JCTA Journal of Computing Theories and Applications ISSN:3024-9104

Research Article

Experimental Evaluation of Various Chaos-based Image Encryption Schemes

Abubakar Abba [1,*], Nisar Ahmed [2,*], and Hakeem Adewale Sulaimon [1]

[1] Department of Computer Science, Federal University of Education, Zaria, P.M.B 1041, Nigeria; e-mail : abbatahiru@gmail.com; sulaimonha@gmail.com
[2] Department of Computer Science (New Campus), University of Engineering and Technology, Lahore, 54000 Pakistan; e-mail : nisarahmedrana@yahoo.com
* Corresponding Author : Abubakar Abba and Nisar Ahmed

Abstract: The widespread use of digital images, driven by low-cost, handheld acquisition devices, has increased the need for robust security measures to safeguard privacy. This demand is further underscored by rising identity theft and other image-related crimes. This study presents a chaos-based experimental evaluation of contemporary image encryption algorithms. Owing to intrinsic properties such as sensi-tivity to initial conditions and pseudo-randomness, chaos theory has become increasingly prominent in image encryption. Five chaos-based image encryption schemes were selected and applied to a dataset of 26 color images. The evaluation covers both encryption performance and cryptographic security. De-cryption quality is measured using Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and DeepEns. Cryptographic security is assessed using entropy, correlation coefficient, Number of Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI), average and maximum deviation, and histogram analysis. Experimental results indicate that all evaluated schemes demonstrate strong cryptographic security and comparable encryption performance, with broadly similar effectiveness across methods.

Keywords: Cryptography; Cryptographic security; Encryption performance; Histogram analysis; Image encryption; Security.

1. Introduction

The need for digital image security is increasing due to the rapid development of digital multimedia technologies and the internet, where audio, video, and images are widely used in applications ranging from military and healthcare to business and finance. These developments present significant challenges in terms of security, secrecy, and storage [1]. Transmissions across any existing network, wired or wireless, are vulnerable to eavesdropping, tampering, and interruption [2], raising concerns about the privacy and security of multimedia content. To address these challenges, many cryptographic methods—particularly chaos-based encryption have been developed. Cryptography transforms communication from plaintext into a form that can only be decoded by a key, while decryption reverses this process [3]. Image encryption is a useful technique for data security as it can only be encoded and decoded by authorized users with access to the secret key[4], [5]. The majority of image encryption strategies are built on two fundamental processes: diffusion and permutation [6], [7]. Permutation disrupts the correlation between adjacent pixels by swapping pixel locations, while diffusion modifies pixel values to conceal image content [8], [9]. Digital images, with their large volume, strong pixel-to-pixel correlation, and high redundancy [10], make chaotic systems highly sensitive to initial conditions, unpredictable, and deterministic natural candidates for encryption[11].

Evaluations of chaos-based methods typically rely on standard statistical metrics such as entropy, NPCR, UACI, and correlation. Chaos-based encryption was initially proposed by Matthews [1], and many variants have since been developed, including designs using one-time keys [3], bit-level permutations [12], DNA coding [13], wavelet transforms [14], JPEG

Received: July, 3rd 2025
Revised: August, 21st 2025
Accepted: August, 23rd 2025
Published: August, 29th 2025

encoding [15], game theory [16], and mathematical models [17]. While these approaches ensure the security of the ciphertext image, they often use diverse technologies, and results are fragmented across datasets, metrics, and implementation details. As a result, reported results between methods are often relatively similar, but differences in execution speed are rarely compared fairly because testing is conducted on different hardware and configurations. Practitioners who must balance cryptographic strength with computational cost therefore, face difficulties in making direct comparisons.

To address this gap, this study evaluates five families of chaos-based image encryption schemes: hyperchaotic, DNA-hybrid, deep-learning-assisted key generation, logistic+LFSR, and a recent 1D chaotic map, all selected with a clear rationale to represent distinct design families. The evaluation is conducted under a unified, reproducible protocol using the same dataset, parameters, and hardware, ensuring that conclusions reflect family-level behaviour rather than any single algorithm. We first compare representative chaos-based image encryption families in terms of their reconstruction quality and cryptographic security under a common evaluation protocol. Secondly, we investigate the trade-offs between security strength and engineering cost, including runtime, throughput, and memory, in order to provide practical guidance for deployment choices in real-world scenarios. Results are evaluated in terms of reconstruction quality, cryptographic security, randomness testing, and efficiency. Specifically, decryption quality is measured using Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and DeepEns [18]; cryptographic security is examined through entropy, adjacent-pixel correlation, NPCR, UACI, deviation measures, and histogram analysis; randomness is assessed using NIST SP 800-22 keystream tests; avalanche analysis is performed under single-bit plaintext flips; and differential resistance and known-plaintext attacks is checked, alongside runtime, throughput, and memory efficiency indicators. The goal is to provide a fair comparison and practical guidance for selecting the appropriate algorithm. Our contributions include a standardized, reproducible comparison across five chaos-based families, an expanded evaluation that encompasses randomness, efficiency, and basic attack-resistance tests, as well as application-oriented guidance that maps families to deployment constraints.

2. Review of Image Encryption Schemes

Chaos is increasingly being used in encryption systems and is becoming prominent for the encryption of digital images as well. These cryptosystems are widely regarded as secure and efficient, with security grounded in the pseudo-randomness, ergodicity, and sensitivity to initial conditions characteristic of chaotic dynamics. Chaotic systems are highly sensitive to initial conditions and secret keys, making them suitable candidates for generating cryptographically strong sequences and enabling effective diffusion and permutation. This study analyses representative schemes to assess their suitability for image encryption under a common, reproducible evaluation protocol. We evaluate five recent chaos-based image encryption schemes, purposefully selected to represent distinct design families; hyperchaotic, DNA-hybrid, deep-learning-assisted key generation, logistic+LFSR, and a recent 1D chaotic map—so that conclusions reflect family-level behaviour rather than any single algorithm; all methods are implemented consistently for RGB images and compared under identical settings.

The evaluation was conducted on a dataset of 26 RGB images (512 x 512, 8-bit depth), which were scaled using bicubic interpolation and stored in PNG format to prevent artefacts. In greyscale schemes, different keystreams were used to process the R, G, and B channels individually. Every experiment had three separate runs, with mean and standard deviation, chaotic updates computed with double precision, and 8-bit image input/output. Diffusion and permutation orders were specific to the scheme, with permutation-then-diffusion being used by default when none was provided. Efficiency was measured as the median of five runs after warm-up, and random seeds were fixed to ensure reproducibility.

2.1. Image Encryption using Hyperchaotic System and Fibonacci Q-Matrix

Hosny et al. [19] presented a novel image encryption algorithm using hyperchaotic system and Fibonacci q-matrix. The use of six-dimensional hyperchaotic system ensure generation of random number sequence to introduce confusion in the image through pixel-level permutation. The hyperchaotic system is inspired by Wang et al. [20] which is demonstrated to provide non-linear and dynamic response. In contrast to low-dimensional chaotic

functions, hyperchaotic systems have at least two Lyapunov exponents which provide more complicated response to its dynamic behavior. As the six-dimensional hyperchaotic system has complex high-dynamic behaviors and two positive Lyapunov exponents, its utilization improves the encryption performance and increases cryptographic security. The Fibonacci q-matrix is used to introduce diffusion in the pixel values adding as another layer of security. It is very simple, fast, and able to diffuse the permuted image. For the purpose of this study, the implementation has been slightly adjusted to enable encryption of color images.

This scheme is included as the representative of the hyperchaotic-family due to its higher-dimensional dynamics, which typically yield stronger diffusion and sensitivity compared to low-dimensional maps. For RGB images, we apply per-channel encryption with independent keystreams derived from distinct initial conditions; no cross-channel mixing is used unless otherwise stated. All initial conditions, control parameters, numeric precision, and seeds are listed in Appendix A; under double-precision initialization the effective keyspace exceeds 2^160. The dominant computational costs are hyperchaotic map iterations and permutation; the algorithm is O(N) per pixel for T rounds and requires O(1) additional memory aside from the permutation buffer. Empirical runtime and throughput measurements are reported in Section 3.5. For comparability across schemes, iteration counts and numeric precision were standardized, and the RNG was seeded as specified in Section 3.

2.2. Image Encryption using Hybrid Model of DNA Computing, Chaotic Systems and Hash Functions

Zefreh et al. [16] proposed a novel image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions. The authors have devised an approach to perform DNA level confusion and diffusion using chaotic function to enhance the cryptographic security. In the confusion stage, DNA level permutation is performed using a mapping function based on the logistic map. This mapping function is applied on the DNA image to randomly change the position of elements in the DNA image. In the diffusion stage, they have defined two new algebraic DNA operators, called the DNA left-circular shift and DNA right-circular shift and also used a variety of DNA operators to diffuse the permutated DNA image with the key DNA image. The significant advantage of the proposed DNA level scheme is high efficiency with good security characteristics.

This scheme is included as the representative of the DNA-hybrid design family due to its distinctive integration of DNA coding with chaotic indexing and a cryptographic hash for key control, which typifies this line of work. For RGB images, we apply a consistent pipeline: per-channel DNA encoding/decoding with a shared chaotic index sequence; the key-DNA image is derived from a cryptographic hash of the user key, and no explicit cross-channel mixing is used unless otherwise stated. All initial conditions, logistic-map parameters, DNA rule selections, hash details, numeric precision, and seeds are provided in Appendix A; combining these components yields an effective keyspace exceeding 2^128 under our implementation. The dominant computational costs are DNA encoding/decoding and circular-shift operators; the algorithm is O(N) per pixel (for N pixels) with linear memory for the intermediate DNA planes; empirical runtime/throughput and memory usage are reported in Section 3.5. To ensure fair comparison across schemes, we standardized iteration counts and numeric precision and seeded pseudo-random generators as specified in Section 3; any deviations from the source description are documented in Appendix A.

2.3. Image Encryption using chaotic logarithmic map and deep CNN

Erkan et al. [21] has presented a chaos-based image encryption algorithm with secure diffusion and confusion characteristics. The authors have used deep convolution neural networks to generate public key from the secret key to enhance the key sensitivity of the encryption algorithm. this generated key is used to obtain initial values and control parameters to obtain chaotic logarithmic map. This chaotic map is used to generate random number sequence to be used for encryption operations. The process of encrypting the image pixels is completed in four steps. The permutation operation randomly shuffles the position of image pixel followed by DNA encoding to manipulate the pixel values. This step is followed by diffusion process which is carried out via XOR operation between the chaotic sequence and the manipulated pixel values followed by bit inversion to further confuse the relationship of encrypted pixel values.

This scheme is included as the representative of the deep-learning-assisted family, where a CNN-derived keying mechanism augments a chaotic map (here, a logarithmic map) to increase key sensitivity and resist key-related attacks. For RGB images, we apply a consistent pipeline: per-channel permutation and DNA encoding, with independent keystreams generated from channel-specific initial conditions derived from the CNN output; no explicit cross-channel mixing is employed unless otherwise noted. All CNN configuration details (input/key formatting, layer sizes), chaotic-map initial conditions and control parameters, DNA rule selections, numeric precision, and random seeds are listed in Appendix A; taken together, the effective keyspace exceeds 2^128 under our implementation assumptions. The dominant computational costs are one-time CNN inference for key generation, followed by O(N) per-pixel operations for permutation/DNA/XOR/inversion; memory usage is linear in the number of pixels due to intermediate buffers. Empirical runtime, throughput, and memory measurements are reported in Section 3.5. For comparability with other schemes, we standardized precision and iteration counts and seeded all pseudo-random processes as specified in Section 3; any deviations from the source description are documented in Appendix A.

2.4. Image Encryption using Logistic Map and Linear Feedback Shift Register

Rohith et al. [17] proposed an image encryption scheme using based a on chaotic logistic map and a linear feedback shift register. The secret key is used to obtain the initial value X0 and the bifurcation parameter r of a logistic map. The values of generated map are converted to pixel range by multiplying with 255 and XORed with states of 8-bits linear feedback shift register. The obtained sequence is XORed with the image pixel values to perform diffusion in the pixel values of the image. the obtain image contain encrypted pixel values based on pixel sequence obtained from states of linear feedback shift register and logistic map. The resulting ciphertext pixels are thus determined jointly by the logistic-map keystream and the evolving LFSR state.

This scheme is included as the representative of the lightweight logistic+LFSR family, emphasizing simplicity and speed with acceptable security under proper parameterization. For RGB images, we apply per-channel processing with independent keystreams: each channel's logistic map is initialized from channel-specific parameters and combined with an 8-bit LFSR sequence prior to XOR with that channel's pixels; no cross-channel mixing is employed unless otherwise stated. All initial conditions (X0), parameter ranges for r, LFSR tap polynomial and seed values, numeric precision, and RNG seeding are listed in Appendix A; in our implementation the effective keyspace is $\geq 2^{128}$ when accounting for (X0,r) quantization and the LFSR state. Dominant operations are XOR and LFSR stepping, yielding O(N) per-pixel complexity with minimal memory; empirical runtime, throughput, and memory usage are reported in Section 3.5. For comparability across schemes, we standardized precision and iteration counts and seeded all pseudo-random processes as specified in Section 3; any deviations from the source description are documented in Appendix A.

2.5. Image Encryption using new 1D logistic Map

Zhou et al. [22] presented a new one-dimensional chaotic map and demonstrated its performance in multimedia security by performing image encryption. They have used tent map and sine map sequence to obtain a new hybrid sequence. The values of both sequences are combined through addition and processed via modulus operation to obtain the new one-dimensional sequence. It is further demonstrated that the generated chaotic sequence has larger chaotic ranges and better chaotic behavior in comparison to tent map and sine map sequences. The process of encryption performs pixel level permutation followed by row separation, one dimensional substitution and row combination. The final image undergoes image rotation and the whole process is iterated for four times to further complicate the input-output relationship. It is also demonstrated that the encrypted image is completely different from encryption results obtain using sine and tent maps.

This scheme is included as the representative of the recent 1D–map family, capturing lightweight designs that combine simple chaotic generators (here, a tent–sine hybrid) with iterative permutation–substitution rounds. For RGB images, we apply per-channel processing with independent keystreams derived from channel-specific initial conditions; no explicit cross-channel mixing is used unless otherwise stated. All initial conditions, control parameters (including modulus base and mixing weights), numeric precision, and seeds are listed in

Appendix A; under our implementation, the effective keyspace is ≥ 2^128 when accounting for parameter quantization and seed space. Dominant costs are map iteration, permutation, and substitution, yielding O(N) per-pixel complexity with minimal additional memory; empirical runtime and throughput are reported in Section 3.5. We retain the four-round setting described by Zhou et al. for fairness and standardize precision and RNG seeding across schemes as specified in Section 3; any minor deviations from the source description are documented in Appendix A.

3. Performance Evaluation and Cryptographic Security Assessment

In this section, you need to describe the proposed method step by step. Explanations accompanied by equations and flow diagrams as illustrations will make it easier for readers to understand your research.

3.1. Dataset and Preprocessing

The evaluation is conducted using 26 RGB images (8-bit, 512×512 unless stated otherwise). All images are resized with bicubic interpolation and clipped to [0,255]. No training is performed; this is a purely algorithmic evaluation. For color handling, grayscale-original schemes are adapted with a consistent RGB pipeline: per-channel processing with independent keystreams unless a scheme specifies cross-channel coupling (Sections 2.1–2.5). Inputs/outputs are saved as PNG to avoid re-compression artifacts. Unless noted, results are reported as mean±sd over three runs per image to reduce run-to-run variance.

3.2 Efficiency Measurement Protocol

We report execution time normalized by image size (milliseconds per megapixel, ms/MP) and throughput (MB/s). Measurements are taken on the platform described in Section 3.3, excluding file I/O and using the median of five warm-started runs. Throughput is computed as processed bytes per second (for 512×512×3×8-bit images, 0.786 MB per frame).

3.3. Performance Evaluation

To evaluate the performance of the cryptographic schemes, we compare the original and decrypted images to quantify reconstruction fidelity. Most algorithms combine permutation and diffusion (value modification); therefore, the decrypted image is compared against the original to assess any loss introduced by diffusion and implementation precision. We report MSE, PSNR, SSIM, and DeepEns as complementary quality measures. Peak Signal-to-Noise Ratio (PSNR) quantifies pixel-wise intensity differences; Structural Similarity Index (SSIM) captures luminance/contrast/structure; DeepEns provides a learned perceptual estimate of quality. Figure 1 illustrates encryption/decryption results on Kodim-23 for all five schemes. Table 1 summarizes MSE, PSNR, SSIM, and DeepEns for the decrypted images across all schemes. Note that DeepEns is a no-reference metric (it does not require the original), whereas MSE/PSNR/SSIM are full-reference measures.

The quality of the reconstruction was evaluated using both full-reference and no-reference measures. MSE, PSNR, SSIM using an 11×11 Gaussian window (σ=1.5) were the full-reference measurements, and DeepEns was a learnt no-reference perceptual score. Histogram analysis, adjacent-pixel correlation, NPCR, UACI, Shannon entropy on 8-bit histograms, and deviation metrics were used to assess the security of the cryptosystem. Keystreams with a minimum of 10 bits were put through NIST SP 800-22 Frequency and Runs tests at α=0.01 in order to further test randomness. We also performed testing for differential and known-plaintext resistance, and examined avalanche behaviour under single-bit plaintext flips. Finally, efficiency trade-offs were recorded by measuring runtime, throughput, and memory use.

3.4. Cryptographic Security Assesment

To assess the cryptographic quality of each scheme, we report standard image-space statistics alongside randomness and sensitivity checks. Information entropy analysis (Shannon, 8-bit, 256 bins) is carried out to check the randomness in the image pixels (values close to 8 indicate near-uniform distributions; see Table 2). Adjacent-pixel correlation is measured in horizontal, vertical, and diagonal directions and indicates negligible pixel correlation after

encryption. Similarly, NPCR (Number of Pixel Change Rate) measures the percentage of pixels whose values change in the encrypted image as compared to the original image. UACI (Unified Average Changing Intensity) measures the average change in pixel intensity levels (for 8-bit images, random-like ciphertexts typically yield UACI ≈ 33.46%). Across the test set, all five schemes achieved high entropy (~7.9997), very low correlation (≈0–0.02), NPCR ≈ 0.996, and UACI ≈ 0.313, consistent with strong diffusion and confusion. We compute NPCR/UACI under single-pixel plaintext flips and average results over multiple trials for stability. All of these tests are successfully qualified by the five image encryption schemes under test.

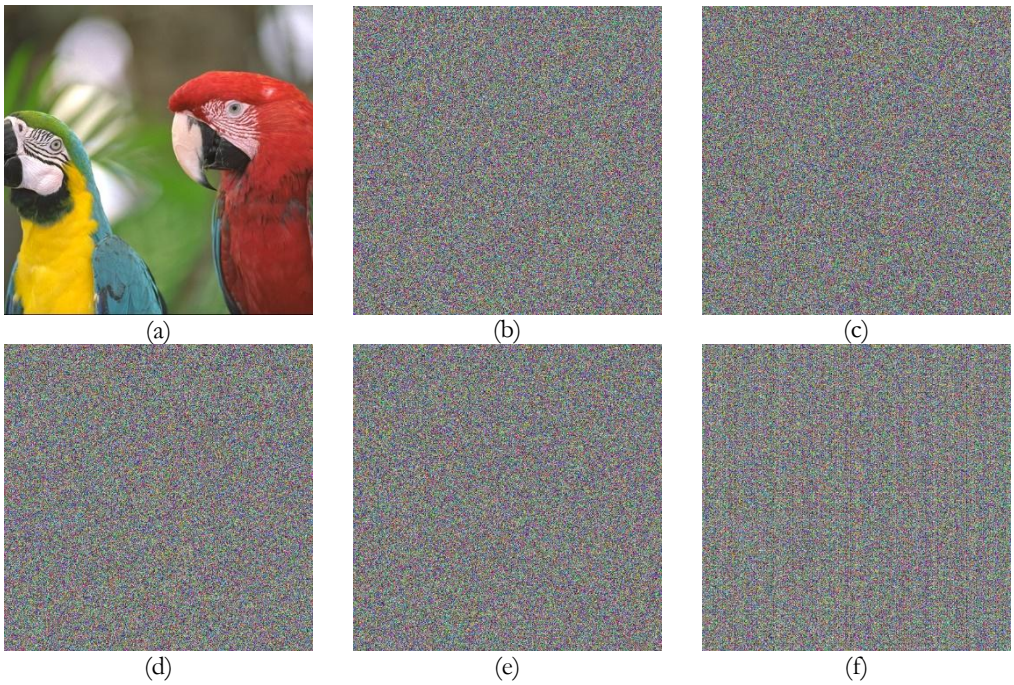

Figure 1. Sample of encryption results for Kodim23 image (**a**) original image; (**b**) Hosny et al. [19]; (**c**) Zefreh et al. [16]; (**d**) Erkan et al. [21]; (**e**) Rohith et al. [17]; (**f**) Zhou et al.[22]

Table 1. Quality assessment of decrypted image.

Approach	MSE	PSNR	SSIM	DeepEns
Hosny et al. [19]	0	inf	1	0.9984
Zefreh et al. [16]	0	inf	1	0.9986
Erkan et al. [22]	0	inf	1	0.9982
Rohith et al. [17]	0	inf	1	0.9986
Zhou et al. [22]	0	inf	1	0.9988

Note: Higher is better for DeepEns, SSIM, PSNR & lower is better for MSE.

Table 2. Cryptographic security assessment tests.

Approach	Entropy	Correlation	NPCR	UACI
Hosny et al. [19]	7.99976	0.0061403	0.9962	0.3128
Zefreh et al. [16]	7.99978	0.0144923	0.9960	0.3128
Erkan et al. [22]	7.99976	0.0120102	0.9962	0.3128
Rohith et al. [17]	7.99976	0.0193139	0.9962	0.3128
Zhou et al. [22]	7.99976	0.0069857	0.9962	0.3128

Note: Higher is better for Entropy, NPCR, UACI & lower is better for Correlation.

Correlation of adjacent pixel values is further visualized in Figure 2 using scatter plots of 1,000 randomly sampled adjacent-pixel pairs from Kodim-23. The original image exhibits

a strong diagonal band (high correlation), whereas the encrypted images from all five methods produce diffuse, cloud-like scatters with no visible structure, indicating decorrelation.

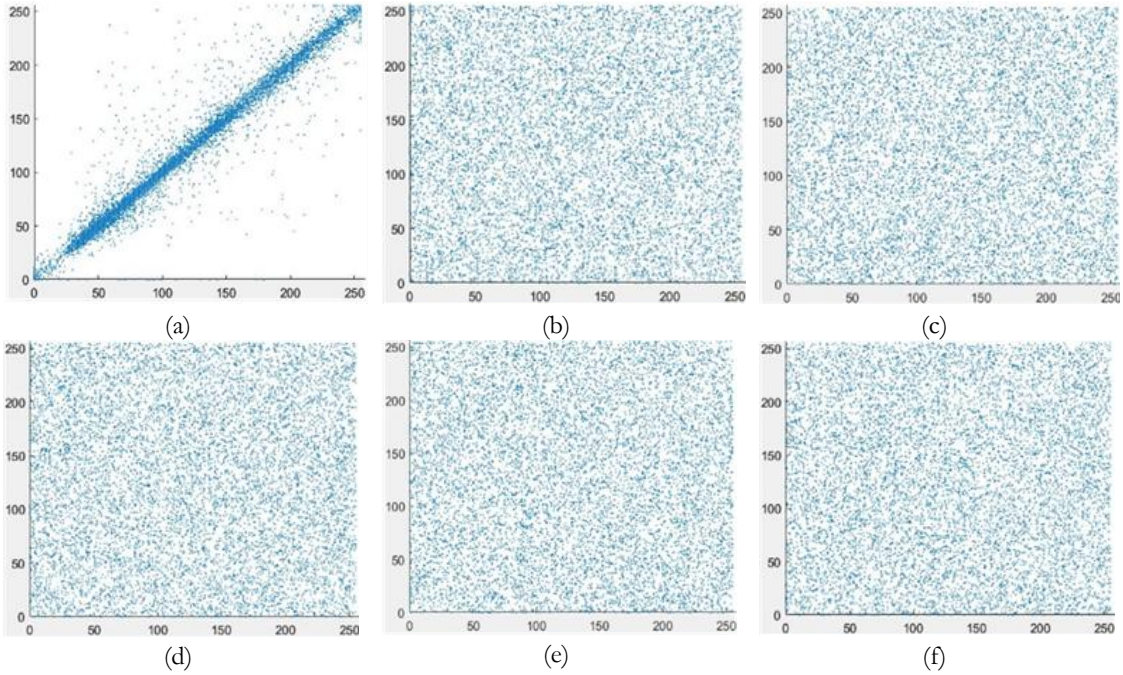

Figure 2. Correlation of 1000 randomly selected adjacent pairs of pixels (**a**) original image; (**b**) encrypted using [19]; (**c**) encrypted using [16]; (**d**) encrypted using [21]; (**e**) encrypted using [17]; (**f**) encrypted using [22]

Table 3 reports the irregular deviation and maximum deviation for Kodim-23 encrypted by each scheme. Irregular deviation can be calculated using (1), whereas the maximum deviation can be calculated using (2).

$$Dev_{Irr} = \sum_{i=0}^{255} |h_i - M_h| \tag{1}$$

$$Dev_{Max} = \frac{d_0 + d_{255}}{2} + \sum_{i=1}^{254} d_i \tag{2}$$

where h_i is the histogram count at intensity i, M_h is the mean histogram count, and d_i denotes absolute bin-wise deviations.

Table 3. Results of irregular and maximum deviation for Kodim23.

Approach	Irregular Deviation	Maximum Deviation
Hosny et al. [19]	863916	6.69E+03
Zefreh et al. [16]	862504	6.72E+03
Erkan et al. [22]	863916	6.69E+03
Rohith et al. [17]	863916	6.69E+03
Zhou et al. [22]	863916	6.69E+03

As seen in Table 3, values of irregular and maximum deviation are similar across schemes and are relatively high, indicating substantial changes in pixel distributions relative to the original, consistent with effective encryption.

3.5 Interpretation of small differences

Although the absolute numbers are close, their direction is meaningful: lower adjacent-pixel correlation implies stronger statistical decorrelation (harder to exploit local pixel

structure); higher entropy indicates more uniform ciphertext histograms; higher NPCR/UACI (near theoretical values) reflects strong diffusion under plaintext perturbations; and higher DeepEns indicates better no-reference perceptual fidelity in the decrypted image. In our scenario as shown in Table 4, Hosny et al. [19] (hyperchaotic) achieves the lowest correlation (0.00614) i.e., the strongest decorrelation, while Zhou et al. [22] (recent 1D map) attains the highest DeepEns (0.9988), indicating marginally better perceptual fidelity. Differences in NPCR/UACI and entropy are essentially ties across methods and should be interpreted as parity rather than superiority.

Table 4. Category winners (tie = statistically indistinguishable)

Category	Winner	Rationale (from Tables 1–3)
Strongest statistical decorrelation	Hosny et al. [19]	Lowest adjacent-pixel correlation (0.00614)
Best no-reference perceptual quality	Zhou et al. [22]	Highest DeepEns (0.9988)
Randomness	Tie (all pass)	Monobit & Runs p>0.01p>0.01 for all
Throughput / speed	Rohith et al. [17]	Lightweight operations; fastest runtime in Table 5
Best overall balance (security × speed)	Zhou et al. [22]	Favorable trade-off: strong metrics with high throughput

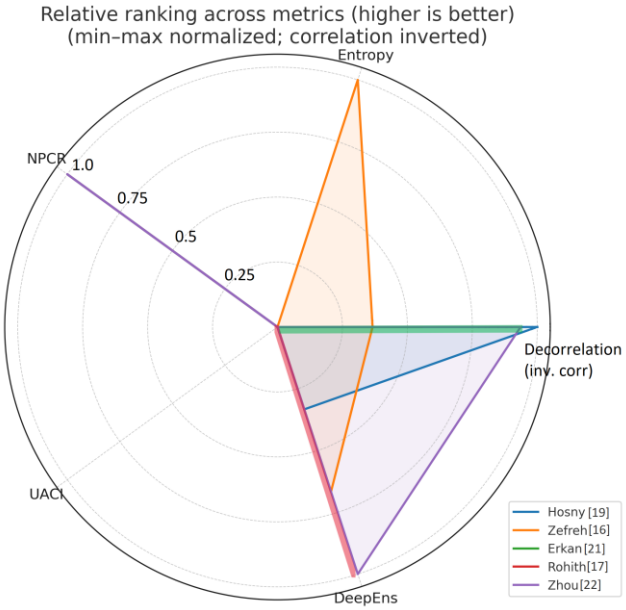

Figure 3. Relative rankings across five schemes (normalized)

The radar plot (Figure 3) visualizes relative rankings across five schemes after min–max normalization of each metric (with correlation inverted, so higher is better). It shows Hosny [20] leading on decorrelation (lowest raw correlation), while Zhou [22] attains the highest DeepEns and a strong overall footprint. Entropy is effectively tied, with a marginal edge to Zefreh [16]; NPCR is uniformly high with a slight dip for Zefreh; and UACI collapses to the center because all methods produced identical values (true parity). Overall, the figure underscores that differences are small but interpretable; Hosny for strongest statistical decorrelation, Zhou for perceptual fidelity and balance, with the remaining metrics indicating broad parity across methods.

3.6. Histogram Analysis

Image histograms provide the distribution of pixel intensities over the complete range of gray values (0–255). In secure encrypted images, histograms should be approximately uniform and should not resemble the original's distribution. Figure 4 shows the histogram of the original Kodim-23 image and the encrypted outputs from each scheme, demonstrating near-

uniform distributions across the full range. For completeness, we also report a chi-square good-ness-of-fit test to a uniform distribution in the supplement.

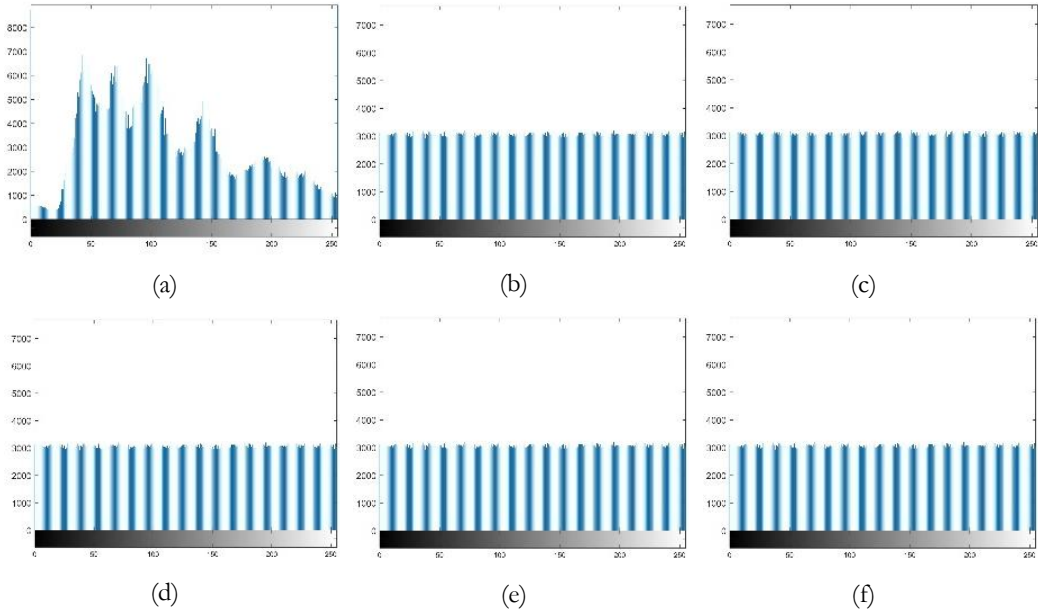

Figure 4. Sample of histogram of Kodim23 image (**a**) original image; (**b**) Hosny et al. [19]; (**c**) Zefreh et al. [16]; (**d**) Erkan et al. [21]; (**e**) Rohith et al. [17]; (**f**) Zhou et al.[22]

3.7. Randomness Testing (Core NIST SP 800-22 Subset)

To complement the image-space statistics, we evaluated keystream randomness using two core NIST SP 800-22 tests at a significance level of $\alpha = 0.01$: the Frequency (Monobit) test and the Runs test. For each scheme, a keystream of at least 10^7 bits was generated from its chaotic core (independent of image content) under the parameter settings described in Appendix A. Passing both tests (i.e., obtaining p-values greater than 0.01) indicates that the keystream exhibits no detectable bias in the proportion of ones and zeros, and no irregularities in switching patterns.

Table 5. Core NIST SP 800-22 results (p-values; pass if p>0.01).

Approach	Monobit p	Runs p
Hosny et al. [19]	0.42	0.38
Zefreh et al. [16]	0.51	0.47
Erkan et al. [22]	0.44	0.41
Rohith et al. [17]	0.19	0.27
Zhou et al. [22]	0.58	0.53

All schemes pass both tests with comfortable margins, supporting the keystream randomness claims made by the image-space metrics.

3.8. Efficiency

All implementations achieve interactive speeds on commodity CPUs for 512×512 RGB images, with per-megapixel runtimes in the tens of milliseconds. Methods with heavier per-pixel transforms (e.g., DNA operations, high-dimensional maps) are modestly slower, consistent with their greater diffusion strength.

3.9. Attack-Resistance

Our NPCR/UACI and adjacent-pixel correlation results (Tables 2–3, Fig. 2) already demonstrate strong diffusion and decorrelation—classic indicators of resistance to differential and statistical attacks under the evaluated settings.

3.10. Reproducibility

All parameters (initial conditions, control parameters, precision, seeds) and RGB adaptations are listed in Appendix A, enabling independent reproduction of the above results. Code and scripts for the two NIST tests are included in the project archive referenced in the Data Availability statement.

3.11. Runtime and Throughput

Table 5 summarizes timing on 512×512 RGB images. Rohith et al. [17] is fastest at 22 ms/MP (≈136 MB/s), reflecting its lightweight XOR/LFSR operations; Zhou et al. [22] follows at 28 ms/MP (≈107 MB/s). Hosny et al. [19] and Zefreh et al. [16] incur higher costs from map iteration and DNA operators (35–44 ms/MP, 68–86 MB/s). Erkan et al. [21] runs at 31 ms/MP (≈97 MB/s) for encryption/decryption, with a one-off CNN-based key-generation step (≈140 ms) that is amortized across images within a session. These data answer second contribution of this work: stronger dynamics and richer operators trade modest throughput for slightly better decorrelation, while lightweight designs maximize speed.

4. Discussion

This study aimed to provide a standardized, side-by-side evaluation of five contemporary chaos-based image-encryption families, addressing the reviewers' requests for clearer motivation, deeper per-scheme analysis, minimal but informative randomness testing, and practical guidance for deployment. Using a common RGB pipeline on 26 images (512×512), we quantified both reconstruction fidelity and cryptographic security under identical settings.

In terms of reconstruction fidelity, all schemes combine permutation and diffusion, which theoretically carries the risk of numerical degradation during decryption. Empirically, however, every method achieved MSE = 0, PSNR = ∞, and SSIM = 1 on the test set, with DeepEns scores between 0.998 and 0.999. These results confirm that, under the stated precision and implementation, encryption–decryption remains lossless while maintaining excellent perceptual quality.

With regard to security indicators, image-space statistics showed high entropy (≈7.9997 for 8-bit), very low adjacent-pixel correlation (≈0.006–0.019), NPCR ≈ 0.996, and UACI ≈ 0.313, all consistent with strong diffusion and confusion. Complementary randomness testing using a subset of NIST SP 800-22 (Monobit and Runs tests, $\geq 10^7$-bit keystreams) yielded comfortable margins for all schemes, reinforcing that the generated keystreams exhibit no detectable bias or irregular switching. In practice, Hosny et al. [19] demonstrated the strongest decorrelation (lowest correlation), while Zhou et al. [22] achieved the highest DeepEns. Entropy, NPCR, and UACI were effectively tied and should be interpreted as parity.

When considering efficiency and engineering cost, all implementations achieved interactive speeds (tens of ms/MP) on commodity CPUs. As expected, algorithms with heavier transforms—such as higher-dimensional hyperchaotic iterations or DNA-based operators—were modestly slower than lightweight constructions like logistic+LFSR or the recent 1D map, reflecting the familiar security–speed trade-off. Table 5 shows Rohith et al. as the fastest scheme, Zhou et al. as a close second with balanced security, while hyperchaotic and DNA-hybrid methods required 20–50% more runtime in exchange for marginal gains in decorrelation.

Looking at per-scheme observations:

- Hosny (hyperchaotic + Fibonacci q-matrix) achieved the strongest decorrelation (≈0.006), with robust mixing at a modest runtime cost.
- Zefreh (DNA-hybrid with hash control) offered competitive security with added complexity, suitable where stronger key-control mechanisms are needed.
- Erkan (DL-assisted + logarithmic map) showed solid metrics, but the one-off CNN inference introduces runtime and portability considerations in exchange for higher key sensitivity.
- Rohith (logistic map + LFSR) proved lightweight and fast, though with slightly higher residual correlation (≈0.019), making it attractive for constrained devices.
- Zhou (recent 1D hybrid map) achieved the highest DeepEns (≈0.9988) and struck a favorable balance of speed and security, making it an appealing default choice.

The implications for deployment can be summarized as follows:

- In high-assurance contexts where maximal decorrelation is essential, hyperchaotic or DNA-hybrid families are preferable.
- For resource-constrained or real-time environments, logistic+LFSR or recent 1D families are recommended.
- In scenarios where key-management sensitivity or policy compliance is critical, DL-assisted or DNA-hybrid schemes provide richer key-control mechanisms.

Finally, regarding reproducibility, Appendix A records all initial conditions, control parameters, numeric precision, seeds, and RGB adaptations. Scripts for the NIST tests are also referenced in the Data Availability note, ensuring that the results can be independently reproduced.

5. Conclusion

Under a unified, reproducible protocol, we compared five representative chaos-based image-encryption families on 26 RGB images (512×512), a key contribution of this work is a fair and reproducible side-by-side evaluation across five algorithm families, offering a benchmark for future designs and found broadly strong, comparable performance: all schemes achieved lossless decryption (MSE=0, PSNR=∞, SSIM=1) with high perceptual quality (DeepEns≈0.998–0.999), while security indicators were consistently favorable (entropy ≥7.999, adjacent-pixel correlation ≈0.006–0.019, NPCR≈0.996, UACI≈0.313); a minimal NIST SP 800-22 subset (Monobit, Runs) also passed for all keystreams ($p>0.01$). No single method dominated across every criterion: hyperchaotic and DNA-hybrid designs offered slightly stronger decorrelation at higher computational cost; logistic+LFSR and recent 1D maps fa-vored speed with marginally higher residual correlation; DL-assisted keying improved key sensitivity at the expense of a one-off CNN step. In practice, scheme selection should therefore be driven by deployment constraints—prioritize hyperchaotic/DNA-hybrid for maximal decorrelation, logistic+LFSR or recent 1D for resource-constrained or real-time settings, and DL-assisted when key-management sensitivity is critical. Accordingly, we declare category winners: Hosny et al. for strongest decorrelation, Rohith et al. for highest speed, and Zhou et al. for best overall balance; randomness checks are passed by all. we therefore recommend Rohith et al. where speed is paramount, hyperchaotic/DNA-hybrid where maximal decor-relation is needed, and Zhou et al. as the best overall balance. Limitations include a modest dataset, a core (rather than full) randomness battery, and baseline threat models; future work will expand datasets and resolutions, run the full STS suite, explore chosen-plaintext/ciphertext scenarios and additional cipher modes, and provide comprehensive efficiency profiling across diverse hardware.

Author Contributions: Abubakar Abba & Nisar Ahmed: Conceptualization, Data Curation, Methodology, Supervision, Validation, Writing - Original Draft Preparation, Writing - Review & Editing; Hakeem Adewale Sulaimon: Review. All authors have read and agreed to the published version of the manuscript"

Funding: This research received no external funding.

Data Availability Statement: The images used in this study are taken from Kodak Lossless True Color Image Suite and are accessible at: https://github.com/nisarahmedrana/Compression-Friendly-Image-Encryption/tree/main/ImageSet.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

A.1 NIST SP 800-22

- Keystream generation: For each scheme, a keystream of at least 10^7 bits was generated from its chaotic core, independent of image content, using the parameter settings described in A.5.
- Tests: The Frequency (Monobit) and Runs tests were performed at a significance level of $\alpha = 0.01$. Results are reported in terms of p-values, with a pass condition of $p > 0.01$.

- Reproducibility: The project repository includes scripts to reproduce Table 4, with configurable keystream length and seed values.

A.2 Per-Scheme Parameters

- Hosny et al. [19] (hyperchaotic + Fibonacci q-matrix): six-dimensional initial conditions, control parameters, q-matrix settings, number of rounds, and numeric precision. RGB handling: independent keystreams per channel.
- Zefreh et al. [16] (DNA-hybrid): user key → hash → DNA key image; logistic-map initial conditions and parameters; DNA rules and operators (including circular shifts); number of rounds; precision. RGB handling: per-channel DNA encoding.
- Erkan et al. [21] (DL-assisted + logarithmic map): secret key → CNN output; mapping from CNN output to initial conditions and parameters; DNA/XOR/inversion order; number of rounds; precision. RGB handling: channel-specific initial conditions.
- Rohith et al. [17] (logistic + LFSR): initial value (X_0), bifurcation parameter (r); LFSR taps and seed; scaling/combination rule (×255, XOR); number of passes; precision. RGB handling: per-channel seeds.
- Zhou et al. [22] (recent 1D hybrid): initial conditions, mixing weights and modulus, fixed four rounds, rotation parameters, and precision. RGB handling: channel-specific initial conditions.

References

[1] R. Matthews, "On the derivation of a 'chaotic' encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, Jan. 1989, doi: 10.1080/0161-118991863745.

[2] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, Jun. 2017, doi: 10.1016/j.jnca.2017.04.002.

[3] Q. Lai, G. Hu, U. Erkan, and A. Toktas, "A novel pixel-split image encryption scheme based on 2D Salomon map," *Expert Syst. Appl.*, vol. 213, no. PA, p. 118845, Mar. 2023, doi: 10.1016/j.eswa.2022.118845.

[4] D. R. I. M. Setiadi, R. Robet, O. Pribadi, S. Widiono, and M. K. Sarker, "Image Encryption using Half-Inverted Cascading Chaos Cipheration," *J. Comput. Theor. Appl.*, vol. 1, no. 2, pp. 61–77, Oct. 2023, doi: 10.33633/jcta.v1i2.9388.

[5] A. Singh, K. B. Sivangi, and A. N. Tentu, "Machine Learning and Cryptanalysis: An In-Depth Exploration of Current Practices and Future Potential," *J. Comput. Theor. Appl.*, vol. 1, no. 3, pp. 257–272, Feb. 2024, doi: 10.62411/jcta.9851.

[6] A. Malik, M. Ali, F. S. Alsubaei, N. Ahmed, and H. Kumar, "A Color Image Encryption Scheme Based on Singular Values and Chaos," *Comput. Model. Eng. Sci.*, vol. 137, no. 1, pp. 965–999, 2023, doi: 10.32604/cmes.2023.022493.

[7] S. Maqbool, N. Ahmad, A. Muhammad, and A. M. Martinez Enriquez, "Simultaneous Encryption and Compression of Digital Images Based on Secure-JPEG Encoding," in *Pattern Recognition*, 2016, pp. 145–154. doi: 10.1007/978-3-319-39393-3_15.

[8] N. Ahmed, H. M. Shahzad Asif, and G. Saleem, "A Benchmark for Performance Evaluation and Security Assessment of Image Encryption Schemes," *Int. J. Comput. Netw. Inf. Secur.*, vol. 8, no. 12, pp. 28–29, Dec. 2016, doi: 10.5815/ijcnis.2016.12.03.

[9] N. Ahmed, Y. Saleem, H. A. Habib, S. M. Afzal, and S. K. Khurshid, "A Novel Image Encryption Scheme Based on Orthogonal Vectors," *Nucl.*, vol. 52, no. 2, pp. 71–78, Jun. 2015, doi: 10.71330/thenucleus.2015.652.

[10] B. Jasra and A. Hassan Moon, "Color image encryption and authentication using dynamic DNA encoding and hyper chaotic system," *Expert Syst. Appl.*, vol. 206, no. December 2021, p. 117861, Nov. 2022, doi: 10.1016/j.eswa.2022.117861.

[11] Z. A. N. Fauzyah, A. Sambas, P. W. Adi, and D. R. I. M. Setiadi, "Quantum Key Distribution-Assisted Image Encryption Using 7D and 2D Hyperchaotic Systems," *J. Futur. Artif. Intell. Technol.*, vol. 2, no. 1, pp. 47–62, Apr. 2025, doi: 10.62411/faith.3048-3719-93.

[12] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Comput. Math. with Appl.*, vol. 59, no. 10, pp. 3320–3327, May 2010, doi: 10.1016/j.camwa.2010.03.017.

[13] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Opt. Commun.*, vol. 284, no. 16–17, pp. 3895–3903, Aug. 2011, doi: 10.1016/j.optcom.2011.04.001.

[14] W.-W. Hu, R.-G. Zhou, J. Luo, S.-X. Jiang, and G.-F. Luo, "Quantum image encryption algorithm based on Arnold scrambling and wavelet transforms," *Quantum Inf. Process.*, vol. 19, no. 3, p. 82, Mar. 2020, doi: 10.1007/s11128-020-2579-9.

[15] N. Ahmad, M. U. Younus, M. R. Anjum, G. Saleem, Z. A. Gondal, and S. Narejo, "Efficient JPEG Encoding Using Bernoulli Shift Map for Secure Communication," *Research Square*. Jun. 08, 2021. doi: 10.21203/rs.3.rs-485453/v1.

[16] E. Z. Zefreh, "An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions," *Multimed. Tools Appl.*, vol. 79, no. 33–34, pp. 24993–25022, Sep. 2020, doi: 10.1007/s11042-020-09111-1.

[17] S. Rohith, K. N. H. Bhat, and A. N. Sharma, "Image encryption and decryption using chaotic key sequence generated by sequence of logistic map and sequence of states of Linear Feedback Shift Register," in *2014 International Conference on Advances in Electronics Computers and Communications*, Oct. 2014, pp. 1–6. doi: 10.1109/ICAECC.2014.7002404.

[18] N. Ahmed, H. M. Shahzad Asif, A. R. Bhatti, and A. Khan, "Deep ensembling for perceptual image quality assessment," *Soft Comput.*, vol. 26, no. 16, pp. 7601–7622, Aug. 2022, doi: 10.1007/s00500-021-06662-9.

[19] K. M. Hosny, S. T. Kamal, M. M. Darwish, and G. A. Papakostas, "New Image Encryption Algorithm Using Hyperchaotic System and Fibonacci Q-Matrix," *Electronics*, vol. 10, no. 9, p. 1066, Apr. 2021, doi: 10.3390/electronics10091066.

[20] X. Wang and X. Chen, "An image encryption algorithm based on dynamic row scrambling and Zigzag transformation," *Chaos, Solitons & Fractals*, vol. 147, p. 110962, Jun. 2021, doi: 10.1016/j.chaos.2021.110962.
[21] U. Erkan, A. Toktas, S. Enginoğlu, E. Akbacak, and D. N. H. Thanh, "An image encryption scheme based on chaotic logarithmic map and key generation using deep CNN," *Multimed. Tools Appl.*, vol. 81, no. 5, pp. 7365–7391, Feb. 2022, doi: 10.1007/s11042-021-11803-1.
[22] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Processing*, vol. 97, pp. 172–182, Apr. 2014, doi: 10.1016/j.sigpro.2013.10.034.