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

Research Article

Image Encryption using Half-Inverted Cascading Chaos Cipheration

De Rosal Ignatius Moses Setiadi [1,*], Robet [2], Octara Pribadi [2], Suyud Widiono [3], and Md Kamruzzaman Sarker [4]

[1] Informatics Engineering Department, Faculty of Computer Science, Dian Nuswantoro University, Indonesia; e-mail : moses@dsn.dinus.ac.id
[2] Department of Informatics Engineering, STMIK TIME, Medan, Indonesia; e-mail : robet@stmik-time.ac.id; octarapribadi@stmik-time.ac.id
[3] Department of Computer Engineering, Faculty of Science and Technology, University of Technology Yogyakarta, Indonesia; e-mail : suyud.w@uty.ac.id
[4] Department of Computer Science, Bowie State University, United States; e-mail : ksarker@bowiestate.edu
* Corresponding Author : De Rosal Ignatius Moses Setiadi

Abstract: This research introduces an image encryption scheme combining several permutations and substitution-based chaotic techniques, such as Arnold Chaotic Map, 2D-SLMM, 2D-LICM, and 1D-MLM. The proposed method is called Half-Inverted Cascading Chaos Cipheration (HIC3), designed to increase digital image security and confidentiality. The main problem solved is the image's degree of confusion and diffusion. Extensive testing included chi-square analysis, information entropy, NCPCR, UACI, adjacent pixel correlation, key sensitivity and space analysis, NIST randomness testing, robustness testing, and visual analysis. The results show that HIC3 effectively protects digital images from various attacks and maintains their integrity. Thus, this method successfully achieves its goal of increasing security in digital image encryption.

Keywords: Chaotic Encryption; Cryptography; Image encryption; Novel image encryption; Secure image transmission.

1. Introduction

Information security has become a major concern in this modern era, along with technological developments and the rapid increase in internet use. Currently, internet users have reached 66% of the world[1]. Sensitive information and personal data must be protected from unauthorized access and potential cyber threats that cause material, time, and financial losses [1], [2]. In an effort to overcome this challenge, cryptographic methods have become one of the main tools in protecting confidential data and information and have high economic value. Cryptography is a security technique used to secure information by converting it into an incomprehensible form, and without the appropriate key, the information cannot be decrypted. In this context, the focus is more on image encryption, a branch of cryptography that aims to protect the integrity and confidentiality of digital images. Image encryption involves a set of techniques designed to maintain the confidentiality and integrity of images, to prevent unauthorized access or modification by unauthorized parties.

There are various encryption techniques used in image encryption, including stream techniques, block ciphers, chaos techniques, deoxyribonucleic acid (DNA), and many others. [3]–[11]. One technique attracting attention is chaos engineering, which uses the randomness and unpredictable nature of changes in non-linear dynamic systems. The main advantage of using chaos methods in image encryption is resistance to strong crypto-analytic attacks. The inherent randomness and unpredictability characteristics of chaotic systems make them difficult to predict, making them a strong choice for securing digital images[12]–[18]. One of the basic principles used in image encryption is developing confusion and diffusion techniques in accordance with Shannon's Law regarding information theory. Confusion technique means confusing the data so that there is no recognizable pattern, while diffusion involves spreading changes through the entire image[19]–[21]. In other words, image encryption aims to make

Received: September, 22th 2023
Revised: October, 17th 2023
Accepted: October, 21th 2023
Published: October, 23th 2023

the image more complicated and scrambled, making it difficult for unauthorized parties to decrypt and obtain the original information from the encrypted image.

In general, the quality of confusion and diffusion in image encryption can be improved by combining level and byte or plane level [21]–[24], 3D encryption technique [25], [26], and combination and modification of patterns [24], [27]–[29]. Apart from these variations in technique, the quality of the random sequence is also the main key to improving the quality of encryption. Random sequences are generally used for substitution and permutation processes [30], [31]. Before the chaos method was popular, random sequences were generally generated with a pseudo-random number generator (PRNG). However, several studies, such as [32], [33], still use and develop PRNG image encryption techniques. The term PRNG in the chaotic method changes to chaotic sequence because the chaotic method generally produces chaotic sequences which are generally of float type, while traditional PRNGs generally have integer or binary values. Lyapunov exponent (LE) and bifurcation, in general, can be one of the randomness-level parameters of a chaotic sequence. The more random the chaotic sequence, the better the encryption quality. The LE value can be positive, negative, or zero. When the LE value is positive and the greater it is, the more unstable and sensitive the chaos method is to the initial value[13], [19], [34]. This characteristic is very suitable for image encryption, with a high correlation between adjacent pixels [34]. Chaos methods have been developed from logistic maps such as the 2D Sine Logistic Modulation Map (2D-SLMM)[35] and 2D Logistic ICMIC cascade map (2D-LICM)[36] has been designed with a large maximum LE value. These two chaos methods are very random and have been proven to apply to image encryption, so this research aims to:

1. Combining several 2D-SLMM and 2D-LICM chaos methods to obtain robust image encryption that is resistant to various attacks.
2. Design a confusion and diffusion technique called half-inverted cascading Cipheration (HIC3) by adding the Arnold Chaotic Map (ACM) and 1D-MLM methods so that the two hybrid chaos methods are perfect and work optimally.
3. Implement encryption techniques at the bit and byte image level and test them with various measuring tools.

The remainder of this article will explain in more depth the motivation and research ideas, theories, and related research explained in the second Preliminaries section. The proposed method, which explains the proposed image encryption stages, is presented in the second section. The fourth section presents the implementation, testing and comparison of methods, and the final section contains research conclusions.

2. Preliminaries

2.1. 2D Sine Logistic modulation map (2D-SLMM)

2D-SLMM is a type of two-dimensional chaotic map introduced in [35]. This chaotic map comes from combining two one-dimensional chaotic maps, namely the Logistic Map and Sine Map. The main advantages of 2D-SLMM are its wider chaotic range, better ergodicity, hyperchaotic nature, and relatively low implementation costs compared with the previous two chaotic maps. Its nature becomes hyperchaotic, and this is one of the important characteristics of 2D-SLMM. This means that 2D-SLMM can produce chaotic series with a high level of chaos and are very sensitive to changes in parameters and initial values. In addition, 2D-SLMM has a wider chaotic range than some other one-dimensional chaotic maps. A wider chaotic range means that these chaotic maps can produce greater variations in chaotic series, which also increases the level of security in the use of these series in the context of image encryption. 2D-SLMM can be used as one of the key tools to develop more secure image encryption algorithms with low implementation costs. 2D-SLMM can be calculated with Equation (1) and Figure 1 presents the resulting chaotic attractor.

$$\begin{cases} x_{i+1} = \alpha(sin(\pi y_i) + \beta)x_i(1 - x_i) \\ y_{i+1} = \alpha(sin\ (\pi x_{i+1}) + \beta)y_i(1 - y_i) \end{cases} \quad (1)$$

Where α and β are control parameters, $\alpha\epsilon[0,1]$, $\beta\epsilon[0,3]$, x_i and y_i are initial conditions.

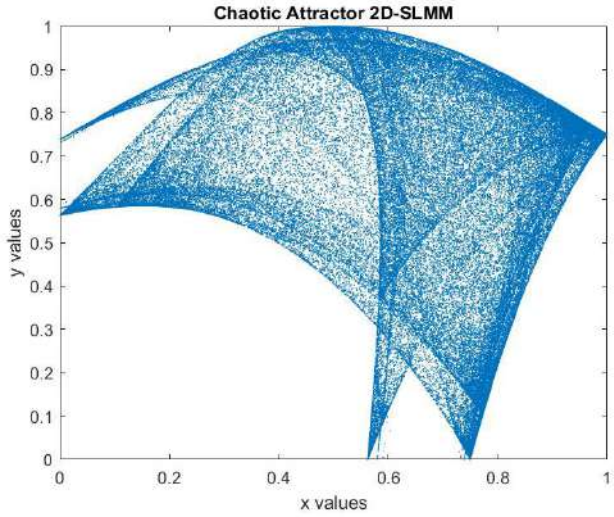

Figure 1. Chaotic Attractor 2D-SLMM.

2.2 2D Logistic ICMIC cascade map (2D-LICM)

2D-LICM is a type of two-dimensional chaotic map introduced in [36]. The uniqueness of 2D-LICM is that the chaotic map is based on the Cascade Modulation Couple (CMC) model, which combines the characteristics of high-dimensional chaotic maps. The main characteristics of 2D-LICM are hyperchaos, wide chaotic range, and high complexity. Hyperchaotic means that this chaotic map produces a chaotic series that is very random and difficult to predict. This makes it suitable for use in image encryption. Wide Chaotic Range means it can produce a greater variety of chaotic series, thereby increasing the level of security in image encryption applications, and with high complexity, it can contribute to a higher level of security in image encryption. 2D-LICM can be implemented for encryption at the bit level and involves permutation and diffusion processes. Bit-level permutation is carried out by shifting bits circularly, while bit-level diffusion is carried out through exclusive OR operations and reverse operations.

$$\begin{cases} x_{i+1} = sin\left(\dfrac{21}{(\alpha(y_i+3)\beta x_i(1-\beta x_i))}\right) \\ y_{i+1} = sin\left(\dfrac{21}{(\alpha(\beta x_i+3)y_i(1-y_i))}\right) \end{cases} \quad (2)$$

Where $\alpha\epsilon[0,+\infty]$, $\beta\epsilon[0,+\infty]$.

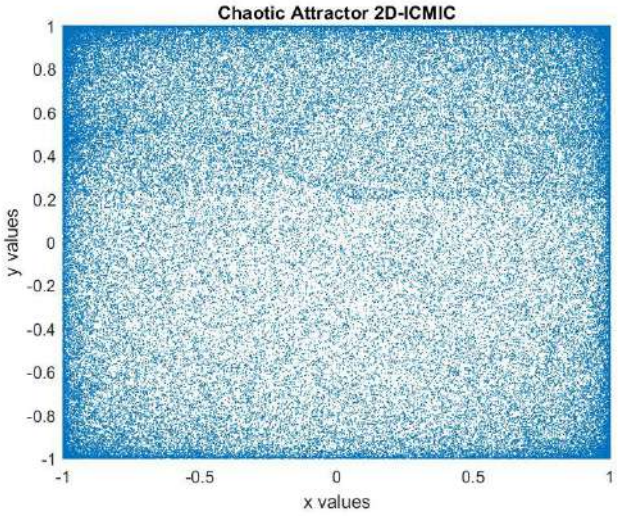

Figure 2. Chaotic Attractor 2D-LICM

In addition, the initial value of the garbled system is updated in real time according to the obtained ciphertext, which improves the algorithm's ability to resist selected-text and known-text attacks. 2D-LICM can be calculated using Equation (2), while in Figure 2 the results of the chaotic attractor plot are presented.

2.3 Arnold Chaotic Map (ACM)

ACM is a chaos method designed in two dimensions by Vladimir Arnold [37], so it is suitable for carrying out the image scramble process. In contrast to other chaotic methods that produce chaotic sequences, this method directly changes the coordinate positions of image pixels in the 2D plane. ACM is also invertible and has fast and simple computing. But, because it does not produce chaotic sequences, ACM can only perform permutations. In recent research such as [38], [39], the ACM method is implemented in image encryption. ACM can be done with Equation (3) for the encryption process and Equation (4) for the decryption process.

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} mod\ M \tag{3}$$

$$\begin{bmatrix} i \\ j \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix}^{-1} \begin{bmatrix} i' \\ j' \end{bmatrix} mod\ M \tag{4}$$

Where the image must have a $M \times M$ dimension, i, and j are the original pixel coordinates, i' and j' are the scrambled pixel coordinates, p and q are positive integers as ACM parameters and the chaotic operation is done with several iterations n.

2.4 1D Modified Logistic Map (1D-MLM)

1D-MLM is an image encryption algorithm based on the use of the modified logistic chaotic map to increase security and key size in image encryption [40]. Logistic chaotic maps are a type of chaotic map that usually has problems related to small key sizes. Modification by multiplying the range of full mapping parameters and chaotic parameters by a factor γ can increase the key size, which in turn will increase security. Experimental simulation results show that the proposed algorithm has a key size that tends to be unlimited and a high level of key sensitivity. This means that this algorithm has a high level of security against attacks that use comprehensive analysis methods. In addition, this algorithm produces encrypted images with an even distribution of pixel values and a weak correlation between adjacent pixel values. This shows that this algorithm is able to resist statistical analysis attacks well. 1D-MLM can be calculated with Equation (5), while Figure 3 shows the chaotic attractor plot and its bifurcation.

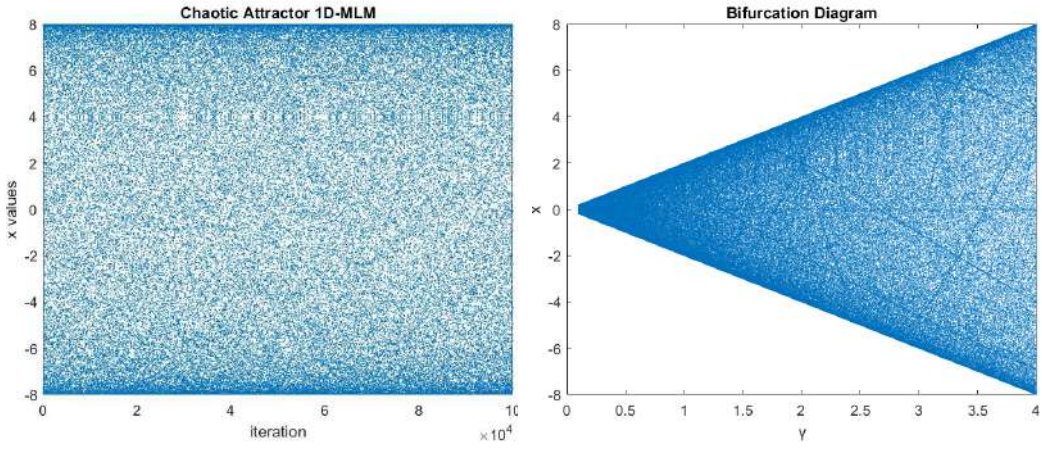

Figure 3. Chaotic Attractor and Bifurcation 1D-MLM.

$$x_{i+1} = 2\gamma - \left(\frac{x_i^2}{\gamma}\right) \quad (5)$$

Where the x_0 is an initial parameter, r is the modified logistic map parameter, $\gamma\epsilon[0,4]$ and the number of image pixels iterations n.

2.5 Related works

Combining encryption methods can provide an additional layer of security and make it more difficult for attacks to penetrate. Zheng and Bao [4] proposed a cascade chaotic map system for image encryption. The chaotic system built is a 2D-Cascade-Transform-Logistic-Sine Map (2D-CTLSM), which is produced by improving the Logistic and Sine maps in the cascade method. Apart from that, the DNA method, zigzag transformation, and alternate row diffusion are also combined. DNA is utilized to improve diffusion operations. Zigzag transformation is used to randomize the position of pixel elements in an image, and alternate row diffusion refers to a diffusion process in which elements in an image are combined in a different order. This ensures that each value in the image undergoes the diffusion operation twice. The application of 2D-CTLSM serves to obtain better chaotic properties and a wider chaotic area resulting in stronger security.

Mfungo et. al [12] developed an image encryption scheme that uses chaotic maps and the concept of fuzzy numbers. The combination of two types of chaotic maps, namely the logistic map and the sine map, forms a new chaotic map called the logistic sine map. The concept of fuzzy numbers is used in the encryption process. This refers to the use of values that are uncertain or more variable than conventional binary values. In this research, the fuzzy triangular membership function is used to modify the initial conditions of the chaotic map during the diffusion process. The encryption process involves several stages, including randomization of image pixels, summation of adjacent row values, and an XOR operation with random numbers generated from the chaotic map. A series of security tests, including statistical attack analysis, local entropy analysis, differential attack analysis, signal-to-noise ratio, signal-to-noise distortion ratio, mean error square, brute force attack analysis, and information entropy analysis. These test results reflect the scheme's security level and resistance to various attacks.

Bhowmik and Acharyya [8] developed an image encryption scheme that uses meta-heuristic techniques along with traditional key generation mechanisms. This research aims to improve the security strength and resistance to attacks in chaotic-based cryptography. Traditional key generation mechanism with meta-heuristic techniques to create a new key generation model for logistic maps. The advantage of this method is the key generation technique, which results from combining a population-based meta-heuristic optimization algorithm known as Differential Evolution and genetic algorithms.

Setiadi and Rijati [19] proposed combining various permutation and substitution techniques at the bit and pixel level using three more sophisticated logistic map methods, namely 2D Logistic-adjusted-Sine map (2D-LASM), 2D Logistic-sine-coupling map (2D-LSCM), and 2D Logistic ICMIC cascade map (2D-LICM). The developed encryption scheme consists of six stages involving permutation operations based on chaotic order, substitution based on modulus and bitXOR, and the use of a hash function. Hash functions are used to improve the quality of the key space and the sensitivity of the key. The research results show that combining encryption at the bit and pixel levels and using three 2D logistic maps has improved encryption security performance. Based on the explanation of several related studies and background, this research combines several techniques, namely 2D-SLMM, 2D-LICM, and 1D-MLM. The HIC3 technique and encryption operations at the pixel and bit levels were designed to improve diffusion and confusion patterns. Further explanation of the proposed method is presented in section 3.

3. Proposed Method

In this section, we introduce the proposed image encryption method, which aims to improve the security and confidentiality of digital images. Our approach emphasizes image encryption techniques that align with Shannon's principles of confusion and diffusion. We combine encryption techniques, including hash functions, chaos-based methods, and

especially half-inverted cascading chaos cipheration (HIC3), to offer a comprehensive solution tailored for image encryption. In this section, we present a detailed description of the proposed method, including the basic principles, step-by-step algorithm, and main components accompanied by flow diagrams, which are discussed in more detail as follows.

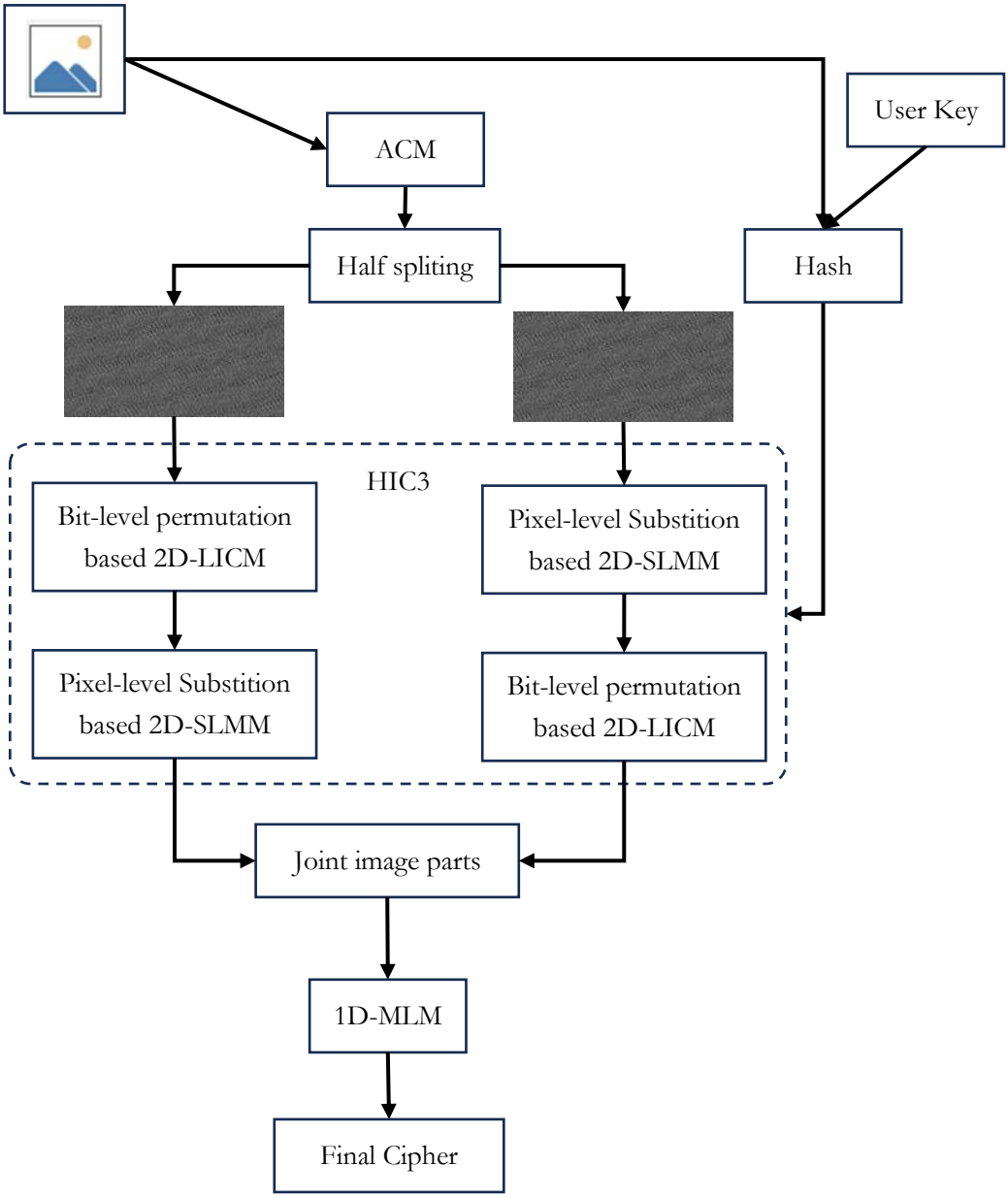

Figure 4. Proposed Method.

3.1. Preparation, Key and Parameters Settings

1. The image to be encrypted is read and stored in variable I.
2. The key used for encryption and decryption is generated from the text key entered by the user and the image itself. Perform a SHA-512 hash function from the text key ($key1$) and image ($key2$), converting the hash to a byte array and combining the booth keys into one key (c_key) with the modulo 256 operation, see Equation (6).

$$c\_key = mod((key1 + key2),256) \tag{6}$$

3. Calculate the initial values of x and y for the three chaotic maps 2D-SLMM, 2D-LICM, and 1D-MLM based on the standard deviation value of the hybrid key (c_key), for more details see Equation (7)-(11).

$$x1 = \sum_{n=0}^{\infty} \frac{\sigma(c\_key_1, \dots, c\_key_{16})}{10^n}, \text{subject to } x1 > 1 \quad (7)$$

$$y1 = \sum_{n=0}^{\infty} \frac{\sigma(c\_key_{17}, \dots, c\_key_{32})}{10^n}, \text{subject to } y1 > 1 \quad (8)$$

$$x2 = \sum_{n=0}^{\infty} \frac{\sigma(c\_key_{33}, \dots, c\_key_{48})}{10^n}, \text{subject to } x2 > 1 \quad (9)$$

$$y2 = \sum_{n=0}^{\infty} \frac{\sigma(c\_key_{49}, \dots, c\_key_{64})}{10^n}, \text{subject to } y2 > 1 \quad (10)$$

$$x0 = \sum_{n=0}^{\infty} \frac{\sigma(c\_key_1, \dots, c\_key_{64})}{10^n}, \text{subject to } x0 > 1 \quad (11)$$

3.2. HIC3 Image Encryption

1. Randomize the image using the ACM with constant parameters and iteration using Equation (3).
2. The image is split into two equal parts (upperHalf and lowerHalf).
3. Convert upperHalf to binary form, then convert it to one dimensional.
4. In upperHalf, perform a permutation operation based on the first sequence of 2D-LICM.
5. Perform Equation (12) on the first sequence of 2D-SLMM to obtain $intSec$.

$$intSec = mod((x1_1 \times 10^{10}, \dots, x1_n \times 10^{10}), 256) \quad (12)$$

6. Continue the substitution operation with the modulus operation between the permuted image and $intSec$.
7. In reverse order (steps 6,4,5), perform lowerHalf encryption is based on the second sequence 2D-LICM and 2D-SLMM.
8. Reshape both parts of the image to their original shape, then combine them into an encrypted image($encImg$).
9. Perform Equation (13) on the 1D-MLM sequence to obtain $intSec2$.

$$intSec2 = mod((x0_1 \times 10^{10}, \dots, x_{0n} \times 10^{10}), 256) \quad (13)$$

10. Perform bitxor operation between $intSec2$ and $encImg$ to get the final encrypted image.
    The key

4. Results and Discussion

This section presents the experimental results and discussion of this research. Experiments were carried out using hardware, namely an i7 11th-generation processor with 16GB memory and Matlab R2021a software. We use several sample images to test the effectiveness of the proposed encryption method. These standard grayscale images are widely used in various research presented in Figure 5. In the evaluation process, we utilize encryption measuring tools such as histogram, chi-square, information entropy, NPCR and UACI, the correlation coefficient of adjacent pixels, keyspace, key sensitivity analysis, NIST randomness, and robustness test. These measuring tools help to analyze the extent to which the proposed encryption method meets the security criteria which are discussed in more detail in sections 4.1 to 4.8. Next, a sample of the encryption and decryption results, along with the histogram, is presented in Figure 6.

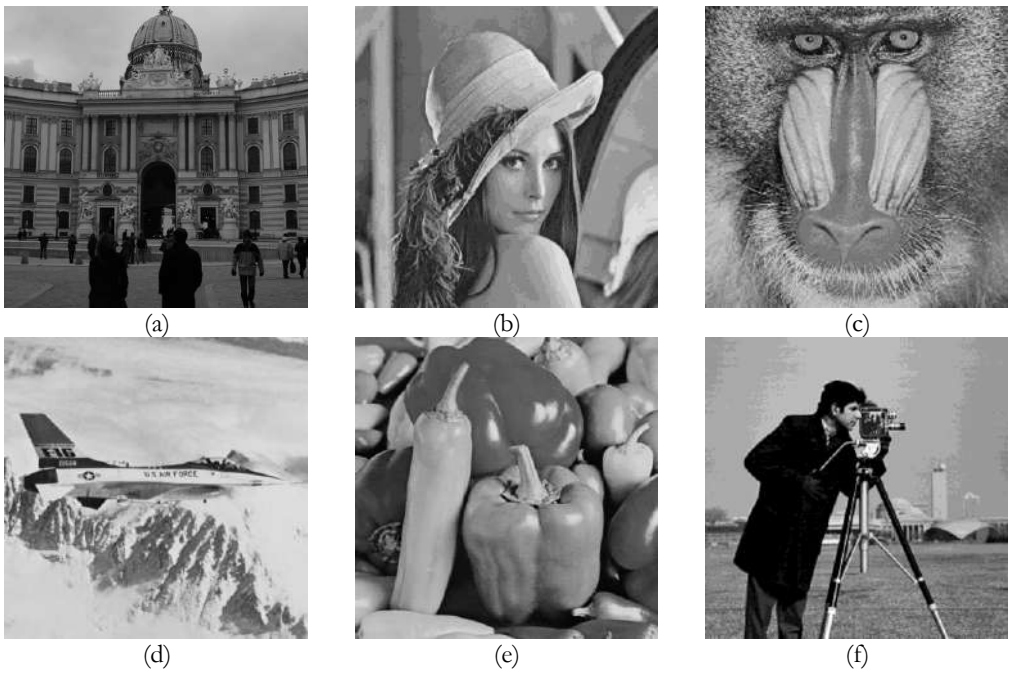

Figure 5. Standard test image used for testing (**a**) 1013.pgm from BossBase Dataset; (**b**) Lena; (**c**) Baboon a.k.a Mandrill; (**d**) Airplane a.k.a F16; (**e**) Peppers; (**f**)Cameraman .

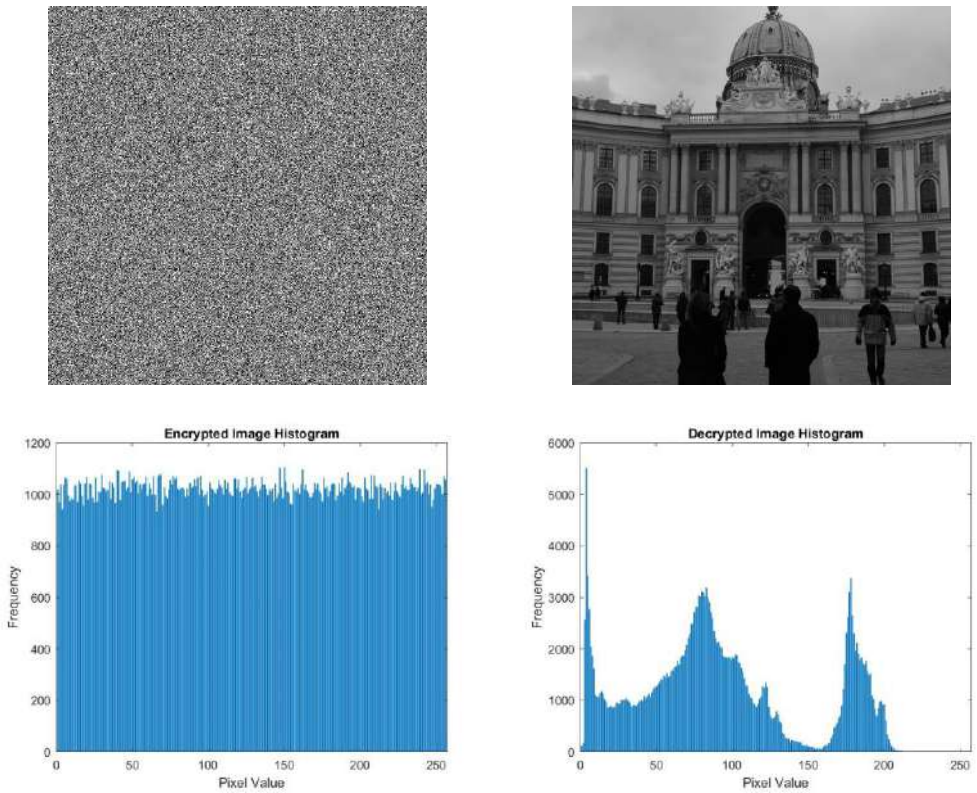

Figure 6. Sample Encryption and Decryption Results.

4.1. Chi-square analysis (χ^2)

Chi-square analysis is a statistical method used to measure the extent to which observed data matches expected data. In the context of testing image encryption quality, it is used to assess the extent to which an encrypted image distributes its pixel values randomly or uniformly, which indicates the level of confusion or complexity in the encrypted image. Two

data sets for χ^2 calculations. The first set is the observed data, namely the encrypted image, and the second set is the expected data, namely the theoretical probability distribution for a perfectly encrypted image[41], [42]. The χ^2 can calculated with Equation (14), if the χ^2 value is less than or equal to $X^2_{\delta,fd}$ =293.2478 with a significance level (δ) of 0.05 and freedom degrees (fd) equal to 255, it suggests that the histogram is deemed to exhibit a uniform distribution.

$$X^2 = \sum_{i=1}^{256} \frac{(O_i - E_i)^2}{E_i} \tag{14}$$

Where $O_i$is the observation frequency (the number of pixels at a certain value in the encrypted image), E_i is the expected frequency (theoretical probability distribution at a given value).

Table 1 presents the results of calculating the chi-square value and a comparison with several related works. It can be seen that the proposed method has outstanding performance where all the values pass and show a uniform histogram. The proposed method is also relatively superior in the majority of results.

Table 1. Chi-square results and its comparison with related works.

Image	**Method**[36]	**Method**[8]	**Method**[19]	Proposed	Passed
1013.pgm	-	-	275.9563	256.3443	☑
Lena	255.7102	244.125	212.6831	234.4334	☑
Baboon	250.6958	246.271	284.3348	250.2232	☑
Airplane	-	243.654	285.0325	248.2332	☑
Peppers	254.8962	241.462	259.1784	240.4343	☑
Cameraman	-	247.285	-	247.1343	☑
Total pass	3/3	5/5	5/5	6/6	

4.2. Information Entropy

Information entropy (IE) is a theoretical measure of uncertainty or confusion in a system. In image encryption terminology, information entropy measures the extent to which pixel values in an image are randomly or uniformly distributed. IE is calculated from the probability distribution of pixel values in the encrypted image[43], [44]. An image's entropy value generally ranges from 0 to 8. A good-quality encrypted image must have a high level of IE, indicating no easily recognizable patterns or structures in the image. Conversely, if IE is low, it may indicate the existence of patterns that unauthorized parties could exploit. IE can be calculated with Equation (15). Meanwhile, the measurement results and comparison with related methods are presented in Table 2.

$$IE(X) = -\sum_{i=1}^{n} p(x_i) log_2\big(p(x_i)\big) \tag{15}$$

Where $IE(X)$ is the information entropy of the random variable X, $p(x_i)$ is the probability of the occurrence of the value x_i, $\sum_{i=1}^{n}$ summing over all possible values in the random variable X, $log_2\big(p(x_i)\big)$ is the base-2 logarithm of the probability $p(x_i)$.

Table 2. IE results and its comparison with related works.

Image	**Method**[36]	**Method**[4]	**Method**[12]	**Method**[8]	Proposed
1013.pgm	-	-	-	-	7.9993
Lena	7.9973	7.9972	7.9968	7.9993	7.9994
Baboon	7.9972	-	-	7.9993	7.9994
Airplane	-	-	-	-	7.9993
Peppers	7.9993	7.9969	7.9969	7.9993	7.9994
Cameraman	-	7.9973	7.9974	7.9993	7.9994
Average					

Table 2 presents the results of information entropy calculations, which are very important in analyzing the quality of image encryption. From the results of these calculations, it can be observed that the entropy values are close to the maximum possible values. This is a very positive indication, showing that the proposed method has excellent performance in maintaining the level of complexity and uncertainty in encrypted images.

4.3. Differential Analysis

NCPCR (Normalized Pixel Change Rate) and UACI (Unified Average Changing Intensity) are two metrics used to measure differential statistics between two images, which are often used in the context of evaluating image encryption[45]. They help assess how much image encryption can disrupt or alter image data. NCPCR measures the extent to which two encrypted images differ regarding pixel percentage change. In other words, how many pixels change after encryption. UACI also measures the difference between two encrypted images but considers the percentage change and the intensity of the change[46], [47]. Equation (16) is used to calculate NPCR, and (17) is used to calculate UACI. The optimal NCPCR and UACI values are 99.6094% and 33.4635%, respectively, but if the values are around 99% and 33%, it already shows a value that tends to be very good.

$$NPCR = \left[\frac{1}{N \times M}\sum_{i=1}^{N}\sum_{j=1}^{M}\delta(i,j)\right] \times 100\%, \;\; \delta(i,j)\begin{cases}0 \; if \; E1(i,j) = E2(i,j)\\1 \; if \; E1(i,j) \neq E2(i,j)\end{cases} \tag{16}$$

$$UACI = \left[\frac{1}{N \times M}\sum_{i=1}^{N}\sum_{j=1}^{M}\frac{|E1(i,j) - E2(i,j)|}{255}\right] \times 100\% \tag{17}$$

Where $E1$ represents the original encrypted image, $E2$ represents the altered encrypted image, N is the number of pixel columns, and M is the number of pixel rows, while i and j represent the coordinates of individual pixels, 255 is the maximum value of pixel intensity in the image.

Table 3 presents the NCPCR calculation results, and Table 4 presents the UACI values. These two tables also provide comparisons with several related studies. It can be observed that the NPCR and UACI values are all close to the ideal values, and their performance is close to or even partly better than the corresponding methods. This means an indication of very high resistance to differential attacks.

Table 3. NPCR results and its comparison with related works.

Image	**Method**[36]	**Method**[4]	**Method**[12]	**Method**[8]	**Proposed**
1013.pgm	-	-	-	-	99.6109
Lena	-	99.6200	99.6399	99.6078	99.6211
Baboon	-	-	-	99.6092	99.6099
Airplane	99.6093	-	-	99.6063	99.6019
Peppers	-	99.6100	99.6094	99.6061	99.6139
Cameraman	-	99.6400	99.5773	99.6018	99.6183
Average	99.6093	99.6233	99.6089	99.6062	99.6127

Table 4. UACI results and its comparison with related works.

Image	**Method**[36]	**Method**[4]	**Method**[12]	**Method**[8]	**Proposed**
1013.pgm	-	-	-	-	33.4524
Lena	-	33.5100	33.4308	33.4599	33.4815
Baboon	-	-	-	33.4772	33.4699
Airplane	33.4791	-	-	33.4838	33.4901
Peppers	-	33.4200	33.5607	33.4526	33.4795
Cameraman	-	33.5000	33.3542	33.4973	33.4398
Average	33.4791	33.4767	33.4486	33.4742	33.4689

4.4 Correlation Coefficient of Adjacent Pixels

Correlation Coefficient of Adjacent Pixels (CCAP) is one of the metrics used to measure image encryption statistics, especially in measuring the level of correlation between adjacent pixels in an encrypted image. CCAP helps evaluate the extent to which image encryption can

randomize and reduce the correlation between adjacent pixels, which is an important indicator of the quality of image encryption[48]. The range of CCAP measurement results ranges from -1 to 1. The value -1 indicates that changes in one pixel are inversely proportional to changes in neighbouring pixels. A value of 1 indicates that there is a perfect positive correlation between neighbouring pixels. A value of 0 indicates that there is no correlation between neighbouring pixels. The CCAP value must be close to zero for good quality in image encryption. Figure 7 shows a sample plot of 10,000 CCAP pixel pairs, the first column is the original image correlation, and the second column shows the encrypted image correlation on the diagonal, horizontal and vertical sides, respectively. Equation (18) is used to calculate CCAP. Table 5 presents the CCAP calculation results and its comparison with related work. All CCAP values from various angles show varying values, namely positive and negative, but all are close to zero. This indicates that the encryption results have reduced correlation significantly, which is beneficial for image security.

$$CCAP = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\sum_{x=1}^{M}\sum_{y=1}^{N}(I(ij)-\bar{I})(I(i+x,j+y)-\bar{I})}{\sqrt{\sum_{x=1}^{M}\sum_{y=1}^{N}(I(ij)-\bar{I})^2\sum_{x=1}^{M}\sum_{y=1}^{N}(I(i+x,j+y)-\bar{I})^2}} \quad (18)$$

Where N is number of pixel columns and M is number of pixel rows, $I(ij)$ is the intensity of the pixel at coordinates (i,j), $\bar{I}$ is the average intensity of pixels in the image, This formula calculates the level of correlation between the pixel at (i,j) and the pixels at a distance (x,y).

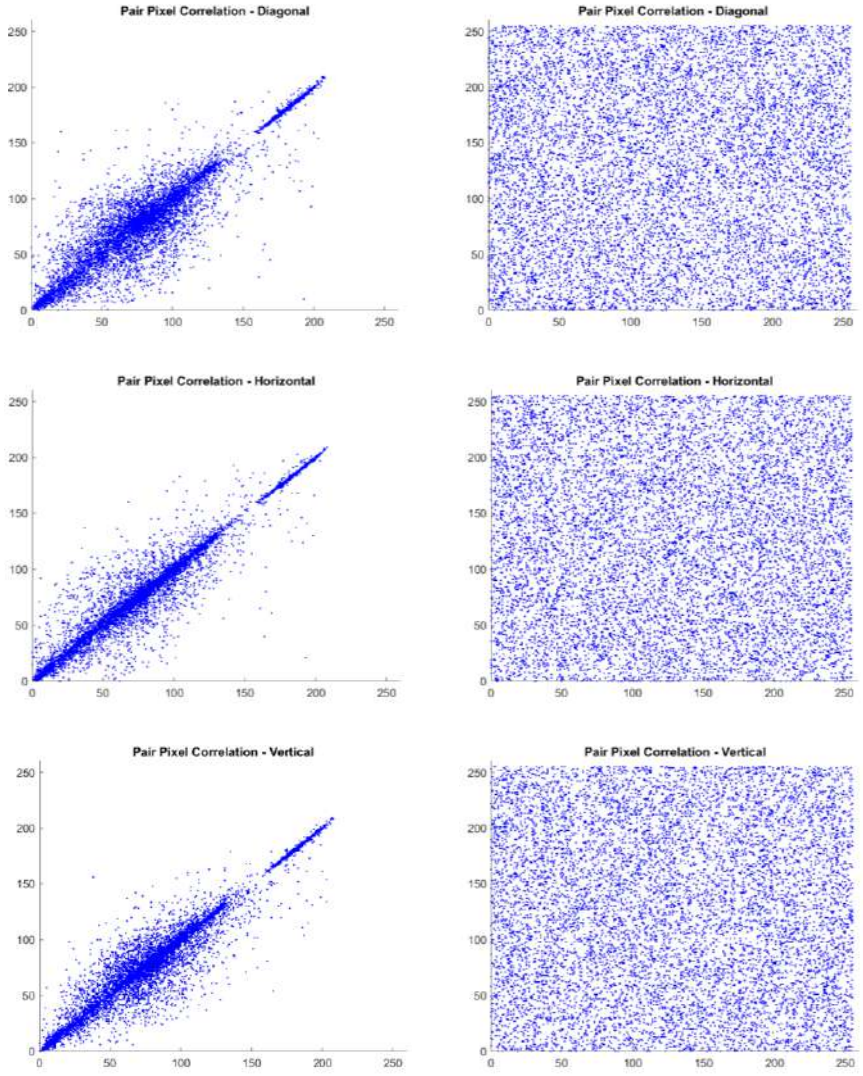

Figure 7. The correlation coefficient of adjacent pixels of plain(left) and encrypted image (right).

Table 5. CCAP results and their comparison with related works.

Image	Direc-tion	**Method**[36]	**Method**[4]	**Method**[12]	**Method**[8]	**Proposed**
1013.pgm	H	-	-	-	-	0.0012
	V	-	-	-	-	-0.0003
	D	-	-	-	-	0.0023
Lena	H	0.0019	0.0018	0.0055	0.0017	0.0008
	V	0.0012	−0.0021	−0.0077	-0.0012	0.0011
	D	0.0009	0.0001	−0.0058	0.0016	-0.0013
Baboon	H	0.0054	-	-	-	0.0018
	V	0.0004	-	-	-	-0.0013
	D	0.0044	-	-	-	0.0005
Airplane	H	-	-	-	-	0.0027
	V	-	-	-	-	-0.0019
	D	-	-	-	-	0.0009
Peppers	H	0.0004	−0.0033	0.0004	0.0017	-0.0011
	V	0.0014	0.0019	−0.0018	0.0015	0.0019
	D	0.0008	−0.0088	−0.0063	0.0015	-0.0007
Cameraman	H	-	−0.0051	0.0070	-	-0.0017
	V	-	−0.0017	−0.0050	-	0.0013
	D	-	−0.0005	−0.0146	-	0.0035

4.5. Key Sensitivity and Keyspace Analysis

Key Sensitivity Analysis is the process of evaluating how small changes to the encryption key can affect the encrypted image and the decryption process. This includes analysis of the image's sensitivity to small changes in the encryption key value (typically 1 bit). Figure 8 presents a sample of decryption results with a change in 1 key bit, where the initial key is "Hello World!", changed to "Hellp Word!".

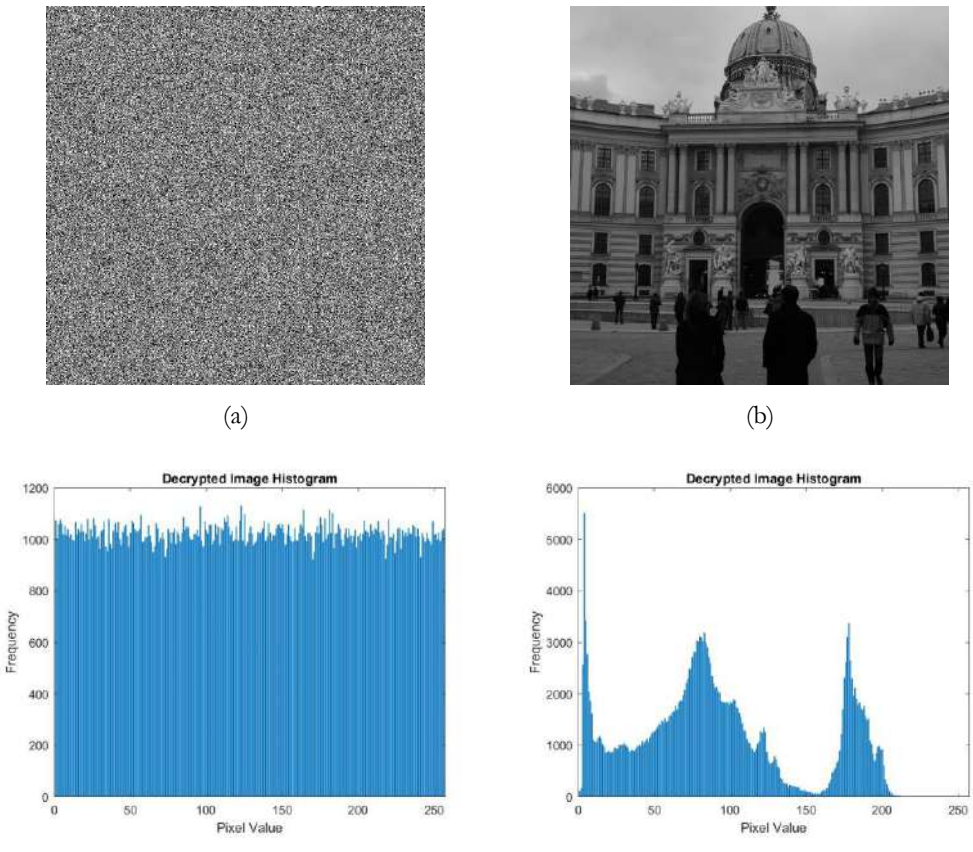

Figure 8. Decrypted results and its histogram (**a**) With 1-bit key modification; (**b**) With corrected key (**c**) Incorrect decryption histogram results; (**d**)Correct decryption histogram results.

Keyspace is all possible key combinations that can be used to secure data with a certain algorithm. This is very important in assessing the security strength of an encryption algorithm. The larger the keyspace, the more difficult it is for an attacker to guess all possible key combinations. The keyspace should have 2^{100} posibilities or more greater[49], [50]. This research uses the SHA-512 hash function, which has a key space of 2^{512}. In addition, the use of parameters from 2D-SLMM, 2D-LICM, and 1D-MLM is more than $\approx 6 \times 10^{16}$. This means the proposed method has a strong keyspace against brute force attacks.

4.6. Visual Analysis

Peak Signal-to-Noise Ratio (PSNR) is a measuring tool used to measure the visual quality of image encryption. PSNR compares the encrypted image with the original image and measures the degree of difference between the two. The higher the PSNR value, the less the difference between the encrypted and original images. PSNR measures visual quality by calculating the level of distortion or interference present in the encrypted image. The lower the PSNR value, the better the encryption quality because the noise that occurs in the encrypted image is greater[51], [52]. The PSNR value can be calculated using Equation (19), and the calculation and comparison results are presented in Table 6. These results show that a very low PSNR value succeeds in scrambling messages very well and provides evidence that the encryption results are visually very different from plaintext.

$$PSNR = 10\, log_{10}\left(\frac{max}{\frac{1}{M \times N}\sum_i^M \sum_j^N \big(O(i,j) - E(i,j)\big)^2}\right) \tag{18}$$

Where N is the number of pixel columns and M is the number of pixel rows, i and j is pixel coordinates, O is the original image and E is the encrypted image

Table 6. PSNR results and its comparison with related works.

Image	**Method**[12]	**Method**[53]	**Method**[30]	**Proposed**
1013.pgm	-	-	-	7.5233
Lena	8.5085	9.2267	8.64176	7.7323
Baboon	-	9.7296	8.91641	7.8267
Airplane	-	-	-	7.6232
Peppers	8.4240	8.8792	8.09877	7.7334
Cameraman	8.3611	8.4045	-	7.3342
Average	8.4312	9.0600	8.5523	7.6289

4.7. NIST Randomness Test

The NIST randomness test is a series of statistical tests designed to test the level of randomness of data sequences, including random data generated by various processes, including encrypted data. This test was developed by the National Institute of Standards and Technology (NIST) to evaluate the level of randomness in data used in security and cybersecurity applications. The NIST Randomness Test typically accepts data sequences in the form of binary .dat files. This is because testing is performed at the bit level, and image data needs to be converted into bit sequences before testing. So in this test experiment, the encrypted image is first converted into a .dat file. The result of this test is the p-value, which measures the extent to which the tested data fits the expected randomness distribution model. A low p-value indicates that the data is more similar to true random data, while a high p-value indicates that the data is more deterministic. In general, the p-value that is considered "passed" is a p-value that is greater than 0.01[20], [54]. The NIST Randomness Test involves several different subtests, such as frequency testing, permutation testing, and others. The test results from all the subtests are added up to give the final result. If all subtests provide a p-value "passed," then the data is considered to pass the overall test. The results of this research's NIST testing are presented in Table 7.

Table 7. NIST Randomness test results.

Test Name	Test function	p-value	Passed
Frequency	To check whether there is an imbalance between the number of 0 and 1 bits in the data.	0.739918	☑
Block Frequency	Tests whether the frequency of appearance of certain blocks in a sequence is random.	0.122325	☑
Cumulative Sums (Forward)	Measures the degree to which sequences tend to increase cumulatively.	0.122325	☑
Cumulative Sums (Reverse)	Same as the Cumulative Sums (Forward) test, but in the opposite direction.	0.350485	☑
Runs	Detect sequential patterns (runs) in data.	0.350485	☑
Longest Run of Ones	Determines the length of the longest run of bit 1 in the sequence.	0.035174	☑
Rank	Measures the ability of data to form a matrix with full rank.	0.534146	☑
Discrete Fourier Transform	Observe the frequency spectrum of the data sequence.	0.350485	☑
Nonperiodic Template Matchings	Search for matches with non-periodic templates in the data.	0.434424	☑
Overlapping Template Matchings	Search for matches with templates that can overlap in the data.	0.534146	☑
Universal Statistical	Measures the level of data compressibility.	0.645343	☑
Approximate Entropy	Measures how irregular the data sequence is.	0.911413	☑
Random Excursions	Analyze random walk patterns in data.	0.433534	☑
Random Excursions Variant	Same as Random Excursions, with certain variations.	0.212133	☑
Serial	Analyze sequential order patterns in data.	0.534146	☑
Linear Complexity	Measures the linear complexity of a data sequence.	0.739918	☑

4.8. Robustness Test

A robustness test in terms of image encryption is designed to measure the extent to which an image encryption system can survive or remain effective when faced with various types of attacks or modifications that unauthorized parties may carry out. Robustness testing is essential in assessing the security of an image encryption system and determining the extent to which the system can protect the integrity and confidentiality of data when faced with various threats. In this study, we tested the robustness of the proposed method by providing an attack of 200x200 pixels on the image and the results are presented in Figure 9. It appears that after manipulation, the image can still be decrypted and is still visually recognizable.

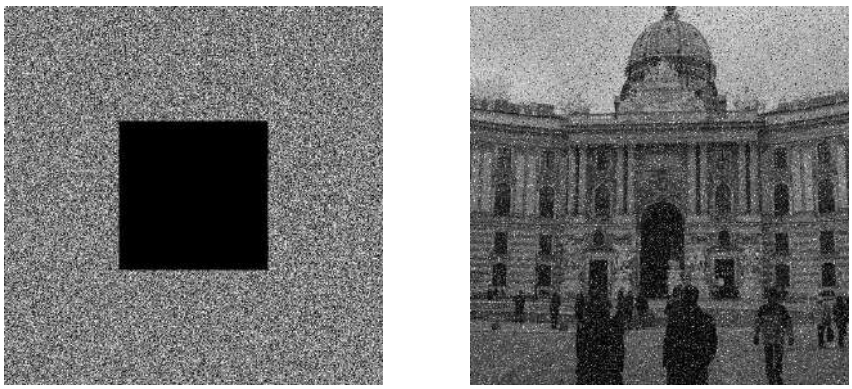

Figure 9. Robustness test using 200×200 pixels attack (**a**) attacked encrypted image; (**b**) decrypted attacked image.

5. Conclusions

In this research, an image encryption scheme has been proposed that combines various permutation, substitution, and chaotic map techniques. This method, known as Half-Inverted

Cascading Chaos Cipheration (HIC3), aims to increase the level of security and confidentiality of digital images. One of the main problems solved by HIC3 is the increased confusion and diffusion in images, following the basic principles in Shannon information theory. HIC3 combines multiple chaotic maps such as ACM, 2D-SLMM, 2D-LICM, and 1D-MLM in image encryption operations and improves the quality of random sequences used for substitution and permutation operations. This method also integrates a hash function, which increases the keyspace and key sensitivity.

The results of tests carried out on HIC3 are very positive and show the effectiveness of this method in protecting digital images from various attacks. Based on chi-square testing, information entropy, NPCR, UACI, adjacent pixel correlation, key sensitivity and key space analysis, NIST randomness testing, robustness testing, and visual analysis, HIC3 has demonstrated excellent performance. The test results show that HIC3 successfully achieved its goal of increasing the level of security in digital image encryption. HIC3 successfully maintains image integrity and prevents attacks on encrypted images. In addition, HIC3 also successfully addresses a major problem in image encryption, namely the increased level of obfuscation and diffusion required to maintain image confidentiality and integrity. This shows that HIC3 is a step forward in developing digital image encryption techniques. With a high level of security and resistance to various attacks, this research contributes to understanding and overcoming information security challenges in today's digital era.

Author Contributions: Conceptualization: D.R.I.M.S.; methodology: D.R.I.M.S., R., and S.W.; software: O.P. and M.K.S.; validation: D.R.I.M.S., R., O.P. and S.W.; formal analysis: M.K.S.; investigation: ALL.; resources: D.R.I.M.S., R., O.P. and S.W.; writing—original draft preparation: D.R.I.M.S.; writing—review and editing: D.R.I.M.S. and M.K.S.; visualization: D.R.I.M.S.; supervision: ALL; project administration: R., O.P., and S. W.; funding acquisition: ALL.

Funding: This research received no external funding.

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

References

[1] B. M. P. Waseso and N. A. Setiyanto, "Web Phishing Classification using Combined Machine Learning Methods," *J. Comput. Theor. Appl.*, vol. 1, no. 1, pp. 11–18, Aug. 2023, doi: 10.33633/jcta.v1i1.8898.

[2] A. A. Ojugo *et al.*, "Forging a User-Trust Memetic Modular Neural Network Card Fraud Detection Ensemble: A Pilot Study," *J. Comput. Theor. Appl.*, vol. 1, no. 2, pp. 1–11, Oct. 2023, doi: 10.33633/jcta.v1i2.9259.

[3] J. G. Sekar, E. Periyathambi, and A. Chokkalingam, "Hybrid chaos-based image encryption algorithm using Chebyshev chaotic map with deoxyribonucleic acid sequence and its performance evaluation," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 6, p. 6952, Dec. 2023, doi: 10.11591/ijece.v13i6.pp6952-6963.

[4] J. Zheng and T. Bao, "An image encryption algorithm based on cascade chaotic map and DNA coding," *IET Image Process.*, 2023, doi: 10.1049/ipr2.12882.

[5] P. Kumari and B. Mondal, "Lightweight image encryption algorithm using NLFSR and CBC mode," *J. Supercomput.*, vol. 79, no. 17, pp. 19452–19472, 2023, doi: 10.1007/s11227-023-05415-9.

[6] Y. Alghamdi and A. Munir, "An Image Encryption Algorithm Based on Trivium Cipher and Random Substitution," *SN Comput. Sci.*, vol. 4, no. 6, p. 713, Sep. 2023, doi: 10.1007/s42979-023-02172-7.

[7] P. Kumari and B. Mondal, "An Encryption Scheme Based on Grain Stream Cipher and Chaos for Privacy Protection of Image Data on IoT Network," *Wirel. Pers. Commun.*, vol. 130, no. 3, pp. 2261–2280, Jun. 2023, doi: 10.1007/s11277-023-10382-8.

[8] S. Bhowmik and S. Acharyya, "Image encryption approach using improved chaotic system incorporated with differential evolution and genetic algorithm," *J. Inf. Secur. Appl.*, vol. 72, no. December 2022, p. 103391, 2023, doi: 10.1016/j.jisa.2022.103391.

[9] S. Dhall, S. K. Pal, and K. Sharma, "A chaos-based probabilistic block cipher for image encryption," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 1, pp. 1533–1543, Jan. 2022, doi: 10.1016/j.jksuci.2018.09.015.

[10] N. Wang *et al.*, "Galois Field-Based Image Encryption for Remote Transmission of Tumor Ultrasound Images," *IEEE Access*, vol. 7, pp. 49945–49950, 2019, doi: 10.1109/ACCESS.2019.2910563.

[11] B. Harjo and D. R. I. M. Setiadi, "Improved Color Image Encryption using Hybrid Modulus Substitution Cipher and Chaotic Method," *Int. J. Intell. Eng. Syst.*, vol. 14, no. 2, pp. 157–165, 2021, doi: 10.22266/ijies2021.0430.14.

[12] D. E. Mfungo, X. Fu, Y. Xian, and X. Wang, "A Novel Image Encryption Scheme Using Chaotic Maps and Fuzzy Numbers for Secure Transmission of Information," *Appl. Sci.*, vol. 13, no. 12, p. 7113, Jun. 2023, doi: 10.3390/app13127113.

[13] A. Toktas, U. Erkan, S. Gao, and C. Pak, "A robust bit-level image encryption based on Bessel map," *Appl. Math. Comput.*, vol. 462, no. March 2023, p. 128340, Feb. 2024, doi: 10.1016/j.amc.2023.128340.

[14] Q. Lai and H. Zhang, "A new image encryption method based on memristive hyperchaos," *Opt. Laser Technol.*, vol. 166, no. March, p. 109626, 2023, doi: 10.1016/j.optlastec.2023.109626.

[15] Y. Hu, H. Wu, and L. Zhou, "Color image encryption base on a 2D hyperchaotic enhanced Henon map and cross diffusion," *Alexandria Eng. J.*, vol. 73, pp. 385–402, 2023, doi: 10.1016/j.aej.2023.04.060.
[16] M. I. Moussa, E. I. Abd El-Latif, and A. H. Abu El-Atta, "Diagonalize three-dimensional nonlinear chaotic map to encrypt color image," *Egypt. Informatics J.*, vol. 24, no. 3, p. 100376, 2023, doi: 10.1016/j.eij.2023.05.001.
[17] M. Wang, X. Wang, C. Wang, S. Zhou, Z. Xia, and Q. Li, "Color image encryption based on 2D enhanced hyperchaotic logistic-sine map and two-way Josephus traversing," *Digit. Signal Process.*, vol. 132, p. 103818, Jan. 2023, doi: 10.1016/j.dsp.2022.103818.
[18] B. Zhang and L. Liu, "Chaos-Based Image Encryption: Review, Application, and Challenges," *Mathematics*, vol. 11, no. 11, 2023, doi: 10.3390/math11112585.
[19] D. R. I. M. Setiadi and N. Rijati, "An Image Encryption Scheme Combining 2D Cascaded Logistic Map and Permutation-Substitution Operations," *Computation*, vol. 11, no. 9, p. 178, Sep. 2023, doi: 10.3390/computation11090178.
[20] W. Alexan, N. Alexan, and M. Gabr, "Multiple-Layer Image Encryption Utilizing Fractional-Order Chen Hyperchaotic Map and Cryptographically Secure PRNGs," *Fractal Fract.*, vol. 7, no. 4, p. 287, Mar. 2023, doi: 10.3390/fractalfract7040287.
[21] W. Feng, X. Zhao, J. Zhang, Z. Qin, J. Zhang, and Y. He, "Image Encryption Algorithm Based on Plane-Level Image Filtering and Discrete Logarithmic Transform," *Mathematics*, vol. 10, no. 15, pp. 1–24, 2022, doi: 10.3390/math10152751.
[22] P. N. Andono and D. R. I. M. Setiadi, "Improved Pixel and Bit Confusion-Diffusion Based on Mixed Chaos and Hash Operation for Image Encryption," *IEEE Access*, vol. 10, no. November, pp. 115143–115156, 2022, doi: 10.1109/ACCESS.2022.3218886.
[23] D. R. I. M. Setiadi, E. H. Rachmawanto, and R. Zulfiningrum, "Medical Image Cryptosystem using Dynamic Josephus Sequence and Chaotic-hash Scrambling," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 9, pp. 6818–6828, Oct. 2022, doi: 10.1016/j.jksuci.2022.04.002.
[24] R. Wang, G.-Q. Deng, and X.-F. Duan, "An image encryption scheme based on double chaotic cyclic shift and Josephus problem," *J. Inf. Secur. Appl.*, vol. 58, p. 102699, May 2021, doi: 10.1016/j.jisa.2020.102699.
[25] E. Winarno, K. Nugroho, P. W. Adi, and D. R. I. M. Setiadi, "Integrated dual hyperchaotic and Josephus traversing based 3D confusion-diffusion pattern for image encryption," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 9, p. 101790, Oct. 2023, doi: 10.1016/j.jksuci.2023.101790.
[26] J. Xu, C. Zhao, and J. Mou, "A 3D Image Encryption Algorithm Based on the Chaotic System and the Image Segmentation," *IEEE Access*, vol. 8, pp. 145995–146005, 2020, doi: 10.1109/ACCESS.2020.3005925.
[27] E. Winarno, K. Nugroho, P. W. Adi, and D. R. I. M. Setiadi, "Combined Interleaved Pattern to Improve Confusion-Diffusion Image Encryption Based on Hyperchaotic System," *IEEE Access*, vol. 11, pp. 69005–69021, 2023, doi: 10.1109/ACCESS.2023.3285481.
[28] F. Budiman and D. R. I. M. Setiadi, "A Combination of Block-Based Chaos with Dynamic Iteration Pattern and Stream Cipher for Color Image Encryption," *Int. J. Intell. Eng. Syst.*, vol. 13, no. 6, pp. 132–141, 2020, doi: 10.22266/ijies2020.1231.12.
[29] F. Budiman, P. N. Andono, and D. R. I. M. Setiadi, "Image Encryption using Double Layer Chaos with Dynamic Iteration and Rotation Pattern," *Int. J. Intell. Eng. Syst.*, vol. 15, no. 2, pp. 57–67, 2022, doi: 10.22266/ijies2022.0430.06.
[30] W. Alexan, Y.-L. Chen, L. Y. Por, and M. Gabr, "Hyperchaotic Maps and the Single Neuron Model: A Novel Framework for Chaos-Based Image Encryption," *Symmetry (Basel).*, vol. 15, no. 5, p. 1081, May 2023, doi: 10.3390/sym15051081.
[31] A. Belazi, M. Khan, A. A. A. El-Latif, and S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 337–361, 2017, doi: 10.1007/s11071-016-3046-0.
[32] M. M. Al-Mhadawi, E. A. Albahrani, and S. H. Lafta, "Efficient and secure chaotic PRNG for color image encryption," *Microprocess. Microsyst.*, vol. 101, no. August 2022, p. 104911, 2023, doi: 10.1016/j.micpro.2023.104911.
[33] S. H. AbdElHaleem, S. K. Abd-El-Hafiz, and A. G. Radwan, "A generalized framework for elliptic curves based PRNG and its utilization in image encryption," *Sci. Rep.*, vol. 12, no. 1, pp. 1–16, 2022, doi: 10.1038/s41598-022-17045-x.
[34] R. Chu, S. Zhang, and X. Gao, "A Novel 3D Image Encryption Based on the Chaotic System and RNA Crossover and Mutation," *Front. Phys.*, vol. 10, no. March, pp. 1–14, 2022, doi: 10.3389/fphy.2022.844966.
[35] Z. Hua, Y. Zhou, C. M. Pun, and C. L. P. Chen, "2D Sine Logistic modulation map for image encryption," *Inf. Sci. (Ny).*, vol. 297, pp. 80–94, Mar. 2015, doi: 10.1016/J.INS.2014.11.018.
[36] C. Cao, K. Sun, and W. Liu, "A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map," *Signal Processing*, vol. 143, pp. 122–133, Feb. 2018, doi: 10.1016/j.sigpro.2017.08.020.
[37] A. Z. Hussain and M. A. A. Khodher, "Medical image encryption using multi chaotic maps," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 21, no. 3, pp. 556–565, 2023, doi: 10.12928/TELKOMNIKA.v21i3.24324.
[38] A. Susanto *et al.*, "Triple layer image security using bit-shift, chaos, and stream encryption," *Bull. Electr. Eng. Informatics*, vol. 9, no. 3, pp. 980–987, Jun. 2020, doi: 10.11591/eei.v9i3.2001.
[39] N. A. Abbas, "Image encryption based on Independent Component Analysis and Arnold's Cat Map," *Egypt. Informatics J.*, vol. 17, no. 1, pp. 139–146, Mar. 2016, doi: 10.1016/j.eij.2015.10.001.
[40] C. Han, "An image encryption algorithm based on modified logistic chaotic map," *Optik (Stuttg).*, vol. 181, no. December 2018, pp. 779–785, Mar. 2019, doi: 10.1016/j.ijleo.2018.12.178.
[41] S. Vaidyanathan *et al.*, "A Novel 3-D Jerk System, Its Bifurcation Analysis, Electronic Circuit Design and a Cryptographic Application," *Electronics*, vol. 12, no. 13, p. 2818, Jun. 2023, doi: 10.3390/electronics12132818.
[42] Y. Dong, G. Zhao, Y. Ma, Z. Pan, and R. Wu, "A novel image encryption scheme based on pseudo-random coupled map lattices with hybrid elementary cellular automata," *Inf. Sci. (Ny).*, vol. 593, pp. 121–154, 2022, doi: 10.1016/j.ins.2022.01.031.
[43] Y. S. Najaf and M. K. Mahmood Al-Azawi, "Public key cryptosystem based on multiple chaotic maps for image encryption," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 22, no. 3, pp. 1457–1466, 2021, doi: 10.11591/ijeecs.v22.i3.pp1457-1466.
[44] O. Omoruyi, C. Okereke, K. Okokpujie, E. Noma-Osaghae, O. Okoyeigbo, and S. John, "Evaluation of the quality of an image encrytion scheme," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 17, no. 6, pp. 2968–2974, 2019, doi: 10.12928/TELKOMNIKA.v17i6.10488.

[45] S. Mortajez, M. Tahmasbi, J. Zarei, and A. Jamshidnezhad, "A novel chaotic encryption scheme based on efficient secret keys and confusion technique for confidential of DICOM images," *Informatics Med. Unlocked*, vol. 20, p. 100396, Jan. 2020, doi: 10.1016/j.imu.2020.100396.
[46] D. A. Q. Shakir and A. J. Dawood, "3D chaos graph deep learning method to encrypt and decrypt digital image," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 25, no. 2, pp. 941–951, 2022, doi: 10.11591/ijeecs.v25.i2.pp941-951.
[47] S. A. Jassim and A. K. Farhan, "Designing a Novel Efficient Substitution-Box by Using a Flower Pollination Algorithm and Chaos System," *Int. J. Intell. Eng. Syst.*, vol. 15, no. 1, pp. 176–187, 2022, doi: 10.22266/IJIES2022.0228.17.
[48] J. S. Khan and S. K. Kayhan, "Chaos and compressive sensing based novel image encryption scheme," *J. Inf. Secur. Appl.*, vol. 58, no. January, p. 102711, May 2021, doi: 10.1016/j.jisa.2020.102711.
[49] J. Wu, X. Liao, and B. Yang, "Color image encryption based on chaotic systems and elliptic curve ElGamal scheme," *Signal Processing*, vol. 141, pp. 109–124, Dec. 2017, doi: 10.1016/j.sigpro.2017.04.006.
[50] Y. Liu and J. Zhang, "A Multidimensional Chaotic Image Encryption Algorithm based on DNA Coding," *Multimed. Tools Appl.*, vol. 79, no. 29–30, pp. 21579–21601, Aug. 2020, doi: 10.1007/s11042-020-08880-z.
[51] M. Kaur, D. Singh, K. Sun, and U. Rawat, "Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5D chaotic map," *Futur. Gener. Comput. Syst.*, vol. 107, pp. 333–350, Jun. 2020, doi: 10.1016/j.future.2020.02.029.
[52] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, "A New Image Encryption Algorithm for Grey and Color Medical Images," *IEEE Access*, vol. 9, pp. 37855–37865, 2021, doi: 10.1109/ACCESS.2021.3063237.
[53] S. Benaissi, N. Chikouche, and R. Hamza, "A novel image encryption algorithm based on hybrid chaotic maps using a key image," *Optik (Stuttg).*, vol. 272, no. November 2022, p. 170316, Feb. 2023, doi: 10.1016/j.ijleo.2022.170316.
[54] L. Moysis, A. Tutueva, C. Volos, D. Butusov, J. M. Munoz-Pacheco, and H. Nistazakis, "A Two-Parameter Modified Logistic Map and Its Application to Random Bit Generation," *Symmetry (Basel).*, vol. 12, no. 5, p. 829, May 2020, doi: 10.3390/sym12050829.