ENHANCED KNOWLEDGE IN SCIENCES AND TECHNOLOGY
e-ISSN: 2773-6385

EKST

Vol. 5 No. 1 (2025) 47-56
https://publisher.uthm.edu.my/periodicals/index.php/ekst

Simulation of Image Encryption Scheme for Secure Data Transmission Based on Logistic Map

Elisa Qian Ru Dragon[1], Kek Sie Long[1*]

[1] *Department of Mathematics and Statistics, Faculty of Applied Sciences and Technology, UTHM Kampus Cawangan Pagoh, Hab Pendidikan Tinggi Pagoh, KM 1, Jalan Panchor, 84600 Pagoh, Muar, Johor, MALAYSIA.*

*Corresponding Author: slkek@uthm.edu.my
DOI: https://doi.org/10.30880/ekst.2025.05.01.007

Article Info

Received: 30 December 2024
Accepted: 17 January 2025
Available online: 30 July 2025

Keywords

Image Encryption, Chaotic System, Logistic Map, Security Analysis, Information Entropy

Abstract

This paper proposes an image encryption scheme based on a logistic map for secure data transmission. The logistic map offers unique properties, including sensitivity to initial conditions, system parameters, and pseudo-randomness, making them ideal for secure encryption. Hence, the parameter ranges causing the chaotic behaviour are determined, and the logistic map solution sequences are appropriately generated. The encryption process requires pixel permutation, key generation using chaotic sequences, and applying the XOR (exclusive OR) operations to the encrypted pixels in binary. Two sets of images are studied to illustrate the encryption scheme. The encryption performance is evaluated through histogram uniformity, entropy analysis, correlation coefficient evaluation, and encryption and decryption speed across various image datasets. The simulation results showed strong encryption capabilities, effectively masked original image content and reduced correlations among adjacent pixels. The encrypted image entropy value approaches the ideal value of eight, indicating high randomness and security. Thus, the logistic map provides efficient encryption performance, completing the encryption process in reasonable time frames suitable for real-time applications while maintaining high security. In conclusion, a logistic map is a practical tool for creating secure image encryption schemes due to its unpredictability and adaptability.

1. Introduction

A digital image is a visual picture in a digital format that we can store, process and transmit through electronic devices, such as computers and digital cameras. Digital images are composed of tiny picture elements called pixels, and each pixel has specific information on colour and brightness, which is expressed in numerical values for red, green and blue (RGB) for colour images or in grayscale intensity for black-and-white images [1]. The resolution of a digital image is the number of pixels the image contains in a unit of length [2]. Thus, a high-quality image will have a higher resolution. With their compression methods and quality characteristics, various file formats, such as JPEG and PNG, are used to store digital images. Thus, these formats can encode and compress image data for storage and transmission purposes [3].

With the increasing use of digital images, the confidentiality and integrity of images during transmission are highly concerning. Data transmission, which involves sending and receiving data between devices, is crucial in the digital era. It enables accessible communication and information exchange across global networks. Because of this, encryption techniques are actively developed to provide a robust means to secure sensitive image data from unauthorized access and tampering [4]. [5] addressed safeguarding ample data privacy throughout the data

storage phase and suggested a searchable encryption system that satisfies personalized privacy requirements. Fang [6] presented a new technique for image encryption that uses a digital redesign sliding mode controller and chaotic synchronization. This approach aims to improve image encryption and data transfer security. Traditional encryption methods with fixed-length keys are vulnerable to brute-force attacks [7], while modern methods with variable key lengths provide enhanced security [8].

Chaotic maps are defined as an evolution function exhibiting chaotic behaviour and can be parameterized by a discrete-time or a continuous-time parameter. Chaotic maps, such as logistic and quadratic maps derived from chaotic dynamic systems, show sensitivity to initial conditions, pseudo-randomness, and deterministic behaviour [9]. The one-dimensional chaotic maps have been used extensively because of their simple structure and convenience [10]. With these properties, chaotic maps are considered suitable for developing encryption schemes to process extensive image data, providing high-security efficiency. Moreover, image encryption schemes can use chaotic maps for key generation, data permutation, and diffusion operations [11]. The computational complexity and robustness of the encryption scheme under various scenarios, for example, different image types, key sizes and encryption parameters, are assessed through simulation. Thus, optimizing the encryption scheme's performance, namely security and efficiency, will validate the scheme's suitability for secure data transmission.

Therefore, using images for secure data transmission motivates us to investigate the efficiency of logistic map in designing an image encryption scheme. We identify types of logistic map and discuss their solution. Then, the image encryption scheme simulation with the solution of logistic map is delivered. This simulation measures the scheme's performance to verify its efficiency. In addition, three objectives of the study are established. First, to design an image encryption scheme for simulating an image data transmission using the logistic map. Second, to identify the parameter ranges for the appearance of chaotic behaviour in the logistic map. Third, to evaluate the performance of the image encryption with the logistic map for a secret key generation by histogram analysis. The entropy analysis, the speed performance test and the correlation coefficient analysis are also conducted to verify the performance of the image encryption scheme.

2. Research Methods

Consider an $m \times n$ pixel image matrix,

$$P = \begin{bmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \ddots & \vdots \\ p_{m1} & \cdots & p_{mn} \end{bmatrix}, \tag{1}$$

with m rows and n columns of pixels. Each pixel in an image can be represented by its colour value, such as RGB (red, green, blue) or grayscale, which is in a single value ranging from 0 to 255. Assume the encryption key generated by a modular arithmetic is given by

$$a = b \mod m, \tag{2}$$

where a is the remainder when b is divided by m, b is the dividend, which is the number being divided, and m is the modulus, which is the divisor setting the range of possible remainders.

Denote the encryption key as

$$K = [k_1, \cdots, k_q], \tag{3}$$

where $k_1, \ldots, k_q$ *are the key elements, either in binary or decimal form,* q *is the total number of pixels expressed by* $q = m \times n$*. Hence, the image encryption using the XOR (exclusive OR) operation is given by*

$$P' = \overline{P} \oplus K, \tag{4}$$

where P' is the encrypted pixel and $\overline{P}$ is the original pixel in an array form. Here, $\oplus$ is the XOR operation, which is a logical operation that outputs true only when the inputs differ. Therefore, the problem described is known as an image encryption problem.

2.1 Logistic Map

The logistic map is a one-dimensional discrete chaotic map frequently used in various applications due to its simple representation, efficient implementation, and good dynamic behaviour [12]. The mathematical definition of the logistic map is given by

$$x_{i+1} = r x_i (1 - x_i), \tag{5}$$

where x_i is the state variable, ranging from 0 to 1, and i is the number of time steps, for $i = 0, 1, \ldots, n$, while x_0 is the initial value bounded between 0 to 1. The parameter r is the model parameter value represented the growth rate of the logistic map, ranging from 0 to 4. However, a logistic map presents the chaotic behaviour only when the model parameter r taking the values from 3.567 to 4.

Enhanced Knowledge in Sciences and Technology Vol. 5 No. 1 (2025) p. 47-56

2.2 Encryption and Decryption Procedures

The image encryption procedure [13] is summarized as follows.

Step 1: Generate the chaotic values from a logistic map model.
Generate the chaotic values x_i using the logistic map (5).

Step 2: Scale the chaotic values.
Convert the chaotic values x_i into integers x_i' in the range [0, 255] by multiplying by 255. That is,

$$x_i' = x_i \times 255. \tag{6}$$

Step 3: Load the image matrix.
Read the image, extract and put its pixels into a matrix form P_m.

Step 4: Flatten the image array.
Convert the image matrix into a flat array P_a.

Step 5: Generate a key.
Apply the modular arithmetic (2) to generate a sequence of keys from

$$k_i = x_i' \mod 255. \tag{7}$$

Step 6: Encrypt the pixels.
Use the XOR operation to each pixel value with the corresponding value from the pseudo-random sequence from

$$P_a' = P_a \oplus K. \tag{8}$$

Step 7: Save the encrypted image.
Convert the encrypted pixels values back to an image matrix P_m'.

Step 8: Decryption process.
Use the XOR operation to the encrypted pixel values with the same pseudo-random sequence from

$$P_m = P_m' \oplus x_i'. \tag{9}$$

Here, it is remarked that

(a) In Step 2, we generate the pseudo-random sequence for encryption.
(b) In Step 6, we convert the pixels and the keys from decimal to binary, then apply the XOR operation to the encrypted pixels in binary. After this, convert the binary encrypted pixels back into decimals.

2.3 Entropy Analysis

The information entropy is used to assess the degree of uncertainty or unpredictability of a variable in an image [14]. This method of information entropy enables us to obtain a critical understanding of the characteristics of randomness and variability. Thus, we can learn the distribution and information content of the image's pixels by using the following equation,

$$E = \sum_{i=1}^{N} P(i) \log\left(\frac{1}{P(i)}\right), \tag{10}$$

where N represents the total number of symbols presented in the image, and $P(i)$ denotes the probability of pixel intensity value i, for $i = 1, 2, \ldots, 256$. A higher entropy value expresses higher security when it is used to assess image encryption. An entropy value extremely near the ideal value of eight (8) is secure against a brute-force attack and gives robust and effective encryption [15-17].

2.4 Correlation Coefficient Analysis

The relation among pixels measures the performance of an image encryption algorithm [12]. A good encryption algorithm should hide this relationship, which attackers find hard to analyse an encrypted image. The definition and measurement of the correlation coefficient (r_{xy}) between the adjacent pixels are shown by

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{11}$$

with

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

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

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

where x_i and y_i represent the pixels and neighbouring pixels of the original and encrypted image, N is the entire number of x and y obtained from an image, $\mathrm{cov}(x,y)$ is the covariance between x_i and y_i, $D(x)$ and $D(y)$ are the variance of x_i and y_i, $E(x)$ is the mean of x_i and $E(y)$ is the mean of y_i.

The correlation coefficient value ranges from -1 to 1, indicating the strength of the relationship between the two variables. For example, in a plain image, the correlation value is positive 1 or close to 1, which means that the correlation of a pixel to its neighbouring pixel is very closely related or has a strong relationship. Positive or negative values mean positive or negative relationships. A value of 0 means they have a weak relationship [18, 19].

The pixels next to each other pixel are very similar in a plain image. A suitable encryption method should scramble the image, so the pixels are no longer related. We can check this by looking at how pixels are related horizontally, vertically, and diagonally in both the original and encrypted images.

There are various types of simulation data techniques, each with its own advantages and limitations. Their effectiveness often depends on the specific characteristics of the data. Numerous previous studies have applied simulation methods combined with mathematical techniques across a wide range of disciplines worldwide [20–22].

3. Results and Discussion

In this study, we set the model parameter $r=3.89$ from the chaotic range, for the logistic map,

$$x_{i+1}=3.89x_i(1-x_i), \tag{12}$$

to generate the chaotic sequences. Fig. 1 shows the solution curve of the logistic map with the initial condition $x_0=0.5$ varying between 0 and 1.

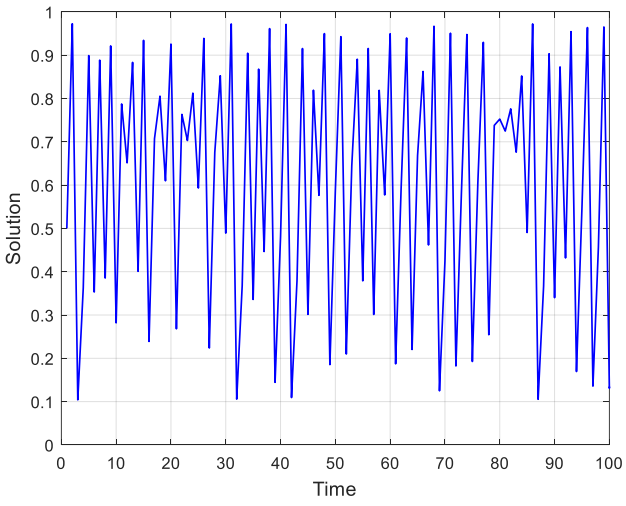
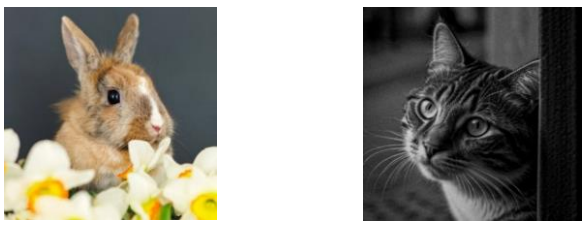


Fig. 1 The solution curve of the logistic map with $r=3.89$, $x_0=0.5$

3.1 Image Encryption

The plaintext images used, as shown in Fig. 2, are loaded into the system. Following this, we generate chaotic sequences by solving the logistic map. The sequence is scaled to the range [0, 255] to match the intensity levels of the image pixels.

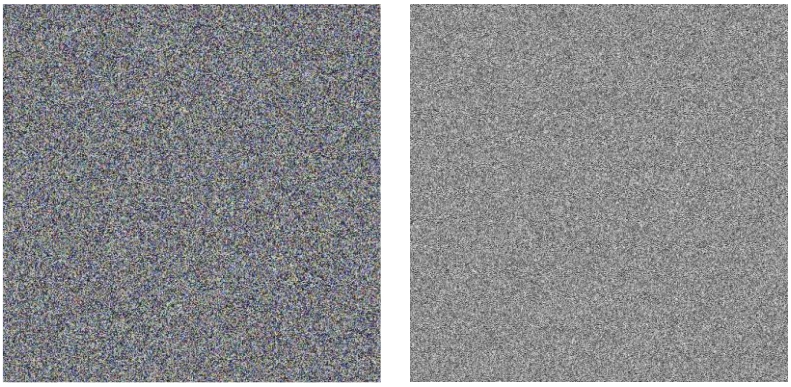


(a) (b)

Fig. 2 Plain Images used in simulation (a) Rabbit; (b) Cat

Enhanced Knowledge in Sciences and Technology Vol. 5 No. 1 (2025) p. 47-56

In the encryption phase, we iterate through each image pixel, applying the XOR operation between the pixel value and the corresponding value from the chaotic sequence. The result is stored as the encrypted pixel value. The encrypted image is visualised to evaluate the level of distortion and apparent randomness, ensuring effectively masks the original image content. The encrypted images using the logistic map are shown in Fig. 3.

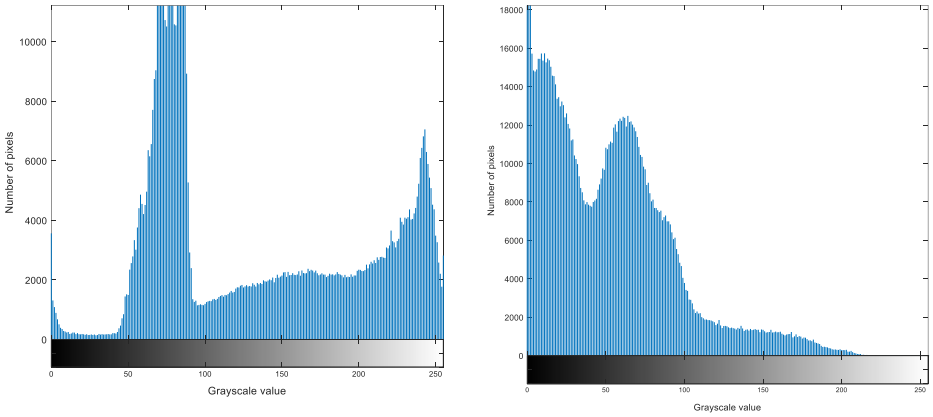


(a) (b)

Fig. 3 Encrypted images (a) Rabbit; (b) Cat

3.2 Histogram Analysis

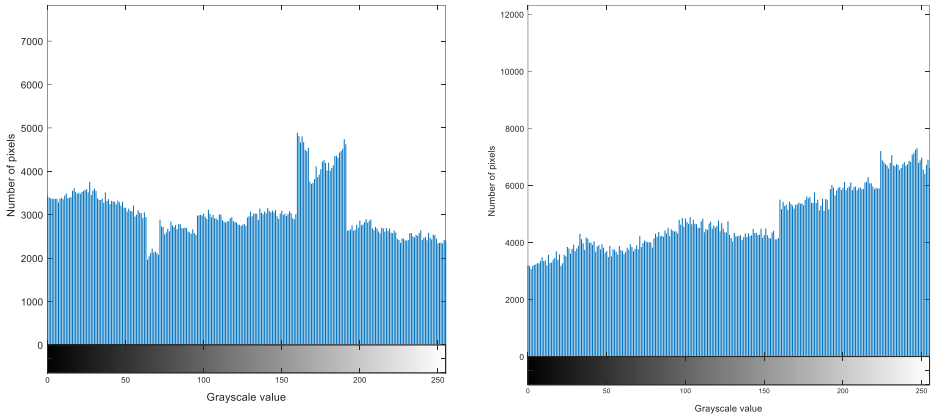
An image histogram is a fundamental tool for visualizing the statistical distribution of pixel values within an image. In an 8-bit colour and grayscale image, the range of pixel values is 0 to 255. Its shape can vary widely, ranging from normal to skewed or flat. A flat histogram, indicating a uniform frequency distribution, is a characteristic of secure and well-encrypted images, making it suitable for secure data transmission. Thus, we apply the histogram analysis to analyse and assess the quality of an image encryption by revealing pixel value distributions. Histograms of plain images (a) rabbit and (b) cat are shown in Fig. 4. The frequency distribution of pixels is not uniform, which does not show significant variation or a clear pattern.



(a) (b)

Fig. 4 Histograms of plain images (a) Rabbit; (b) Cat

After we perform the image encryption scheme using the logistic map, the results of the encrypted image for (a) rabbit and (b) cat presented in a uniform distribution in the interval [0, 255], as shown in Fig. 5. Hence, we can enhance data security by encrypting the images of (a) rabbit and (b) cat using the logistic map sequences during transmission.



(a) (b)

Fig. 5 Histograms of encrypted images (a) Rabbit; (b) Cat

3.3 Entropy Analysis

Entropy reflects the randomness of an image with values ranging from 0 to 8 for 256 grayscale levels. A high entropy value of nearly eight (8) shows significant randomness in the encrypted image, enhancing its security. Table 1 shows the local entropy of plain and encrypted images. The entropy values of encrypted images are higher than those of plaintext images, approaching the ideal eight (8) for entirely random images. Therefore, from these results of the entropy values, using the logistic map to the image encryption demonstrates the adaptability of the logistic map for a variety of datasets.

Table 1 Local entropy of plain and encrypted images

	Images	Dimensions	Local entropy of plain image	Entropy of encrypted image
(a)	Rabbit	512×512×3	7.3829	7.9756
(b)	Cat	640×640×1	7.0638	7.9639

3.4 Speed Performance Test

The encryption speed is a crucial component in assessing the performance of a cryptographic system [16]. Table 2 shows the result of the encryption and decryption speeds, demonstrating an effective approach to achieving both speed and security in data encryption. From the results, we notice that an image with a larger size and complexity takes longer to encrypt. Also, images with three colour channels, such as (a) rabbit, take longer to encrypt compared to single-channel images of similar sizes, highlighting the algorithm's sensitivity to the total number of pixels and the number of colour channels. The data also reveals that decryption without chaotic sequences is fast, predictable, and computationally efficient, as seen in the lower decryption times. In contrast, decryption with chaotic sequences is slower due to the added complexity of chaotic systems but offers enhanced security benefits, making it suitable for applications where security is prioritized over speed [17]. These findings demonstrate that while chaotic systems introduce additional computational overhead, they provide a robust framework for secure image encryption, particularly in scenarios where data security is critical.

Table 2 Encryption and decryption speed

Images		Dimensions	Encryption time (s)		Decryption time (s)	
			No Chaos	With Chaos	No Chaos	With Chaos
(a)	Rabbit	512 × 512 × 3	1.5078	2.7783	3.4947	5.4157
(b)	Cat	640 × 640 × 1	1.0986	2.0757	3.3239	5.2632

3.5 Correlation Coefficient Analysis

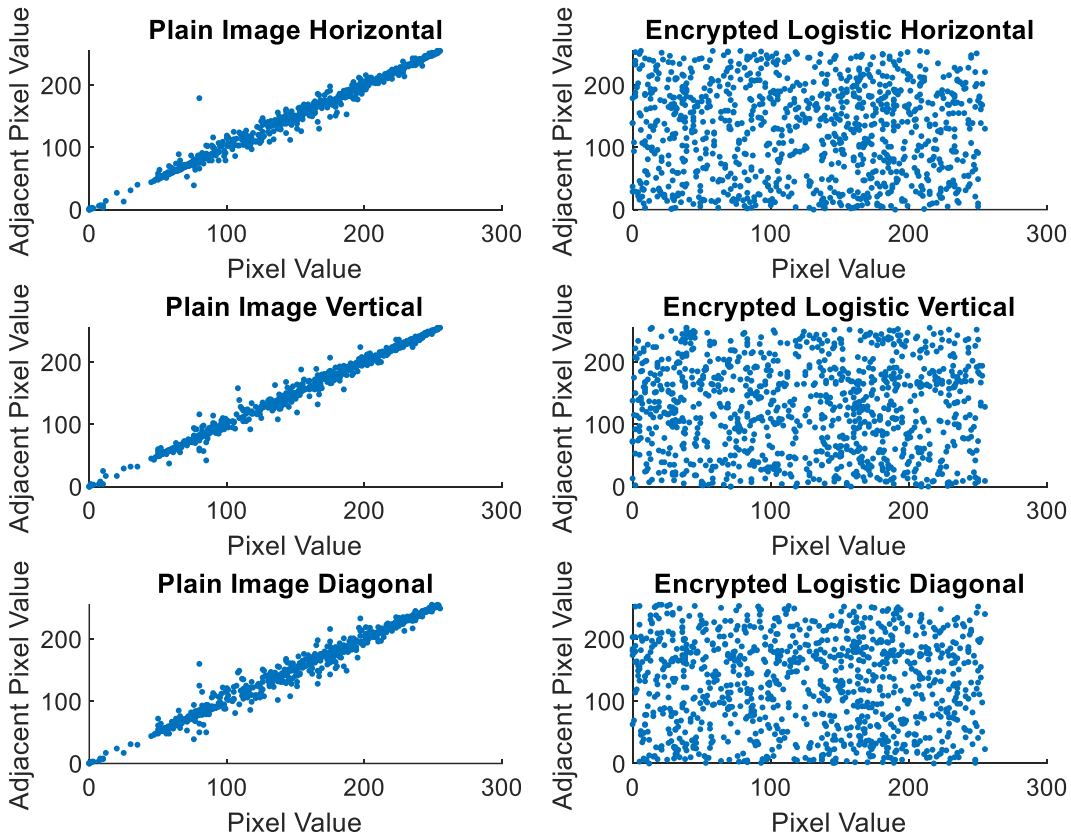
Table 3 shows correlation values of plain and encrypted images, using the logistic map, for the rabbit and cat images along the horizontal, vertical, and diagonal directions. The plain images have high correlation values close to 1 in all directions, pointing out strong pixel relationships. Correlation outcomes for encrypted images are typically around zero or slightly negative, indicating very few or no pixel correlations.

Enhanced Knowledge in Sciences and Technology Vol. 5 No. 1 (2025) p. 47-56

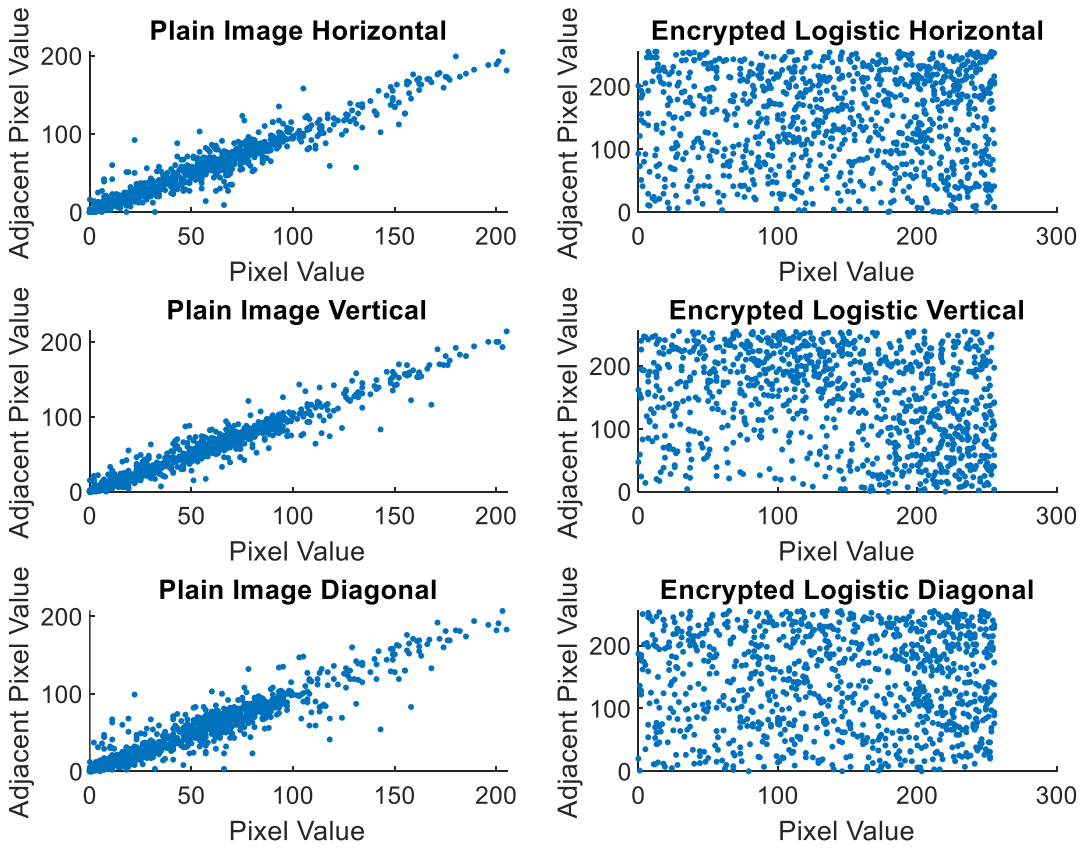
Table 3 Correlation coefficient results of plain and encrypted images in the horizontal, vertical and diagonal directions

	Images	Dimensions	Direction	Plain image	Encrypted image
(a)	Rabbit	512×512×3	Horizontal	0.9951	-0.0160
			Vertical	0.9963	-0.0225
			Diagonal	0.9929	-0.0373
(b)	Cat	640×640×1	Horizontal	0.9622	0.0047
			Vertical	0.9728	-0.2687
			Diagonal	0.9448	0.0051

Fig. 6 shows the random distribution of the plain and encrypted images, including those in a horizontal, vertical, and diagonal directions. The left column of the figure illustrates positive straight lines mean that the plain images have a strong linear relationship between adjacent pixel values in all directions. In contrast, for the right column of the figure, the pixel values of encrypted images are randomly distributed, with no apparent correlation in any direction.



(a)



(b)

Fig. 6 Schematic diagram of the horizontal, vertical and diagonal correlation coefficients between plain and encrypted images (a) Rabbit; (b) Cat

4. Conclusion

In this paper, the chaotic behaviour within the logistic map was accurately identified, ensuring proper implementation of the encryption process. The scheme was designed to shuffle pixel positions, enhancing randomness and improving resistance to cryptanalytic attacks. Experiments using rabbit and cat images confirmed the scheme's ability to mask original content, producing encrypted images with uniform pixel distributions and high entropy values close to the ideal, indicating near-perfect randomness. The correlation coefficient analysis showed minimal relationships between adjacent pixels in the encrypted images, highlighting the scheme's robustness. The findings in the study emphasized the logistic map's capability as a robust and efficient tool for practical applications in secure data transmission. In conclusion, the image encryption scheme based on the logistic map met the goals of security, efficiency and randomness, demonstrating its suitability for secure image data transmission. While this study validates the logistic map's potential for secure image transmission, future research could extend the scheme to larger, more diverse datasets, including high-resolution and domain-specific images. Exploring other chaotic systems, such as Henon or Lorenz maps, and applying the encryption to other multimedia data types, like video and audio, would enhance the scheme's applicability and provide broader insights.

Acknowledgement

The authors would like to thank the Faculty of Applied Sciences and Technology, Universiti Tun Hussein Onn Malaysia, for its support.

Conflict of Interest

Authors declare that there is no conflict of interests regarding the publication of the paper.

Author Contribution

The authors confirm contribution to the paper as follows: ***study conception and design:*** *Elisa Qian Ru Dragon, Kek Sie Long;* ***data collection:*** *Elisa Qian Ru Dragon;* ***analysis and interpretation of results:*** *Elisa Qian Ru Dragon, Kek Sie Long;* ***draft manuscript preparation:*** *Elisa Qian Ru Dragon, Kek Sie Long. All authors reviewed the results and approved the final version of the manuscript.*

References

[1] K. Agung, Fatmawati, and H. Suprajitno, "Image encryption based on pixel bit modification," Journal of Physics: Conference Series, vol. 1008, no. 1, pp. 012016, Apr. 2018, doi: 10.1088/1742-6596/1008/1/012016.

[2] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R. M. López-Gutiérrez, and O. R. Acosta Del Campo, "A RGB image encryption algorithm based on total plain image characteristics and chaos," Signal Processing, vol. 109, pp. 119–131, Apr. 2015, doi: 10.1016/j.sigpro.2014.10.033.

[3] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, "Secure medical data transmission model for IoT-based healthcare systems," IEEE Access, vol. 6, pp. 20596–20608, Mar. 2018, doi: 10.1109/ACCESS.2018.2817615.

[4] K. Rajeswari and D. Ghatge, "A review study on various image security techniques and emerging trends for visual data protection," Tuijin Jishu/Journal of Propulsion Technology, vol. 44, no. 3, pp. 4213-4237, 2023, doi: 10.52783/tjjpt.v44.i3.2310.

[5] S. Li, M. Li, H. Xu, and X. Zhou, "Searchable encryption scheme for personalized privacy in IoT-based big data," Sensors, vol. 19, no. 5, pp. 1059, Mar. 2019, doi: 10.3390/s19051059.

[6] J. S. Fang, J. S. H. Tsai, J. J. Yan, L. H. Chiang, and S. M. Guo, "Secure data transmission and image encryption based on a digital-redesign sliding mode chaos synchronization," Mathematics, vol. 10, no. 3, pp. 518, Feb. 2022, doi: 10.3390/math10030518.

[7] H. Kolivand, S. F. Hamood, S. Asadianfam, and M. S. Rahim, "Image encryption techniques: A comprehensive review," Multimedia Tools and Applications, vol. 83, no. 29, pp. 73789, Sep. 2024, doi: 10.1007/s11042-023-17896-0.

[8] M. SaberiKamarposhti, A. Ghorbani, and M. Yadollahi, "A comprehensive survey on image encryption: Taxonomy, challenges, and future directions," Chaos, Solitons & Fractals, vol. 178, pp. 114361, Dec. 2024, doi: 10.1016/j.chaos.2023.114361.

[9] U. Zia, M. McCartney, B. Scotney, J. Martinez, M. AbuTair, J. Memon, and A. Sajjad, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," International Journal of Information Security, vol. 21, no. 4, pp. 917–935, Aug. 2022, doi: 10.1007/s10207-022-00588-5.

[10] Y. Zhang, Y. Xiang, L. Y. Zhang, Y. Rong, and S. Guo, "Secure Wireless Communications Based on Compressive Sensing: A Survey," IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1093–1111, 2019, doi: 10.1109/COMST.2018.2878943.

[11] G. Ye, K. Jiao, X. Huang, B. M. Goi, and W. S. Yap, "An image encryption scheme based on public key cryptosystem and quantum logistic map," Scientific Reports, vol. 10, no. 1, pp. 21044, Dec. 2020, doi: 10.1038/s41598-020-78127-2.

[12] M. K. Khairullah, A. A. Alkahtani, M. Z. Bin Baharuddin, and A. M. Al-Jubari, "Designing 1D chaotic maps for fast chaotic image encryption," Electronics, vol. 10, no. 17, pp. 2116, Aug. 2021, doi: 10.3390/electronics10172116

[13] Y. Hu, and R. Tian, "Image encryption and decryption based on chaotic algorithm," Journal of Applied Mathematics and Physics, vol. 8, no. 9, pp. 1814-1825, Sep. 2020, doi: 10.4236/jamp.2020.89136.

[14] P. Ramasamy, V. Ranganathan, S. Kadry, R. Damaševičius, and T. Blažauskas, "An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic-tent map," Entropy, vol. 21, no. 7, pp. 656, Jul. 2019, doi: 10.3390/e21070656.

[15] R. Ge, G. Yang, J. Wu, Y. Chen, G. Coatrieux, and L. Luo, "A novel chaos-based symmetric image encryption using bit-pair level process," IEEE Access, vol. 7, pp. 99470-99480, Jul. 2019, doi: 10.1109/ACCESS.2019.2927415.

[16] S. Bhattacharjee, M. Gupta, and B. Chatterjee, "Time efficient image encryption-decryption for visible and COVID-19 X-ray images using modified chaos-based logistic map. Applied Biochemistry and Biotechnology, vol. 195, no. 4, pp. 2395–2413, Apr. 2023, doi: 10.1007/s12010-022-04161-7.

[17] H. Wen, Y. Lin, Z. Xie, and T. Liu, "Chaos-based block permutation and dynamic sequence multiplexing for video encryption," Scientific Reports, vol. 13, no. 1, pp. 14721, Sep. 2023, doi: 10.1038/s41598-023-41082-9.

[18] Lagak, N.E.A.P. and Mohamad M. (2023). Numerical Analysis of An Improved SIR Model For COVID-19 Outbreak in Malaysia Using Variational Iteration Method. Enhanced Knowledge in Sciences and Technology, 3 (2), 138-147.

[19] Fam, C.L. and Mohamad M. (2022). Technical Analysis of Malaysia Stock Performance, Enhanced Knowledge in Sciences and Technology, 2 (1), 332-341.
[20] [20] Bamahel A.S. (2022). Prevalence of Diabetic Nephropathy among Type 2 Diabetes Mellitus Patients in Mukalla City, Yemen. Enhanced Knowledge in Sciences and Technology, 2 (2), 432-440.
[21] Abd Rahman, S., Mohamad, M. and Shab N.F.M. (2021). The Modified Decomposition Method for Solving A Nonlinear System of Two-dimensional Volterra-Fredholm Integral Equation. Enhanced Knowledge in Sciences and Technology, 1 (2), 116-123.
[22] En, T.B. (2021). Prediction of Unemployment Rate in Malaysia Based on Macroeconomic Factors. Enhanced Knowledge in Sciences and Technology, 1 (2), 30-39.