The Visual Computer
https://doi.org/10.1007/s00371-025-04014-4

RESEARCH

Privacy Image Secrecy Scheme Based on Chaos-Driven Fractal Sorting Matrix and Fibonacci Q-Matrix

Liao Yunlong[1] · Lin Yiting[2,3] · Xing Zheng[1] · Yuan Xiaochen[1]

Accepted: 15 May 2025

Abstract
In the digital age, the proliferation of social media platforms has significantly increased public awareness of privacy security. The potential leakage of image privacy poses a grave threat as it can expose sensitive information and cause severe crises. To address this critical issue, this paper introduces an advanced privacy protection scheme that integrates chaos-driven Fractal Sorting Matrix (FSM) and Fibonacci Q-Matrix (FQM) techniques. The proposed scheme, known as the privacy image secrecy scheme based on chaos-driven FSM and FQM (PICFF), utilizes a 2D-LSM chaotic system to generate secure pseudo-random sequences for encryption. The FSM permutation technique, driven by chaos, effectively alters the positional information of the image, enhancing security through iterative and self-similar transformations. Additionally, the FQM encryption matrix, which traditionally employs static encryption, is dynamically enhanced by incorporating a chaotic system, ensuring strong correlation with the plaintext and further bolstering encryption reliability. Experimental validation demonstrates that the PICFF scheme excels in terms of information entropy and robustness. The encrypted images exhibit a uniform pixel distribution, reduced pixel correlation, and high information entropy, closely aligning with theoretical values. The scheme also showcases exceptional resistance to various attacks, including cropping attacks and salt-and-pepper noise, effectively preventing privacy information leakage and providing robust support for maintaining information security and enhancing privacy protection.

Keywords Image Encryption · Cryptography · Multimedia Security · Privacy Protection · Chaotic System

1 Introduction

In today's digital world, images have become integral carriers of information across diverse sectors such as healthcare, finance, e-commerce, and social media [5, 19, 22, 50]. However, the widespread use of digital images also raises significant security concerns, as these images often contain sensitive or private data that must be protected against unauthorized access or malicious exploitation [13, 20, 25, 48]. Traditional encryption algorithms, designed primarily for text-based data, are often inadequate when applied to images, which possess distinct characteristics such as high redundancy and intricate spatial correlations [8, 14, 31, 35]. These characteristics make images more susceptible to certain types of cryptographic attack, highlighting the urgent need for customized encryption techniques [15, 30, 36, 42]. Furthermore, as digital threats continue to evolve, more advanced and efficient methods are required to ensure the integrity and confidentiality of image data [4, 39, 53, 54]. The challenge lies not only in securing the data, but also in overcoming the intrinsic structural properties of images, such as pixel dependence and visual redundancy, that can expose vulnerabilities when improperly encrypted [7, 26, 33].

To address these challenges, a growing body of research has focused on developing specialized image encryption methods [3, 3, 45] that address the unique needs of image data security [6, 12, 38]. Among the most promising approaches are those that utilize chaotic systems, which are known for their inherent unpredictability and the ability to generate highly complex encryption keys [29, 47, 52]. At the same time, many scholars have also combined hash functions with chaotic systems[1, 2]. In 2023, Erkan et al.[11] introduces a novel 2D hyperchaotic system called the Schaf-

✉ Yuan Xiaochen
xcyuan@mpu.edu.mo

1 Macao Polytechnic University, Macao SAR, China

2 Guangdong Provincial/Zhuhai Key Laboratory of Interdisciplinary Research and Application for Data Science, Beijing Normal-Hong Kong Baptist University, Zhuhai, China

3 Department of Computer Science, Hong Kong Baptist University, Hong Kong, China

Published online: 29 May 2025

fer map, inspired by the Schaffer function known for its strict oscillation properties, aiming to meet high complexity requirements in applications like communication and multimedia encryption. The 2D Schaffer map's chaotic performance, evaluated with multiple indicators, shows superior ergodicity and erraticity. Its hyperchaotic performance in image encryption is due to its diversity. In 2024, Kocak et al. [18] proposed an image encryption scheme using a novel MILE map and PSO for key optimization. The map shows superior chaotic performance, and the scheme demonstrates excellent numerical and visual encryption results. In 2025, Toktas et al. [32] introduced the Cross-Channel Color Image Encryption algorithm using a 2D hyperchaotic hybrid map combining the Rastrigin and Griewank functions. The algorithm features high shuffling ability with diagonal permutation and bi-directional diffusion across RGB channels, enhancing resistance to cyberthreats. However, many existing image encryption systems are increasingly falling short in the face of the ever-changing big data era. For example, traditional encryption algorithms [27, 34, 49], while well-established and secure, often require extensive computation time and significant processing power, which can be a bottleneck in the fast-paced big data environment. As a result, remedial measures must be taken to improve the resilience of image encryption schemes [21, 24, 55, 56] against potential attacks by the cryptanalysis community in the future. This includes exploring more efficient and robust algorithms, integrating multiple layers of security, and performing detailed security analyzes [40, 41, 43] to ensure that image encryption systems can keep pace with the demands of the big data era the use of new technologies, such as the quantum field and deep learning [28].

In this paper, we propose a novel privacy image secrecy scheme that significantly enhances the security of traditional encryption methods. To address the issue of insufficient security in conventional schemes [37, 44, 47], we introduce the fractal sorting matrix (FSM) driven by a chaotic system. This innovative approach leverages the inherent unpredictability and complexity of chaotic systems to generate highly secure pseudo-random sequences, thereby strengthening the overall security of the encryption algorithm. Existing FSM algorithms face a significant issue: although they employ chaotic sequences to generate the initial sorting matrix, subsequent repeated permutations typically use the same iterative matrix derived from the initial matrix for positional changes. This introduces a risk of recover during the image encryption process. To address this, we propose grouping chaotic sequences to generate multiple initial sorting matrices, ensuring that each positional change differs from the previous one, thereby preventing recovey and enhancing unpredictability.

Additionally, current FQM algorithms often use a fixed number of iterations. However, for image encryption, the limited iteration count of FQM makes it vulnerable to brute-force attacks. To mitigate this, we integrate a chaotic system to dynamically determine the iteration count for each FQM operation, strengthening its nonlinearity and resistance to cryptanalysis.

By combining these two innovative strategies, our proposed scheme effectively mitigates the vulnerabilities associated with traditional encryption methods, providing a more secure and reliable solution to protect image privacy in the digital age.

2 Encryption Method

Privacy Image Secrecy Scheme Based on Chaos-Driven FSM and FQM (PICFF) utilizes chaos-driven FSM and FQM to process privacy images, and the flowchart of the process is shown in Fig. 1. Combining chaos with FSM can make the position transformation of images more unpredictable. The combination of FQM and confusion can change the pixel values of the images and make them more uniform, thereby balancing the information density.

The following sections will explain the relevant theories and the proposed scheme.

2.1 2D-LSM chaotic system

The 2D-LSM was proposed by Hua et al. [16] This chaotic system has excellent randomness and dynamical characteristics, which can provide sufficiently secure pseudo-random sequences for encryption schemes. The equation of this algorithm is defined as follows:

$$\begin{cases} x_{i+1} = \cos(4ax_i(1-x_i) + b\sin(\pi y_i) + 1) \\ y_{i+1} = \cos(4ay_i(1-y_i) + b\sin(\pi x_i) + 1) \end{cases} \tag{1}$$

where a and b are system's parameters. In the paper, set $a = 5, b = 5$, with initial values $x_0 = 0.1$, $y_0 = 0.2$, respectively. The phase diagram of the chaotic system under these parameters is shown in Fig. 2.

2.2 Fractal-Sorting Matrix

Xian et al. [46] proposed a FSM permutation technique for two-dimensional images. This technique utilizes iterativeness and self-similarity to effectively alter the positional information of the image. For the FSM of the n generation, it can be defined by the following formula:

$$A^n = \begin{bmatrix} 4 \times (A^1_{(1,1)} - 1) + A^{n-1} & 4 \times (A^1_{(1,2)} - 1) + A^{n-1} \\ 4 \times (A^1_{(2,1)} - 1) + A^{n-1} & 4 \times (A^1_{(2,2)} - 1) + A^{n-1} \end{bmatrix} \tag{2}$$

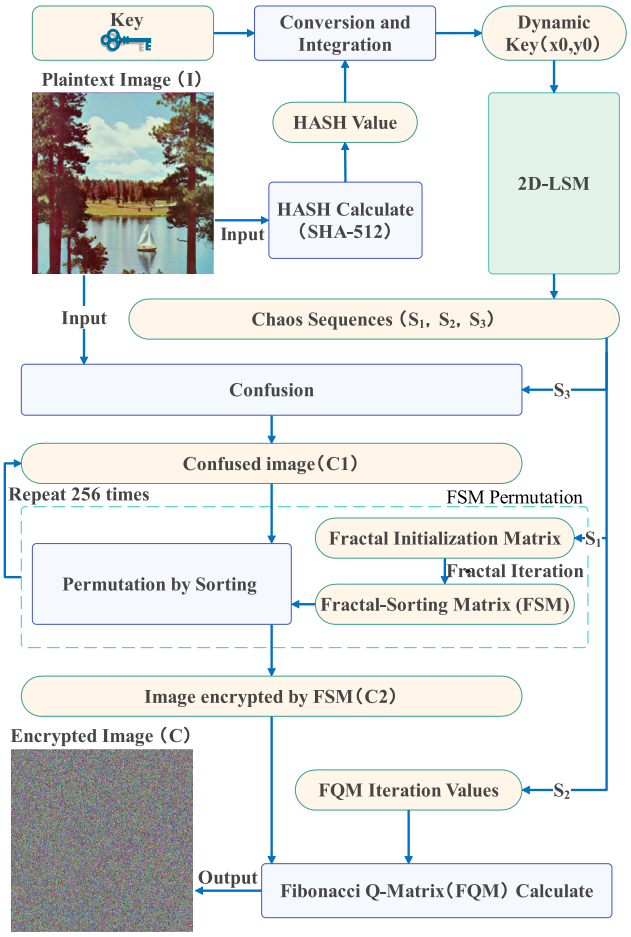

Fig. 1 Flowchart of the proposed PICFF

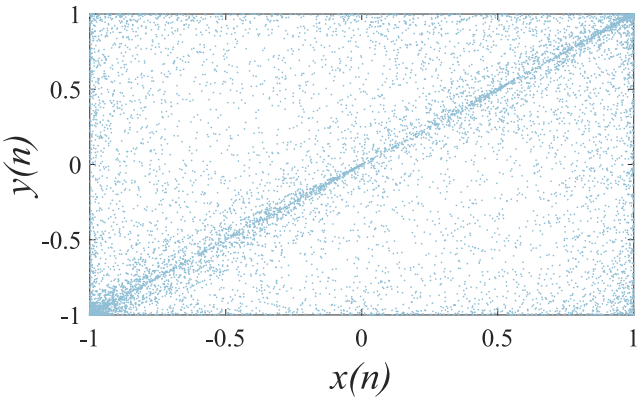

Fig. 2 Visualization of phase diagrams of 2D-LSM chaotic maps

where n represents the number of iterations, and the values of A^1 is as follows:

$$A^1 = \begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix} \tag{3}$$

In this algorithm, the value of A^1 will be generated by chaos driving.

2.3 Fibonacci Q-Matrix

FQM is an encryption matrix that utilizes the characteristics of the Fibonacci sequence. The FQM is difficult to reverse without the correct key, effectively preventing decryption operations. The Fibonacci sequence, denoted as F_n, is defined as follows:

$$F_n = F_{n-1} + F_{n-2}, \quad n > 1 \tag{4}$$

where $F_1 = F_2 = 1$. Therefore, the definition of Q^n used for encryption and Q^{-n} used for decryption is as follows:

$$Q^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}^n \tag{5}$$

$$Q^{-n} = \begin{bmatrix} F_{n-1} & -F_n \\ -F_n & F_{n+1} \end{bmatrix}^n \tag{6}$$

2.4 Encryption Steps

The following are the specific steps of the proposed PICFF:

Step 1: Calculate the hash value of the plaintext image using SHA-512. Then, take every 8 bits to form a new sequence T and calculate the number of bits in T, denoted as L. Next, convert T to decimal and divide it by 10^L to obtain the initial value x_s. Similarly, for the second group, obtain y_s. These are the initial values $x_0(0.1 + x_s)$ and $y_0(0.2 + y_s)$ for the 2D-LSM.

Step 2: The 2D-LSM outputs sequences S_1 and S_2, and the first 5000 values were discarded to ensure the chaotic effect. For the sequence S_1, we take 4 numbers at a time in order, calculate the sorting value for each group, and convert it into a 2×2 matrix as A^1.

Step 3: Take half of the sequence S_1 and half of sequence S_2 to form the sequence S_3, and then perform the following processing on S_3.

$$S_3 = \text{mod}(\text{floor}(S_3 \times 10^8), 256) \tag{7}$$

where the functions are defined as follows:

- $\text{mod}(x, y)$ computes the remainder of x divided by y.
- $\text{floor}(x)$ returns the greatest integer less than or equal to x.

Step 4: Use sequence S_3 to perform a Confusion operation on the plaintext image I is as follows:

$$C_1(i) = S_3(i) \oplus I(i) \quad i = 1, 2, \ldots, H \times W \tag{8}$$

where C_1 is confused image, H and W are the height and width of plaintext image I.

Step 5: According to the theory of FSM, iterate to obtain an index matrix of the same size as the plaintext image and use the following formula for reordering:

$$C_2(A^n(i)) = C_1(i) \quad i = 1, 2, \ldots, H \times W \tag{9}$$

where C_2 is the image encrypted by FSM. This step will be repeated 256 times.

Step 6: The following processing is performed on S_2:

$$S_2 = \text{floor}(\text{mod}(S_2 \times 10^{10}, 64)) \tag{10}$$

Then, process all the numbers in S_2 to be even numbers.

Step 7: For FQM encryption, the following operations are performed on the selected C_x:

$$C_x = \begin{bmatrix} C_2(i, j) & C_2(i, j+1) \\ C_2(i+1, j) & C_2(i+1, j+1) \end{bmatrix} \tag{11}$$

where $i \in \{1, 3, 5, \ldots, H\}$ and $j \in \{1, 3, 5, \ldots, W\}$.

Then, use the following formula to continue operating on C_x to obtain the encrypted result C_3.

$$U = Q^{S_2(k)} \tag{12}$$

$$F_z = UC_x \tag{13}$$

$$\begin{cases} C_3(i, j) = F_z(1, 1) \\ C_3(i, j) = F_z(1, 2) \\ C_3(i, j) = F_z(2, 1) \\ C_3(i, j) = F_z(2, 2) \end{cases} \tag{14}$$

where $i \in \{1, 3, 5, \ldots, H\}$, $j \in \{1, 3, 5, \ldots, W\}$ and $k \in \{1, 3, 5, \ldots, End\}$. Finally, the following operations are executed to complete the encryption and obtain the ciphertext image C:

$$C = \text{mod}(C_3, 256) \tag{15}$$

This algorithm will perform the same operations repeatedly on the three red (R), green (G), and blue (B) channels. The decryption is the inverse process of the symmetric encryption.

3 Experimental validation and discussion

The algorithm was tested on a desktop personal computer with the following configuration and environment: AMD Ryzen 7-7745HX-CPU, Laptop 4060-GPU, 64-bit Windows 11 operating system, and 16GB of RAM, using MATLAB 2022b as software.

3.1 Performance

The number of pixel change rate (NPCR) and the unified average changing intensity (UACI) are common indicators used to measure encryption algorithms. Among them, NPCR mainly measures the proportion of different pixels between two images, while UACI mainly measures the difference in pixel values between two images. The formulae relating to NPCR and UACI are as follows:

$$\begin{cases} NPCR = \frac{1}{H \times W} \times \sum_{i=1}^{H} \sum_{j=1}^{W} D_N(i, j) \\ UACI = \frac{1}{H \times W} \times \sum_{i=1}^{H} \sum_{j=1}^{W} \frac{|v_1(i,j) - v_2(i,j)|}{255} \end{cases} \tag{16}$$

where $D_N(i, j)$ is the result of comparing two images at the same position, same outputs 0 and different outputs 1. v_1 and v_2 are two different images used for the calculation.

By calculating the NPCR and UACI values of multiple images using the same algorithm, the encryption effect of the algorithm is observed. The results are shown in Table 1. The experiments show that the encryption effect of the algorithm is close to the theoretical value. At the same time, the NPCR and UACI values of the same encrypted image under different algorithms were also tested. The results are shown in Table 2 and Table 3. The results also indicate that the algorithm in this paper has certain advantages in encryption performance, demonstrating the security of the algorithm and its ability to resist relevant attacks.

3.2 Encryption time

The time required for encryption by an algorithm is an important performance indicator of the algorithm. It can reflect the computational complexity of the algorithm to a certain extent, and also indicate whether the algorithm is feasible for practical application. To evaluate the computational performance of the algorithm, an image was encrypted ten times and the average encryption time was calculated. A comparison between the proposed algorithm and other algorithms is shown in Table 4. From the results, it can be seen that the proposed PICFF is capable of encrypting images at a satisfactory rate, which makes it worth considering for deployment in practical applications.

Table 1 Result of NPCR of PICFF: different images

Image	NPCR			UACI		
	Red	Green	Blue	Red	Green	Blue
Oakland	99.6098	99.6098	99.6197	33.4752	33.4125	33.4786
Splash	99.6017	99.6075	99.6113	33.3964	33.4713	33.3748
Mandrill	99.6101	99.6459	99.6197	33.4952	33.3928	33.4106
F-16	99.6204	99.6056	99.6059	33.4124	33.3987	33.4764
Sailboat	99.5964	99.6159	99.6208	33.4294	33.4130	33.3871
Peppers	99.6353	99.6143	99.6258	33.4108	33.4974	33.4222
House	99.6296	99.6029	99.6204	33.4124	33.3925	33.4715

Table 2 Comparison of NPCR with different algorithms

Image	NPCR			
	Algorithm	Red	Green	Blue
Mandrill	2024 [9]	99.5991	99.6243	99.6044
	2024 [23]	99.6076	99.5995	99.6149
	2024 [51]	99.6045	99.5965	99.5928
	2025 [17]	99.6103	99.6120	99.6116
	2025 [33]	99.6134	99.6246	99.6250
	Proposed	99.6101	99.6459	99.6197
Peppers	2024 [9]	99.6197	99.5895	99.6254
	2024 [23]	99.6148	99.6109	99.6012
	2024 [51]	99.5841	99.6116	99.6236
	2024 [10]	99.6200	99.6300	99.6300
	2025 [33]	99.6082	99.6086	99.6227
	Proposed	99.6353	99.6143	99.6258

Table 3 Comparison of UACI with different algorithms

Image	UACI			
	Algorithm	Red	Green	Blue
Mandrill	2024 [9]	33.4444	33.5114	33.4760
	2024 [23]	33.4589	33.4654	33.4704
	2024 [51]	33.4253	33.4947	33.5560
	2025 [17]	33.4532	33.4815	33.4948
	2025 [33]	33.4566	33.4591	33.4248
	Proposed	33.4952	33.3928	33.4106
Peppers	2024 [9]	33.5635	33.4107	33.4337
	2024 [23]	33.4922	33.4882	33.4712
	2024 [51]	33.4965	33.3683	33.4616
	2024 [10]	33.5400	33.4700	33.4700
	2025 [33]	33.4774	33.4538	33.4400
	Proposed	33.4108	33.4974	33.4222

Table 4 Comparison of time with different algorithms

Image Size	Time(s)			
	2024 [9]	2023 [57]	2024 [56]	Proposed
512 × 512	1.3011	–	–	0.6272
256 × 256	0.2546	0.6010	0.9830	0.2840

3.3 Histogram

Histograms can effectively determine the pixel distribution of an image. The histogram distribution of the encrypted image shown in Fig. 3 indicates that the pixel distribution after encryption is uniform, thereby enhancing the security of the algorithm.

3.4 Correlation

Pixel correlation reveals the degree of correlation between adjacent pixels in an image, effectively measuring the effectiveness of image encryption. The formula for calculating pixel correlation is as follows:

$$\begin{cases} E(x) = \frac{1}{N}\sum_{N}^{i=1} x_i \\ D(x) = \frac{1}{N}\sum_{N}^{i=1} (x_i - E(x))^2 \\ cov(x, y) = \frac{1}{N}\sum_{N}^{i=1} (x_i - E(x))(y_i - E(y)) \\ \gamma_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\times\sqrt{D(y)}} \end{cases} \tag{17}$$

where x and y represent any two pixel values, $E(x)$ denotes the mean of pixel values, $D(x)$ represents the variance, $cov(x, y)$ is the covariance between x and y, and γ_{xy} is the correlation coefficient. As depicted in Fig. 4 and Table 5, the pixel correlation after encryption becomes more uniform. The correlation among pixels is reduced and homogenized post-encryption, which indicates that the algorithm successfully disrupts the original information of the image and bolsters its secrecy. This demonstrates the algorithm's capability to effectively counteract attacks that exploit correlated pixels.

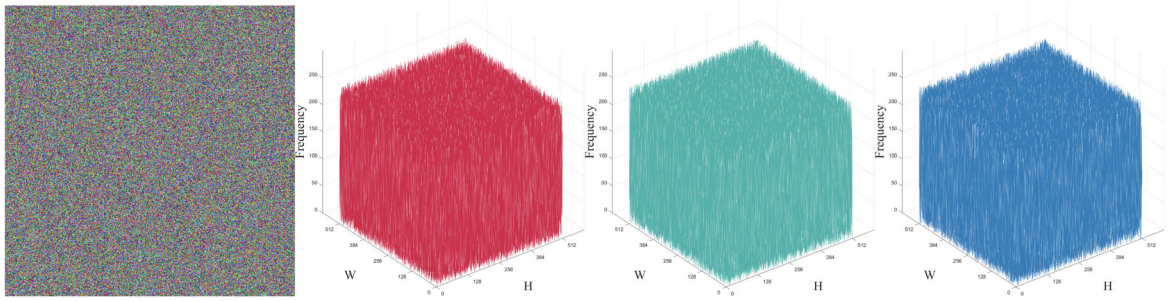

Fig. 3 Results of proposed the PICFF: image histograms

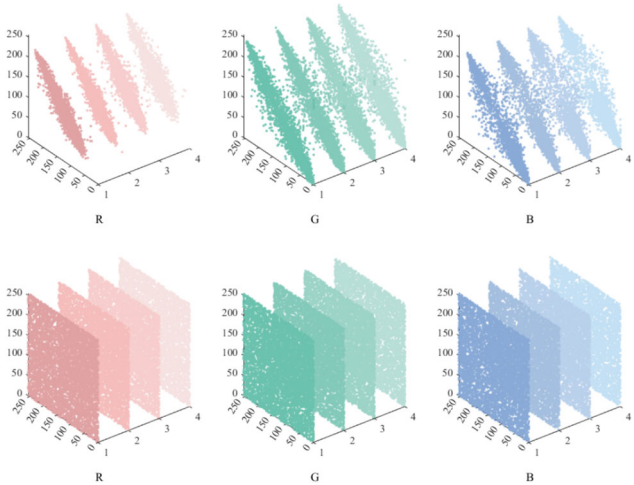

Fig. 4 Results of the proposed PICFF: the correlation of the plain image of 'Sailboat' and its encrypted image

3.5 Entropy

Information entropy is used to measure the degree of disorder in image information, and for encrypted images, it is usually directly proportional to the strength of encryption. Generally, the higher the information entropy of an encrypted image, the better the encryption effect. The formula for calculating information entropy is as follows:

$$H(n) = -\sum_{i=0}^{H\times W-1} P(n_i)\, log_2 P(n_i) \tag{18}$$

where $p(i)$ represents the occurrence frequency of the i gray level in the image. In Table 6, the information entropy of different images encrypted by this algorithm is calculated. The results show that the information entropy of the encrypted images is highly consistent with the theoretical value, which fully proves the high security of the encryption effect of this algorithm. In addition, Table 6 also compares the information entropy of the same image encrypted by other algorithms, and the comparison results are detailed in Table 7. Through this comparison, it can be clearly seen that this algorithm has significant advantages in ensuring information security and resisting attacks compared to other algorithms.

Table 5 Comparison of 'Peppers' image components in different directions

Component	Direction	Original image	2024 [32]	2025 [33]	Proposed
Red channel	Horizontal	0.9648	0.0067	0.0014	–0.0008
	Vertical	0.9670	0.0036	0.0025	0.0033
	Diagonal	0.9607	–0.0073	–0.00009	0.0094
Green channel	Horizontal	0.9827	–0.0062	0.0008	–0.0039
	Vertical	0.9852	0.0037	0.0019	0.0044
	Diagonal	0.9730	–0.0040	–0.0034	–0.0080
Blue channel	Horizontal	0.9656	0.0048	0.0012	–0.0075
	Vertical	0.9488	0.0043	–0.0003	–0.0007
	Diagonal	0.9671	0.0041	0.0041	0.0022

Table 6 Result of entropy for images encrypted by PICFF

Image	Entropy		
	Red	Green	Blue
Oakland	7.9994	7.9994	7.9994
Splash	7.9993	7.9992	7.9993
Mandrill	7.9993	7.9993	7.9992
F-16	7.9994	7.9993	7.9992
Sailboat	7.9994	7.9992	7.9994
Peppers	7.9992	7.9992	7.9994
House	7.9994	7.9992	7.9993

Table 7 Comparision of the image information entropy

Image	Algorithm	Red	Green	Blue
Mandrill	2024 [9]	7.9993	7.9993	7.9992
	2024 [51]	7.9993	7.9986	7.9991
	2024 [32]	7.9993	7.9992	7.9993
	2025 [17]	7.9975	7.9975	7.9972
	2025 [33]	7.9993	7.9993	7.9993
	Proposed	7.9993	7.9993	7.9992
Pepper	2024 [9]	7.9993	7.9993	7.9992
	2024 [51]	7.9984	7.9992	7.9985
	2024 [32]	7.9993	7.9994	7.9992
	2025 [17]	7.9993	7.9993	7.9993
	2025 [33]	7.9992	7.9992	7.9993
	Proposed	7.9992	7.9992	7.9994

3.6 Key sensitivity

A highly sensitive key is crucial to ensure that an encryption algorithm can effectively withstand various attacks, including brute-force attempts. To assess this sensitivity, we conducted an experiment in which we slightly altered the size of the key and then encrypted the same image with both the original and the altered key. We subsequently compared the two encrypted images using the Structural Similarity Index Measure (SSIM).

SSIM is a metric that measures the similarity between two images. If the two images are identical, the SSIM value is 1. The closer the SSIM value is to 0, the more dissimilar the images are. The definition of SSIM is as follows:

$$\mathrm{SSIM}(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \tag{19}$$

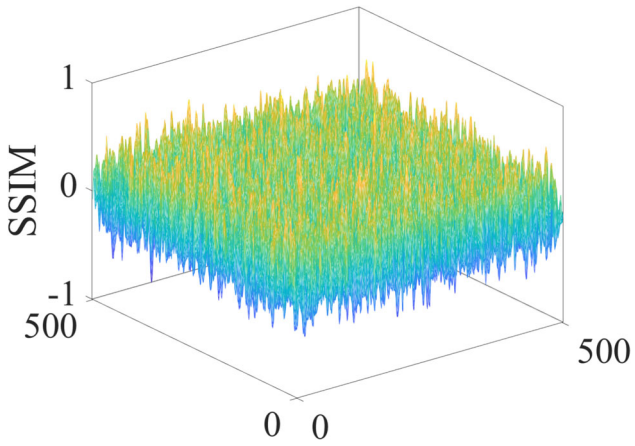

Fig. 5 The result of encrypting the same image using PICFF with two keys that have a slight difference(10^{-17}) in terms of SSIM

where μ_x, μ_y are the local means of x and y, σ_{xy} is the covariance between x and y, σ_x^2, σ_y^2 are the variances of x and y, $C_1 = 6.5025$, $C_2 = 58.5225$ are small constants to stabilize division.

The SSIM results are shown in Fig. 5. From the results, we can observe that the SSIM values fluctuate around 0, indicating that the algorithm is highly sensitive to the key.

3.7 Plain sensitivity

Plaintext attacks are a method of exploring encryption patterns by replacing plaintext, therefore the sensitivity of encryption algorithms to plaintext is of great importance. In this section's experiment, an image is encrypted multiple times, with one pixel point randomly selected from the image and altered each time, and both the number and size of the changed pixels are fixed at 1, to observe whether the ciphertext images generated each time are consistent. If there are differences in the encrypted images each time, it indicates that the encryption algorithm is highly sensitive to changes in plaintext and can effectively resist plaintext attacks. During the experiment, the NPCR and UACI indicators were tested on a fixed random image, and the results are shown in Fig. 6. The data in the figure show that the NPCR and UACI values are different each time, which fully proves that the algorithm is extremely sensitive to plaintext.

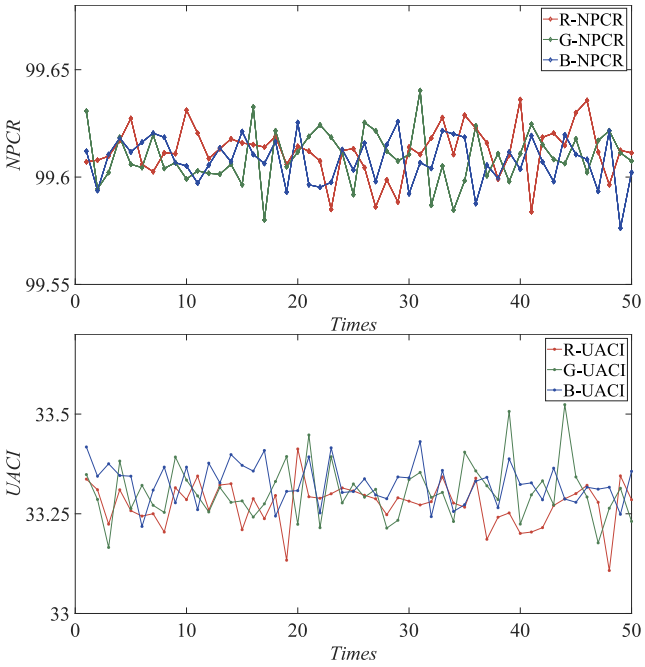

Fig. 6 Results of the proposed PICFF: NPCR and UACI of randomly altered plain image pixels

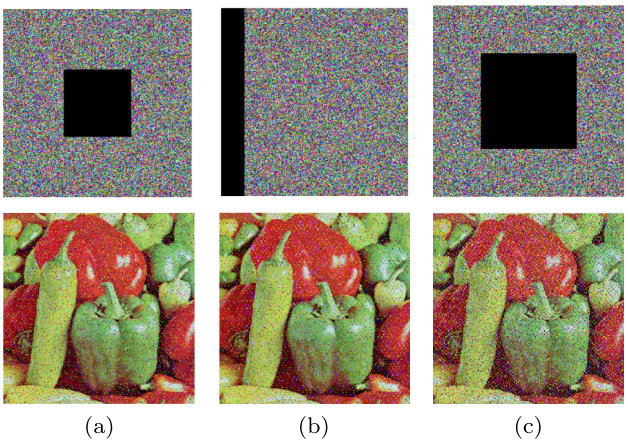

Fig. 7 Visualization of the proposed PICFF: 'Peppers' decrypted images with cropping: (a) cropping ratio of 12.5%; (b) cropping ratio of 12.5%; (c) cropping ratio of 25%

3.8 Cropping attack

During the process of information transmission, cropping attacks occur often. Such attacks inevitably lead to data loss in cipher images. Therefore, whether an encryption algorithm has strong robustness is extremely crucial for ensuring the security of the algorithm. We can artificially crop cipher images in different sizes and positions, and then decrypt them to determine the degree of retention of the decrypted image information. The specific results of the decryption are shown in Fig. 7.

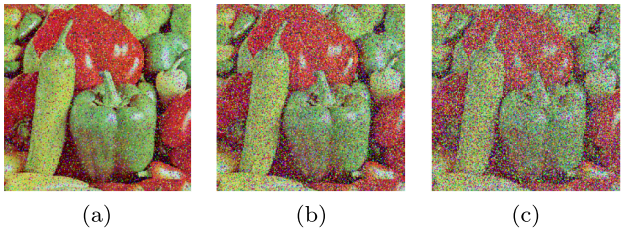

Fig. 8 Visualization of proposed PICFF: 'Peppers' decrypted images with Salt-and-Pepper noise: (a) level of 10%; (b) level of 20%; (c) level of 30%

3.9 Salt-and-pepper noise

The incorporation of salt-and-pepper noise serves as a powerful simulation tool to emulate disruptive noises and potential assaults that occur during communication. It also functions as a reliable means to assess the resilience of encryption algorithms. By subjecting the cipher images to varying intensities of salt-and-pepper noise and subsequently decrypting it, we can ascertain the extent to which the information is preserved in the decrypted image. The results of this process are shown in Fig. 8. These dual experiments underscore the algorithm's exceptional robustness, highlighting its ability to safeguard the core image information even in the face of data loss.

4 Conclusion

This paper proposes a novel method to effectively address the issue of privacy image leakage by introducing an encryption scheme that integrates chaos-driven FSM and FQM. Using the self-iterative properties of FSM, the scheme overcomes the security deficiencies of traditional permutation methods, thereby significantly improving the security of the encryption process. Moreover, to address the periodic nature of traditional FQM encryption and its vulnerability to exhaustive attacks, chaos theory is incorporated into the scheme. The introduction of dynamic encryption through chaos-generated pseudo-random sequences further strengthens the encryption capabilities of FQM. Experimental results indicate that the proposed scheme achieves excellent performance in terms of information entropy and robustness, effectively preventing privacy information from being leaked due to various attacks. Future research will focus on further optimizing the permutation method of the algorithm to improve its security performance. This optimization will provide more robust technical support for the fields of information security and privacy protection, ensuring that the proposed scheme remains effective against evolving threats in the digital landscape.

Author Contributions Y. Liao wrote the main manuscript text and proposed the methodology, and completed the main experiments. Y. Lin

wrote part of the manuscript text and completed part of the experiments. Z. Xing revised the manuscript and adjusted the figures. X. Yuan was in charge of the manuscript editing and overall management and communication. All authors reviewed the manuscript.

Funding This work was supported in part by the Science and Technology Development Fund of Macau SAR under grant 0045/2022/A, and the Macao Polytechnic University under grant RP/FCA-04/2024.

Data Availability No datasets were generated or analysed during the current study.

Declaration

Competing Interests. The authors declare no competing interests.

References

1. Alawida, M.: A novel image encryption algorithm based on cyclic chaotic map in industrial iot environments. IEEE Transactions on Industrial Informatics **20**(8), 10530–10541 (2024)
2. Alawida, M., Samsudin, A., Teh, J.S., Alshoura, W.H.: Deterministic chaotic finite-state automata. Nonlinear Dynamics **98**(3), 2403–2421 (2019)
3. Alawida, M., Teh, J.S., Oyinloye, D.P., Alshoura, W.H., Ahmad, M., Alkhawaldeh, R.S.: A new hash function based on chaotic maps and deterministic finite state automata. IEEE Access **8**, 113,163–113,174 (2020)
4. Bao, B., Tang, H., Su, Y., Bao, H., Chen, M., Xu, Q.: Two-dimensional discrete bi-neuron hopfield neural network with polyhedral hyperchaos. IEEE Transactions on Circuits and Systems I: Regular Papers **71**(12), 5907–5918 (2024)
5. Bi, X., Shuai, C., Liu, B., Xiao, B., Li, W., Gao, X.: Privacy-preserving color image feature extraction by quaternion discrete orthogonal moments. IEEE Transactions on Information Forensics and Security **17**, 1655–1668 (2022)
6. li Chai, X., Cao, G., Gan, Z., Zhang, Y., Ma, Y., He, X.: Tpe-ap: Thumbnail-preserving encryption based on adjustable precision for jpeg images. IEEE Internet of Things Journal **11**(22), 37021–37031 (2024)
7. Chen, C., Min, F., Cai, J., Bao, H.: Memristor synapse-driven simplified hopfield neural network: Hidden dynamics, attractor control, and circuit implementation. IEEE Transactions on Circuits and Systems I: Regular Papers **71**(5), 2308–2319 (2024)
8. Chuman, T., Sirichotedumrong, W., Kiya, H.: Encryption-then-compression systems using grayscale-based image encryption for jpeg images. IEEE Transactions on Information Forensics and Security **14**(6), 1515–1525 (2018)
9. Ding, D., Zhu, H., Zhang, H., Yang, Z., Xie, D.: An n-dimensional polynomial modulo chaotic map with controllable range of lyapunov exponents and its application in color image encryption. Chaos, Solitons & Fractals **185**, 115,168 (2024)
10. Elmenyawi, M.A., Abdel Aziem, N.M., Bahaa-Eldin, A.M.: Efficient and secure color image encryption system with enhanced speed and robustness based on binary tree. Egyptian Informatics Journal **27**(100), 487 (2024)
11. Erkan, U., Toktas, A., Lai, Q.: 2d hyperchaotic system based on schaffer function for image encryption. Expert Systems with Applications **213**(119), 076 (2022)
12. Feng, W., Zhang, J., Chen, Y., Qin, Z., Zhang, Y., Ahmad, M., Woźniak, M.: Exploiting robust quadratic polynomial hyperchaotic map and pixel fusion strategy for efficient image encryption. Expert Systems with Applications **246**(123), 190 (2024)
13. Gao, S., Iu, H.H., Mou, J., Erkan, U., Liu, J., Wu, R., Tang, X.: Temporal action segmentation for video encryption. Chaos, Solitons & Fractals **183**(114), 958 (2024)
14. Gao, S., Iu, H.H.C., Erkan, U., Şimşek, C., Mou, J., Toktas, A., Wu, R., Tang, X.: Design, dynamical analysis, and hardware implementation of a novel memcapacitive hyperchaotic logistic map. IEEE Internet of Things Journal **11**(18), 30368–30375 (2024)
15. Hua, Z., Wu, Z., Zhang, Y., Bao, H., Zhou, Y.: Two-dimensional cyclic chaotic system for noise-reduced ofdm-dcsk communication, pp. 1–14. Regular Papers, IEEE Transactions on Circuits and Systems I (2024)
16. Hua, Z., Zhu, Z., Chen, Y., Li, Y.: Color image encryption using orthogonal Latin squares and a new 2D chaotic system. Nonlinear Dynamics **104**(4), 4505–4522 (2021)
17. Huang, Y., Zhang, Q., Zhao, Y.: Color image encryption algorithm based on hybrid chaos and layered strategies. Journal of Information Security and Applications **89**(103), 921 (2025)
18. Kocak, O., Erkan, U., Toktas, A., Gao, S.: Pso-based image encryption scheme using modular integrated logistic exponential map. Expert Systems with Applications **237**(121), 452 (2023)
19. Lai, Q., Wang, H., Zhao, X.W., Ahmad, M.: Shuffle medical image encryption scheme based on 4d memristive hyperchaotic map. Nonlinear Dynamics (2024)
20. Lai, Q., Yang, L., Chen, G.: Two-dimensional discrete memristive oscillatory hyperchaotic maps with diverse dynamics. IEEE Transactions on Industrial Electronics **72**(1), 969–979 (2025)
21. Li, C., Zhang, Y., Li, H., Zhou, Y.: Visual image encryption scheme based on inter-intra-block scrambling and weighted diffusion. The Visual Computer **40**(2), 1–16 (2023)
22. Li, Q., Li, Q., Ling, B., Pun, C.M., Huang, G., Yuan, X., Zhong, G., Ayouni, S., Chen, J.: Dppad-ie: Dynamic polyhedra permutating and arnold diffusing medical image encryption using 2d cross gaussian hyperchaotic map. IEEE Transactions on Consumer Electronics pp. 1–1 (2025)
23. Li, X., Sun, B., Bi, X., Yan, H., Wang, L.: A Novel Color Image Encryption Algorithm Based on Cross-plane Scrambling and Diffusion. Mobile Networks and Applications **29**(3), 583–594 (2024). https://doi.org/10.1007/s11036-023-02147-1
24. Liao, Y., Lin, Y., Li, Q., Xing, Z., Yuan, X.: Lightweight image encryption algorithm using 4d-nds: Compound dynamic diffusion and single-round efficiency. IEEE Access pp. 1–1 (2025). 10.1109/ACCESS.2025.3560686
25. Lin, Y., Xie, Z., Chen, T., Cheng, X., Wen, H.: Image privacy protection scheme based on high-quality reconstruction dct compression and nonlinear dynamics. Expert Systems with Applications **257**(124), 891 (2024)
26. Liu, P., Wang, X., Su, Y.: Image encryption via complementary embedding algorithm and new spatiotemporal chaotic system. IEEE Transactions on Circuits and Systems for Video Technology **33**(5), 2506–2519 (2023)
27. Liu, Z., Xue, R.: Visual image encryption based on compressed sensing and cycle-gan. The Visual Computer **40**(8), 5857–5870 (2023)
28. Mehmood, A., Shafique, A., Alawida, M., Khan, A.N.: Advances and vulnerabilities in modern cryptographic techniques: A comprehensive survey on cybersecurity in the domain of machine/deep learning and quantum techniques. IEEE Access **12**, 27530–27555 (2024). https://doi.org/10.1109/ACCESS.2024.3367232
29. Mou, J., Cao, H., Zhou, N., Cao, Y.: An fhn-hr neuron network coupled with a novel locally active memristor and its dsp implementation. IEEE Transactions on Cybernetics **54**(12), 7333–7342 (2024)
30. Peng, Y., Lan, Z., Li, Z., Li, C.: An effective anti-object-detection image privacy protection scheme based on robust chaos. IEEE Transactions on Industrial Informatics **20**(5), 7227–7237 (2024)

31. Toktas, A., Erkan, U., Ustun, D., Lai, Q.: Multiobjective design of 2d hyperchaotic system using leader pareto grey wolf optimizer. IEEE Transactions on Systems, Man, and Cybernetics: Systems **54**(9), 5237–5247 (2024)
32. Toktas, F., Erkan, U., Yetgín, Z.: Cross-channel color image encryption through 2d hyperchaotic hybrid map of optimization test functions. Expert Systems with Applications **249**(123), 583 (2024)
33. Wang, M., Teng, L., Zhou, W., Yan, X., Xia, Z., Zhou, S.: A new 2d cross hyperchaotic sine-modulation-logistic map and its application in bit-level image encryption. Expert Systems with Applications **261**(125), 328 (2024)
34. Wang, X., Chen, X.: Image encryption algorithm based on cross-scrambling and rapid-mode diffusion. The Visual Computer **39**(10), 5041–5068 (2022)
35. Wang, X., Yuan, X., Li, M., Sun, Y., Tian, J., Guo, H., Li, J.: Parallel multiple watermarking using adaptive inter-block correlation. Expert Systems with Applications **213**(119), 011 (2022)
36. Wang, Y., Chen, L., Yu, K., Fu, T.: A secure spatio-temporal chaotic pseudorandom generator for image encryption. IEEE Transactions on Circuits and Systems for Video Technology **34**(9), 8509–8521 (2024)
37. Wen, H., Feng, Z., Bai, C., Lin, Y., Zhang, X., Feng, W.: Frequency-domain image encryption based on iwt and 3d s-box. Physica Scripta **99**(5), 055,254 (2024)
38. Wen, H., Huang, Y., Lin, Y.: High-quality color image compression-encryption using chaos and block permutation. Journal of King Saud University - Computer and Information Sciences **35**(8), 101,660 (2023)
39. Wen, H., Kang, S., Wu, Z., Lin, Y., Huang, Y.: Dynamic rna coding color image cipher based on chain feedback structure. Mathematics **11**(14), 3133 (2023)
40. Wen, H., Lin, Y.: Cryptanalysis of an image encryption algorithm using quantum chaotic map and dna coding. Expert Systems with Applications **237**(121), 514 (2023)
41. Wen, H., Lin, Y., Feng, Z.: Cryptanalyzing a bit-level image encryption algorithm based on chaotic maps. Engineering Science and Technology, an International Journal **51**(101), 634 (2024)
42. Wen, H., Lin, Y., Xie, Z., Liu, T.: Chaos-based block permutation and dynamic sequence multiplexing for video encryption. Scientific Reports **13**(1) (2023)
43. Wen, H., Lin, Y., Yang, L., Chen, R.: Cryptanalysis of an image encryption scheme using variant hill cipher and chaos. Expert Systems with Applications **250**(123), 748 (2024)
44. Wen, H., Yang, L., Bai, C., Lin, Y., Liu, T., Chen, L., Hu, Y., He, D.: Exploiting high-quality reconstruction image encryption strategy by optimized orthogonal compressive sensing. Scientific Reports **14**(1) (2024)
45. Wen, W., Huang, H., Qi, S., Zhang, Y., Fang, Y.: Joint coverless steganography and image transformation for covert communication of secret messages. IEEE Transactions on Network Science and Engineering **11**(3), 2951–2962 (2024)
46. Xian, Y., Wang, X.: Fractal sorting matrix and its application on chaotic image encryption. Information Sciences **547**, 1154–1169 (2021)
47. Xie, Z., Lin, Y., Liu, T., Wen, H.: Face privacy protection scheme by security-enhanced encryption structure and nonlinear dynamics. iScience **27**(9), 110,768 (2024)
48. Xing, Z., Lam, C., Yuan, X., Im, S.K., Machado, P.: Mmqw: Multi-modal quantum watermarking scheme. IEEE Transactions on Information Forensics and Security **19**, 5181–5195 (2024)
49. Yu, J., Peng, K., Zhang, L., Xie, W.: Image encryption algorithm based on dna network and hyperchaotic system. The Visual Computer **40**(11), 1–21 (2024)
50. Zeng, W., Zhang, C., Liang, X., Luo, Y., Wang, X., Qiu, K.: Chaotic phase noise-like encryption based on geometric shaping for coherent data center interconnections. Optics Express **32**(2), 1595–1608 (2023)
51. Zhang, H., Hu, H., Ding, W.: Vsdhs-ciea: Color image encryption algorithm based on novel variable-structure discrete hyperchaotic system and cross-plane confusion strategy. Information Sciences **665**(120), 332 (2024)
52. Zhang, L., Lin, Y., Yang, X., Chen, T., Cheng, X., Cheng, W.: From sample poverty to rich feature learning: A new metric learning method for few-shot classification. IEEE Access **12**, 124,990–125,002 (2024)
53. Zhang, S., Chen, C., Zhang, Y., Cai, J., Wang, X., Zeng, Z.: Multidirectional multidouble-scroll hopfield neural network with application to image encryption. IEEE Transactions on Systems, Man, and Cybernetics: Systems pp. 1–12 (2024)
54. Zhang, Y., Hua, Z., Bao, H., Huang, H.: Multi-valued model for generating complex chaos and fractals. IEEE Transactions on Circuits and Systems I: Regular Papers **71**(6), 2783–2796 (2024)
55. Zhang, Z., Zhang, J.: Parallel multi-image encryption based on cross-plane dna manipulation and a novel 2d chaotic system. The Visual Computer **40**(12), 8615–8637 (2024)
56. Zhao, L., Zhao, L., Cui, F., Sun, T.: Satellite image encryption based on rna and 7d complex chaotic system. The Visual Computer **40**(8), 1–21 (2023)
57. Zhu, S., Deng, X., Zhang, W., Zhu, C.: Image encryption scheme based on newly designed chaotic map and parallel dna coding. Mathematics **11**(1) (2023)

Liao Yunlong received the Bachelor of Engineering degree from University of Electronic Science and Technology of China Zhongshan Institute in 2022. He is currently pursuing a Master's degree in Big Data and Internet of Things at the Faculty of Applied Sciences, Macau Polytechnic University. His research interests include multimedia security, image processing, AI security, and cryptography.

Lin Yiting Yiting Lin received the BSc degree in computer science and technology from the University of Electronic Science and Technology of China, Zhongshan Institute in 2024. He is currently a Research Assistant at Beijing Normal-Hong Kong Baptist University (Guangdong Provincial/ Zhuhai Key Laboratory of Interdisciplinary Research and Application for Data Science) and holds a Teaching and Research Position at University of Electronic Science and Technology of China, Zhongshan Institute. His research interests include Cryptography, Blockchain, Information Security, Multimedia Security, Artificial Intelligence, Signal Processing and Nonlinear Dynamics.

Xing Zheng received the B.S. degree in computer science and technology from Zhengzhou University in Henan Province, China, in 2014, and the M.S. degree in computer technology from Chongqing University of Posts and Telecommunications in Chongqing, China, in 2017. He is currently pursuing his Ph.D. in Computer Application Technology at the Faculty of Applied Sciences of the Macau Polytechnic University. From 2018 to 2021, he worked as a lecturer in the College of Mobile Communication at Chongqing University of Posts and Telecommunications. His research interests include quantum secure communication, blind quantum computing protocols, and quantum cryptography.

Yuan Xiaochen received her Ph.D. degree in Software Engineering from the University of Macau in 2013. From 2014 to 2015, she was a postdoctoral fellow at the Department of Computer and Information Science of the University of Macau. From 2016 to 2021, she was an Assistant Professor and an Associate Professor at the Faculty of Information Technology of the Macau University of Science and Technology. She is currently an Associate Professor with the Faculty of Applied Sciences of the Macao Polytechnic University. Her research interests include Multimedia Forensics and Security, Digital Watermarking, AI Model Security, Quantum Watermarking, Remote Image Processing, and Deep Learning Techniques and Applications.