. https://doi.org/10.1007/s10207-022-00588-5

[7] Alghamdi, Y., Munir, A. (2024). Image encryption algorithms: A survey of design and evaluation metrics. Journal of Cybersecurity and Privacy, 4(1): 126-152. https://doi.org/10.3390/jcp4010007

[8] Tuo, Z. (2023). A comparative Analysis of AES and RSA algorithms and their integrated application. Theoretical and Natural Science, 25: 28-35. https://doi.org/10.54254/2753-8818/25/20240893

[9] Alsaffar, D.M., Almutiri, A.S., Alqahtani, B., Alamri, R.M., Alqahtani, H.F., Al+qahtani, N.N., Ali, A.A. (2020). Image encryption based on AES and RSA algorithms. In 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS), pp. 1-5. https://doi.org/10.1109/ICCAIS48893.2020.9096809

[10] Yakubu, H.J., Joseph, S.B., Yahi, N.M. (2023). RGB image encryption algorithm using RSA algorithm and 3D chaotic system. Arid Zone Journal of Basic and Applied Research, 2(2): 151-167. https://doi.org/10.55639/607.080706

[11] Khudzaifah, M., Ma'rifah, S.H., Fahmi, H. (2023). Implementation of Rubik's cube algorithm and Rivest-Shamir-Adleman (RSA) algorithm on iris digital image security. In 12th International Conference on Green Technology (ICGT 2022), Malang, Indonesia, pp. 312-323. https://doi.org/10.2991/978-94-6463-148-7_31

[12] Ibrahim, D., Ahmed, K., Abdallah, M., Ali, A.A. (2022). A new chaotic-based RGB image encryption technique using a nonlinear rotational 16 × 16 DNA playfair matrix. Cryptography, 6(2): 28. https://doi.org/10.3390/cryptography6020028

[13] Bao, Z., Xue, R. (2021). Survey on deep learning applications in digital image security. Optical Engineering, 60(12): 120901. https://doi.org/10.1117/1.OE.60.12.120901

[14] Chen, J., Li, X.W., Wang, Q.H. (2019). Deep learning for improving the robustness of image encryption. IEEE Access, 7: 181083-181091. https://doi.org/10.1109/ACCESS.2019.2959031

[15] Alsubaei, F.S., Alneil, A.A., Mohamed, A., Mustafa Hilal, A. (2023). Block-scrambling-based encryption with deep-learning-driven remote sensing image classification. Remote Sensing, 15(4): 1022. https://doi.org/10.3390/rs15041022

[16] Kolhar, M., Aldossary, S.M. (2023). Privacy-preserving convolutional Bi-LSTM network for robust analysis of encrypted time-series medical images. Ai, 4(3): 706-720. https://doi.org/10.3390/ai4030037

[17] Trujillo-Toledo, D.A., López-Bonilla, O.R., García-Guerrero, E.E., Tlelo-Cuautle, E., López-Mancilla, D., Guillén-Fernández, O., Inzunza-González, E. (2021). Real-time RGB image encryption for IoT applications using enhanced sequences from chaotic maps. Chaos, Solitons & Fractals, 153: 111506. https://doi.org/10.1016/j.chaos.2021.111506

[18] Hanif, M., Abbas, S., Khan, M.A., Iqbal, N., Rehman, Z.U., Saeed, M.A., Mohamed, E.M. (2020). A novel and efficient multiple RGB images cipher based on chaotic system and circular shift operations. IEEE Access, 8: 146408-146427. https://doi.org/10.1109/ACCESS.2020.3015085

[19] Ran, B., Zhang, T., Wang, L., Liu, S., Zhou, X. (2022). Image security based on three-dimensional chaotic system and random dynamic selection. Entropy, 24(7): 958. https://doi.org/10.3390/e24070958

[20] Ding, Y., Tan, F.Y., Qin, Z., Cao, M.S., Choo, K.K.R., Qin, Z.G. (2021). DeepKeyGen: A deep learning-based stream cipher generator for medical image encryption and decryption. IEEE Transactions on Neural Networks and Learning Systems, 33(9): 4915-4929. https://doi.org/10.1109/TNNLS.2021.3062754

[21] Ding, Y., Wu, G., Chen, D., Zhang, N., Gong, L., Cao, M., Qin, Z. (2020). DeepEDN: A deep-learning-based image encryption and decryption network for internet of medical things. IEEE Internet of Things Journal, 8(3): 1504-1518. https://doi.org/10.48550/arXiv.2004.05523

[22] Ahmed, F., Rehman, M.U., Ahmad, J., Khan, M.S., Boulila, W., Srivastava, G., Lin, J.C.W., Buchanan, W.J. (2023). A DNA based colour image encryption scheme using a convolutional autoencoder. ACM Transactions on Multimedia Computing, Communications and Applications, 19(3s): 128. https://doi.org/10.1145/3570165

[23] Natiq, H., Roy, A., Banerjee, S., Misra, A.P., Fataf, N.A.A. (2023). Enhancing chaos in multistability regions of Duffing map for an image encryption algorithm. Soft Computing, 27(24): 19025-19043. https://doi.org/10.1007/s00500-023-08170-4

[24] Huang, Y., Zhou, L. (2023). A hyper-chaos-based image encryption scheme with double parity alternate scrambling. Multimedia Tools and Applications, 82(27): 41879-41893. http://doi.org/10.2139/ssrn.3994132

[25] Chai, X., Fu, X., Gan, Z., Lu, Y., Chen, Y. (2019). A color image cryptosystem based on dynamic DNA encryption and chaos. Signal Processing, 155: 44-62. https://doi.org/10.1016/j.sigpro.2018.09.029

[26] Zhang, Y. (2020). The fast image encryption algorithm based on lifting scheme and chaos. Information Sciences, 520: 177-194. https://doi.org/10.1109/ACCESS.2022.3194730

[27] Veena, G., Ramakrishna, M. (2021). A survey on image encryption using chaos-based techniques. International Journal of Advanced Computer Science and Applications, 12(1): 379-384. https://doi.org/10.14569/IJACSA.2021.0120145

[28] Bayesh, M.R., Das, D., Ahadullah, M. (2026). A dual-layer image encryption framework using chaotic AES with dynamic S-Boxes and steganographic QR codes. Journal of Information Security and Applications, 96: 104322. https://doi.org/10.1016/j.jisa.2025.104322

[29] Chaudhary, N., Shahi, T.B., Neupane, A. (2022). Secure image encryption using chaotic, hybrid chaotic and block cipher approach. Journal of Imaging, 8(6): 167. https://doi.org/10.3390/jimaging8060167