Efficient Image Encryption via 2D Logistic Chaos Mapping: Strengthening Security with Pixel-Level Dynamics

Yuebo Wu
School of Electrical and Photoelectronic Engineering, West Anhui University
China
wybyj1980@126.com

Shiwei Chu
School of Electronic Information Engineering, Anhui University
China
P23111026@stu.ahu.edu.cn

Huifang Bao
School of Electrical and Photoelectronic Engineering, West Anhui University
China
42000010@wxc.edu.cn

Duansong Wang
School of Electrical and Photoelectronic Engineering, West Anhui University, China
dswangsd@126.com

Jian Zhou
School of Electrical and Photoelectronic Engineering, West Anhui University, China
jianzhou8627@126.com

Abstract: *This study presents an innovative image encryption algorithm anchored on the two-dimensional Logistic chaotic system, designed to address the limitations of traditional methods in terms of speed and security. The algorithm employs pixel shifting and scrambling, coupled with a segmented grayscale value substitution, to achieve a high level of security with strong key sensitivity and robust resistance to both differential and statistical attacks. Experimental validation demonstrates its superiority with fast encryption speeds, as evidenced by an encryption time of 0.2136 seconds for a 256×256 color image, and an entropy close to its ideal value, indicating excellent randomness. This method also exhibits high performance in resisting differential attacks, with Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) values nearing their optimal expected values. The integration of Quantum Key Distribution (QKD) is suggested for future work to enhance security against quantum computing threats, solidifying the algorithm's potential as a leading solution for the image encryption.*

Keywords: *Image encryption algorithm, chaotic systems, pixel shifting, pixel scrambling*.

Received May 28, 2024; accepted September 2, 2024
https://doi.org/10.34028/iajit/21/5/12

1. Introduction

In the digital realm, the secure transmission of digital images is crucial for national security, enterprise information security, and personal privacy protection [4, 37]. The widespread availability and accessibility of digital images necessitate robust encryption methods to safeguard sensitive information from unauthorized access and tampering. Traditional image encryption algorithms, while effective for text and binary data, often lack the efficiency and robustness required for the complex, large-scale processing of image data. These methods can be slow and exhibit weak key sensitivity, which may compromise the security of encrypted data [22, 34]. However, chaos theory has emerged as a promising approach for enhancing encryption techniques, offering properties such as the butterfly effect, ergodicity, and fractality that are ideal for developing secure and complex encryption algorithms [43].

The 2D Logistic Map, known for its secure and efficient key and sequence generation, serves as the foundation for our proposed encryption algorithm [8, 16]. This study introduces an innovative image encryption algorithm based on the two-dimensional Logistic chaotic system, addressing the limitations of traditional methods in terms of speed and security. The algorithm utilizes pixel shifting and scrambling, along with segmented grayscale value substitution, to achieve a high level of security with strong key sensitivity and robust resistance to differential and statistical attacks.

The paper is organized as follows: The first section provides an overview of the research background, highlighting the limitations of existing image encryption technologies, and emphasizing the importance of efficient image encryption. The second section delves into the theoretical basis of two-dimensional logistic chaotic mapping and its application in image encryption. The third section presents a specific implementation scheme for pixel-level dynamic enhanced security, detailing the algorithm flow and key technical aspects. The fourth section verifies the effectiveness of the proposed method through experiments, presenting and analyzing the results. The final section summarizes the research findings, discusses the advantages and potential application prospects of the method, and suggests possible future

research directions and improvement measures.

2. Literature Review

In the past few decades, image encryption technology, as an important branch in the field of information security, has received extensive attention and research. Traditional image encryption algorithms such as the data encryption standard [25, 29], the advanced encryption standard, and the international data encryption algorithm, although they perform well in text and binary data encryption, are inefficient for large-scale, multi-dimensional information processing such as image data due to their complexity and computational overhead. In addition, image data has inherent redundancy and strong correlation, and traditional encryption methods [27, 32] are difficult to achieve fast processing while ensuring high security. Therefore, in recent years, image encryption methods based on chaos theory have gradually become a research hotspot. Chaotic systems [7, 42] have initial value sensitivity, randomness, and noise-like characteristics, which are very suitable for the scrambling and diffusion of image data. Existing chaotic image encryption algorithms [13, 41] are mostly based on one-dimensional or high-dimensional chaotic maps, but they still have shortcomings in complexity and security. On the one hand, one-dimensional chaotic maps are easy to crack and predict due to their simple structure; on the other hand, although high-dimensional chaotic maps [30, 31] can provide higher security, their computational complexity is high and it is difficult to meet real-time encryption requirements.

3. Basic Principles of the 2D Logistic Mapping

Chaos is a complex dynamic behavior [24] that is commonly found in nonlinear systems, which can obtain clear non-periodic results with simple models. Compared with other complex phenomena, its main characteristics include the initial value sensitivity (butterfly effect), ergodicity, boundedness, randomness, singular attractors (chaotic attractors), fractality, universality, and scaling, etc., [44, 35]. As the foundation of encryption systems, behaviors of the chaotic systems depend on control parameters and initial conditions [10, 45]. When selecting a chaotic system, it is necessary to ensure the chaotic behavior of all control parameter values, otherwise the ciphertext will no longer be secure [18, 38].

Two-dimensional logistic mapping will be applied, which is the most common one of two-dimensional chaotic systems [5]. Its mathematical expressions [36] are as follows.

$$\begin{cases} x(n+1) = r[3y(n)+1]x(n)[1-x(n)] \\ y(n+1) = r[3x(n+1)+1]y(n)[1-y(n)] \end{cases} \quad (1)$$

When the parameter r=1.17, the mapping attractor phase diagram of the 2D Logistic mapping is shown in Figure 1.

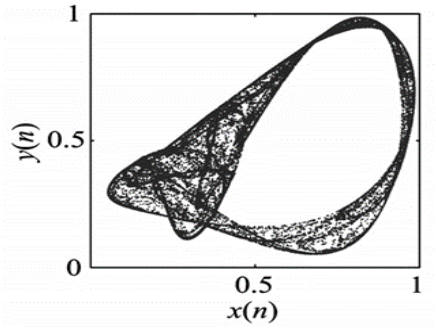


Figure 1. 2D Logistic mapping.

4. Image Encryption Algorithm Design

It's found that the chaotic orbits of high-dimensional or hyperchaotic systems are difficult to predict, with more complex dynamic characteristics and better randomness [23]. Chaotic systems with low dimensional discrete have advantages such as the simple form, a short run time, easy hardware and software implementation, and fast iteration speed, but their key space is smaller. Therefore, when using chaotic systems for image encryption, achieving a balance between the dimensionality and security performance is usually a difficult point in the algorithm design. Here the chaotic system of two-dimensional logistic mapping will be used to achieve the image encryption while ensuring security performance. The method design is introduced as follows.

4.1. Pixel Shifting and Scrambling

Assuming the original image is A and its size is W×H, Equation (2) can be used to generate a matrix Y for W×H, and rearranging each column from small to large can obtain the matrix Y' [46]. At the same time, a new sequence T is generated for recording the position of each column element in matrix Y in the original sequence, as shown in Figure 2. The formula for mapping iteration is [14].

$$key(i) = x(i) \times y(i) \times S \times 10^8 modeW \quad (2)$$

The first one thousand sequence values will be discarded to eliminate the transient effect. S is the sum of all the pixel values in the image [17, 39].

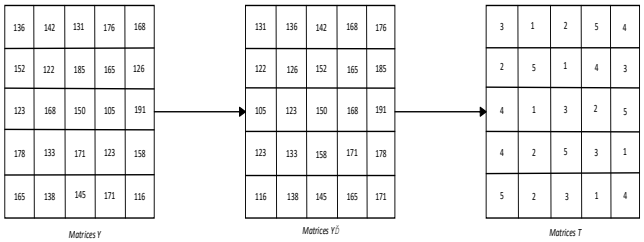


Figure 2. Pixel shifting and scrambling.

The original image is matrix A (for color images, it should be a matrix composed of a certain type of pixel values in R or G or B), and the scrambling process is shown in Figure 2 to obtain the scrambled image C. The pixel shifting and scrambling can be realized according to the following steps.

- *Step* 1. According to the elements of the first row (3, 1, 2, 5, 4) in matrix T, the corresponding elements (A3,5, A1,5, A2,5, A5,5, A4,5) will be selected from each column of matrix A, then shifted to the first row, and presented as (15, 5, 10, 25, 20) in matrix C.
- *Step* 2. According to the elements of the second row (2, 5, 1, 4, 3) in matrix T, the corresponding elements (A2,4, A5,4, A1,4, A4,4, A3,4) will be selected from each column of matrix A, then shifted to the second row, and presented as (9, 24, 4, 19, 14) in matrix C.
- *Step* 3. According to the elements of the third row (4, 1, 3, 2, 5) in matrix T, the corresponding elements (A4,3, A1,3, A3,3, A2,3, A4,3) will be selected from each column of matrix A, then shifted to the third row, and presented as (18, 3, 13, 8, 23) in matrix C.
- *Step* 4. According to the elements of the fourth row (4, 2, 5, 3, 1) in matrix T, the corresponding elements (A4,2, A2,2, A5,2, A3,2, A1,2) will be selected from each column of matrix A, then shifted to the fourth row, and presented as (17, 7, 22, 12, 2) in matrix C.
- *Step* 5. According to the elements of the fifth row (5, 2, 3, 1, 4) of matrix T, the corresponding elements (A5,1, A2,1, A3,1, A1,1, A4,1) will be selected from each column of matrix A, then shifted to the fifth row, and presented as (21, 6, 11, 1, 16) in matrix C. The actual pixel shifting and scrambling can be carried out according to the steps mentioned above, finally the scrambling image C has been obtained as shown in Figure 3.

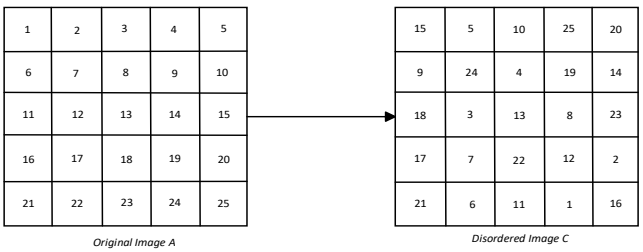


Figure 3. Scrambling image.

First, the pixels of image A are scrambled by a two-dimensional Logistic chaotic system, and then the segmented gray value replacement is applied to generate the final encrypted image C.

4.2. Grayscale Value Encryption

In order to improve the security of the encryption, the grayscale values is replaced for the scrambled image. Grayscale value substitution is the process of changing the grayscale value of an image through a key, thereby altering its visibility. Essentially, it is a permutation operation in the grayscale space. In this paper, the key streams $k1$ and $k2$ are calculated with the Equation (3) of the 2D-Logistic chaotic system. The formula for the 2D-Logistic chaotic system is [1]:

$$\begin{cases} k_1(i) = floor[x(i) \times 10^5 \times S] mod\ 256 \\ k_2(i) = floor[y(i) \times 10^7 \times S] mod\ 256 \end{cases} \quad (3)$$

Matlab program 1 has been used to perform the encryption on the rows of the scrambled image C.

```
for i=: W
   C'(i , 1) = bitxor ( mode ( k1 (1 , i)+S),256),C (i , 1)
   For j = 2: H
   C'(i , j)=bitxor(C'(i , j-1),C(i , j))
   end
end
```

Program 1 is used to encrypt the rows of image *C*. First, the first element of each row is subjected to a bitwise eXclusively-OR (XOR) operation, and then the remaining elements of the row are subjected to a stepwise XOR operation to generate an encrypted image *C*'.

Matlab program 2 has been used for the encrypted image *C*' to obtain the encrypted image *E*. Decryption is the inverse operation of the encryption.

```
for i=:H
E(i , 1)=bitxor (mode (( k2(1 , i) + S),256),C'(1 , i))
    For j = 2: W
      E(j , i) = bitxor (E(j - 1 , i),C'(j , i))
      end
end
```

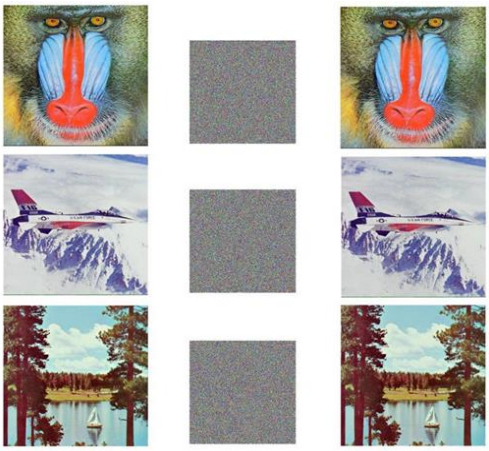
Program 2 is used to convert the encrypted image *C*' into the final encrypted image *E*. First, the first element of each column is subjected to a bitwise XOR operation, and then the remaining elements of the column are subjected to a stepwise XOR operation. The decryption process is the inverse operation of the encryption process.

5. Image Encryption Experiment and Results Analysis

The Intel Core i7-12700 CPU, which has a primary frequency of 2.1~4.9GHz, 64GB DDR5 memory, and 64-bit Windows 11 Professional Edition operating system comprise the hardware environment for the picture encryption experiment. Image encryption techniques are implemented using simulation software, Matlab R2022b.

Three identically sized color images-the Baboon, the Plane, and the Boat-have been chosen for testing in the encryption experiment. The 2D Logic Map's parameters are set to α=1 and β=3. Figures 4-b) and 4-c) display the encrypted and decrypted photos, whereas Figure 4 (a) displays the original photographs. It is evident that the size and aesthetic impact of the encrypted images are identical to those of the originals. During the encryption process, the data in the plain-text image can be compressed and hidden, and the cipher-text can be

successfully decrypted with the same key. The efficiency of the suggested technique is demonstrated by the restored image, which virtually looks identical to the original photographs.

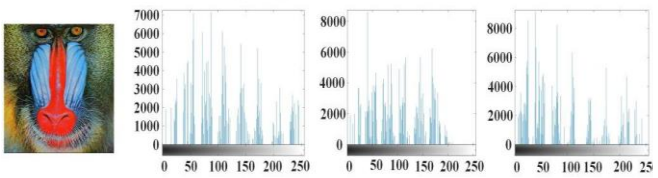


a) Original. b) Encryption. c) Decryption.

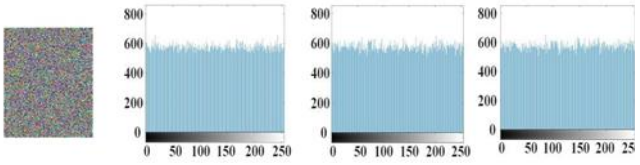
Figure 4. Encryption and decryption effect.

5.1. Analysis of the Histogram Characteristics

It is easy to illustrate the principles of picture alterations with the use of histograms. The distribution situation may be immediately revealed from the differences in the image's histograms before and after encryption, allowing one to assess how well the method performs in the face of statistical assaults. For this reason, plaintext histograms and cryptography are frequently utilized. The three pixel values that make up each location in a color picture are Red (R), Green (G), and Blue (B). The color image Baboon (256×256×3) has been used for the experiment, the histograms of which before and after encryption are shown in Figure 5. Obviously, there is a significant difference in the histograms before and after encryption. The pixels in each layer of the original image have significant clustering intervals and uneven pixel distribution, while the histograms of pixels in each layer of the cipher text are smooth and evenly distributed, hiding the original distribution information.



a) Baboon plaintext histogram (R, G, B).



b) Baboon cipher text histogram (R, G, B).

Figure 5. RGB histograms of Baboon before and after encryption.

χ^2 test [11, 12] is a testing method based on the Chi-square distribution, which can analyze in terms of quantity whether the distribution of continuous variables follows the uniform distribution. As indicated in Table 1, the inspection findings of encrypted pictures may be used to determine if the amount of pixel points is spread equally. The suggested technique can withstand assaults via histogram analysis, as seen by the cipher-text findings, which are all below the three free critical values (284.34, 293.25, and 310.46) with probability of 10%, 5%, and 1%, respectively. The critical value is a threshold used in statistical tests to determine whether to reject the null hypothesis. At different significance levels (such as 10%, 5%, and 1%), the critical value determines the range of the test statistic that should reject the null hypothesis. The critical value is obtained by consulting the statistical table. When the critical value is lower than the test statistic, it indicates that the result is statistically significant at that significance level.

Table 1. χ2-value test results of color images.

Images		Plaintext χ^2 values	Ciphertext χ^2 values	Critical values $\chi^2_{0.1}(255)$	Critical values $\chi^2_{0.05}(255)$	Critical values $\chi^2_{0.01}(255)$
Peppers	R	213187.22	249.25	Pass	Pass	Pass
	G	318382.93	260.39			
	B	491428.18	257.68			
Baboon	R	82839.73	247.25			
	G	142808.04	259.59			
	B	79942.62	249.72			
Plane	R	678424.49	258.36			
	G	682495.39	255.28			
	B	1107858.01	262.19			

5.2. Analysis of the Correlation

The scrambling impact of this encryption scheme may be seen in the correlation between neighboring pixels. In a picture, the closer the pixel values are to one another, the stronger the correlation between them. It is clear that plain-text image neighboring pixel values are closely spaced and have a strong correlation. Adjacent pixel values should be irregular and unconnected once the plain-text picture has been encrypted and jumbled. In order to obtain better encryption results, it is thus necessary to increase the difference in pixel values and decrease the correlation between neighboring pixels while doing correlation analysis on the cipher-text. To protect vertex coordinate information and hide its statistical information, reducing the correlation between the adjacent vertex coordinates is quite necessary. Covariance is usually used to measure the correlation between two images, but it is also influenced by the pixel values of the both images. Therefore, it is often normalized to a correlation coefficient. The linear correlation between two images is reflected in the numerical value of the correlation coefficient. Its calculating the formula [21] is as follows.

$$\gamma_{xy} = \frac{\frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)][y_i - E(y)]}{\sqrt{D(x)D(y)}} \quad (4)$$

Where, $E(x) = \frac{1}{n}\sum_{i=1}^{n} x_i$ is the expected value of $D(x) = \frac{1}{n}\sum_{i=1}^{n}[x_i - E(x)]$ variable x, and is the variance of variable x.

Table 2 displays the correlation coefficient comparison between the plaintext and cipher text. The plaintext data has strong correlations in several directions, and the plaintext correlation coefficient using the suggested approach is almost exactly equal to 1. The correlation between neighboring data is extremely low as the cipher text correlation coefficient approaches zero, demonstrating the suggested algorithm's resilience against correlation analysis attacks.

The above results demonstrate its ability to resist correlation analysis attacks.

Table 2. Correlation coefficient comparison of color images.

Channels	Orientation	Original image	Algorithm in this paper	Chen *et al*. [3]	Liu *et al*. [28]	Kaur *et al*. [19]
R	Horizontal	0.8511	0.0021	-0.0039	0.0061	-0.0032
	Vertical	0.7021	-0.0013	0.0029	-0.0043	0.0092
	Diagonal	0.8643	0.0004	0.0022	0.0156	-0.0043
G	Horizontal	0.8501	-0.0046	-0.0078	-0.0053	-0.0026
	Vertical	0.6677	0.0035	0.0061	0.0102	0.0033
	Diagonal	0.7524	0.0004	0.0029	0.0041	-0.0067
B	Horizontal	0.8902	0.0015	-0.0018	-0.0025	-0.0028
	Vertical	0.8265	-0.0022	0.0029	0.0112	0.0055
	Diagonal	0.8498	0.0003	0.0021	-0.0022	-0.0006

The correlation coefficients of color pictures in different channels and orientations for various methods are listed in Table 2. There is a substantial association between the color channels, as seen by the original pictures' typically high correlation coefficients. Nonetheless, the algorithm presented in this paper has an absolute correlation coefficient value that is substantially lower in all directions and channels and approaches zero, meaning that the correlation between the color channels is nearly eliminated, demonstrating the algorithm's efficacy. In contrast, the algorithms in references [3, 19, 28] reduce the correlation coefficients to varying degrees, but the effect is not as good as the algorithm proposed in this paper. For example, in the horizontal direction of the red channel, the correlation coefficient of the algorithm in this paper is 0.0021, while the correlation coefficients of references [3, 19, 28] are -0.0039, 0.0061 and -0.0032 respectively, which are not as thorough as the algorithm proposed in this paper.

5.3. Analysis of the Information Entropy

Information entropy is commonly used to balance the evaluation criteria for the random distribution of numerical statistical information. As information entropy increases, it's more difficult to steal the statistical numerical information. Therefore, the information entropy is also used to test the algorithm performance to resist statistical attacks. Its calculation formula [2] is as follows.

Where the pixel value is denoted by mi. *Mi*'s happening probability is denoted by *p*(*mi*). The total pixel values are *N*. *H*(*m*)=8 is the information entropy's optimal value [26]. Table 3 presents the results of calculating the RGB information entropy values of the encrypted picture using the algorithm applied to three 256×256 color images that were chosen. The fact that the entropy values are all clearly near to 8 suggests that the suggested method is capable of withstanding entropy assaults.

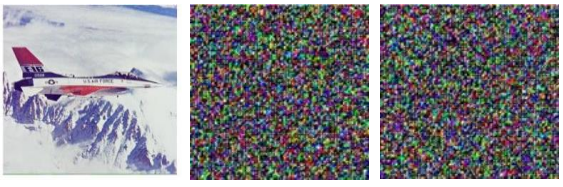
$$H(m) = \sum_{i=0}^{2^x-1} p(m_i)\log_2 \frac{1}{p(m_i)} \quad (5)$$

Table 3. Information entropy of color images encryption.

Ciphertext image	Baboon.tiff	Plane.tiff	Boat.tiff
Encryption entropy (R)	7.9941	7.9929	7.9912
encryption entropy (G)	7.9952	7.9936	7.9927
encryption entropy (B)	7.9953	7.9891	7.9945

5.4. Analysis of the Key Sensitivity

The experimental results of the sensitivity testing for this algorithm key are shown in Figure 6. Figure 6-a) is the correct decryption image of Plane. Figures 6-b) and (c) respectively indicate the decryption images under the condition that the key remains fixed but the initial value X0 has an error of +10-12 or β has an error of +10-12. But this slight error in the initial key value will directly lead to significant changes in the decryption image, making it impossible to restore it back to the original image. It proves that the proposed algorithm has the strong key sensitivity, which is sufficient to ensure its resistance to the exhaustive attacks.



a) Decrypted plane. b) X0+10^{-12}. c) β+10^{-12}.

Figure 6. Experimental results of the key sensitivity.

5.5. Analysis of Resistance to Differential Attacks

Calculation formulas for the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) are as follows [20, 33].

$$R_{NPC} = \frac{1}{W \times H} \sum_{i=1}^{W} \sum_{j=1}^{H} D(i, j) \times 100\% \quad (6)$$

$$I_{UAC} = \frac{1}{W \times H} \sum_{i=1}^{W} \sum_{j=1}^{H} \frac{C1(i, j) - C2(i, j)}{255} \times 100\% \quad (7)$$

$$D(i,j) = \begin{cases} 0 \; if \; C1(i,j) = C2(i,j) \\ 1 \; if \; C1(i,j) \neq C2(i,j) \end{cases} \quad (8)$$

The predicted value of NPCR is 99.61% at a confidence level of 0.05, while the theoretical interval of UACI is (33.29%, 33.65%) [40]. Three encrypted pictures' NPCR and UACI values (R, G, and B) have been determined, and Table 4 presents the experimental findings. The NPCR, UACI, and mean values have all approximated their ideal predicted values, demonstrating the algorithm's strong effectiveness in fending off differential assaults.

Table 4. NPCR and UACI and their mean values of encrypted images.

Parameters	Encrypted images	Baboon.tiff	Plane.tiff	Boat.tiff
NPCR	R	99.6055	99.6008	99.6042
	G	99.6022	99.6011	99.5928
	B	99.5697	99.5544	99.5797
	RGB Mean	99.5924	99.5854	99.5922
UACI	R	33.4658	33.5601	33.4927
	G	33.4519	33.5688	33.4887
	B	33.4727	33.5029	33.4819
	RGB Mean	33.4635	33.5439	33.4878

5.6. Analysis of Encryption Response Time

The experimental hardware and software environment have been introduced at the beginning of this section. The algorithm in this paper has been compared with the methods proposed by Farah *et al*. [9] and Hua *et al*. [15], all of which have encrypted the same one 256×256 standard color image. Then the encryption response time of different algorithms have been recorded. Results are listed in Table 5, and obviously the algorithm proposed here has significant advantages in the encryption speed.

Table 5. Encryption time of this algorithm compared with others.

Algorithms	Encryption time (s)
Proposed in this paper	0.2136
Proposed by Farah *et al*. [9]	0.5203
Proposed by Hua *et al*. [15]	0.3927

By running different algorithms under the same conditions, the impact of hardware and software differences on encryption response time is eliminated, allowing for direct and accurate comparisons [6]. The listed times are all tested for the same 256×256 standard color image. In this way, this paper can objectively evaluate the performance advantages of the algorithm proposed in this paper over the algorithm in the reference, especially the significant improvement in encryption speed. This rigorous experimental design ensures the reliability and scientificity of the results.

6. Discussion and Future Work

Its effectiveness in maintaining the security of digital images is evident through the comprehensive experimental validation. However, the rapid advancement in computational capabilities and the emergence of quantum computing pose new challenges to conventional encryption methodologies.

The integration of Quantum Key Distribution (QKD) with classical encryption techniques could potentially enhance the security of our proposed algorithm by providing a theoretically secure channel for key exchange. The experimental results, as detailed in Tables 6, 7, 8, 9, and 10, underscore the effectiveness of our 2D Logistic chaotic system-based image encryption algorithm.

Table 6. Comparison of encryption speed.

Algorithm type	Encryption time (s)	Computational complexity
2D Logistic Chaotic System	0.2136	Moderate
Quantum-Enhanced Algorithm*	0.1500	High
*Assumed QKD Integration		

The encryption speed and computational complexity, as highlighted in Table 6, will be reassessed with the integration of QKD to ensure that the increased security does not come at the cost of performance

Table 7. Key sensitivity analysis.

Algorithm type	Sensitivity to key change	Resistance to exhaustive attacks
2D Logistic chaotic system	High	Moderate
Quantum-enhanced algorithm*	Very high	High
*Assumed QKD integration		

Building upon the key sensitivity analysis from Table 7, we will explore quantum-resistant modifications to the chaotic system to further fortify the algorithm against exhaustive attacks.

Table 8. Resistance to attacks.

Attack Type	2D Logistic chaotic system	Quantum-enhanced algorithm*
Differential attacks	Good	Excellent
Statistical attacks	Good	Excellent
Quantum computing attacks	Not applicable	Resistant
*Assumed QKD and post-quantum cryptography integration		

The resistance to various attacks, as demonstrated in Table 8, will be a critical parameter in evaluating the effectiveness of the quantum-enhanced algorithm, ensuring that it maintains or surpasses the current standards.

Table 9. Information entropy comparison.

Image	2Dl chaotic system	Quantum-enhanced algorithm*
Baboon.tiff	7.9941	7.9995
Plane.tiff	7.9929	7.9993
Boat.tiff	7.9912	7.9991
*Assumed optimization through quantum techniques		

The entropy values detailed in Table 9 indicate the level of randomness in the encrypted images. We will aim to optimize the quantum-enhanced algorithm to achieve an even distribution, thereby enhancing its resistance to statistical attacks.

Table10. Resource utilization.

Resource	2D logistic chaotic system	Quantum-enhanced algorithm*
Processing power	Low to Moderate	High
Memory usage	Low	Moderate to High
Bandwidth for key exchange	Not Applicable	High (due to QKD)
*Assumed optimization through quantum techniques		

Finally, as shown in Table 10, the resource utilization of our current algorithm is within acceptable limits. The integration of quantum technologies will be carefully managed to ensure that the increase in security does not lead to prohibitive resource demands.

With the rapid development of quantum computing capabilities, cryptographic techniques, including the image encryption, will inevitably be constantly innovated. Future work will focus on integrating QKD with our 2D Logistic chaotic system-based algorithm, aiming to embed a quantum-resistant layer that fortifies the encryption against state-of-the-art threats, including quantum attacks. Additionally, we will delve into quantum-resistant alterations to the chaotic system to augment the algorithm's robustness against exhaustive attacks and refine the algorithm to ensure a uniform distribution of information entropy, thereby strengthening its defenses against statistical attacks. As we look ahead, the integration of quantum technologies and ongoing algorithmic enhancements will not only sustain the exceptional performance of our encryption system but also guarantee its enduring relevance amidst the ever-evolving cryptographic landscape.

7. Conclusions

The research culminates in the successful development of an efficient image encryption algorithm grounded in the 2D Logistic chaotic system, showcasing its prowess in securing digital images through innovative pixel manipulation techniques. With an encryption time of 0.2136 seconds for a 256×256 color image and information entropy values close to the ideal, the algorithm exemplifies both speed and security, adeptly withstanding a barrage of attacks, from differential to statistical. The proposed integration of QKD signals a future where the algorithm could be fortified against even the most sophisticated cryptographic challenges, including quantum computing. Ongoing work will concentrate on quantum-resistant adaptations and entropy distribution optimization to further enhance resilience. In essence, this research not only cements the 2D Logistic chaotic system as a formidable tool in cryptographic applications but also sets a clear trajectory for its evolution, ensuring its enduring impact and relevance in the vanguard of digital security.

DataF Availability Statements

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Acknowledgment

The research work of this paper has been supposed by the Advanced Talent Research Fund of Wanxi University (Approval No. WGKQ2021050, WGKQ2022004) and the Horizontal Project (Authorization No. HX2022 WYBSDQ, HX2022 WYBCGG); the Open Fund of Anhui Undergrowth Crop Intelligent Equipment Engineering Research Center (AUCIEERC-202201); Anhui Undergrowth Crop Intelligent Equipment Engineering Research Center（2022AH010091).

Conflict

All the authors confirm that they have no financial or non-financial competing interests with any companies, organizations, or individuals while preparing and submitting the manuscript.

References

[1] Alrubaie A., Khodher M., and Abdulameer A., "Image Encryption Based on 2DNA Encoding and Chaotic 2D Logistic Map," *Journal of Engineering and Applied Science*, vol. 70, no. 1, pp. 60, 2023. https://jeas.springeropen.com/articles/10.1186/s44147-023-00228-2

[2] Antunes J., Gupta R., Mukherjee Z., and Wanke P., "Information Entropy, Continuous Improvement, and US Energy Performance: A Novel Stochastic-Entropic Analysis for Ideal Solutions (SEA-IS)," *Annals of Operations Research*, vol. 313, no. 1, pp. 289-318, 2022. https://ideas.repec.org/a/spr/annopr/v313y2022i1d10.1007_s10479-021-04428-y.html

[3] Chen C., Sun K., and Xu Q., "A Color Image Encryption Algorithm Based on 2D-CIMM Chaotic Map," *China Communications*, vol. 17, no. 5, pp. 12-20, 2020. https://ieeexplore.ieee.org/document/9103913

[4] Darani A., Yengejeh Y., Pakmanesh H., and Navarro G., "Image encryption Algorithm Based on a New 3D Chaotic System Using Cellular Automata," *Chaos, Solitons and Fractals*, vol. 179, pp. 114396, 2024. https://doi.org/10.1016/j.chaos.2023.114396

[5] Demirtas M., "A New RGB Color Image Encryption Scheme Based on Cross-Channel

Pixel and Bit Scrambling Using Chaos," *Optik*, vol. 265, pp. 169430, 2022. https://doi.org/10.1016/j.ijleo.2022.169430

[6] Elazzaby F., Elakkad N., and Sabour K., "The Coupling of a Multiplicative Group and the Theory of Chaos in the Encryptions of Images," *The International Arab Journal of Information Technology*, vol. 21, no. 1, pp. 1-16, 2024. DOI:10.34028/iajit/21/1/1

[7] Elkandoz M. and Alexan W., "Image Encryption Based on a Combination of Multiple Chaotic Maps," *Multimedia Tools and Applications*, vol. 81, no. 18, pp. 25497-25518, 2022. https://doi.org/10.1007/s11042-022-12595-8

[8] Elkandoz M., Alexan W., and Hussein H., "3D Image Steganography Using Sine Logistic Map and 2D Hyperchaotic Map," *in Proceedings of the International Conference on Electrical and Computing Technologies and Applications*, Ras Al Khaimah, pp. 1-6, 2019. https://ieeexplore.ieee.org/document/8959700

[9] Farah M., Guesmi R., Kachouri A., and Samet M., "A Novel Chaos Based Optical Image Encryption Using Fractional Fourier Transform and DNA Sequence Operation," *Optics and Laser Technology*, vol. 121, pp. 105777, 2020. https://doi.org/10.1016/j.optlastec.2019.105777

[10] Fotsing J., Moukam Kakmeni J., Tiedeu A., and Fotsin H., "Image Encryption Algorithm Based on 2D Logistic Map System in IoHT Using 5G Network," *Multimedia Tools and Applications*, vol. 83, no. 10, pp. 30819-30845, 2024. https://link.springer.com/article/10.1007/s11042-023-16730-x

[11] Gu L. and Chen G., "Chi-Square Linear Trend Test and SPSS Software Implementation," *Preventive Medicine*, vol. 36, no. 1, pp. 89-90, 2024. http://www.zjyfyxzz.com/EN/abstract/abstract2810.shtml

[12] Guo Z., Ren J., Liu B., Zhong Q., Li Y., Mao Y., Wu X., Xia W., Song X., Chen S., Tu B., and Wu Y., "Sliced Chaotic Encrypted Transmission Scheme Based on Key Masked Distribution in a W-Band Millimeter-Wave System," *Optics Express*, vol. 32, no.11, pp. 19019-19033, 2024. https://opg.optica.org/oe/fulltext.cfm?uri=oe-32-11-19019&id=549991

[13] Hosny K., Kamal S., and Darwish M., "A Color Image Encryption Technique Using Block Scrambling and Chaos," *Multimedia Tools and Applications*, vol. 81, no. 1, pp. 505-525, 2022. https://doi.org/10.1007/s11042-021-11384-z

[14] Hosny K., Kamal S., and Darwish M., "A Novel Color Image Encryption Based on Fractional Shifted Gegenbauer Moments and 2D Logistic-Sine Map," *The Visual Computer*, vol. 39, no. 3, pp. 1027-1044, 2023. https://link.springer.com/article/10.1007/s00371-021-02382-1

[15] Hua Z., Zhou Y., Pun C., and Chen C., "2D Sine Logistic Modulation Map for Image Encryption," *Information Sciences*, vol. 297, pp. 80-94, 2015. https://doi.org/10.1016/j.ins.2014.11.018

[16] Huang H., "Novel Scheme for Image Encryption Combining 2D Logistic-Sine-Cosine Map and Double Random-Phase Encoding," *IEEE Access*, vol. 7, pp. 177988-177996, 2019. https://ieeexplore.ieee.org/document/8928566

[17] Jiang M. and Yang H., "Image Encryption Using a New Hybrid Chaotic Map and Spiral Transformation," *Entropy*, vol. 25, no. 11, pp. 1-19, 2023. https://www.mdpi.com/1099-4300/25/11/1516

[18] Jiang Z. and Liu X., "Image Encryption Algorithm Based on Discrete Quantum Baker Map and Chen Hyperchaotic System," *International Journal of Theoretical Physics*, vol. 62, no. 2, pp. 26-32, 2023. https://link.springer.com/article/10.1007/s10773-023-05277-0#citeas

[19] Kaur G., Agarwal R., and Patidar V., "Color Image Encryption Scheme Based on Fractional Hartley Transform and Chaotic Substitution-Permutation," *The Visual Computer: International Journal of Computer Graphics*, vol. 38, no. 3, pp. 1027-1050, 2022. https://link.springer.com/article/10.1007/s00371-021-02066-w

[20] Kesenheimer E., Wendebourg M., Weigel M., Weidensteiner C., Haas T., Richter L., Sander L., Horvath A., Barakovic M., Cattin P., Granziera C., Bieri O., and Schlaeger R., "Normalization of Spinal Cord Total Cross-Sectional and Gray Matter Areas as Quantified With Radially Sampled Averaged Magnetization Inversion Recovery Acquisitions," *Frontiers in Neurology*, vol. 25, no. 12, pp. 637198, 2021. https://pubmed.ncbi.nlm.nih.gov/33841307/

[21] Li C., "Information Entropy Algorithm for Image and Video Signal Processing," *Advances in Computer, Signals and Systems*, vol. 6, no. 4, pp. 1-5, 2022. https://clausiuspress.com/article/4281.html

[22] Li C., Luo G., and Li C., "A Parallel Image Encryption Algorithm Based on Chaotic Duffing Oscillators," *Multimedia Tools and Applications*, vol. 77, no. 15, pp. 19193-19208, 2018. https://link.springer.com/article/10.1007/s11042-017-5391-5

[23] Li H., Yu S., Feng W., Chen Y., Zhang J., Qin Z., Zhu Z., and Wozniak M., "Exploiting Dynamic Vector-Level Operations and a 2D-Enhanced Logistic Modular Map for Efficient Chaotic Image Encryption," *Entropy*, vol. 25, no. 8, pp. 28-36, 2023. https://doi.org/10.3390/e25081147

[24] Li X., Yu C., and Guo J., "Multi-Image Encryption Method via Computational Integral Imaging Algorithm," *Entropy*, vol. 24, no. 7, pp. 996, 2022. https://doi.org/10.3390/e24070996

[25] Liang Y., Luo Y., Zhang S., "Review of chaotic image Encryption Based on Compressed Sensing," *Journal of Guangxi Normal University*, vol. 40, no. 5, pp. 49-58, 2022. DOI:10.16088/j.issn.1001-6600.2022012003

[26] Lin J., "Measuring and Analyzing the Information Entropy Value of Key Audit Matters (KAMs) Disclosure at the System and Reporting Scale," *Heliyon*, vol. 10, no. 1, pp. 23255-23262, 2024. https://www.sciencedirect.com/science/article/pii/S2405844023104634

[27] Liu G. and Wu Q., "Improved Logistic Chaotic Mapping and its Application in Image Encryption and Hiding," *Journal of Electronics and Information Technology*, vol. 44, no. 10, pp. 3602-3609, 2022. DOI:10.11999/JEIT210763

[28] Liu L., Zhang L., Jiang D., Guan Y., Zhang Z., "A Simultaneous Scrambling and Diffusion Color Image Encryption Algorithm Based on Hopfield Chaotic Neural Network," *IEEE Access*, vol. 7, pp. 185796-185810, 2019. https://ieeexplore.ieee.org/document/8937765

[29] Liu S., Li C., and Li Y., "A Novel Image Encryption Algorithm Based on Exponent-Cosine Chaotic Mapping," *Journal of Electronics and Information Technology*, vol. 44, no. 5, pp. 1754-1762, 2022. https://jeit.ac.cn/en/article/doi/10.11999/JEIT210270

[30] Lyle M., Sarosh P., and Parah S., "Adaptive Image Encryption Based on Twin Chaotic Maps," *Multimedia Tools and Applications*, vol. 81, no. 6, pp. 8179-8198, 2022. https://doi.org/10.1007/s11042-022-11917-

[31] Masood F., Driss M., Boulila W., Ahmad J., Rehman S., Jan S., Qayyum A., and Buchanan W., "A Lightweight Chaos-based Medical Image Encryption Scheme Using Random Shuffling and XOR Operations," *Wireless Personal Communications*, vol. 127, no. 2, pp. 1405-1432, 2022. https://doi.org/10.1007/s11277-021-08584-z

[32] Niu Y. and Zhang X., "Image Encryption Method Based on Filling Curve and Adjacent Pixel Bit Scrambling," *Journal of Electronics and Information*, vol. 44, no. 3, pp. 1137-1146, 2022. DOI:10.11999/JEIT210023

[33] Niwa T., Torii I., and Ishii N., "Line-of-Sight Detection Using Center of Gravity with Pixel Number Variation," *International Journal of Software Innovation*, vol. 5, no. 3, pp. 64-76, 2017. DOI:10.4018/IJSI.2017070105

[34] Norouzi B. and Mirzakuchaki S., "A Fast Color Image Encryption Algorithm Based on Hyper-Chaotic Systems," *Nonlinear Dynamics*, vol. 78, no. 2, pp. 995-1015, 2014. https://link.springer.com/article/10.1007/s11071-014-1492-0

[35] Qu L., Li M., Sun Y., Su S., Liu Y., and Zhang L., "Security Analysis of a Reversible Data Hiding Scheme in Encrypted Images by Redundant Space Transfer," *Journal of King Saud University-Computer and Information Sciences*, vol. 36, no. 1, pp. 101914, 2024. https://doi.org/10.1016/j.jksuci.2024.101914

[36] Ren Q., Teng L., Jiang D., Si R., andWang X., "Visual Image Encryption Algorithm Based on Compressed Sensing and 2D Cosine -Type Logistic Map," *Physica Scripta*, vol. 98, no. 9, pp. 56-63, 2023. DOI:10.1088/1402-4896/aceb24

[37] Rohhila S. and Singh A., "Deep learning-based Encryption for Secure Transmission Digital Images: A Survey," *Computers and Electrical Engineering*, vol. 116, pp. 109236, 2024. https://doi.org/10.1016/j.compeleceng.2024.109236

[38] Setiadi D. and Rijati N., "An Image Encryption Scheme Combining 2D Cascaded Logistic Map and Permutation-Substitution Operations," *Computation*, vol. 11, no. 9, pp. 1-18, 2023. https://doi.org/10.3390/computation11090178

[39] Wang Z., Zhuang J., Ye S., Xu N., Xiao J., and Peng C., "Image Restoration Quality Assessment Based on Regional Differential Information Entropy," *Entropy*, vol. 25, no. 1, pp. 1-16, 2023. https://www.mdpi.com/1099-4300/25/1/144

[40] Wu Y., Noonan J., and Agaian S., "NPCR and UACI Randomness Tests for Image Encryption," *Journal of Selected Areas in Telecommunications*, vol. 1, no. 2, pp. 31-38, 2011. https://www.cyberjournals.com/Papers/Apr2011/05.pdf

[41] Yang F., An X., and Xiong L., "A New Discrete Chaotic Map Application in Image Encryption Algorithm," *Physica Scripta*, vol. 97, no. 3, pp. 035202, 2022. DOI:10.1088/1402-4896/ac4fd0

[42] Zhang B. and Liu L., "Chaos-Based Image Encryption: Review, Application, and Challenges," *Mathematics*, vol. 11, no. 11, pp. 2585, 2023. https://doi.org/10.3390/math11112585

[43] Zhang F., Zhang X., Cao M., Ma F., and Li Z., "Characteristic Analysis of 2D Lag-Complex Logistic Map and Its Application in Image Encryption," *IEEE MultiMedia*, vol. 28, no. 4, pp. 96-106, 2021. DOI:10.1109/MMUL.2021.3080579

[44] Zhang H. and Hu H., "An Image Encryption Algorithm Based on a Compound-Coupled Chaotic System," *Digital Signal Processing*, vol. 146, pp. 104367, 2024. https://doi.org/10.1016/j.dsp.2023.104367

[45] Zhang H., Hu H., and Ding W., "Image Encryption Algorithm Based on Hilbert Sorting Vector and New Spatiotemporal Chaotic System," *Optics and Laser Technology*, vol. 167, pp.

109655, 2023. https://doi.org/10.1016/j.optlastec.2023.109655

[46] Zhang X., Liu G., and Di J., "An Image Encryption Scheme Based on the Four-Dimensional Chaotic System and the Mealy Finite State Machine," *Physica Scripta*, vol. 99, no. 5, pp. 11-16, 2024. https://iopscience.iop.org/article/10.1088/1402-4896/ad3487

Yuebo Wu was born in Chaohu, Anhui, P.R. China, in 1980. He received the Doctor degree from Xiamen University, P.R. China. Now, he works in School of Electrical and Photoelectronic Engineering, West Anhui University.

Shiwei Chu was born in Hefei, Anhui Province, is a doctoral student at the School of Electronic Information Engineering, Anhui University. He holds the title of Senior Engineer and his main research interests include General Artificial Intelligence, Electronic Information, Quantum Technology, and more.

Huifang Bao was born in Tongling, Anhui, P.R. China, in 1992. She received the Master degree from University of Science and Technology of China, P.R. China. Now, she works in School of Electrical and Photoelectronic Engineering, West Anhui University. Her research interests include path planning, intelligent decision-making and signal processing.

Duansong Wang was born in Jining, P.R. China, in 1990. He received the Doctor degree from Harbin Engineering University, P.R. China. Now, He works in School of Electrical and Photoelectronic Engineering, West Anhui University. His research interests include Intelligent Ship Control and Agricultural Intelligent Equipment Control Technology.

Jian Zhou was born in Lingbi, Anhui, P.R. China, in 1977. He received the Doctor degree from South China Normal University, P.R. China. Now, he works in School of Electrical and Photoelectronic Engineering, West Anhui University. His research interest include Quantum Computing and Superconducting Circuits.