

Analysis of Chaos-Based Cryptography Using Logistic Map and Arnold's Cat Map for Digital Image Encryption

Sulthan Yustr Suwardhi¹, Budi Handoko², Eko Hari Rachmawanto³

Department of Informatics Engineering, Universitas Dian Nuswantoro, Indonesia
111202315253@mhs.dinus.ac.id¹, handoko@dsn.dinus.ac.id², eko.hari@dsn.dinus.ac.id³

Article Info

Article history:

Received 2026-09-02

Revised 2026-10-09

Accepted 2026-10-17

Keyword:

*Image Cryptography,
Chaos Theory,
Arnold's Cat Map,
Logistic Map,
Medical Image Security.*

ABSTRACT

Medical images transmitted over public networks are vulnerable to interception because of their large volume and strong spatial correlation among neighboring pixels. Conventional ciphers such as AES are not specifically designed for this redundancy and may leave residual statistical structure when applied directly to images. This study evaluates a hybrid chaos-based image encryption scheme that combines Arnold's Cat Map for pixel-position confusion with the Logistic Map for value diffusion. Instead of introducing an additional chaotic map, the diffusion stage is strengthened using a double-pass cipher-block chaining (CBC) mechanism with modulo addition. The method was tested on 20 grayscale brain-tumor images (256×256 pixels) from a public medical dataset. Security was assessed using histogram analysis, adjacent-pixel correlation, information entropy, differential NPCR and UACI, key sensitivity analysis, and execution time. A baseline ACM–Logistic XOR scheme was also compared under the same key parameters. The proposed CBC-enhanced scheme achieved an average encrypted-image entropy of 7.997, correlation coefficients close to zero, differential NPCR of 99.35%, and differential UACI of 32.84%. Key sensitivity tests yielded NPCR values above 99.6% for perturbations of the logistic parameters as small as 10^{-14} , and multi-delta analysis confirmed stable avalanche behavior down to 10^{-15} . Decryption with the correct key recovered all images without pixel loss. These results indicate that double-pass CBC can improve differential diffusion in a lightweight two-map architecture suitable for protecting grayscale medical images.



This is an open access article under the [CC-BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.

I. INTRODUCTION

Digital images are more and more used in critical applications, especially in the medical field, where visual data such as MRI and CT scans play an essential role in diagnosis and telemedicine services. Along with the rapid growth of digital communication, the exchange of medical images over public networks has become more frequent. Unfortunately, this condition also increases the risk of unauthorized access, interception, and misuse of sensitive patient information [1], [2].

Conventional cryptographic algorithms such as the Advanced Encryption Standard (AES) are widely recognized for their strong security performance on textual data. Nevertheless, when applied directly to digital images, these

algorithms often become inefficient. This is mainly because digital images contain a large amount of data and exhibit strong spatial correlation between neighboring pixels. As a result, standard block ciphers alone are often insufficient to completely eliminate visual patterns in the encrypted image [1], [3], [20], [21].

To address these limitations, chaos based cryptography has been widely explored as an alternative approach for image encryption. Chaotic systems are characterized by high sensitivity to initial conditions, ergodicity, and the ability to generate complex pseudo random sequences with relatively low computational cost [4], [5], [22]. These properties make chaos theory suitable for designing encryption schemes that can effectively disrupt both the structure and intensity distribution of an image.

According to the classical principles of cryptography introduced by Shannon, a strong encryption system should provide both confusion and diffusion. In the context of image encryption, confusion refers to the process of rearranging pixel positions, while diffusion refers to the process of changing pixel intensity values [6], [25]. Arnold's Cat Map (ACM) is commonly used for the confusion phase because of its ability to scramble pixel coordinates through iterative transformation. Meanwhile, the Logistic Map is frequently used for the diffusion phase because it can generate highly sensitive pseudo random sequences for value substitution [7], [8], [11].

Previous studies have shown that using only a single chaotic map may leave residual patterns or provide limited key complexity. Therefore, hybrid schemes that combine more than one chaotic map are considered more robust [12], [13], [14], [15]. Several works have also demonstrated that combining chaotic maps with additional mechanisms can further improve randomness and resistance against statistical attacks [23], [24]. Among the various hybrid strategies reported in the literature, the pairing of Arnold's Cat Map and the Logistic Map offers several practical advantages over more complex multi-map or multi stage architectures. First, both maps require only a small number of control parameters, the number of ACM iterations and the Logistic Map's initial value and control parameter r which keeps key management simple while still providing a sufficiently large key space. Second, unlike schemes that stack three or more chaotic systems to increase security [7], [12], [14], the ACM and Logistic Map pair keeps computational overhead low, which is beneficial for time sensitive applications such as telemedicine image transmission. Third, rather than introducing an additional chaotic map to strengthen diffusion, this study reinforces the Logistic Map based diffusion phase with a lightweight double-pass CBC mechanism, increasing the avalanche effect without adding another chaotic generator or key parameter to manage. This design choice is intended to preserve computational efficiency while still achieving competitive security performance.

In the medical domain, the need for secure image protection is even more critical. Medical images often contain private and sensitive information, and any leakage during transmission may lead to serious privacy violations. Recent studies have explored chaos based methods specifically for medical image security, including hybrid chaotic systems and multi stage encryption frameworks [16], [17], [18], [19]. However, many existing studies still focus on general test images rather than real medical datasets [16].

Based on these considerations, this study proposes and evaluates a hybrid image encryption scheme that integrates Arnold's Cat Map for confusion and the Logistic Map for diffusion. The diffusion process is further strengthened using a double-pass CBC mechanism to improve the avalanche effect. The method is implemented in Python and tested on 20 grayscale brain-tumor images, each with a resolution of 256×256 pixels, sampled from a publicly available medical

imaging dataset [26]. The security performance is analyzed using histogram analysis, correlation coefficient, information entropy, NPCR, UACI, key sensitivity analysis, and execution time. In particular, NPCR and UACI are evaluated under a differential attack setting, in which two plaintexts differing by only one pixel are encrypted with the same key. Key sensitivity is further examined through fixed-parameter perturbations and a multi-delta analysis.

The contribution of this study is threefold. First, a lightweight two-map ACM–Logistic pipeline is strengthened with double-pass CBC instead of adding a third chaotic map. Second, a controlled comparison between the baseline XOR-based diffusion and the CBC-enhanced diffusion is reported under the same key parameters. Third, the scheme is evaluated on real brain-tumor images using differential NPCR/UACI and multi-delta key sensitivity analysis, complementing conventional statistical metrics commonly reported in related work.

II. METHODS

A. Literature Review

To place this work against recent literature, Table 1 pulls together five studies on chaos-based image encryption from the last five years (2021–2026) a mix of hybrid chaotic map designs, medical image specific schemes, and layered multi map approaches. Compared to the studies summarized in Table 1, the present study is distinguished in three main aspects. Unlike previous studies that rely on complex multi-map systems to increase security [5], [27], this research optimizes a simpler two-map architecture. By integrating a lightweight double-pass CBC mechanism, the diffusion process is strengthened without adding significant computational cost or secret parameters. Furthermore, instead of using general-purpose images (e.g., Lena, Baboon) [3]–[5], [27], the proposed scheme is evaluated directly on authentic grayscale brain-tumor images. This specifically addresses the lack of real clinical dataset validation highlighted by Pankaj and Dua [16]. To provide a more comprehensive security assessment, NPCR and UACI are evaluated under both plain-cipher and differential attack settings, going beyond the standard single-setting measurements commonly reported in the literature.

Research on digital image security using chaos theory has grown significantly due to the limitations of conventional encryption methods when applied to visual data. Conventional algorithms such as AES are highly effective for textual data but become inefficient when applied to images [1], [2]. Sari et al. [3] demonstrated that AES must be combined with an additional permutation mechanism to effectively disrupt pixel correlation before further encryption.

Modern chaos-based cryptographic frameworks emphasize that a robust image encryption algorithm should clearly separate the confusion and diffusion processes [6]. Recent studies on hybrid chaotic encryption demonstrate that decoupling the process into spatial permutation (to neutralize

pixel correlation) and chaotic diffusion (to spread pixel values) provides the extreme sensitivity required to achieve optimal NPCR and UACI scores [9]. In practical applications, Putra et al. [10] implemented the hybrid ACM and Logistic

Map method for securing identity document images. Their results showed average NPCR values above 99.6% and relatively low correlation coefficients, indicating strong diffusion capability.

TABLE I
STATE OF THE ART STUDIES ON CHAOS BASED IMAGE ENCRYPTION

Author	Method	Image type/Dataset	Key Findings
Ibrahim et al. (2024) [4]	Modified Logistic Map + Gingerbread Man + Arnold's Cat Map	General grayscale test images	It combines three mechanisms sequentially and yields entropy and NPCR/UACI values close to the ideal, although this addition makes the scheme significantly more computationally intensive.
Alexan et al. (2025) [5]	5D hyperchaotic system + Arnold's Cat Map	General grayscale/color test images	The 5D system gives a very large key space and strong statistics, but that dimensionality comes at a real computational cost.
Musthofa & Setiadi (2025) [27]	Layered Logistic Map, Hénon Map, and Sine Map	General test images	Layering three maps for permutation and substitution can enhance randomness, but the consequence is an increase in the number of parameters that must be managed and secured.
Sari et al. (2025) [3]	AES combined with Arnold scrambling	3D color images	demonstrates that using AES alone is insufficient for images, a preliminary chaotic scrambling stage is still required to break pixel correlations.
Pankaj & Dua (2024) [16]	Comprehensive review of chaos-based medical image encryption	Various medical image datasets	A review pointing out that most chaos based medical encryption work is still tested on generic images rather than actual clinical datasets.

B. Dataset

This study uses 20 grayscale brain-tumor (glioma) images sampled from the publicly available “Brain Tumors 256×256” dataset on Kaggle [26], a grayscale-normalized collection of brain-tumor MRI slices intended for image-processing and machine-learning research. All images were standardized to a resolution of 256×256 pixels before the encryption process. Among these samples, five representative images (G_897–G_901) are presented in detailed per-image tables and figures to support visual inspection, histogram analysis, correlation plots, and differential visualization. In parallel, average quantitative metrics are computed over the full set of 20 images, so that the reported entropy, correlation, NPCR, UACI, and key-sensitivity values are not based on only a very small sample. The use of authentic medical images, rather than only generic test images such as Lena or Baboon, is intended to represent a realistic scenario in which sensitive clinical visual data requires strong protection during storage and transmission.

C. Encryption Process

The proposed encryption scheme follows the classic structure of confusion and diffusion, with an additional double-pass CBC mechanism to strengthen diffusion.

- Confusion Phase (Arnold's Cat Map)

Arnold's Cat Map is used to scramble the spatial positions of pixels without changing their intensity values. For an image of size $N \times N$, the transformation of a pixel coordinate (x, y) to a new coordinate (x', y') is defined as in (1).

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod{N} \quad (1)$$

This process is repeated for a predefined number of iterations. The number of iterations serves as one of the secret key parameters. Due to the periodic nature of ACM, the original image can be restored when the inverse transformation is applied with the same number of iterations.

- Diffusion Phase (Logistic Map)

After the confusion phase, the Logistic Map is used to generate pseudo random key streams. The Logistic Map is defined as in (2).

$$x_{n+1} = r \cdot x_n \cdot (1 - x_n) \quad (2)$$

$x_n \in (0, 1)$ and r is selected within the chaotic range $3.56995 < r \leq 4.0$. In this study, two key streams are generated using different initial values (x_0 and $x_{0r} = 1 - x_0$) for the forward and backward passes. To improve the avalanche effect, diffusion is performed using double-pass CBC with modulo 256 addition:

1. Forward pass: each pixel depends on the previous cipher pixel and key stream k_1
2. Backward pass: each pixel depends on the next cipher pixel and key stream k_2

This bidirectional chaining ensures that a one pixel change in the plaintext propagates across the entire ciphertext. The complete encryption process is as illustrated in Figure 1.

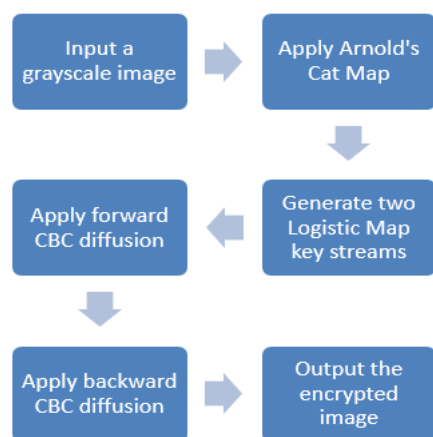


Figure 1. Encryption process

D. Decryption Process

Decryption is performed in the exact reverse order of encryption using the identical secret parameters. The process begins with the inverse backward CBC applied using key stream k2, followed by the inverse forward CBC using key stream k1. Finally, the inverse Arnold's Cat Map is executed with the matching number of iterations to restore the original pixel positions. When the correct key is applied, the original medical image is recovered without any information loss. Decryption integrity is then verified through a strict pixel-wise comparison between the original and decrypted images.

E. Evaluation Metrics

The proposed scheme is evaluated using histogram analysis, correlation coefficient, information entropy, NPCR, UACI, key sensitivity analysis, and execution time. Histogram analysis is used to assess the uniformity of pixel intensity distribution, while the correlation coefficient measures dependency between adjacent pixels in the horizontal, vertical, and diagonal directions. Information entropy is used to evaluate randomness, with an ideal value of 8 for 8-bit images.

NPCR and UACI are calculated under two complementary settings. In the baseline (before CBC) setting, both metrics are computed between the plaintext and the corresponding ciphertext. In the proposed (after CBC) setting, NPCR and UACI are evaluated under a differential attack model, where two plaintexts that differ by only one pixel are encrypted with the same key and the metrics are computed between the resulting ciphertexts.

Key sensitivity is assessed by re-encrypting each image with a slightly modified secret key. A fixed perturbation of 10^{-14} is applied independently to the logistic parameters x_0 and r , and the number of Arnold iterations is increased by one; NPCR and UACI are then computed between the reference and modified ciphertexts. In addition, a multi-delta key sensitivity analysis is performed on a representative image by varying the perturbation magnitude from 10^{-2} to 10^{-15} for x_0 and r .

Execution time is measured to assess computational efficiency, and decryption integrity is verified through a strict pixel-wise comparison between the original and decrypted images to confirm lossless recovery.

F. Testing Procedure

The proposed algorithm was implemented in Python 3.14.6 using NumPy for array/matrix operations and OpenCV for reading and saving images. All experiments were executed on a computer system equipped with an Intel Core i5-4210U CPU @ 2.70 GHz and 8 GB of RAM, running the Arch Linux operating system. The algorithm was tested following the stages below:

- Baseline testing (before CBC): Each of the 20 test images is encrypted using Arnold's Cat Map followed by single-pass Logistic Map diffusion with XOR. Histogram statistics, correlation coefficients, information entropy, and plain-cipher NPCR/UACI are computed for every image and then averaged.
- Enhanced testing (after double-pass CBC): The same 20 images are encrypted using the complete proposed scheme. The statistical metrics are recomputed, and NPCR/UACI are evaluated under a differential attack setting, in which two plaintexts that differ by only one pixel are encrypted with the same key.
- Differential attack test: A modified plaintext is created for each image by altering a single, randomly selected pixel by one intensity level. Both the original and modified images are encrypted with an identical secret key, and the NPCR and UACI metrics are calculated between the two resulting ciphertexts.
- Decryption/integrity test: Each encrypted image is decrypted using the correct key parameters. The result is then compared pixel by pixel against the original plaintext to confirm lossless recovery.
- Execution time test: Encryption and decryption times are measured and averaged across the twenty test images to assess computational efficiency.
- Comparative analysis: The averaged results from the first two stages are compared against each other and against performance metrics reported in related studies to objectively evaluate the proposed method.
- Key sensitivity test (fixed delta): For each of the 20 images, encryption is repeated after a perturbation of 10^{-14} is applied to x_0 and to r , and after the number of Arnold iterations is increased by one. NPCR and UACI are computed between the reference ciphertext and each modified-key ciphertext.
- Multi-delta key sensitivity: On one representative image, the perturbation magnitude for x_0 and r is varied from 10^{-2} to 10^{-15} , and NPCR/UACI are recorded for each delta.

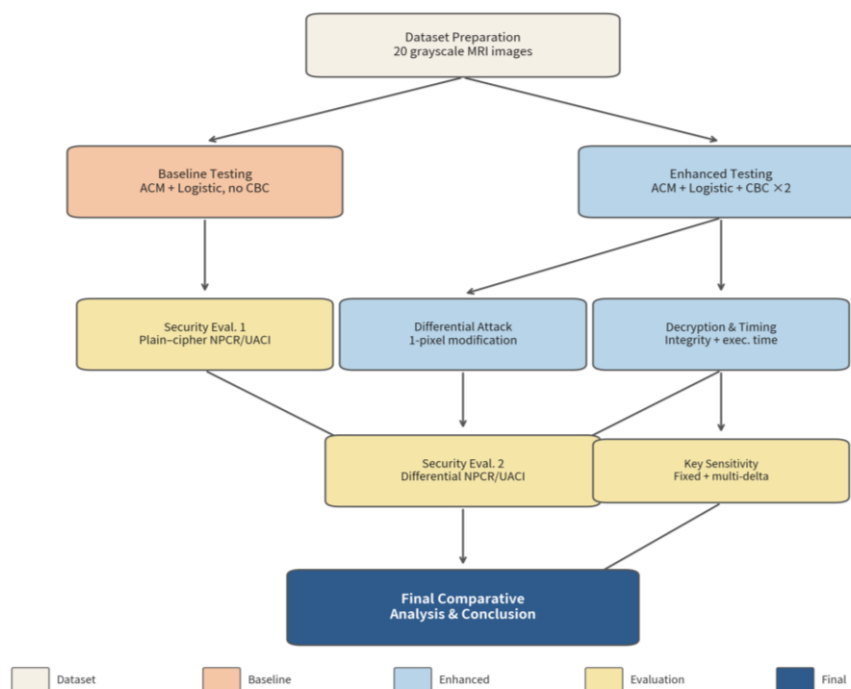


Figure 2. Testing procedure

III. RESULTS AND DISCUSSION

A. Visual and Histogram Analysis

The experimental results show that the original brain-tumor images are successfully transformed into noise-like encrypted images. The visual structure of the original images

is no longer recognizable after encryption. When the correct key is applied, the decryption process restores the original images without noticeable visual degradation. The complete visual analysis of image G_900 is presented in Figure 3, including the plain image, cipher image, decrypted image, histograms, and differential visualization. The corresponding analysis for image G_899 is shown in Figure 4.

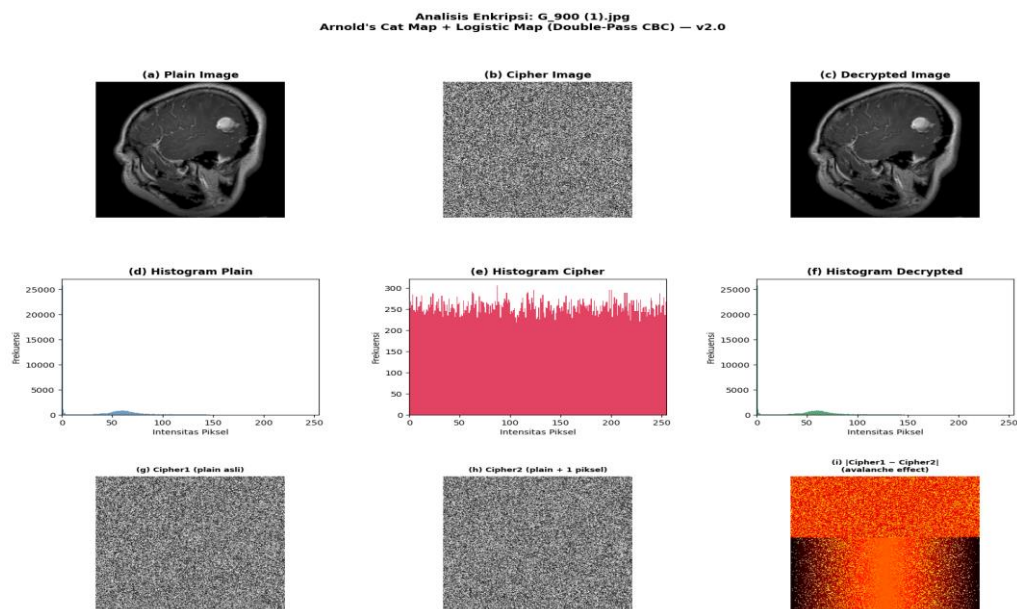


Figure 3. Full encryption analysis of brain tumor image G_900: (a) plain image, (b) cipher image, (c) decrypted image, (d–f) histograms, and (g–i) differential avalanche visualization.

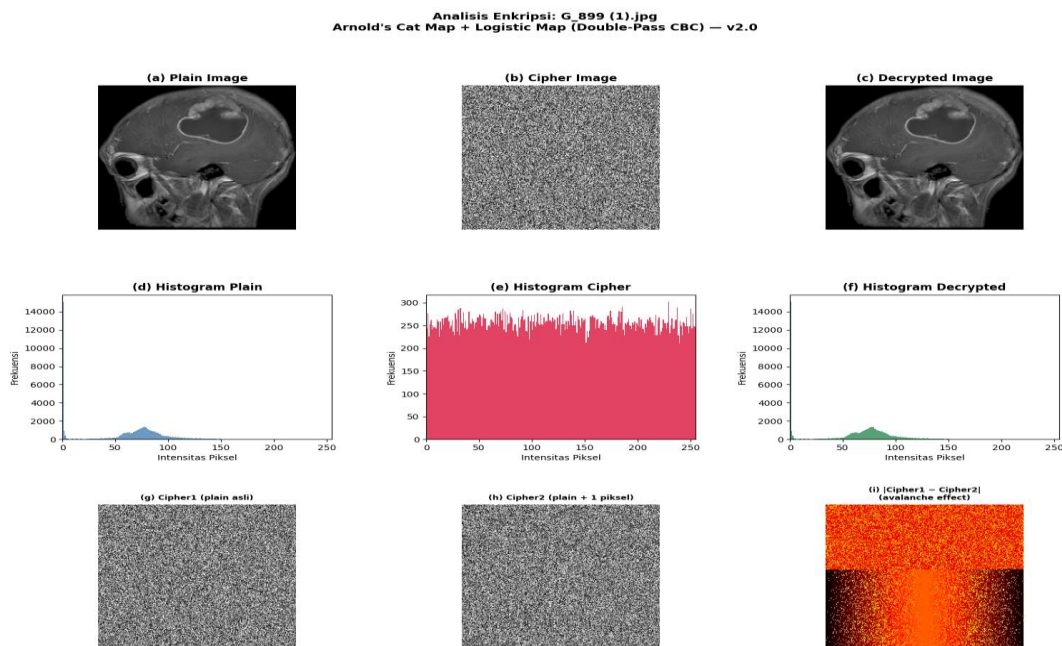


Figure 4. Full encryption analysis of brain tumor image G_899: (a) plain image, (b) cipher image, (c) decrypted image, (d–f) histograms, and (g–i) differential avalanche visualization.

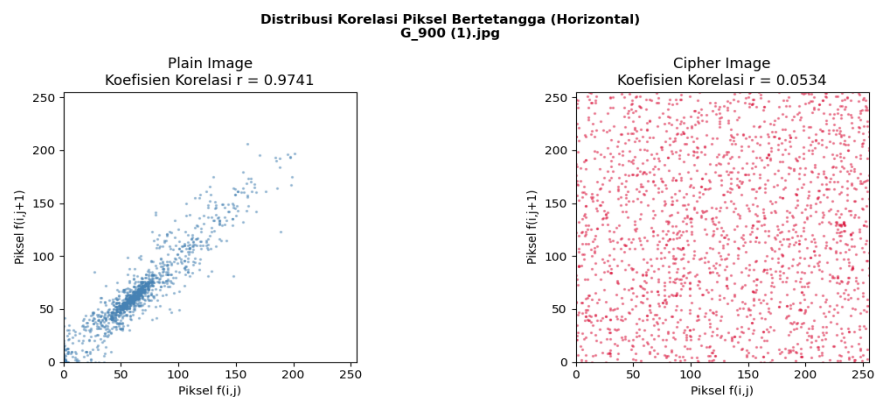


Figure 5. Horizontal adjacent-pixel correlation of image G_900 for plain and cipher images.

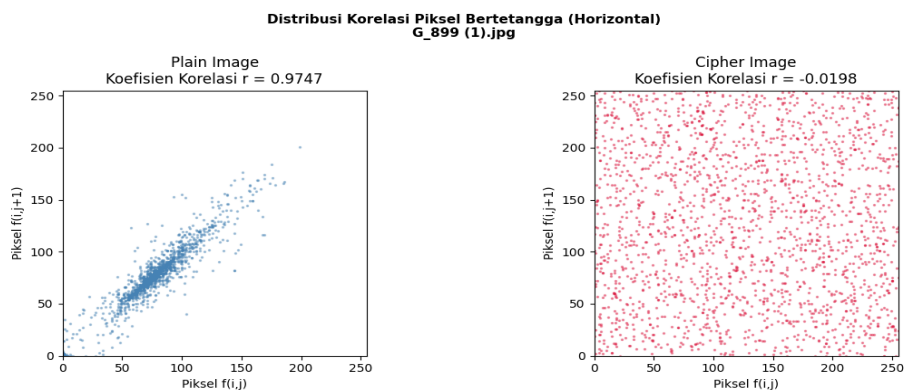


Figure 6. Horizontal adjacent-pixel correlation of image G_899 for plain and cipher images.

Histogram analysis shows that the original images have intensity values concentrated in a limited range, while the encrypted images produce a nearly uniform distribution across all intensity levels. This indicates that the diffusion process effectively spreads pixel values. The decrypted image histograms also return to a pattern similar to the original images, confirming successful recovery.

The correlation distribution of adjacent pixels is also presented in Figure 5 and Figure 6. In the plain images, neighboring pixels form a strong linear pattern with high correlation values. In the cipher images, the pixel pairs are widely scattered and the correlation coefficients approach zero. This confirms that the spatial dependency among neighboring pixels has been effectively reduced.

The differential visualization in Figure 3 and Figure 4 also shows widespread pixel differences between two ciphertexts generated from plaintexts that differ by only one pixel. This supports the strong avalanche effect obtained after the double-pass CBC enhancement.

B. Quantitative Results

The quantitative evaluation is divided into two stages: the scheme before CBC enhancement and the scheme after double-pass CBC enhancement. Table II presents the security metrics of the proposed scheme before the addition of CBC.

The entropy values of the encrypted images approach the ideal value of 8. Correlation coefficients are close to zero, and NPCR values exceed 99.6% when calculated between the original and encrypted images, indicating substantial pixel value changes after encryption. UACI values are slightly higher than the theoretical ideal ($\pm 33.46\%$) but remain within an acceptable range for measuring intensity differences between the original and encrypted images.

Table III presents the results after the diffusion stage is strengthened using double-pass CBC. In this stage, NPCR and UACI are evaluated under a differential attack setting, where two plaintexts differing by only one pixel are encrypted with the same key.

TABLE II
SECURITY METRICS BEFORE CBC

Image	Entropy Orig	Entropy Enc	Corr H	Corr V	Corr D	NPCR (%)	UACI (%)
G_901.jpg	5.379	7.959	-0.075	0.000	-0.003	99.696	41.26
G_900.jpg	5.149	7.952	-0.077	0.003	-0.006	99.710	42.00
G_899.jpg	5.834	7.972	-0.051	0.000	-0.009	99.658	36.27
G_898.jpg	5.238	7.955	-0.064	-0.001	-0.006	99.707	40.46
G_897.jpg	5.312	7.954	-0.084	0.004	-0.003	99.706	41.46
Average(5)	5.382	7.958	-0.070	0.001	-0.005	99.695	40.29
Average (20)	-	7.960	-0.068	0.001	-0.005	99.700	39.81

TABLE III
SECURITY METRICS AFTER DOUBLE-PASS CBC

Image	Entropy Enc	Corr H	Corr V	Corr D	NPCR Diff (%)	UACI Diff (%)
G_901.jpg	7.9971	-0.0026	0.0013	0.0003	99.768	32.24
G_900.jpg	7.9972	0.0063	0.0005	0.0019	99.771	31.54
G_899.jpg	7.9975	-0.0012	-0.0031	0.0061	99.767	32.50
G_898.jpg	7.9971	-0.0008	-0.0022	0.0015	99.855	30.60
G_897.jpg	7.9972	-0.0053	-0.0032	0.0064	99.837	38.81
Average(5)	7.9972	-0.0007	-0.0013	0.0032	99.800	33.14
Average(20)	7.9973	-0.0012	0.0000	0.0011	99.352	32.84

TABLE IV
COMPARISON OF PERFORMANCE BEFORE AND AFTER DOUBLE-PASS CBC

Metric	Before CBC	After CBC
Average Entropy	7.96068	7.997
Horizontal Correlation	-0.068	-0.001
Vertical Correlation	0.001	0.000
Diagonal Correlation	-0.005	0.001
NPCR (Plain-cipher) (%)	99.70	—
UACI (Plain-cipher) (%)	39.81	—
NPCR (Differential) (%)	—	99.35
UACI (Differential) (%)	—	32.84

After CBC enhancement, the average entropy increases to 7.997, and the correlation coefficients remain close to zero. Under the differential attack setting, the average NPCR and UACI over 20 images are 99.35% and 32.84%, respectively. Most individual images yield high differential NPCR values; however, the overall mean is affected by trial-level variation

in one sample. To provide a clearer comparison, Table IV summarizes the average performance before and after the CBC enhancement.

Table IV shows that both schemes produce high entropy and low correlation. Before CBC, NPCR and UACI were obtained from plain-cipher comparison and already exceeded

99.70% for NPCR. After double-pass CBC, NPCR and UACI were evaluated under a differential attack setting, reaching 99.35% and 32.84%, respectively. This confirms that the CBC mechanism improves diffusion relative to the baseline XOR scheme, while decryption with the correct key remains lossless.

Beyond the statistical and differential tests, the proposed scheme was also examined in terms of key sensitivity. Across all 20 images, a fixed perturbation of 10^{-14} was applied independently to the logistic parameters x_0 and r , while the number of Arnold iterations was increased by one. The corresponding average NPCR values were 99.60% for x_0 , 99.64% for r , and about 99.60% for the iteration change. These results indicate that ciphertexts generated under nearly identical keys still differ in most pixel positions.

To observe this behavior more closely, a multi-delta experiment was conducted on a representative image. The perturbation magnitude for x_0 and r was varied from 10^{-2} down to 10^{-15} , and NPCR/UACI were recorded for each delta. As summarized in Table V, NPCR remained within 99.56–99.64% over the full range, while UACI stayed close to 33.3–33.6%. Even at the smallest tested perturbation, the ciphertext remained substantially different from the reference encryption, which supports a strong key-related avalanche effect under the proposed scheme.

TABLE V
MULTI-DELTA KEY SENSITIVITY RESULTS ON A REPRESENTATIVE IMAGE

Parameter	Delta	NPCR(%)	UACI(%)
x_0	10-2	99.64	33.54
x_0	10-4	99.60	33.37
x_0	10-6	99.59	33.32
x_0	10-10	99.61	33.36
x_0	10-14	99.60	33.54
x_0	10-15	99.60	33.28
r	10-2	99.58	33.35
r	10-4	99.64	33.60
r	10-6	99.61	33.45
r	10-10	99.59	33.46
r	10-14	99.64	33.46
r	10-15	99.61	33.51
Iterations	+1	99.58	33.49
Iterations	+5	99.61	33.50
Iterations	+10	99.63	33.46

Figure 7 presents a visual example of key sensitivity for image G_901. The left and middle panels show the ciphertexts obtained with the correct key and with a slightly modified key ($x_0 + 10^{-14}$), respectively. Although both images appear noise-like, the absolute-difference map on the right is densely filled, indicating that the two ciphertexts differ across nearly the entire image.

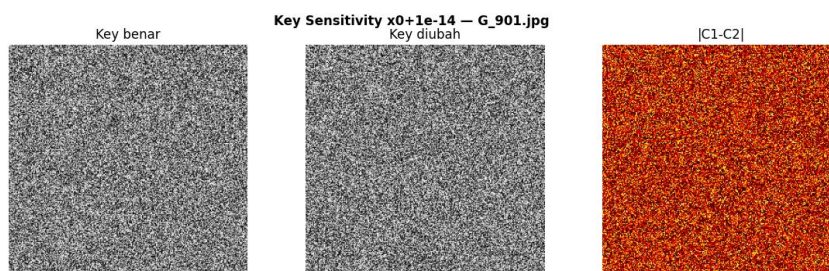


Figure 7. Key sensitivity visualization for image G_901 with a perturbation of 10^{-14} in x_0 : (a) ciphertext with the correct key, (b) ciphertext with the modified key, and (c) absolute difference $|C1-C2|$

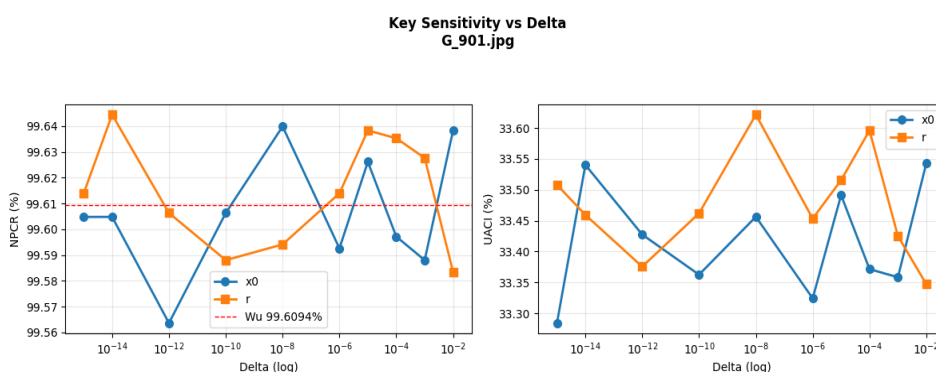


Figure 8. Multi-delta key sensitivity for a representative image: NPCR (left) and UACI (right) as functions of the perturbation magnitude for parameters x_0 and r . The dashed line indicates the critical NPCR threshold of 99.6094%.

Figure 8 shows the multi-delta key sensitivity curves for a representative image. For both x_0 and r , the NPCR values remain close to or above the commonly used threshold of

99.6094% over a wide range of perturbation magnitudes, while the corresponding UACI values stay near 33.3–33.6%. These results confirm that the proposed scheme remains highly sensitive even when the key change is extremely small.

C. Comparison with Related Studies

To evaluate the relative performance of the proposed scheme, Table VI compares its quantitative results with related chaos-based studies, including recent approaches that report entropy and NPCR/UACI values under comparable conditions. Table VI shows that the entropy achieved by the proposed scheme after double-pass CBC enhancement (7.997) is higher than that reported by Salman and Salman [28] (≈ 7.99) and closely approaches the ideal value of 8. While it is fractionally lower than the complex three-map architecture by Ibrahim et al. [4] and the AES-hybrid scheme by Sari et al. [3] (both ≈ 7.999), it remains highly competitive for a lightweight two-map design. In terms of NPCR, the plain-cipher value obtained before CBC enhancement (99.70%) is comparable to, and slightly higher than, the

values reported by Putra et al. [10] (99.607% on average).

Most notably, after CBC enhancement, the proposed scheme achieves a differential UACI of 32.84%, which is reasonably close to the theoretical ideal of approximately 33.46%, and a differential NPCR of 99.35%. These values are competitive with related reports, including Salman and Salman [28] (UACI 33.77%, NPCR 99.60% under a differential setting) and Sari et al. [3] (NPCR 99.81% under a plain-cipher setting). This suggests that the double-pass CBC mechanism provides a well-balanced diffusion effect and strong avalanche characteristics without requiring a third chaotic dimension. It should be noted that NPCR/UACI values across studies are not always measured under identical settings or on the same image type, so these comparisons should be interpreted as indicative rather than as a strictly controlled benchmark.

TABLE VI
COMPARISON OF SECURITY METRICS WITH RELATED ACM-LOGISTICMAP-BASED STUDIES

Title	Method	Entropy (Enc.)	Measurement Setting	NPCR (%)	UACI (%)
Ibrahim et al. (2024) [4]	Mod. Logistic Map + GGM + ACM	7.999	Plain-cipher	99.89	33.29
Sari et al. (2025) [3]	AES + Arnold Scrambling	7.999	Plain-cipher	99.81	33.60
Salman & Salman (2020) [28]	ACM + 3D Logistic Map	7.99 (avg.)	Differential attack	99.60 (avg.)	33.77 (avg.)
Putra et al. (2022) [10]	ACM + Logistic Map (KTP/KK images)	-	Plain-cipher	99.607 (avg.)	37.53 (avg.)
This study – before CBC	ACM + single-pass Logistic Map	7.960	Plain-cipher	99.70	39.81
This study – after double-pass CBC	ACM + Logistic Map + double-pass CBC	7.997	Differential attack	99.35	32.84

D. Discussion

After the addition of double-pass CBC, NPCR and UACI were evaluated under a differential attack setting, in which two plaintexts differing by only one pixel were encrypted with the same key. Over 20 images, the proposed scheme achieved an average differential NPCR of 99.35% and an average differential UACI of 32.84%, which satisfy commonly adopted thresholds. While this confirms that the CBC stage strengthens the avalanche effect, a rigorous evaluation revealed that the slightly reduced NPCR average is driven by a rare edge case inherent to additive modulo-256 diffusion. In extremely rare instances, a single pixel difference can mathematically cancel out during the backward pass, a limitation strictly isolated to plaintext differences.

However, key sensitivity analysis demonstrates that this limitation is fully mitigated by the secret parameters. Fixed perturbations of 10-14 in the Logistic Map keys, as well as a one-step change in the Arnold iterations, produced average NPCR values above 99.6% across all tested images. The multi-delta experiment summarized in Table V confirms that altering the secret key by even a microscopic margin completely circumvents the modulo cancellation, ensuring stable avalanche characteristics. In addition, decryption with the correct key recovered every image without pixel-level loss.

To further ensure resistance against brute-force attacks, the theoretical key space was analyzed. In the proposed scheme, the independent secret keys consist of the Logistic Map initial

condition, the control parameter, and the Arnold's Cat Map iteration count. Based on the standard 64-bit double-precision used in modern systems, the combination of these parameters provides a total key space of approximately 2104. Combined with the algorithm's extreme key sensitivity, this key space is sufficiently large to secure lightweight medical image encryption against exhaustive search attacks.

The hybrid ACM-Logistic Map scheme with double-pass CBC provides high randomness, low correlation, strong differential performance, and high key sensitivity, making it effective for securing grayscale medical images. Relative to related two-map designs, the proposed method remains competitive while avoiding the additional complexity of three-map or high-dimensional hyperchaotic architectures [5], [27], [28]. The identification of the modulo-cancellation property further demonstrates a transparent cryptanalytic validation of the scheme. Nevertheless, the present evaluation is limited to grayscale 256×256 brain-tumor images, and broader cryptanalytic tests are left for future work.

IV. CONCLUSION

This study has presented a hybrid digital image encryption scheme based on chaos theory by combining Arnold's Cat Map and the Logistic Map. Arnold's Cat Map is applied for confusion, while the Logistic Map is used to generate key streams for diffusion. To strengthen the avalanche effect, a double-pass CBC mechanism with modulo addition is incorporated into the diffusion stage rather than an additional chaotic map, keeping the scheme computationally simple.

Experimental results on 20 grayscale brain-tumor images show that the encrypted images appear as random noise. The average entropy reaches 7.997, and the correlation coefficients are close to zero. Under rigorous multi-trial differential attack evaluation, the scheme achieves an average NPCR of 99.35% and an average UACI of 32.84%, uncovering a rare modulo-cancellation edge case intrinsic to additive CBC that is fully mitigated by the scheme's high key sensitivity. Furthermore, the algorithm provides a key space of approximately 2104, ensuring robust resistance against brute-force attacks. Comparison with the baseline scheme without CBC indicates a clear improvement in differential diffusion, while comparison with related ACM-Logistic Map studies suggests competitive performance despite the lower architectural complexity. When the correct key parameters are used, decryption recovers the original images without information loss. These findings indicate that the proposed architecture is effective for securing grayscale medical images. The present evaluation is limited to grayscale data and a selected set of security metrics; future work may extend the method to color medical images and broader cryptanalytic tests.

REFERENCES

- [1] B. Zhang and L. Liu, "Chaos-based image encryption: Review, application, and challenges," *Mathematics*, vol. 11, no. 11, p. 2585, 2023, doi: 10.3390/math11112585.
- [2] S. Jadoon, L. Pan, S. Huda, and K. H. Khan, "A survey of image encryption schemes: Arnold transformation, chaos, bit-plane extraction and permutation based algorithms," *Multimedia Tools and Applications*, vol. 85, p. 210, 2026, doi: 10.1007/s11042-026-21425-0.
- [3] W. S. Sari, E. Z. Astuti, and C. Jatmoko, "A hybrid encryption using Advanced Encryption Standard and Arnold scrambling for 3D color images," *KINETIK*, vol. 10, no. 1, 2025, doi: 10.22219/kinetik.v10i1.2058.
- [4] L. J. Ibrahim, J. B. Idoko, and A. M. Alwhelat, "Robust chaos image encryption system using modification Logistic Map, Gingerbread Man and Arnold Cat Map," *Int. J. Adv. Comput. Sci. Appl. (IJACSA)*, vol. 15, no. 6, pp. 1305–1316, 2024, doi: 10.14569/IJACSA.2024.01506132.
- [5] W. Alexan et al., "A secure and efficient image encryption scheme based on chaotic systems and nonlinear transformations," *Sci. Rep.*, vol. 15, p. 31246, 2025, doi: 10.1038/s41598-025-15794-z.
- [6] N. Chaudhary, T. B. Shahi, and A. Neupane, "Secure Image Encryption Using Chaotic, Hybrid Chaotic and Block Cipher Approach," *Journal of Imaging*, vol. 8, no. 6, p. 167, 2022, doi: 10.3390/jimaging8060167.
- [7] F. Masood et al., "A novel image encryption scheme based on Arnold cat map, Newton-Leipnik system and Logistic Gaussian map," *Multimedia Tools and Applications*, vol. 81, pp. 30931–30959, 2022, doi: 10.1007/s11042-022-12844-w.
- [8] T. Wang, B. Ge, C. Xia, and G. Dai, "Multi-Image Encryption Algorithm Based on Cascaded Modulation Chaotic System and Block-Scrambling-Diffusion," *Entropy*, vol. 24, no. 8, p. 1053, 2022, doi: 10.3390/e24081053.
- [9] X. Chen, Q. Wang, L. Fan, and S. Yu, "A Novel Chaotic Image Encryption Scheme Armed with Global Dynamic Selection," *Entropy*, vol. 25, no. 3, p. 476, 2023, doi: 10.3390/e25030476.
- [10] T. A. Putra, I. Ruslianto, and S. Bahri, "Application of Arnold Cat Map and Logistic Map methods for securing citizens' data image," *CESS (Journal of Computer Engineering, System and Science)*, vol. 7, no. 2, pp. 470–481, 2022, doi: 10.24114/cess.v7i2.36302.
- [11] M. Rajendran, A. M. Hassan, M. Hashim, R. A. Alhussein, N. Nsrulaah Faris and A. J. Alhani, "Image Encryption Using Chaotic Logistic Map and Arnold Cat Transform for Secure Visual Data Transfer," 2025 International Conference on Next Generation Computing Systems (ICNGCS), Coimbatore, India, 2025, pp. 1-5, doi: 10.1109/ICNGCS64900.2025.11183494.
- [12] M. M. Hashim, "Image cryptography scheme based on improvement chaos Logistic function, chaos Arnold Cat Map and Gingerbread Man process," in *Proc. IEEE Int. Conf. Artificial Intelligence and Mechatronics Systems (AIMS)*, 2024, doi: 10.1109/AIMS61812.2024.10513196.
- [13] S. Amine et al., "Securing visual data: A fresh approach with Arnold Cat Map and Chebyshev Map encryption," in *Digital Technologies and Applications (ICDTA)*, 2024, doi: 10.1007/978-3-031-68653-5_27.
- [14] A. Pourjabbar Kari et al., "A new image encryption scheme based on hybrid chaotic maps," *Multimedia Tools and Applications*, vol. 80, pp. 2753–2772, 2021, doi: 10.1007/s11042-020-09648-1.
- [15] D. Das and C. Pradhan, "Image Encryption Based on Cyclic Chaos, PRNG and Arnold's Cat Map," in *Proceedings of Data Analytics and Management*, A. Khanna, Z. Polkowski, and O. Castillo, Eds., *Lecture Notes in Networks and Systems*, vol. 572. Singapore: Springer, 2023, doi: 10.1007/978-981-19-7615-5_25.
- [16] S. Pankaj and M. Dua, "Chaos based medical image encryption techniques: A comprehensive review and analysis," *Information Security Journal: A Global Perspective*, vol. 33, no. 3, pp. 332–358, 2024, doi: 10.1080/19393555.2024.2312975.
- [17] A. H. Mansour, S. Aboelenin, M. M. Eltoukhy, H. I. Mohamed, O. Elkomy, and K. M. Hosny, "A new medical image encryption using modular integrated logistic exponential map and multi-level Q-Sequence matrix," *Sci. Rep.*, 2025, doi: 10.1038/s41598-025-16343-4.
- [18] A. S. Andreatos and A. P. Leros, "Secure chaotic cryptosystem for 3D medical images," *Mathematics*, vol. 13, no. 20, p. 3310, 2025, doi: 10.3390/math13203310.
- [19] H. Xie et al., "A secure and privacy-preserving technique based on coupled chaotic system and plaintext encryption for multimodal medical images," *Multimed. Tools Appl.*, vol. 84, pp. 22701–22726, 2025, doi: 10.1007/s11042-024-19956-5.
- [20] Y. Alghamdi and A. Munir, "Image Encryption Algorithms: A Survey of Design and Evaluation Metrics," *Journal of Cybersecurity and Privacy*, vol. 4, no. 1, pp. 126–152, 2024, doi: 10.3390/jcp4010007.
- [21] P. Fang, H. Liu, C. Wu, and M. Liu, "A survey of image encryption algorithms based on chaotic system," *The Visual Computer*, vol. 39, no. 5, pp. 1975–2003, 2023, doi: 10.1007/s00371-022-02454-7.
- [22] Y. Abdul et al., "A dynamic image encryption scheme through 2-D cellular automata and chaotic logistic map," *Sci. Rep.*, vol. 15, p. 36116, 2025, doi: 10.1038/s41598-025-21225-w.
- [23] R. Amutha and A. V. Phamila, "Chaotic cosine and logistic map based robust image encryption with dual-stage confusion-diffusion architecture," *Sci. Rep.*, vol. 16, p. 16951, 2026, doi: 10.1038/s41598-026-40337-5.
- [24] F. Musanna, "Quantum inspired image encryption using dual chaotic maps," *Quantum Inf. Process.*, vol. 24, p. 382, 2025, doi: 10.1007/s11128-025-04999-w.
- [25] R. Dijaya and H. Setiawan, *Buku Ajar Pengolahan Citra Digital*. Sidoarjo, Indonesia: UMSIDA Press, 2023, doi: 10.21070/2023/978-623-464-075-5.
- [26] T. Dubail, "Brain Tumors 256x256," Kaggle, 2023. [Online]. Available: <https://www.kaggle.com/datasets/thomasdubail/brain-tumors-256x256>
- [27] A. Musthofa and D. R. I. M. Setiadi, "Layered image encryption method based on combination of Logistic Map, Hénon Map, and Sine Map to enhance digital image security," *Journal of Applied Informatics and Computing (JAIC)*, vol. 9, no. 4, pp. 1280–1289, 2025, doi: 10.30871/jaic.v9i4.9569.
- [28] F. A. Salman and K. A. Salman, "Enhanced image encryption using two chaotic maps," *Journal of ICT Research and Applications*, vol. 14, no. 2, pp. 134–148, 2020, doi: 10.5614/itbj.ict.res.appl.2020.14.2.3.