International Journal of Computer Applications (0975 - 8887)
Volume 187 - No.140, September 2026

BLAKE3-based Color Image Encryption using Key-Driven Adaptive Quadtree Decomposition

Mohammed Hassan
Department of IS
College of Computers
Seiyun University
Seiyun, Republic of Yemen

Esra Maqsa
Department of IS
College of Computers
Seiyun University
Seiyun, Republic of Yemen

Wala Alzafeni
Department of IS
College of Computers
Seiyun University
Seiyun, Republic of Yemen

Zainab Alsaggaf
Department of IS
College of Computers
Seiyun University
Seiyun, Republic of Yemen

ABSTRACT

Color image encryption has received considerable research attention with many schemes proposed to address practical security needs. However, most of these schemes process plain images as a single unified block and often remain vulnerable to differential attacks and show poor sensitivity to plain image changes. Built on the substitution–permutation network architecture, this paper constructs a new scheme that adopts adaptive quadtree decomposition and the BLAKE3 hash function to enhance the security and sensitivity of the encryption process. Performance evaluations confirm that the scheme withstands brute-force, statistical, and differential attacks.

Keywords

Image encryption, BLAKE3, quadtree decomposition, substitution-permutation network.

1. INTRODUCTION

The need for encryption systems created especially for visual data has increased along with the growth of image sharing over public networks. However, standard encryption algorithms like AES, DES, and RSA were designed for text and are inappropriate for image encryption because of the intrinsic features of images, such as high computational cost, data redundancy, and significant correlation between neighboring pixels. Compared to conventional encryption methods, chaotic encryption techniques are more widely applicable. This perspective is reinforced by [8, 25], whose fundamental characteristics have since been verified by independent research. As a result, one of the most active areas of study in this area is chaotic image encryption.

Recent chaos-based security schemes generally integrate chaos logic with cryptographic components such as hash functions to strike a balance among security, computing speed, and practicality for real-world deployment [19, 2, 12]. No single method suits every deployment scenario, and the main open challenges are scalability, real-time performance, and robustness in constrained environments [2, 39, 5].

Image encryption approaches are classified based on the design methodology applied for the encryption and decryption systems. The main categories encompass classical ciphers, chaotic systems, DNA-based techniques, compressive sensing, frequency/transform-domain methods, neural network approaches, and hybrid schemes [6, 28]. Traditional ciphers such as AES, RSA, and Blowfish remain a reference class in image-encryption investigations [39]. Several assessments indicate that typical text-oriented ciphers are often less appropriate for real-time picture encryption as pictures have large size, high redundancy, and strong pixel correlation [6, 15, 43].

Chaotic-system methods are one of the most active groups and are sometimes categorised further into spatial, temporal, and spatiotemporal designs [71]. In reality, most chaotic image-encryption algorithms function in the spatial domain, directly shuffling or modifying pixels, and may be structured as block-cipher-like or stream-cipher-like schemes [65]. In DNA-based techniques, image pixels are encoded into DNA sequences and then employ DNA rules or operations to generate the encrypted image [65]. These algorithms are typically connected with chaos when chaotic sequences are exploited to drive DNA encoding, scrambling, or replacement [34, 66]. Compressed sensing image encryption accomplishes both sample compression and initial-layer encryption via its measurement stage, while post-processing processes such as scrambling complete the overall protective system [21, 67, 69]. The primary design problem is not whether compressive sensing can unify the pipeline, but how to boost security, key management, and reconstruction quality beyond the basic compressed sensing architecture [10, 67].

Frequency-domain image encryption techniques encrypt frequency coefficients or sub-bands rather than raw pixels, most frequently such as DWT, IWT, ILWT, DCT, FrDCT, FrFT, or lifting-wavelet transformations [42, 55, 36, 61, 50, 40]. The important design choice is which coefficients to protect: low-frequency, high-frequency, both, or nested sub-bands, and how intensely to process each [60, 61, 35].

In the case of neural network image encryption, research is mostly based on learning transformations and models, in addition to the use of classical permutation, diffusion, chaos or keying, and not purely on a single neural network [51, 24, 38]. The learnable component is widely utilised to derive information such as content-aware mappings, keys, features, and inversely derived transformations, which improve the flexibility, resilience, and future potentiality of encryption schemes [24, 22, 52]. Hybrid image encryption

schemes are based on combining chaos-based diffusion with another mechanism, which can be a classical cipher, DNA operation, hash function, optimization algorithms, compressed sensing, or a neural network [56, 64, 1].
Combining more than one cryptographic primitive often expands the key space, improves the confusion and diffusion properties and even improves key dependency [53, 14, 41].
This paper presents a new efficient image encryption system. This system is based on three core ingredients: the BLAKE3 cryptographic hash function, a key-driven adaptive quadtree decomposition, and a layered substitution-permutation network.
The main contribution of this work is to design a hybrid image encryption scheme that provides robust security against a broad range of classical cryptanalytic attacks, which results in both secure transmission of images as well as substantially increasing the difficulty of recovering the original image for adversaries with bounded computational resources. The 256-bit key space provides a large key space that makes exhaustive brute-force attacks computationally infeasible under conventional security assumptions. In addition, the proposed scheme can encrypt images of arbitrary dimensions without imposing specific restrictions on their width and height.
The rest of the paper is organised as follows. Section 2 presents the proposed system, describing the BLAKE3 cryptographic hash function, the key-driven adaptive quadtree decomposition, and the layered encryption and decryption process. Experimental results and security analysis are presented in Section 3, comparative evaluation in Section 4, and Section 5 concludes the paper.

2. THE PROPOSED SYSTEM

BLAKE3 is the latest member of the BLAKE cryptographic hash family, introduced in 2020 [44]. Unlike its predecessors, it employs a tree-based internal structure that enables native parallelism and efficient memory use, making it well suited as the key-derivation and keystream-generation primitive in the proposed scheme [45, 9].

2.1 Notation

The following notations are used consistently throughout the description of the proposed system to avoid ambiguity in the formal specification of the encryption and decryption processes:

—K: 256-bit (32-byte) master key.
—I: plain image of height H, width W, and c channels.
—$H_3(m, \ell)$: BLAKE3 extendable-output hash of message m, truncated to ℓ bytes.
—$\|$: byte-string concatenation.
—$\oplus$: bitwise XOR.
—$LE_{32}(v)$: v encoded as an unsigned little-endian 32-bit integer.
—$R = (y, x, h, w)$: a rectangular image region: top-left corner (y, x), height h, width w.
—$FY(N, \kappa)$: the length-N permutation of $\{0, \ldots, N-1\}$ produced by a key-seeded streaming Fisher-Yates shuffle under key κ (Definition 1).

Definition 1 (Keyed Fisher–Yates Permutation):
For $i = N-1, N-2, \ldots, 1$, draw the swap index

$$j_i = \mathrm{U}_{32}\Big(H_3\big(\kappa \,\|\, LE_{32}(i),\ 4\big)\Big) \bmod (i+1)$$

and swap positions i and j_i in the identity array $[0, 1, \ldots, N-1]$, where $\mathrm{U}_{32}(\cdot)$ interprets 4 bytes as a little-endian unsigned 32-bit integer. The result is a deterministic, key-dependent bijection on $\{0, \ldots, N-1\}$.

2.2 Encryption Steps

The encryption of plain-image I using a 32-byte key K proceeds in eleven steps organized into three groups: tile-preparation (Steps 1–3), per-tile encryption (Steps 4–7), and whole-Image diffusion and substitution (Steps 8–11). Figure 1 shows the architecture diagram of the proposed encryption system.
Step 1, Key-Driven Pseudo-Entropy Score: For every region $R = (y, x, h, w)$, a deterministic key-derived pseudo-entropy score H_p is defined in the range $[0, 8]$ that guides the quadtree decomposition of regions into smaller ones in later steps. It also allows identical reconstruction from the master key without information leakage during decryption:

$$\mathrm{coords}(R) = LE_{32}(y) \,\|\, LE_{32}(x) \,\|\, LE_{32}(h) \,\|\, LE_{32}(w)$$

$$v(R, K) = \mathrm{U}_{64}\Big(H_3\big(K \,\|\, \mathrm{coords}(R),\ 8\big)\Big)$$

$$H_p(R, K) = \frac{v(R, K)}{2^{64} - 1} \times 8.0 \ \in [0,\ 8]$$

Step 2, Size-Adaptive Split Threshold: For each region R, given constants $T_0 = 6.5, T_{min} = 2.0, \lambda = 1.0$, $m = 16$, determine the size-adaptive split threshold $T(h, w)$ which varies with tile size such that large regions are easier to split up and small regions cannot be split up excessively: Let $s(h, w) = \frac{hw}{m^2}$ denote the normalized tile size, then

$$T(h, w) = \max\left(T_{\min}, \frac{T_0}{1 + \lambda \ln s(h, w)}\right).$$

Step 3, Key-Driven Quadtree Decomposition: Recursively divides an image into a hierarchy of non-overlapping rectangular tiles which is fully reconstructible from the master key. Figure 2 shows the resultant tile layout of the example image. Larger tiles mean the pseudo entropy score was below the threshold, while smaller tiles mean that the tile was repeatedly subdivided.
A Region $R = (y, x, h, w)$ is split into four quadrants of sizes $\lfloor h/2 \rfloor, \lceil h/2 \rceil$ by $\lfloor w/2 \rfloor, \lceil w/2 \rceil$ if and only if

$$\big(h > m \ \wedge\ w > m\big) \ \wedge\ \big(H_p(R, K) > T(h, w)\big).$$

Recursion from $R_0 = (0, 0, H, W)$ terminates in a leaf set $\mathcal{T} = \{R_1, \ldots, R_L\}$ that partitions I exactly (no gaps, no overlap).

Step 4, Per-Tile Sub-Key Derivation: For each tile, three 16-byte sub-keys are generated from a single 48-byte BLAKE3 output for each tile using the master key and tile coordinates. This ensures a per-tile, unique key for each layer and cryptographically separates permutation, chaotic shift, and stream cipher layers. For every leaf tile $R_i = (y, x, h, w) \in \mathcal{T}$:

$$\mathrm{seed}_i = H_3\big(K \,\|\, \mathrm{coords}(R_i),\ 48\big)$$

$$K_p^i = \mathrm{seed}_i[0{:}16], \quad K_d^i = \mathrm{seed}_i[16{:}32], \quad K_s^i = \mathrm{seed}_i[32{:}48]$$

Step 5, Byte Permutation (Layer 1): Key-dependent Fisher-Yates shuffle [13] re-arranges the bytes within each tile. Since operation happens on byte level, it is possible that three color channels of one pixel will go to different positions in the permutation. Let T_i be the actual pixel array of tile i flattened to $N_i = h\,w\,c$ bytes (c = channel count), K_p^i be the permutation sub-key for tile i, then the Fisher-Yates shuffle P_i is given by:

$$P_i = FY(N_i,\ K_p^i)$$

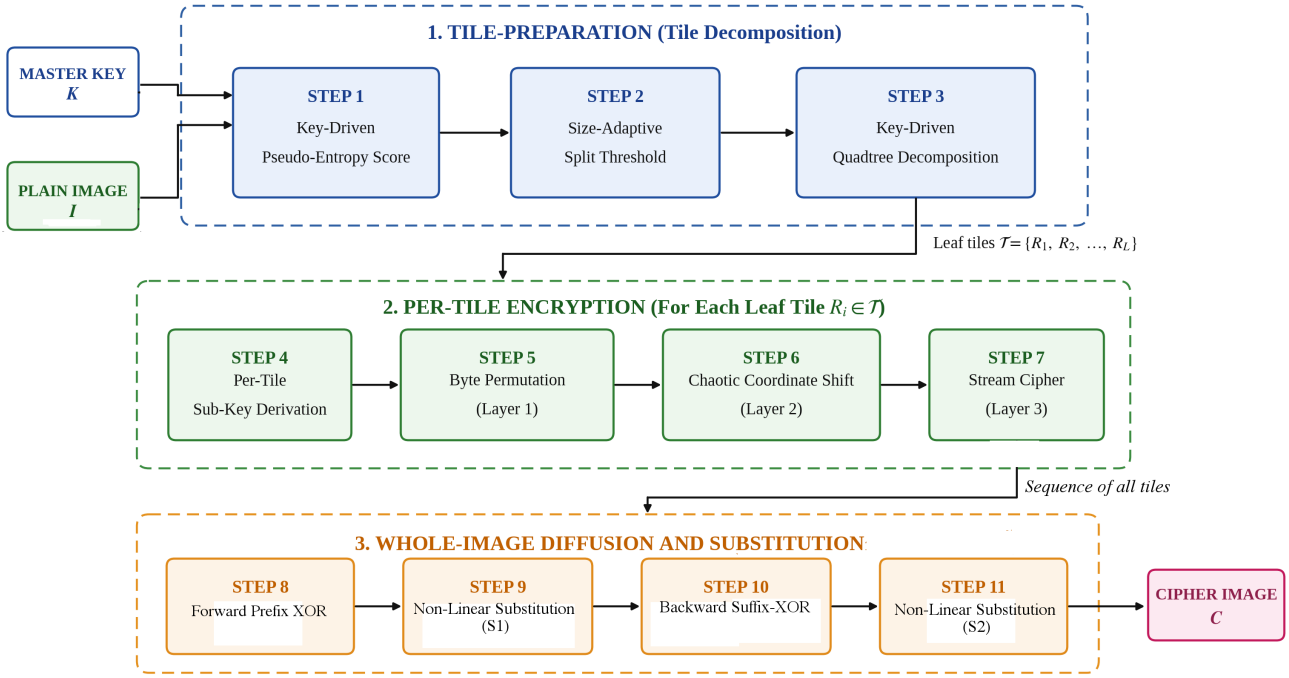


Fig. 1. Architecture diagram of Encryption system.

Fig. 2. Quadtree Decomposition of Lena Image.

The permuted array is obtained by iterating over positions j:

$$T_i^{(1)}[j] = \mathrm{flat}(T_i)\big[P_i[j]\big], \qquad j = 0, \ldots, N_i - 1$$

Step 6, Chaotic Coordinate Shift (Layer 2): For each tile, the array of pixels is reordered across the tile grid in several key-dependent rounds to enhance the spatial diffusion. To decide how many rounds to perform, the algorithm computes:

$$r_i = \big\lfloor H_p(R_i, K_d^i) \times 2 \big\rfloor + 1 \;\; (\geq 1)$$

where H_p is a pseudo-entropy value. To generate a different permutation for each round the algorithm combines the tile key K_d^i with the round number ρ.

$$\pi_\rho = FY\big(h\,w,\; H_3(K_d^i \,\|\, LE(\rho),\; h\,w \cdot 4)\big)$$

Applying all rounds in sequence:

$$T_i^{(2)} = \big(\pi_{r_i-1} \circ \cdots \circ \pi_1 \circ \pi_0\big)\big(T_i^{(1)}\big)$$

Step 7, Stream XOR Masking (Layer 3): Performs forward and backward cumulative XORs using two independently derived key-dependent S-box substitutions in order to have each byte of cipher image dependent on every byte of the plain image, to provide value confusion while preserving efficient and reversible decryption.

$$\mathrm{mask}_i = H_3(K_s^i,\; h\,w\,c)$$

$$T_i^{(3)} = T_i^{(2)} \oplus \mathrm{mask}_i \qquad \text{(element-wise, flattened)}$$

$T_i^{(3)}$ is written into the assembled intermediate image E at region R_i. Steps 4–7 repeat independently for every tile in $\mathcal{T}$.

Step 8, Forward Prefix-XOR Diffusion (Layer 4): Executes a cumulative forward XOR on the flattened image, where each byte output depends on every byte that came before it, so that local modifications affect the rest of the image.

$$d[0] = E[0], \qquad d[i] = d[i-1] \oplus E[i], \quad i = 1, \ldots, M-1$$

where $M = H \times W \times c$ is the total byte count of the flattened image.

Step 9, Non-Linear Substitution (S_1): The first key-derived S-box is then applied to the concatenated sequence of bytes to introduce nonlinearity. It converts easily recognizable patterns of XORS to pseudo random numbers prior to entering backward diffusion

phase.

$$d_s[i] = S_1\big(d[i]\big), \qquad i = 0, \ldots, M-1$$

Step 10, Backward Suffix-XOR Diffusion: Executes a cumulative backwards XOR through the substituted bytes so that the diffusion propagates backwards, such that each bit of the cipher image depends on each bit of the plain image for perfect whole-image diffusion.

$$e[M-1] = d_s[M-1], \qquad e[i] = d_s[i] \oplus e[i+1], \quad i = M-2, \ldots, 0$$

Step 11, Non-Linear Substitution (S_2): The second key-derived S-box is used to transform the backward-diffused byte sequence into the final cipher image by performing a final nonlinear operation to make it more resilient against both statistical and differential attacks.

$$C[i] = S_2\big(e[i]\big), \qquad i = 0, \ldots, M-1$$

Reshaping C to $H \times W \times c$ yields the ciphertext image.

2.3 Decryption

The decryption process follows the reverse order of steps performed in encryption process to reconstruct quadtree, subkeys, and S-boxes from the master key. It is guaranteed that no auxiliary storage or side information is required to reconstruct everything and then, recover the original image.

$$e[i] = S_2^{-1}(C[i])$$

$$d_s[i] = e[i] \oplus e[i+1] \ (i < M-1), \quad d_s[M-1] = e[M-1]$$

$$d[i] = S_1^{-1}(d_s[i])$$

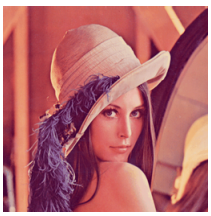
$$E[0] = d[0], \quad E[i] = d[i] \oplus d[i-1] \ (i \geq 1)$$

For each tile: $T_i^{(2)} = T_i^{(3)} \oplus \text{mask}_i$ (XOR is self-inverse); then $T_i^{(1)} = \pi_0^{-1} \circ \pi_1^{-1} \circ \cdots \circ \pi_{r_i-1}^{-1}\big(T_i^{(2)}\big)$; then apply P_i^{-1} to recover T_i. Assembling all tiles reconstructs I exactly.

3. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

To comprehensively illustrate the benefits of the proposed approach, seven widely adopted standard color test images of size 512 × 512 with three 8-bit channels were used, as shown in Table 1. These images were selected because they collectively span a broad range of statistical profiles.

Table 1. Dataset.

Image No	Image Name	Standard color images
1	Peppers	
2	Lena	
3	Airplane	
4	Baboon	
5	Barbara	
6	Boats	
7	Goldhill	

3.1 Key space

The key space size of an encryption scheme has to be large enough to make exhaustive brute-force search computationally infeasible. The 2^{100} threshold is widely cited in the image-encryption literature as the minimum key-space size needed to resist brute-force attacks, including those leveraging parallel hardware [7]. The proposed design uses a master key of 256 bits (32 bytes) and this key K is picked from a cryptographically secure pseudorandom number generator (CSPRNG); brute-force attacks are computationally infeasible:

$$|\mathcal{K}| = 2^{256} \approx 1.16 \times 10^{77}$$

which exceeds the conventional 2^{100} security threshold by a factor of approximately 10^{47}, therefore brute force attack against it is of

Table 2. Key Sensitivity Analysis.

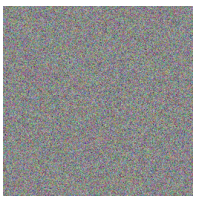
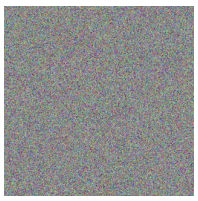
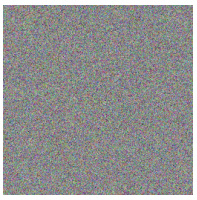
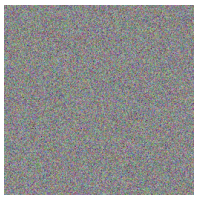
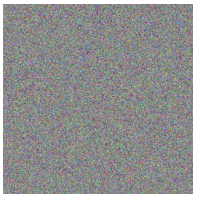
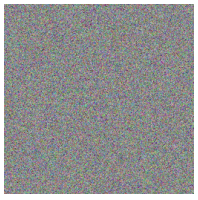
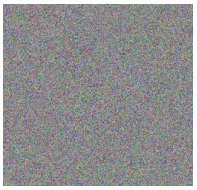
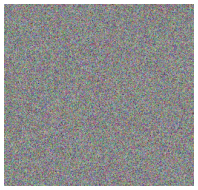
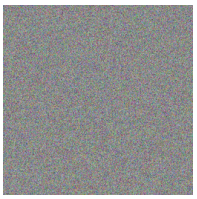
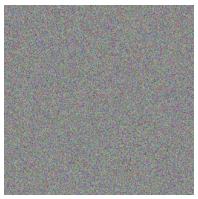
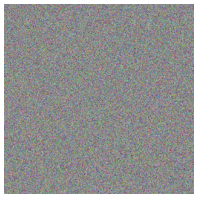
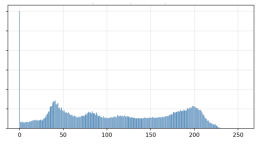
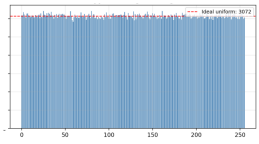
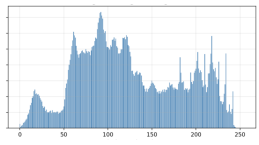
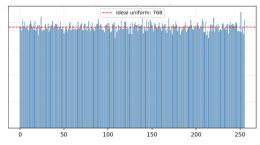
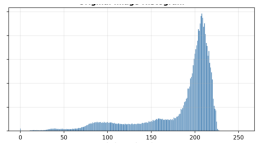
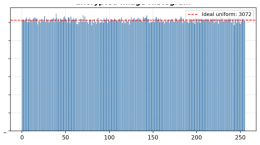
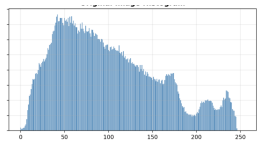
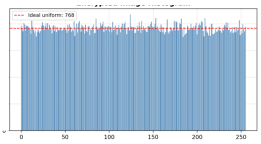
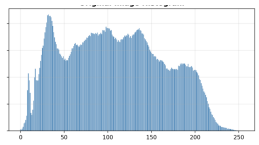
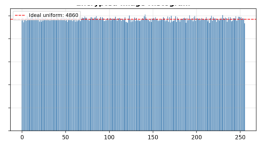
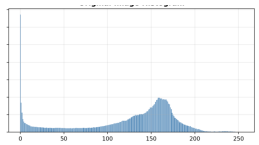
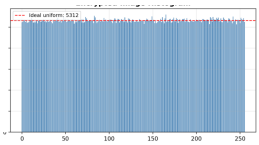
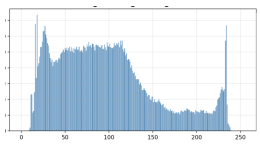
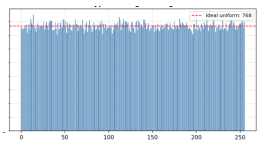
Image No	Encrypted (keyset-1)	Decrypted (keyset-1′)
1		
2		
3		
4		
5		
6		
7		

Table 3. Histogram Analysis.

Image	Plain Image	Encrypted Image
1		
2		
3		
4		
5		
6		
7		

no concern. To put this into perspective, even if an adversary could check 10^{18} keys per second, they would still expect to take about 10^{59} seconds, or roughly 10^{51} years, which is many orders of magnitude longer than the actual age of the universe (approximately 1.38×10^{10} years) to recover K via brute force.

3.2 Key sensitivity

A secure cryptosystem is expected to produce a completely different cipher image even when tiny modification is made to the secret key, and the decryption using invalid key should give an image unrelated to the plain image [58].
To quantify this property, each test image was first encrypted with an original 256-bit key denoted keyset-1 to obtain the cipher image C. A second key keyset-1′ was then constructed by flipping exactly one bit of keyset-1 (the least significant bit of the first byte), and the decryption was performed on C using keyset-1′ to produce a candidate recovered image. The resultant recovered images show clearly that small alteration of key generates a totally different output with no structural and spatial relation with plain image which resemble purely random noise as observed in the last column of Table 2. The difference between the two decryption attempts is enough to demonstrate that the proposed system exhibits perfect key sensitivity to the keys.

Table 4. Variance Analysis.

Image	Channel	Plain Image	k	k_1	k_2	k_3
Peppers	R	56752.34	251.44	242.98	273.09	251.34
	G	49437.01	259.84	222.77	268.48	244.25
	B	102106.44	276.77	268.23	250.40	258.61
Lena	R	74593.08	283.01	241.89	275.87	205.73
	G	30625.35	232.20	248.41	239.90	259.67
	B	94212.71	235.42	269.63	242.39	221.77
Boats	R	64320.09	267.02	248.30	229.19	230.32
	G	102659.41	288.66	286.66	212.09	268.41
	B	146018.17	245.02	283.18	274.78	227.20

3.3 Histogram Analysis

A histogram of an image shows the occurrences of every pixel value across the image and is one of the simplest statistical analyses that an attacker could perform in order to learn about plain image. Therefore, an encryption scheme is considered to be strong if it ensures that the histogram of the encrypted image is uniformly distributed, thus removing all correlations between the plain and encrypted image histograms [70]. Table 3 shows histograms of the original plain images and their corresponding encrypted images.
Clearly, the plain image histograms are strongly non-uniform, with peak and valley patterns mirroring the compositional structure of the underlying scene, whereas the encrypted image histograms are flat throughout the entire intensity range [0, 255], with absolutely no peaks, valleys or any periodic features.
Such uniformity helps to prevent the encrypted image being statistically distinguishable from a random number uniformly distributed on the intensity range [0, 255]. Thus, it is impossible to recover information about the underlying image through a histogram analysis of the encrypted image alone.

3.4 Variance of Histogram

Histogram variance serves as a quantitative measure of how uniform pixel counts are across the 256 grey levels of an encrypted image [57, 46]. Ideally, this variance should be as small as possible. Because the flatness of histogram is related to how evenly pixel values are distributed (lower variance values means more uniform, more likely to hide the structure of the plain image), whereas peaked histogram can reveal some of the plain text features and high variance is a signature of the histogram peak [48]. Hence variance serves as a statistical measure for testing encryption strength and is computed as:

$$\texttt{VAR}(Z) = \frac{1}{N^2} \cdot \frac{1}{2} \sum_{i=1}^{N} \sum_{j=1}^{N} (z_i - z_j)^2$$

where $Z = z_1, z_2, \ldots, z_{256}$ is the vector of histogram bin counts, and z_i, z_j represent the number of pixels whose grey values equal i and j, respectively.
To test the proposed scheme, the same test image was encrypted several times, once for each in a set of randomly generated keys $K = k, k_1, k_2, ...$ to produce several different cipher images. We then computed the variance of the plain image histogram and for each of the generated cipher images independently across the three R, G and B channels [26].
Table 4 indicates that the plain image histogram variances ranged considerably from 30,625.35 for the green channel of the Lena test image to 146,018.17 for the blue channel of the Boats test image as expected given the natural variance in such images. All the variances for the encrypted images lie within the relatively narrow range from 205 to 289; in every instance this is over a 99% decrease in variance and this demonstrates that the proposed system's histogram uniformity is consistent across different keys.

3.5 Correlation Analysis

Each natural image has a strong correlation between neighboring pixels because real-world objects contain smoothly varying surface features that make nearby points appear similar [16, 18]. A good encryption scheme has to completely disrupt any such correlation to hide the statistical structure of plain images [17]. We test decorrelating property of the adjacent pixels in the proposed encryption scheme by computing the Pearson correlation coefficient r_{xy} for neighboring pixels taken in three different directions (Horizontal H, vertical V and Diagonal D). The correlation coefficient is calculated as follows:

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

where:

$$E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i, \qquad D(x) = \frac{1}{N} \sum_{i=1}^{N} \big(x_i - E(x)\big)^2$$

$$\operatorname{cov}(x, y) = \frac{1}{N} \sum_{i=1}^{N} \big(x_i - E(x)\big)\big(y_i - E(y)\big)$$

Where (x, y) are two sequences of vertically, horizontally, and diagonally adjacent pixel intensity values respectively and N is the total number of selected pixel pairs.
Table 5 shows the distribution of correlations between neighbor pixels for R, G, and B channels of "Peppers" plain image in three different directions V, H and D and their respective scatter plots. The scatter plot of plain image for the R, G and B channels in the three directions shows tightly correlated neighboring pixels. The scatter plots for encrypted image show that pixels are uniformly scattered and no correlation can be visually detected.
The correlation coefficients of the cipher images for each color channels in all three directions are given in Table 6. As shown in that table, the correlation coefficients between neighbor pixels in cipher images are close to zero for all directions (horizontal, vertical and diagonal) and all channels (red, green and blue) satisfying a close to zero constraint $|r_{xy}| < 0.05$ for each direction and channel. Hence the proposed encryption scheme successfully hides all the statistical features of images for all channels and makes them robust to correlation attacks.

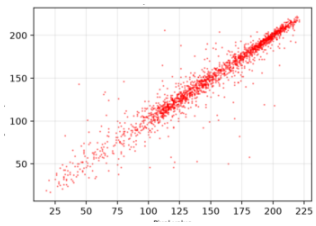
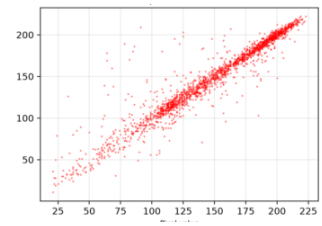
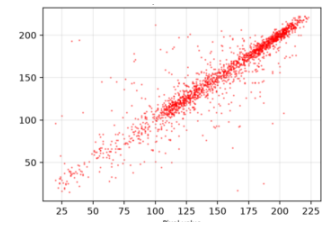
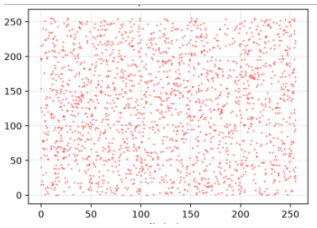
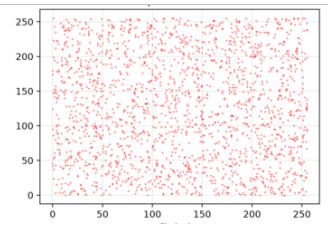
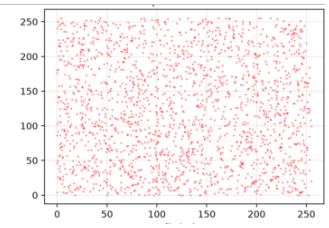
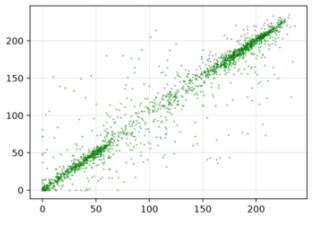
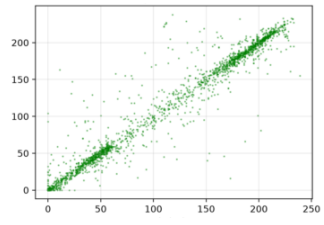
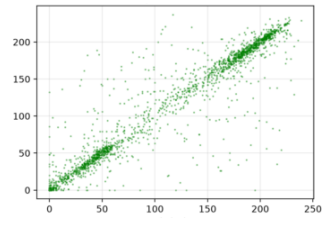
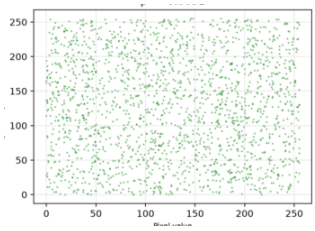
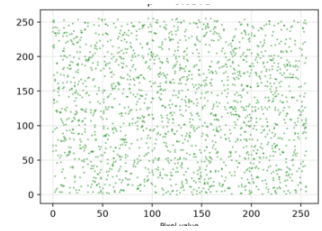
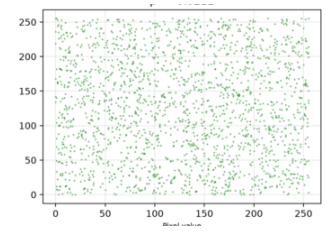
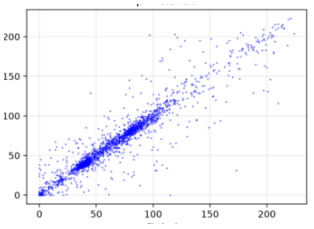
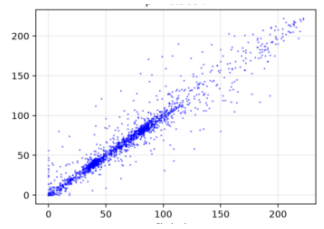
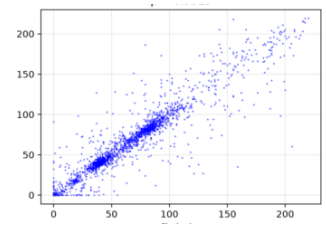
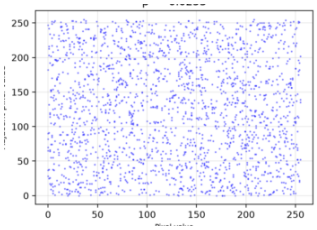
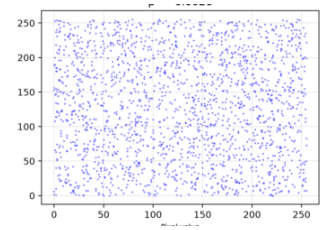
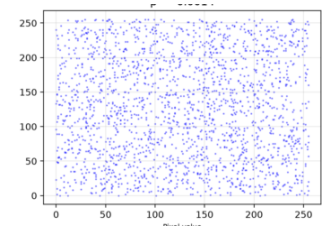
3.6 Shannon Entropy

Shannon entropy is the standard measure of uncertainty or randomness and it is commonly used for quantifying the information content carried by an image [59]. Entropy is desirable for security of a cipher image, since an ideally uniform distribution of pixel values in a cipher image cannot reveal any statistical property for an attacker to utilize. The Shannon entropy of an 8-bit image is expressed as the following:

$$H(m) = -\sum_{i=0}^{255} P(x_i) \cdot \log_2 P(x_i)$$

where x_i is the i^{th} grey level, $P(x_i)$ is the probability of occurrence of the grey level in the image and the summation is over all

Table 5. Correlation Analysis of Peppers Image.

Image	Channel	Horizontal	Vertical	Diagonal
Plain Image	R			
Encrypted Image	R			
Plain Image	G			
Encrypted Image	G			
Plain Image	B			
Encrypted Image	B			

possible 256 8-bit values. The theoretical maximum entropy of an 8-bit image is 8.0 bits. This is achieved if each of the 256 possible values occurs with the same probability; i.e., the image has a perfect uniform distribution and the image is statistically indistinguishable from white noise.

For testing purpose, the entropy is computed on all pixel values of the cipher image by using one histogram of 256 bins over all the color channels combined. This provides a global measure of the global randomness introduced by the cipher. Table 7 shows the Shannon entropy values of plain image and encrypted image for all test images. From this table, it is evident that plain images

Table 6. Values of Correlation Coefficients.

Image No	Channel	Horizontal	Vertical	Diagonal
1	R	-0.0226	-0.0064	0.0064
	G	-0.0029	0.0128	0.0052
	B	0.0157	-0.0108	-0.0027
2	R	-0.0047	0.0124	0.0358
	G	-0.0459	0.0265	-0.0421
	B	0.0142	0.0001	0.0364
3	R	0.0104	-0.0188	0.0216
	G	0.0129	0.0387	-0.0289
	B	0.0091	0.0388	0.0228
4	R	0.0098	0.0478	0.0018
	G	0.0114	-0.0166	0.0165
	B	-0.0040	-0.0090	-0.0075
5	R	-0.0108	0.0005	0.0130
	G	-0.0072	-0.0020	0.0036
	B	-0.0021	-0.0107	0.0328
6	R	0.0009	-0.0065	-0.0058
	G	-0.0068	0.0040	-0.0090
	B	0.0215	0.0233	-0.0479
7	R	0.0173	0.0152	0.0028
	G	0.0130	0.0123	-0.0093
	B	0.0199	-0.0211	-0.0143

Table 7. Shannon Entropy.

Image No	Plain image entropy	Cipher image entropy
1	7.7079	7.9990
2	7.7200	7.9990
3	6.6908	7.9991
4	7.7248	7.9991
5	7.6867	7.9991
6	7.3140	7.9989
7	7.6083	7.9991

contain significantly low values of Shannon entropy because of real world images having intrinsic structure and spatial correlation among pixel. On the other hand, each encrypted image after using the proposed scheme possesses very high Shannon entropy values above 7.998 bits which is close to the theoretical value 8.0 bits. This high entropy indicates that the proposed scheme is capable of effectively eliminating all detectable statistical bias in the cipher image, which makes it highly resistant to entropy-based statistical attacks.

3.7 NPCR and UACI

One known attack against image encryption systems is differential cryptanalysis, in which an attacker perturbs the original plain image by a small, imperceptible amount, then encrypts both the original image and the perturbed version and looks at the differences between the two cipher images to glean information about the key or the structure of the cipher [63]. In order to be resistant to this attack, an encryption scheme must exhibit good avalanche behavior on the plain image. There are two commonly used measures of avalanche behavior: the Number of Pixel Change Rate (NPCR) and the Unified Average Changing Intensity (UACI), defined as:

$$\texttt{NPCR} = \frac{\sum_{i,j} D(i,j)}{m \times n} \times 100$$

Table 8. NPCR and UACI Analysis.

Image	Pixel position	Pixel value	Changed value	NPCR (%)	UACI(%)
1	(1, 1, 1)	141	140	99.641	33.426
	(256, 1, 1)	112	111	99.988	33.908
	(1, 1, 2)	27	26	99.644	33.597
	(129, 65, 2)	188	187	99.814	33.814
	(65, 129, 3)	39	38	99.738	33.530
2	(1, 1, 1)	223	222	99.618	33.546
	(256, 1, 1)	79	78	99.992	34.955
	(1, 1, 2)	133	132	99.621	33.534
	(129, 65, 2)	125	124	99.799	33.835
	(65, 129, 3)	142	141	99.729	34.049
3	(1, 1, 1)	179	178	99.632	33.398
	(256, 1, 1)	113	112	99.992	33.660
	(1, 1, 2)	105	104	99.636	33.368
	(129, 65, 2)	137	136	99.817	31.934
	(65, 129, 3)	200	199	99.717	33.551
4	(1, 1, 1)	68	67	99.816	33.575
	(256, 1, 1)	34	33	99.934	34.437
	(1, 1, 2)	70	69	99.759	34.799
	(129, 65, 2)	68	67	99.895	33.667
	(65, 129, 3)	43	42	99.740	32.514
5	(1, 1, 1)	9	8	99.621	33.567
	(256, 1, 1)	9	8	99.982	34.153
	(1, 1, 2)	17	16	99.621	33.534
	(129, 65, 2)	198	197	99.841	32.065
	(65, 129, 3)	185	184	99.723	33.503
6	(1, 1, 1)	0	1	99.593	33.458
	(256, 1, 1)	1	0	99.982	33.283
	(1, 1, 2)	2	1	99.605	33.417
	(129, 65, 2)	198	197	99.812	33.853
	(65, 129, 3)	162	161	99.708	32.620
7	(1, 1, 1)	13	12	99.604	33.472
	(256, 1, 1)	50	49	99.983	33.536
	(1, 1, 2)	20	19	99.595	33.399
	(129, 65, 2)	71	70	99.804	34.444
	(65, 129, 3)	116	115	99.697	33.775

$$\texttt{UACI} = \frac{1}{m \times n} \sum_{i,j} \frac{|C(i,j) - C_1(i,j)|}{255} \times 100$$

where C and C_1 are the two cipher images corresponding to the original plain image and the slightly modified plain image, respectively; m and n denote the width and height of the image; and $D(i,j)$ is defined as:

$$D(i,j) = \begin{cases} 0, & \texttt{if } C(i,j) = C_1(i,j), \\ 1, & \texttt{if } C(i,j) \neq C_1(i,j). \end{cases}$$

NPCR measures the fraction of pixels that differ between the two cipher images, expressed as a percentage. The theoretical ideal for a perfectly random cipher is 99.6094, derived from the probability that two independently drawn uniform random bytes differ ($\frac{255}{256} \approx 99.6094\%$). UACI measures the average intensity difference between corresponding pixels of the two cipher images, normalized to the maximum possible intensity of 255. The theoretical ideal for a uniformly random cipher is 33.4635 ($\approx \frac{1}{3}$ of the full scale).

In order to show that the proposed cipher is resistant to differential attack, five pixel positions were randomly selected to span different spatial regions and all three color channels of each test image.

At each position, the pixel value changed by one unit (a change that cannot be visually seen and therefore a minimal perturbation of the plain image). Both the original image and each minimally modified version were then encrypted using the same key and the NPCR and UACI values were computed between the two resulting cipher images. These results for all seven test images can be seen in Table 8 and they reveal that NPCR never falls below 99.59% approaching the theoretical ideal of 99.6094%. The highest recorded value, 99.992% (Images 2 & 3, position (256, 1, 1)), confirms that even a single-unit plain image perturbation is sufficient to alter virtually every byte of the cipher image.
The UACI values range between 31.934% and 34.799%, closely centred on the theoretical ideal of 33.464% indicating that the magnitude of cipher image change is uniformly distributed and not biased toward small or large differences. Notably, the results remain consistent even when the modified pixel carries an extreme intensity value, such as the near-zero pixels in Image 6, demonstrating that the cipher's diffusion is independent of the plain image distribution. These findings confirm that the proposed scheme provides strong resistance against differential attacks: an adversary who knows the plain image can obtain no useful information about the key by observing how a one-unit plain image change propagates through the cipher image.

3.8 Salt-and-Pepper Noise

In practical transmission channels, impulse noise, commonly known as salt-and-pepper noise, randomly forces a fraction of pixels to either their maximum value (255, salt) or minimum value (0, pepper), causing bright spots in dark regions and dark spots in bright regions. This type of noise arises from analogue-to-digital converter errors, stuck sensor pixels, and bit errors during transmission [32]. To evaluate the proposed scheme's resilience against this type of degradation, each encrypted test image was corrupted with salt-and-pepper noise at densities of 3% and 5% of the pixels were forced to extreme values and then decrypted using the correct key. Visual inspection of the decrypted images, summarised in Table 13, shows that the decrypted images are still recognizable and readable by human eyes at both noise levels, which confirms the robustness of the proposed scheme to recover meaningful visual content from a noise contaminated cipher image.

3.9 Occlusion Noise

During network transmission, packets may be lost due to congestion or malicious interference, effectively zeroing out contiguous regions of the received encrypted image [11]. To evaluate the cipher's resilience to such data loss, an occlusion attack was simulated by randomly placing 16 × 16 zero-pixel blocks over the encrypted image until 5% and 15% of the total pixel area had been destroyed. The occluded cipher image was then decrypted using the correct key, and the recovered images were examined for visual quality. Table 14 demonstrates that the decrypted images retain their overall structure and remain visually interpretable at both occlusion levels, confirming that the cipher is capable of recovering a human-readable image even when a significant portion of the cipher image has been lost or deliberately destroyed during transmission.

4. COMPARATIVE PERFORMANCE EVALUATION

To show where the proposed scheme stands relative to the current state of the art, this section compares it with fifteen representative works from the recent image-encryption literature, as summarized in Tables 9 to 12. The evaluation covers standard cryptographic metrics, including cipher-image information entropy, adjacent-pixel correlation coefficients, differential-attack resistance measures (NPCR and UACI), and Peak Signal-to-Noise Ratio (PSNR) between plain and cipher images. To ensure a direct and fair comparison, identical test images are used across all evaluated ciphers. As demonstrated in the comparison, the performance metrics of the proposed scheme consistently meet or surpass those of the compared works, confirming that the proposed algorithm delivers superior security performance while preserving structural robustness under realistic transmission conditions.

Table 9. Comparative Entropy Analysis.

Algorithm	Lena	Baboon	Pepper
[23]	7.9997	7.9996	7.9994
[31]	7.9996	7.9993	7.9992
[62]	7.9973	7.9973	-
[30]	7.9896	7.9896	-
[3]	7.9990	7.9990	7.9990
[37]	7.9991	7.9991	-
Proposed	7.9990	7.9991	7.9990

Table 10. Comparative UACI and NPCR.

Algorithm		Lena	Baboon	Pepper
[23]	NPCR (%)	99.751	99.7503	99.7323
	UACI (%)	33.3755	33.4198	33.417
[37]	NPCR (%)	99.61	99.62	99.62
	UACI (%)	30.42	29.79	32.20
[31]	NPCR (%)	99.60	99.61	-
	UACI (%)	33.37	33.31	-
[62]	NPCR (%)	99.6089	99.6119	-
	UACI (%)	33.4727	33.4846	-
[27]	NPCR (%)	99.60	-	99.60
	UACI (%)	33.48	-	33.48
[54]	NPCR (%)	99.5721	-	99.6154
	UACI (%)	33.1264	-	33.1437
Proposed	NPCR (%)	99.992	99.934	99.988
	UACI (%)	34.955	34.437	33.908

Table 11. Comparative PSNR.

Algorithm	Lena	Baboon	Airplane	Pepper
[23]	10.6237	10.7692	7.9774	9.6796
[30]	8.6984	9.3308	7.9556	8.1447
[33]	8.6237	8.7692	7.9774	8.0796
[29]	10.0454	10.0754	8.1809	9.3950
[4]	8.6510	8.9283	-	8.1624
[47]	8.6000	8.9600	-	9.1700
Proposed	8.5977	8.3037	8.0100	8.0969

5. CONCLUSION

In this paper, a novel hybrid image encryption method is presented which combines three coordinated mechanisms: the BLAKE3 cryptographic hash function as an underpinning key-derivation and keystream primitive, a key-dependent adaptive quadtree decom-

Table 12. Comparative Correlation Analysis.

Algorithm	Image		R	G	B
[23]	Lena	Horizontal	0.0063	0.0005	0.0095
		Vertical	0.0158	0.0030	-0.0048
		Diagonal	-0.0022	0.0123	-0.0094
	Baboon	Horizontal	-0.0111	0.0031	-0.0080
		Vertical	-0.0161	-0.0038	-0.0007
		Diagonal	-0.0031	-0.0040	0.0012
[49]	Lena	Horizontal	0.0005	-0.004	0.0034
		Vertical	0.001	-0.001	-0.002
		Diagonal	0.0005	0.0008	-0.0019
	Baboon	Horizontal	0.0014	0.0068	0.0006
		Vertical	0.0014	-0.003	-0.005
		Diagonal	0.0029	-0.0023	-0.0058
[20]	Lena	Horizontal	0.0064	0.0009	0.0091
		Vertical	0.0160	0.0034	-0.0045
		Diagonal	-0.0026	0.0125	-0.0090
	Baboon	Horizontal	-0.0213	0.0126	-0.0102
		Vertical	0.0072	0.0120	0.0015
		Diagonal	0.0011	-0.0133	0.0025
[68]	Lena	Horizontal	0.0014	0.0033	0.0021
		Vertical	0.0048	-0.0006	0.0002
		Diagonal	0.0002	0.0048	-0.0040
	Baboon	Horizontal	0.0014	-0.0081	-0.0089
		Vertical	0.0047	0.0008	0.00001
		Diagonal	0.0003	0.0053	0.0017
Proposed	Lena	Horizontal	-0.0047	-0.0459	0.0142
		Vertical	0.0124	0.0265	0.0001
		Diagonal	0.0358	-0.0421	0.0364
	Baboon	Horizontal	0.0098	0.0114	-0.0040
		Vertical	0.0478	-0.0166	-0.0090
		Diagonal	0.0018	0.0165	-0.0075

position whereby each image is divided into dynamically sized rectangular sub-images called "tiles" whose boundaries are derived deterministically from the 256-bit master key, and a 4-stage permutation-substitution pipeline that is applied within each tile and then to the image as a whole. The work herein demonstrates that it is indeed possible to integrate all three techniques into a single cipher whose security performance over a diverse collection of test images and against each typical attack category known in the literature does not degrade on natural inputs. Empirical analysis covering key sensitivity, histogram uniformity, histogram variance, correlation analysis, Shannon entropy, NPCR and UACI, and robustness against noise and occlusion confirms that the proposed scheme achieves strong resistance to statistical and differential attacks. In future work, the inherent independence of the quadtree tiles combined with BLAKE3's native support for parallel hashing can be fully exploited to parallelize encryption across multiple processor cores, further improving computational efficiency.

6. REFERENCES

[1] Aqsa Zafar Abbasi, Ayesha Rafiq, Badr M Alshammari, and Ines Hilali Jaghdam. Advanced image encryption scheme based on generalized triangle group and neural networks. *Ain Shams Engineering Journal*, 16(8):103488, 2025.

[2] Moatsum Alawida. A novel image encryption algorithm based on cyclic chaotic map in industrial iot environments. *IEEE Transactions on Industrial Informatics*, 20(8):10530–10541, 2024.

[3] Wassim Alexan, Mohamed ElBeltagy, and Amr Aboshousha. Rgb image encryption through cellular automata, s-box and the lorenz system. *Symmetry*, 14(3):443, 2022.

[4] Wassim Alexan, Marwa Elkandoz, Maggie Mashaly, Eman Azab, and Amr Aboshousha. Color image encryption through chaos and kaa map. *IEEE Access*, 11:11541–11554, 2023.

[5] Wassim Alexan, Noura H El Shabasy, Noha Ehab, and Engy Aly Maher. A secure and efficient image encryption scheme based on chaotic systems and nonlinear transformations. *Scientific Reports*, 15(1):31246, 2025.

[6] Yousef Alghamdi and Arslan Munir. Image encryption algorithms: A survey of design and evaluation metrics. *J. Cybersecur. Priv.*, 4:126–152, 2024.

[7] Gonzalo Alvarez and Shujun Li. Some basic cryptographic requirements for chaos-based cryptosystems. *International journal of bifurcation and chaos*, 16(08):2129–2151, 2006.

[8] MS Baptista. Cryptography with chaos. *Physics letters A*, 240(1-2):50–54, 1998.

[9] Samarth Bhadane, Disha Gupta, Priyanka V Deshmukh, and Nivedita Mishra. A hybrid hash framework for post quantum secure zero knowledge identification. *Scientific Reports*, 15(1):42176, 2025.

[10] A. H. Brahim, Ali-Pacha Adda, and N. Hadj-Said. A new image compression-encryption scheme based on compressive sensing & classical aes algorithm. *Multimedia Tools and Applications*, pages 1–31, 2023.

[11] Xiuli Chai, Yiran Chen, and Lucie Broyde. A novel chaos-based image encryption algorithm using dna sequence operations. *Optics and Lasers in Engineering*, 88:197–213, 2017.

[12] Sanjay Das, Lotugada Jagan, Gaurav Kumar Singh, Sujal Kumar, Jayanti Rout, Ashutosh Soni, Surendra Kumar Nanda, and Manob Jyoti Saikia. Multilayered digital image encryption approach to resist cryptographic attacks for cybersecurity. *PeerJ Computer Science*, 11:e3260, 2025.

[13] Richard Durstenfeld. Algorithm 235: Random permutation. *Communications of the ACM*, 7:420, 1964.

[14] M. B. Farah, A. Farah, and Tarek Farah. An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. *Nonlinear Dynamics*, 99:3041 – 3064, 2019.

[15] Wei Feng, Zhentao Qin, Jing Zhang, and Musheer Ahmad. Cryptanalysis and improvement of the image encryption scheme based on feistel network and dynamic dna encoding. *IEEE Access*, 9:145459–145470, 2021.

[16] D. Field. Relations between the statistics of natural images and the response properties of cortical cells. *Journal of the Optical Society of America. A, Optics and image science*, 4 12:2379–94, 1987.

[17] Xing-Quan Fu, Bo-Cheng Liu, Yi-Yuan Xie, Wei Li, and Yong Liu. Image encryption-then-transmission using dna encryption algorithm and the double chaos. *IEEE Photonics Journal*, 10(3):1–15, 2018.

[18] Holly E Gerhard, Felix A Wichmann, and Matthias Bethge. How sensitive is the human visual system to the local statistics of natural images? *PLoS computational biology*, 9(1):e1002873, 2013.

[19] Nawal El Ghouate, Mohamed Amine Tahiri, Ahmed Bencherqui, Hanaa Mansouri, Ahmed El Maloufy, Hicham Karmouni, Mhamed Sayyouri, Sameh Askar, and Mohamed

Abouhawwash. A high-entropy image encryption scheme using optimized chaotic maps with josephus permutation strategy. *Scientific Reports*, 15(1):29439, 2025.

[20] Khalid M Hosny, Sara T Kamal, and Mohamed M Darwish. A color image encryption technique using block scrambling and chaos. *Multimedia Tools and Applications*, 81(1):505–525, 2022.

[21] Guiqiang Hu, Di Xiao, Yong Wang, and Tao Xiang. An image coding scheme using parallel compressive sensing for simultaneous compression-encryption applications. *Journal of Visual Communication and Image Representation*, 44:116–127, 2017.

[22] Yuanyuan Huang, Chenghao Liu, Fei Yu, Diqing Liang, Yuqing Song, and Jinmei He. An image encryption framework based on chaotic sequence combined with deep learning. *Physica Scripta*, 100(11):115208, 2025.

[23] Ayşegül İhsan and Nurettin Doğan. An innovative image encryption algorithm enhanced with the pan-tompkins algorithm for optimal security. *Multimedia Tools and Applications*, 83(35):82589–82619, 2024.

[24] Ayesha Iqbal, Hina Sattar, Umar Farooq Shafi, Aqsa Mahmood, Syeda Sitara Waseem, Syed Rizwan Hassan, and Abdurrahman S Hassan. An endtoend convolutional neural network for secure image transmission via joint encryption and steganography. *Scientific Reports*, 16(1):8228, 2026.

[25] Goce Jakimoski and Ljupco Kocarev. Chaos and cryptography: block encryption ciphers based on chaotic maps. *IEEE transactions on circuits and systems i: fundamental theory and applications*, 48(2):163–169, 2001.

[26] KC Jithin and Syam Sankar. Colour image encryption algorithm combining arnold map, dna sequence operation, and a mandelbrot set. *Journal of Information Security and Applications*, 50:102428, 2020.

[27] Shouqiang Kang, Yaqi Liang, Yujing Wang, and Mikulovich VI. Color image encryption method based on 2d-variational mode decomposition. *Multimedia Tools and Applications*, 78(13):17719–17738, 2019.

[28] Mandeep Kaur, Surender Singh, and Manjit Kaur. Computational image encryption techniques: a comprehensive review. *Mathematical Problems in Engineering*, 2021(1):5012496, 2021.

[29] Abdulrahman Dira Khalaf. Fast image encryption based on random image key. *International Journal of Computer Applications*, 134(3):35–43, January 2016.

[30] Majid Khan, Ammar S Alanazi, Lal Said Khan, and Iqtadar Hussain. An efficient image encryption scheme based on fractal tromino and chebyshev polynomial. *Complex & Intelligent Systems*, 7(5):2751–2764, 2021.

[31] Majid Khan and Fawad Masood. A novel chaotic image encryption technique based on multiple discrete dynamical maps. *Multimedia Tools and Applications*, 78(18):26203–26222, 2019.

[32] Jianzhong Li. Asymmetric multiple-image encryption based on octonion fresnel transform and sine logistic modulation map. *Journal of The Optical Society of Korea*, 20:341–357, 2016.

[33] Panchi Li and Ya Zhao. A simple encryption algorithm for quantum color image. *International Journal of Theoretical Physics*, 56(6):1961–1982, 2017.

[34] Lili Liu, Qiang Zhang, and Xiaopeng Wei. A rgb image encryption algorithm based on dna encoding and chaos map. *Comput. Electr. Eng.*, 38:1240–1248, 2009.

[35] Zhe Liu, Mee Loong Yang, and Wei Qi Yan. A framework for image encryption on frequency domain. In *Exploring Security in Software Architecture and Design*, pages 247–259. IGI Global Scientific Publishing, 2019.

[36] Zhengjun Liu, Jingmin Dai, Xiaogang Sun, and Shutian Liu. Triple image encryption scheme in fractional fourier transform domains. *Optics Communications*, 282:518–522, 2009.

[37] Zhentao Liu, Chunxiao Wu, Jun Wang, and Yuhen Hu. A color image encryption using dynamic dna and 4-d memristive hyper-chaos. *IEEE Access*, 7:78367–78378, 2019.

[38] Bofeng Long, Zhong Chen, Tongzhe Liu, Ximei Wu, Chenchen He, and Lujie Wang. A novel medical image encryption scheme based on deep learning feature encoding and decoding. *Ieee Access*, 12:38382–38398, 2024.

[39] K. Mahalakshmi and Sivakumar Nagarajan. Comprehensive review and analysis of image encryption techniques. *IEEE Access*, 13:109783–109813, 2025.

[40] Hemalatha Mahalingam, Thanikaiselvan Veeramalai, Anirudh Rajiv Menon, Subashanthini S, and Rengarajan Amirtharajan. Dual-domain image encryption in unsecure medium—a secure communication perspective. *Mathematics*, 11(2):457, 2023.

[41] Fawad Masood, Wadii Boulila, Abdullah Alsaeedi, J. Khan, Jawad Ahmad, M. Khan, and S. Rehman. A novel image encryption scheme based on arnold cat map, newton-leipnik system and logistic gaussian map. *Multimedia Tools and Applications*, 81:30931 – 30959, 2022.

[42] Abid Mehmood, Arslan Shafique, Shehzad Ashraf Chaudhry, Moatsum Alawida, Abdul Nasir Khan, and Neeraj Kumar. A time-efficient and noise-resistant cryptosystem based on discrete wavelet transform and chaos theory: An application in image encryption. *J. Inf. Secur. Appl.*, 78:103590, 2023.

[43] Ying Niu, Hangyu Zhou, and Xuncai Zhang. Image encryption scheme based on improved four-dimensional chaotic system and evolutionary operators. *Scientific reports*, 14(1):7033, 2024.

[44] Jack O'Connor, Jean-Philippe Aumasson, Samuel Neves, and Zooko Wilcox-O'Hearn. Blake3: one function, fast everywhere. *Real World Crypto*, 2020.

[45] Marut Pandya. Performance evaluation of hashing algorithms on commodity hardware. *arXiv preprint arXiv:2407.08284*, 2024.

[46] A. Raghuvanshi, Muskan Budhia, K. A. K. Patro, and B. Acharya. Fsr-spd: an efficient chaotic multi-image encryption system based on flip-shift-rotate synchronous-permutation-diffusion operation. *Multimedia Tools and Applications*, 83:57011 – 57057, 2023.

[47] V Sangavi and P Thangavel. An image encryption algorithm based on fractal geometry. *Procedia Computer Science*, 165:462–469, 2019.

[48] Parsa Sarosh, S. A. Parah, and G. M. Bhat. An efficient image encryption scheme for healthcare applications. *Multimedia Tools and Applications*, 81:7253 – 7270, 2022.

[49] KU Shahna and Anuj Mohamed. Novel hyper chaotic color image encryption based on pixel and bit level scrambling with diffusion. *Signal Processing: Image Communication*, 99:116495, 2021.

[50] Xiangqun Shi, Yifan Su, Xiaole Yang, Wei Feng, Xian Zhang, Zhenhua Chen, Guangjun Wen, and Heping Wen. Lossless frequency-domain image encryption via 3d exponential hyper-chaotic map and integer lifting wavelet transform. *Axioms*, 15(5):315, 2026.

[51] O. Singh, K. Singh, Amit Kumar Singh, and A. K. Agrawal. Deep learning-based image encryption techniques: Fundamentals, current trends, challenges and future directions. *Neurocomputing*, 612:128714, 2024.

[52] S Subathra and V Thanikaiselvan. Image adaptive encryption using efficientnet b3 feature guided multi scroll chaotic map with modulo controlled pseudo parallel processing. *Scientific Reports*, 15(1):43435, 2025.

[53] Enes Eren Suzgen, Muhammet Emin Sahin, and Hasan Ulutas. A novel hybrid medical image encryption scheme based on memristive chaos and dna-arx-3des with real-time implementation. *Scientific Reports*, 16(1):6230, 2026.

[54] Muhammad Tanveer, Tariq Shah, Amjad Rehman, Asif Ali, Ghazanfar Farooq Siddiqui, Tanzila Saba, and Usman Tariq. Multi-images encryption scheme based on 3d chaotic map and substitution box. *IEEE Access*, 9:73924–73937, 2021.

[55] Sara Tedmori and Nijad A. Al-Najdawi. Lossless image cryptography algorithm based on discrete cosine transform. *Int. Arab J. Inf. Technol.*, 9:471–478, 2012.

[56] Hasan Ulutas. A novel memristor-based hyperchaotic hybrid encryption system with dna for image encryption on the jetson tx2. *Scientific Reports*, 15(1):35745, 2025.

[57] Aminu Bello Usman, Mohammad Mazyad Hazzazi, Mujeeb Ur Rehman, Arslan Shafque, Aljaedi Amer, and Bassfar Zaid. Enhancing image security via chaotic maps, fibonacci, tribonacci transformations, and dwt difusion: a robust data encryption approach. *Scientific Reports*, 14(12277), 2024.

[58] Elaheh Vaferi and Reza Sabbaghi-Nadooshan. A new encryption algorithm for color images based on total chaotic shuffling scheme. *Optik*, 126:2474–2480, 2015.

[59] Xingyuan Wang, Lintao Liu, and Yingqian Zhang. Image encryption algorithm based on dynamic random growth technique. *Optics and Lasers in Engineering*, 66:10–18, 2015.

[60] Heping Wen, Zefeng Chen, Jiehong Zheng, Yiming Huang, Shuwei Li, Linchao Ma, Yiting Lin, Zhen Liu, Rui Li, Linhao Liu, et al. Design and embedded implementation of secure image encryption scheme using dwt and 2d-lasm. *Entropy*, 24(10):1332, 2022.

[61] Heping Wen, Zhaoyang Feng, Chixin Bai, Yiting Lin, Xiangyu Zhang, and Wei Feng. Frequency-domain image encryption based on iwt and 3d s-box. *Physica Scripta*, 99(5):055254, 2024.

[62] Jiahui Wu, Xiaofeng Liao, and Bo Yang. Image encryption using 2d hénon-sine map and dna approach. *Signal processing*, 153:11–23, 2018.

[63] Lu Xu, Xu Gou, Zhi Li, and Jian Li. A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion. *Optics and Lasers in Engineering*, 91:41–52, 2017.

[64] Ebrahim Zarei Zefreh. An image encryption scheme based on a hybrid model of dna computing, chaotic systems and hash functions. *Multimedia Tools and Applications*, 79:24993 – 25022, 2020.

[65] Bowen Zhang and Lingfeng Liu. Chaos-based image encryption: Review, application, and challenges. *Mathematics*, 11(11):2585, 2023.

[66] Qiang Zhang, Ling Guo, and Xiaopeng Wei. A novel image fusion encryption algorithm based on dna sequence operation and hyper-chaotic system. *Optik - International Journal for Light and Electron Optics*, 124(18):3596–3600, 2013.

[67] Rui Zhang and Di Xiao. Double image encryption scheme based on compressive sensing and double random phase encoding. *Mathematics*, 10(8):1242, 2022.

[68] Ying-Qian Zhang, Yi He, Pi Li, and Xing-Yuan Wang. A new color image encryption scheme based on 2dnlcml system and genetic operations. *Optics and Lasers in Engineering*, 128:106040, 2020.

[69] Nanrun Zhou, Aidi Zhang, Fen Zheng, and L. Gong. Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing. *Optics and Laser Technology*, 62:152–160, 2014.

[70] Hegui Zhu, Cheng Zhao, Xiangde Zhang, and Lianping Yang. An image encryption scheme using generalized arnold map and affine cipher. *Optik*, 125:6672–6677, 2014.

[71] Unsub Zia, M. McCartney, B. Scotney, Jorge Martínez, Mamun AbuTair, Jamshed Memon, and A. Sajjad. Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. *International Journal of Information Security*, 21:917 – 935, 2022.

Table 13. Salt and Pepper Noise Analysis.

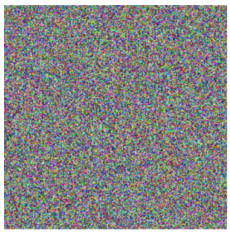
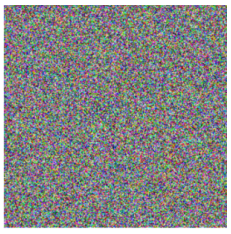
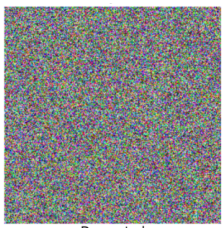
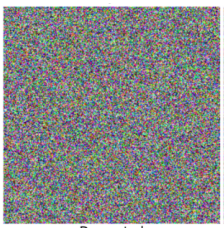
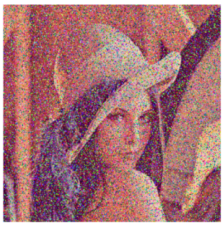
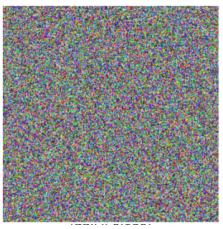
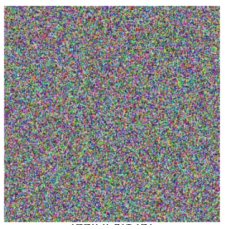
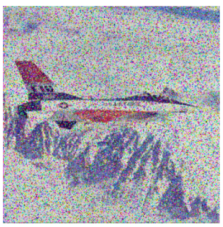
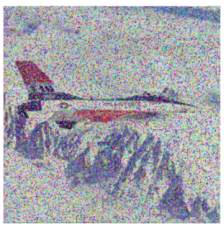
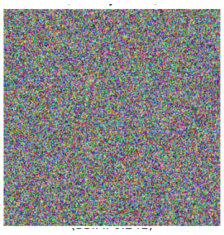
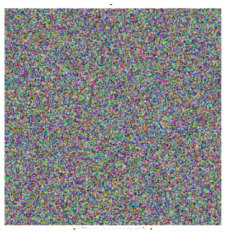
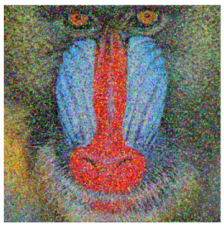
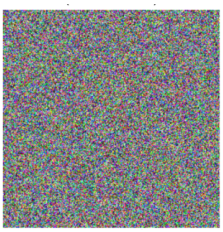
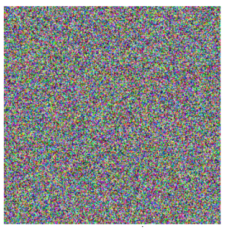
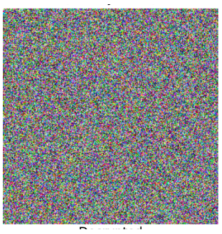
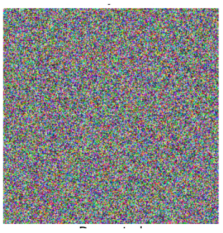
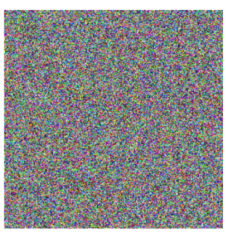
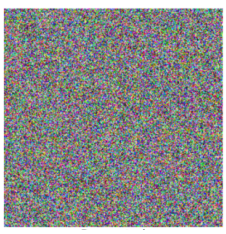
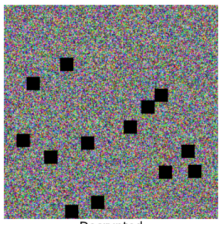
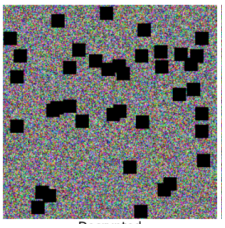
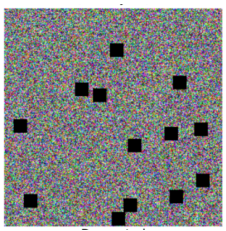
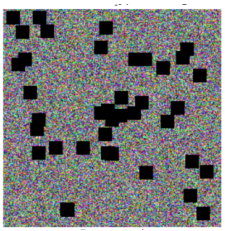
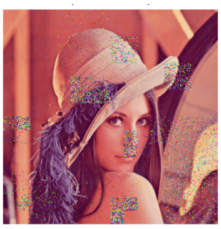
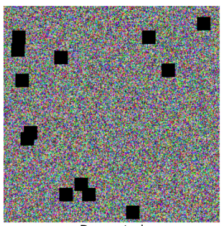
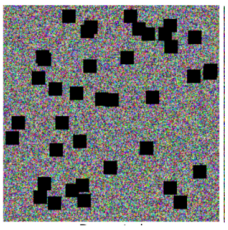
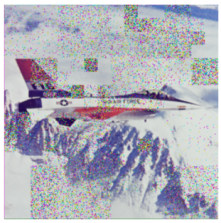
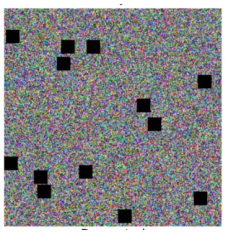
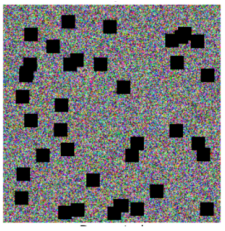
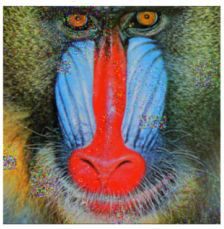
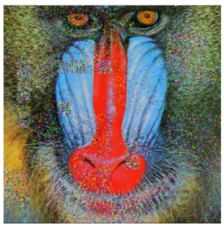
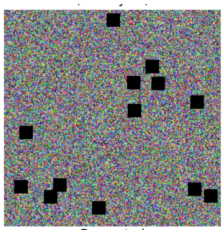
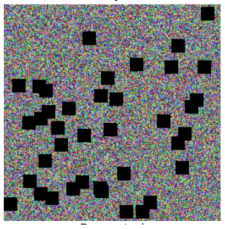
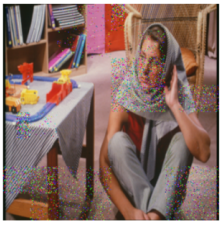
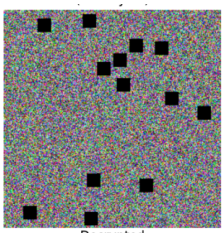
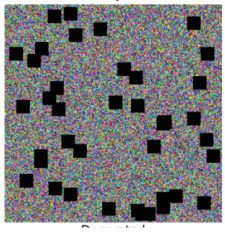
Image	Encrypted (3%)	Encrypted (5%)	Decrypted (3%)	Decrypted (5%)
1				
2				
3				
4				
5				
6				
7				

Table 14. Occlusion Noise Analysis.

Image	Encrypted (5%)	Encrypted (15%)	Decrypted (5%)	Decrypted (15%)
1				
2				
3				
4				
5				
6				
7