1. Experimental analysis and numerical simulation

Various grayscale test images are selected as the plain images. Each are first encrypted and then embedded into color carrier images “2.2.01”, “2.2.02”, “2.2.05”, “4.2.03”, “4.2.05”, “4.2.06”. The corresponding output is described in Figure1. As observed, the encryption successfully obscures all recognizable details of the plain images. Additionally, the cover and corresponding ciphertext images appear visually similar, with no obvious traces of the embedded content, demonstrating strong concealment and high imperceptibility.

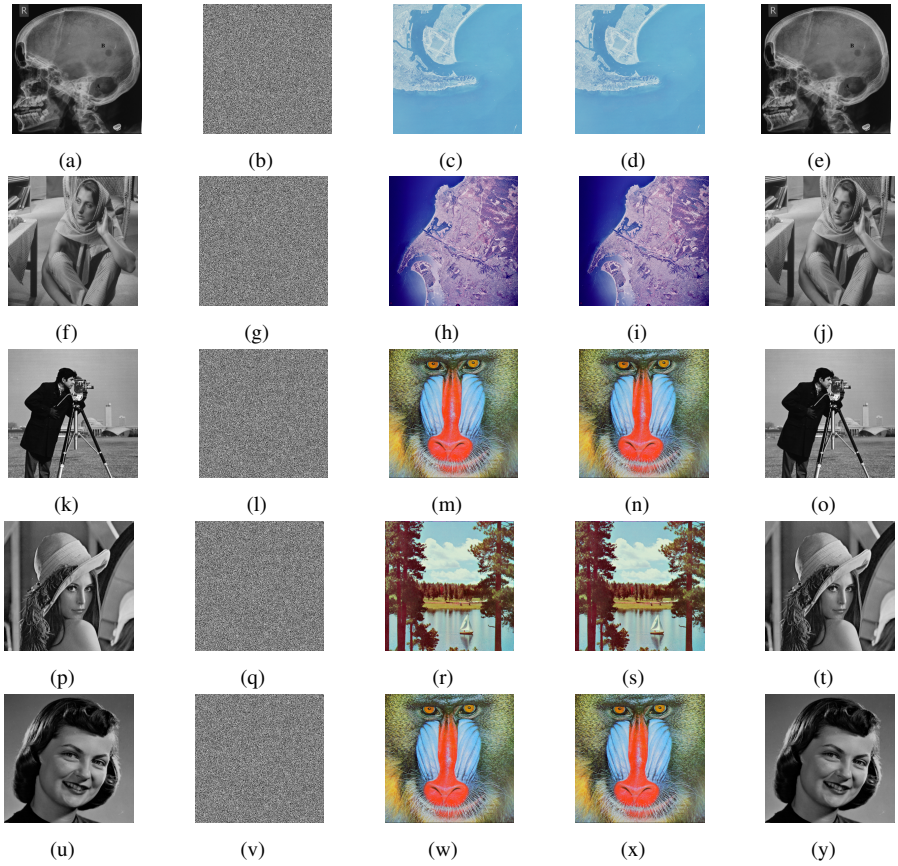


Figure 1: Visual analysis: first column represent plaintext images “Brain”, “Barbara”, “Cameraman”, “Lena”, “Girlface” ; second column depicts encrypted (secret) images; third column illustrate carrier images “2.2.02”, “2.2.01”, “4.2.03”, “4.2.06”; fourth column represents visually secure ciphertext (stego) images; fifth column described reconstructed (extracted) images.

1.1. Histogram analysis

This subsection assesses the encryption and concealment capabilities of the proposed algorithm using histogram analysis, as shown in Figure 2. The plain image histogram shows distinct pixel patterns, while the encrypted version exhibits a flat distribution, indicating strong diffusion [1]. The cipher image histograms remain visually similar to their carriers, confirming effective concealment.

1.2. Chi-square analysis

The (χ^2) test has been conducted to validate the uniformity of the histogram of the encrypted images [2]. A significance level of 0.05 was selected for this analysis. The following formula applied in this analysis is:

$$\chi^2 = \sum_{i=0}^{n} \frac{(x_i - y_i)^2}{y_i} \tag{1}$$

where $y_m = \frac{MN}{256}$ and x_m represents the expected and calculated frequencies respectively of each possible pixel value in the image, for $m = 0, 1, 2, 3, 4, 5.....255$ maximum pixel intensity. Table 1 presents the computed (χ^2)-values for both plain and encrypted images. The results demonstrate that the images encrypted using the proposed algorithm successfully pass the (χ^2)- test, as all calculated (χ^2)-values are lower than the corresponding critical values.

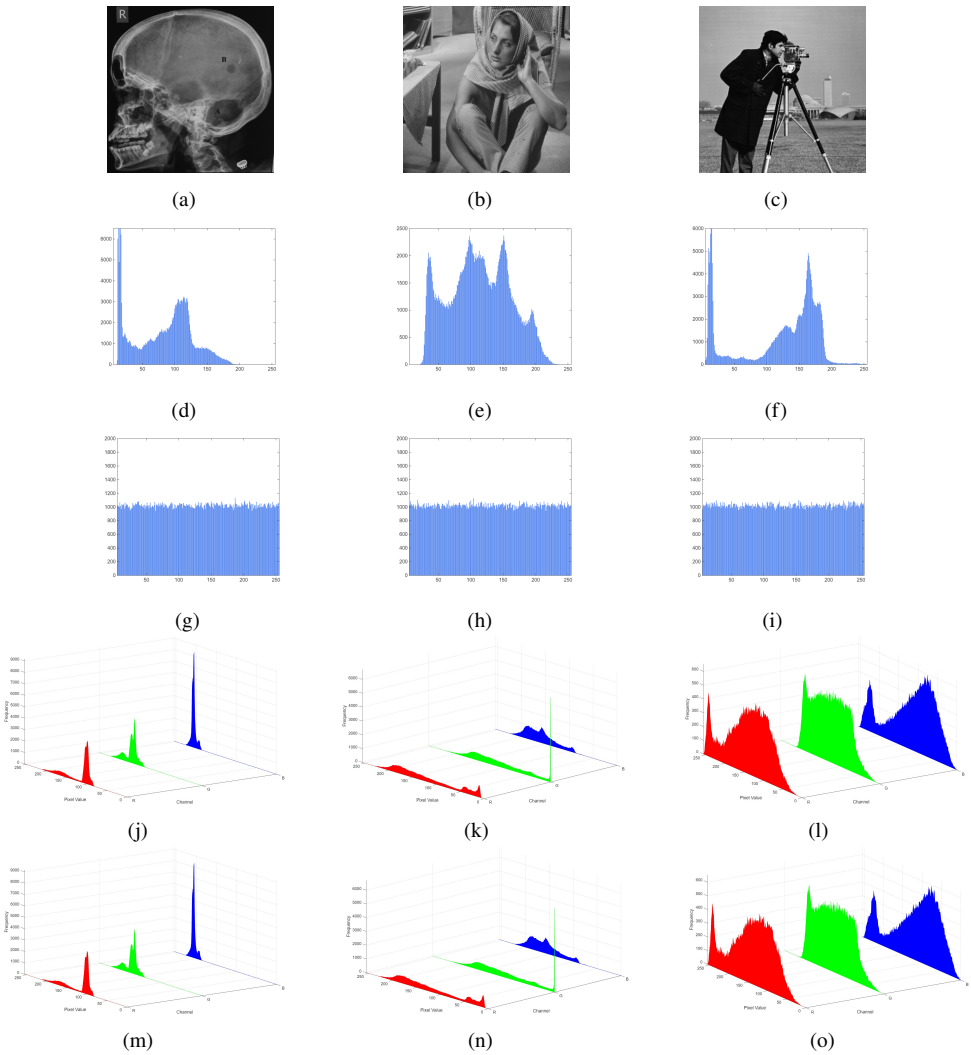


Figure 2: Histogram analysis: first row represent plain images “Brain”, “Barbara”, “Cameraman”; second row depicts histogram of plain images; third row illustrate encrypted images histogram; fourth row represents cover images “2.2.02”, “2.2.01”, “4.2.03” histogram; fifth row described ciphertext (stego) images histogram.

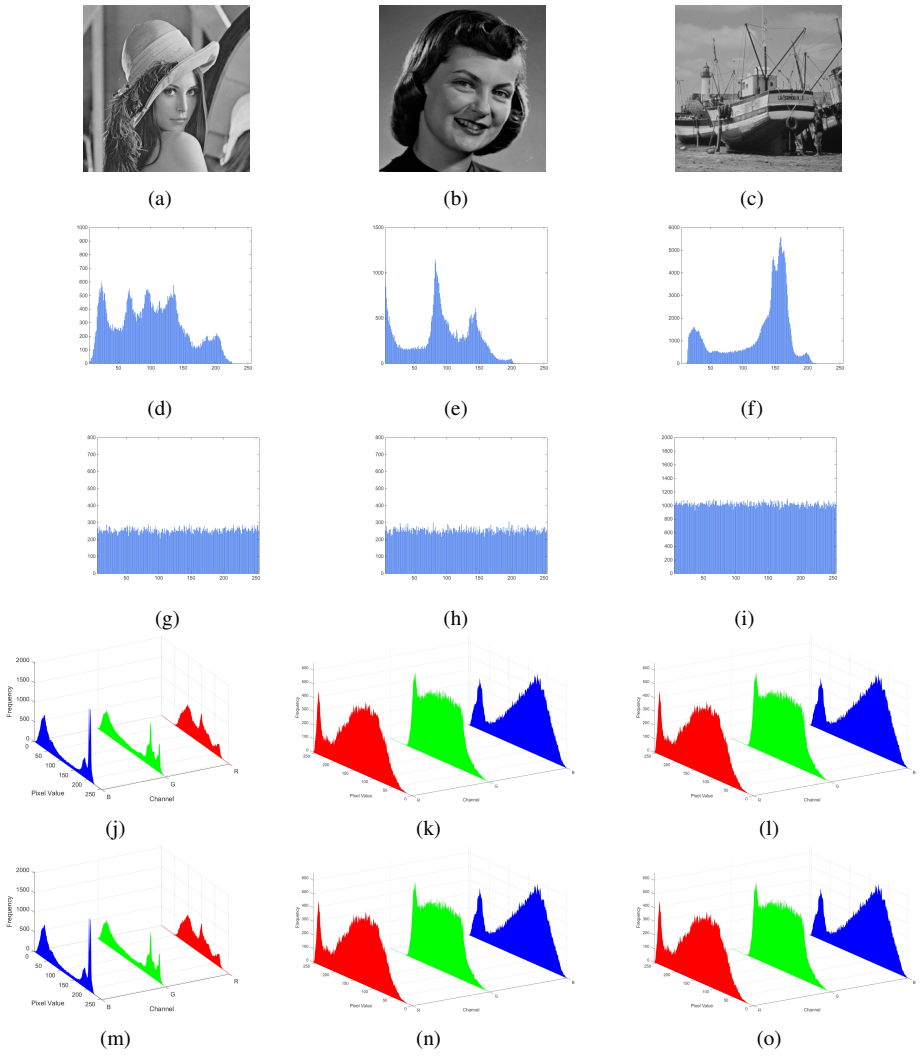


Figure 3: Histogram analysis: first row represent plain images “Lena”, “Girlface”, “Boats.512”; second row depicts histogram of plain images; third row illustrate encrypted images histogram; fourth row represents cover images “4.2.06”, “4.2.03” histogram; fifth row described ciphertext (stego) images histogram.

Table 1: χ^2 outcomes for images at significance level ($\alpha = 0.05$)

Theoretical Values [3]				
$\chi^2_{0.05(255)} = 293.2478$	$\chi^2_{0.01(255)} = 310.4574$	$\chi^2_{0.1(255)} = 284.3359$		
Obtained values of the propounded algorithm				
Images	Size	Initial images	Encrypted images	Output
Boats.512	512×512	435888.3417	249.7461	Pass
Lena	512×512	160421.8359	233.1184	Pass
Peppers	512×512	138836.1738	248.9060	Pass
Baboon	512×512	187598.9082	243.3320	Pass
Barbara	512×512	144101.1191	223.8691	Pass
Cameraman	512×512	418530.14648	228.9062	Pass
Cecum	512×512	965642.71093	262.6016	Pass
MRI	512×512	4093094.80468	261.5684	Pass
Eyeball	512×512	15354561.38671	257.7637	Pass
Feet	512×512	20860358.96679	266.3242	Pass
Cervical	512×512	1351899.36132	254.9844	Pass
Hand	512×512	8992808.01953	254.7539	Pass
Inbrain	512×512	11551188.46875	244.4434	Pass
Joint	512×512	11258287.16210	233.3301	Pass
Girlface	256×256	715065.9375	247.4512	Pass
Cameraman	256×256	110973.3046	247.4512	Pass
Lena	256×256	30665.7031	196.0781	Pass

1.3. Visual quality analysis

A widely used metric for assessing the fidelity of a stego image in comparison to its original host is the Peak Signal-to-Noise Ratio (PSNR). Mathematically, the PSNR is described as follows:

$$\text{PSNR} = 20 \log \left(\frac{255\sqrt{3 \times 2^{2m}}}{\sum_{u=0}^{2^m-1} \sum_{v=0}^{2^m-1} \sum_{w=0}^{3} [H(u,v,w) - W(u,v,w)]^2} \right) \tag{2}$$

The seven color host images employed in this study, as enumerated in Table 2, attain PSNR values specified in the Table 2 when embedded with different secret images. As illustrated in Figure 1 and supported by Table 2, the steganographic embedding process does not produce any visually perceptible variations to the host images. The resulting embedded images demonstrate an average PSNR of approximately 54 dB, validating their high visual fidelity.

To complement the extensively used PSNR metric for image quality evaluation, the Structural Similarity Index Measure (SSIM) and Normalized Cross-Correlation (NCC) are commonly utilized to assess structural similarity and image correspondence. The SSIM is characterized by the following formulation:

$$\text{SSIM}(p,q) = \frac{(2\mu_p\mu_q + I_1)\,(2\sigma_{pq} + I_2)}{(\mu_p^2 + \mu_q^2 + I_1)(\sigma_p^2 + \sigma_q^2 + I_2)} \tag{3}$$

Therein, μ_p, μ_q represent the mean intensity (average brightness) of the two images, while σ_p, σ_q denote their standard deviations (contrast). The term σ_{pq} is the covariance between the images, and I_1 and I_2 are small constants introduced to prevent division by zero and ensure computational stability.

The NCC measures the overall linear correlation between two images and is extensively utilized in image matching and quality assessment. NCC is hereby defined as:

$$\text{NCC} = \frac{\sum_{u=0}^{m-1}\sum_{v=0}^{m-1} s(u,v)\hat{s}(u,v)}{\sqrt{\sum_{u=0}^{m-1}\sum_{v=0}^{m-1} s(u,v)^2 \cdot \sum_{u=0}^{m-1}\sum_{v=0}^{m-1} \hat{s}(u,v)^2}} \tag{4}$$

Here $s(u,v), \hat{s}(u,v)$ depicts the pixel values of host and the steganographic image at coordinate (u,v). As demonstrated in Table 2, the SSIM and NCC metrics for this scheme are both approximately 0.99, indicating that the embedded image preserves high visual fidelity and exhibits a strong structural resemblance to the original.

Table 2: PSNR(dB) and SSIM outcomes proposed algorithm.

Plain Images	**Host images**	**PSNR**cip **(dB)**	**SSIM**$_{cip}$	**NCC**
Brain	2.2.01	54.1448	0.9998	0.996
	2.2.02	54.1486	0.9997	0.997
	2.2.05	54.1506	0.9997	0.996
Barbara	2.2.01	54.1508	0.9997	0.996
	2.2.02	54.1514	0.9998	0.995
	2.2.05	54.1408	0.9997	0.996
Women	2.2.01	54.1469	0.9998	0.997
	2.2.02	54.1524	0.9998	0.995
	2.2.05	54.1454	0.9997	0.998
Girlface	4.2.03	54.1469	0.9997	0.994
	4.2.05	54.1524	0.9998	0.996
	4.2.06	54.1549	0.9997	0.995
Lena	4.2.03	54.1296	0.9997	0.995
	4.2.05	54.1576	0.9997	0.996
	4.2.06	54.1119	0.9996	0.996
Cameraman	4.2.03	54.1472	0.9996	0.996
	4.2.05	54.1409	0.9997	0.995
	4.2.06	54.1575	0.9997	0.996
Hand	2.2.01	54.1520	0.9997	0.994
	2.2.02	54.1460	0.9998	0.995
	2.2.05	54.1417	0.9997	0.995
Inbrain	2.2.01	54.1410	0.9997	0.997
	2.2.02	54.1563	0.9996	0.997
	2.2.05	54.1683	0.9997	0.996
Joint	2.2.01	54.1401	0.9998	0.995
	2.2.02	54.1488	0.9998	0.996
	2.2.05	54.1539	0.9997	0.996
Cervical	2.2.01	54.1529	0.9997	0.997
	2.2.02	54.1592	0.9996	0.997
	2.2.05	54.1499	0.9996	0.996
Feet	2.2.01	54.1544	0.9997	0.995
	2.2.02	54.1566	0.9997	0.994
	2.2.05	54.1440	0.9996	0.994
MRI	2.2.01	54.1525	0.9998	0.996
	2.2.02	54.1492	0.9998	0.997
	2.2.05	54.1535	0.9996	0.996
Eyeball	2.2.01	54.1508	0.9998	0.997
	2.2.02	54.1490	0.9996	0.997
	2.2.05	54.1555	0.9996	0.994
Cecum	2.2.01	54.1491	0.9997	0.996
	2.2.02	54.1526	0.9998	0.995
	2.2.05	54.1582	0.9997	0.995

1.4. Information entropy

The Shannon entropy $S(R)$ of a random variable R is mathematically expressed as:

$$S(R) = -\sum_{j=0}^{U-1} p(w_i) \log_2(p(w_i)) \tag{5}$$

where U represents the total number of possible symbols in the sample space, and $p(w_i)$ denotes the probability of occurrence of symbol w_i. Table 3 presents the entropy results obtained from simulations for several original and corresponding encrypted images. The bolded values indicate that the proposed algorithm achieves entropy levels near the optimal threshold, confirming its effectiveness in enhancing unpredictability and its robustness against brute-force and statistical cryptanalysis.

Although global entropy efficiently quantifies the overall irregularity of an image, it may not identify non-uniform distributions within localized areas. Local entropy analysis overcomes this constraint by computing the average entropy across tiny, overlapping regions within the image. The LSE is determined by calculating the mean of the information entropy values of the blocks that were randomly chosen, as described in Eq. 8.

$$L_{r,T_A}(P) = \sum_{j=1}^{r} \left(\frac{L(P_{A_j})}{r} \right) \tag{6}$$

where $L\left(P_{A_j}\right)$ depicts the non overlapping blocks P_j. r, T_A represents the number of blocks and the number of pixels in each block respectively. Using parameters $(r, T_A) = (30, 1936)$ and applying a significance level of $\alpha = 0.001$, the expected LSE acceptance interval is $(7.901515698, 7.903422936)$. For an encrypted image to satisfy the LSE requirements, its LSE values must fall within the specified range. The results compiled in Table 4 confirm that the LSE values of the cipher images generated by the algorithm all reside within this range. This verifies that the encryption achieves a high degree of local randomness, ensuring a uniform and unpredictable distribution of pixel values in every region of the encrypted output.

Table 3: Comparison of Information Entropy metrics

Image	Size	Proposed	Cipher Entropy					
			[4]	[5]	[6]	[7]	[8]	[9]
Baboon	512×512	**7.9993**	7.9990	7.9993	7.9993	7.9993	7.9878	7.9915
Peppers	512×512	**7.9993**	7.9993	7.9993	7.9993	7.9993	7.9894	7.9918
Barbara	512×512	**7.9994**	–	–	–	–	7.9898	–
Lena	512×512	**7.9993**	7.9994	–	7.9992	7.9993	–	7.9910
Boats.512	512×512	**7.9994**	–	7.9992	7.9994	7.9991	–	–
Girlface	512×512	**7.9995**	–	–	–	–	–	–
Brain	512×512	**7.9993**	–	–	–	–	–	–
Cameraman	512×512	**7.9993**	–	–	–	–	7.9896	–
Girlface	512×512	**7.9994**	–	–	–	–	–	–
Cecum	512×512	**7.9993**	–	–	–	–	–	–
MRI	512×512	**7.9993**	–	–	–	–	–	–
Eyeball	512×512	**7.9994**	–	–	–	–	–	–
Feet	512×512	**7.9993**	–	–	–	–	–	–
Cervical	512×512	**7.9994**	–	–	–	–	–	–
Hand	512×512	**7.9993**	–	–	–	–	–	–
Inbrain	512×512	**7.9993**	–	–	–	–	–	–
Joint	512×512	**7.9994**	–	–	–	–	–	–
Cameraman	256×256	**7.9973**	–	–	–	–	–	–
Lena	256×256	**7.9972**	–	–	–	7.9971	–	–

Table 4: Outcomes of Local Shannon Entropy.

Images	Size	Cipher Image
Boat.512	512×512	7.9019
Barbara	512×512	7.9028
Peppers	512×512	7.9030
Baboon	512×512	7.9034
Brain	512×512	7.9027
Cameraman	512×512	7.9024
Cecum	512×512	7.9022
MRI	512×512	7.9032
Eyeball	512×512	7.9034
Feet	512×512	7.9031
Cervical	512×512	7.9026
Hand	512×512	7.9029
Inbrain	512×512	7.9030
Joint	512×512	7.9033
Girlface	256×256	7.9024
Cameraman	256×256	7.9022
Lena	256×256	7.9031

1.5. Adjacent correlation analysis

The relationship between neighboring pixels in an image can be determined by calculating the horizontal, vertical, and diagonal correlation coefficients [10]. These coefficients are computed using the following mathematical formula:

$$C_c(p,q) = \frac{\sum_{i=1}^{N}\left(\left(p_i - \frac{1}{N}\sum_{i=1}^{N} p_i\right)\left(q_i - \frac{1}{N}\sum_{i=1}^{N} q_i\right)\right)}{\sqrt{\sum_{i=1}^{N}\left(p_i - \frac{1}{N}\sum_{i=1}^{N} p_i\right)^2}\sqrt{\sum_{i=1}^{N}\left(q_i - \frac{1}{N}\sum_{i=1}^{N} q_i\right)^2}} \tag{7}$$

When p, q are neighboring pixels and N is the size of image [11]. A total of 5000 pairs of neighboring pixels were randomly sampled from both plain and encrypted images to calculate the average correlation coefficient values in the horizontal, vertical, and diagonal directions. The results, displayed in Table 5, show that the encrypted images produced by the propounded algorithm exhibit negative or near-zero correlation coefficients, indicating a minimal relationship

between neighboring pixels. Furthermore, Figure 4 illustrates scatter plots that visually depict the pixel correlations. The linear patterns in the scatter plots for the plain images reveal a strong relationship between adjacent pixels, whereas the non-linear patterns for the cipher images reflect a significantly weakened correlation. These results confirm the capability of the proposed algorithm to effectively safeguard information against statistical attacks.

Table 5: Correlation outcomes of different images

Image	**Color**	**Plain Image**			**Cipher Image**		
		H	**V**	**D**	**H**	**V**	**D**
Baboon	Gray	0.9261	0.8689	0.9543	-0.0014	-0.0028	-4.8114 e^{-04}
Brain	Gray	0.9905	0.9912	0.9845	-0.0006	-0.0015	0.0096
Peppers	Gray	0.9532	0.9419	0.9610	-0.0011	6.3418 e^{-04}	0.0004
Barbara	Gray	0.8914	0.9612	0.8284	0.0009	0.0213	-0.0021
Boat.512	Gray	0.9582	0.9821	0.9638	1.3997 e^{-04}	-0.0069	0.0042
Cameraman	Gray	0.9881	0.9902	0.9686	0.0007	-0.0039	-0.0089
Cecum	Gray	0.9791	0.9854	0.9647	-0.0077	0.0021	0.0016
MRI	Gray	0.9864	0.9567	0.9714	-0.0036	-0.0010	-0.0068
Eyeball	Gray	0.9832	0.9950	0.9771	-0.0008	-0.0047	-0.0012
Feet	Gray	0.9952	0.9981	0.9516	-0.0051	-0.0030	3.9912 e^{-04}
Cervical	Gray	0.9790	0.9814	0.9595	-0.0055	-0.0020	-0.0031
Hand	Gray	0.9789	0.9417	0.9651	-0.0028	-0.0516	-0.0019
Inbrain	Gray	0.9568	0.9643	0.9209	-0.0087	-0.0092	-0.0069
Joint	Gray	0.9879	0.9390	0.9844	-0.0117	-0.0022	-0.0075
Girlface	Gray	0.9743	0.9777	0.9628	-0.0016	-5.2157 e^{-04}	-0.0044
Lena	Gray	0.9667	0.9749	0.9812	-0.0095	-0.0084	0.0007
Cameraman	Gray	0.9499	0.9574	0.9814	-0.0018	0.0061	-0.0082

1.6. Chosen-Plaintext Attack Analysis

In cryptographic analysis, adversarial attacks are categorized based on the amount of information available to the attacker. These include ciphertext-only attacks, known-plaintext attacks, and chosen-plaintext attacks (CPA). In a CPA—the most powerful of these models—the adversary can encrypt arbitrary plaintexts and analyze the corresponding ciphertexts. A cryptosystem that resists CPA is therefore generally considered secure against weaker attack models as well.
In the proposed algorithm, CPA resistance is achieved through a multi-stage diffusion mechanism combining 2D semi-magic matrix-based diffusion with mHNN-driven chaotic diffusion. The core of this resistance lies in the construction of the 2D semi-magic matrix $\mathbf{M}^{(t)}$ for each encryption instance:

$$\mathbf{M}^{(t)} = \mathcal{C}\big(L_{r_1}, L_{r_2}, \ldots, L_{r_k}\big), \qquad r_i \in \{1, \ldots, N_{\text{layers}}\},$$

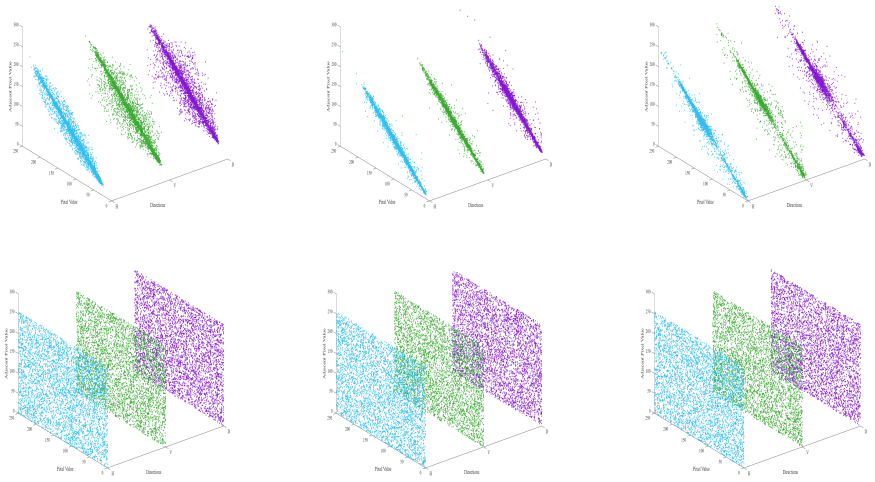
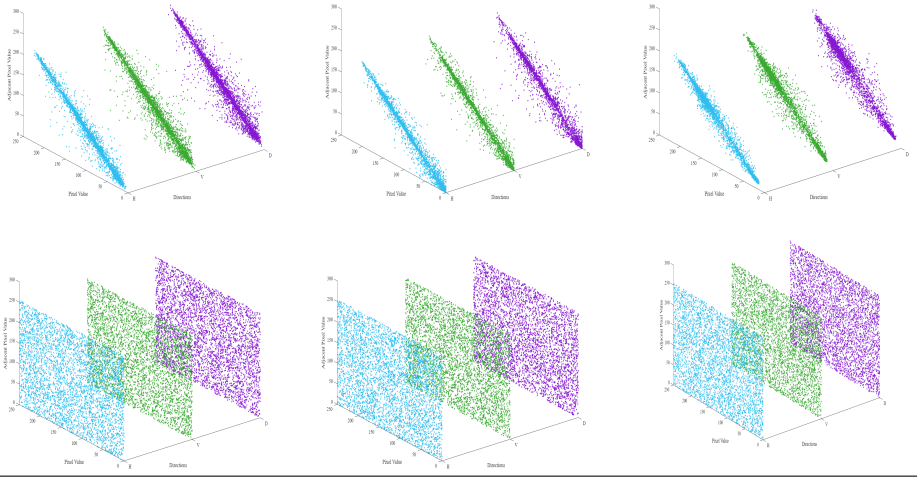
Barbara	Brain	Cameraman
		
Lena	Girlface	Boat.512
		

Figure 4: CC plots: first and third rows depict plain images coefficients in each of three H,V,D directions respectively; second and fourth rows depict the corresponding plots for the encrypted image.

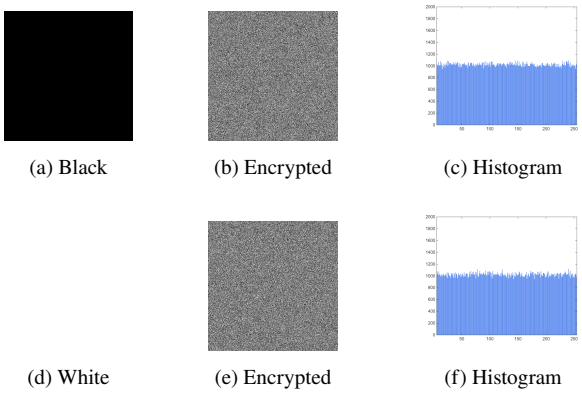
where $\mathcal{C}(\cdot)$ denotes the compounding operation and each L_{r_i} is a layer randomly selected from Trenkler's 3D magic matrix. Along with, diffusion via quantum XOR operations, driven by pseudo-random sequences from the mHNN model, further ensures that plaintext–ciphertext relationships are non-repeatable from an adversarial viewpoint. Unlike conventional diffusion structures that remain fixed for a given key, this dynamic construction ensures that repeated encryption of chosen plaintexts does not reveal a stable diffusion pattern. The complete encryption pipeline can be expressed as

$$C = \mathcal{G}_{\text{quantum}} \circ \mathcal{X}_{\text{mHNN}} \circ \mathcal{D}_{\mathbf{M}^{(t)}} \circ \mathcal{P}_{\text{GQAT}}(P),$$

where each operator introduces independent, key-controlled nonlinearity. To evaluate the statistical resilience of the scheme under a CPA scenario, uniform all-black and all-white images of size 512×512 were encrypted. The resulting cipher images exhibit near-uniform histograms and negligible pixel correlation, as shown in Fig. 5 and Table 6. These results confirm the strong randomness of the ciphertext and the scheme's effective resistance to both known-plaintext and chosen-plaintext attacks.

Table 6: Statistical metrics of encrypted uniform images

Image	**Entropy**	**Chi-square**	**Correlation coefficient**		
			H	V	D
Black	7.9994	212.7871	-0.0094	-0.0110	0.0007
White	7.9994	221.6328	-0.0025	-0.0045	-0.0051



(a) Black (b) Encrypted (c) Histogram

(d) White (e) Encrypted (f) Histogram

Figure 5: Encryption results for uniform black and white images: (a,d) plain images; (b,e) corresponding cipher images; (c,f) histograms of the cipher images, demonstrating uniform distribution.

References

[1] N. Rani, V. Mishra, S. R. Sharma, Image encryption model based on novel magic square with differential encoding and chaotic map, Nonlinear Dynamics 111 (3) (2023) 2869–2893. doi:10.1007/s11071-022-07958-7.

[2] N. Zhou, Y. Hu, L. Gong, G. Li, Quantum image encryption scheme with iterative generalized arnold transforms and quantum image cycle shift operations, Quantum Information Processing 16 (2017) 1–23. doi:10.1007/s11128-017-1612-0.

[3] V. Verma, S. Kumar, N. Rani, Novel image encryption algorithm using hybrid 3d-icpcm and hessenberg decomposition, Nonlinear Dynamics (2024) 1–27doi:10.1007/s11071-024-09620-w.

[4] X.-D. Liu, Q.-H. Chen, R.-S. Zhao, G.-Z. Liu, S. Guan, L.-L. Wu, X.-K. Fan, Quantum image encryption algorithm based on four-dimensional chaos, Frontiers in Physics 12 (2024) 1230294. doi:10.3389/fphy.2024.1230294.

[5] M. Hu, J. Li, X. Di, Quantum image encryption scheme based on 2d s ine 2-l ogistic chaotic map, Nonlinear Dynamics 111 (3) (2023) 2815–2839. doi:10.1007/s11071-022-07942-1.

[6] W. Hao, T. Zhang, X. Chen, X. Zhou, A hybrid neqr image encryption cryptosystem using two-dimensional quantum walks and quantum coding, Signal Processing 205 (2023) 108890. doi:10.1016/j.sigpro.2022.108890.

[7] S.-X. Jiang, Y. Li, J. Shi, R. Zhang, Double quantum images encryption scheme based on chaotic system, Chinese Physics B 33 (4) (2024) 040306. doi:10.1088/1674-1056/ad1174.

[8] S. Sridharan, G. Ts, R. Amirtharajan, P. Praveenkumar, Quantum scrambling and dna based multilayer image encryption with qtrng and 6d hyperchaotic keys, Scientific Reports 15 (1) (2025) 33933. doi:10.1038/s41598-025-10133-8.

[9] M. Li, X. Song, Y. Zhao, A. A. A. El-Latif, Space-frequency-based multichannel dual encryption for quantum color images using chaotic system

and quantum walks, Quantum Information Processing 24 (9) (2025) 266. doi:10.1007/s11128-025-04871-x.

[10] N. Zhou, X. Yan, H. Liang, X. Tao, G. Li, Multi-image encryption scheme based on quantum 3d arnold transform and scaled zhongtang chaotic system, Quantum Information Processing 17 (2018) 1–36. doi:10.1007/s11128-018-2104-6.

[11] Y. Zhang, H. Xiang, S. Zhang, L. Liu, Construction of high-dimensional cyclic symmetric chaotic map with one-dimensional chaotic map and its security application, Multimedia Tools and Applications 82 (12) (2023) 17715–17740. doi:10.1007/s11042-022-14044-y.