IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 4 August 2024, accepted 19 August 2024, date of publication 21 August 2024, date of current version 2 September 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3447239

RESEARCH ARTICLE

Optimization of Image Encryption Algorithm Based on Henon Mapping and Arnold Transformation of Chaotic Systems

YUEBO WU[1], SHIWEI CHU[2], HUIFANG BAO[1], DUANSONG WANG[1], (Member, IEEE), AND JIAN ZHOU[1]

[1]School of Electrical and Photoelectronic Engineering, West Anhui University, Lu'an 237012, China
[2]School of Electronic Information Engineering, Anhui University, Hefei 230039, China

Corresponding author: Shiwei Chu (P23111026@stu.ahu.edu.cn)

This work was supported in part by the Advanced Talent Research Fund of Wanxi University under Grant WGKQ2021050 and Grant WGKQ2022004, and in part by the Horizontal Project under Grant HX2022WYBSDQ and Grant HX2022WybCGG.

ABSTRACT This study introduces an optimized image encryption algorithm that integrates Henon mapping and Arnold transformation to enhance the security and randomness of digital image encryption. The algorithm is designed to address the vulnerabilities of open network environments where data theft or corruption can compromise image quality during encryption. Initially, images are processed through grayscale conversion to reduce dimensionality, followed by Henon mapping to induce a chaotic sequence that scrambles the pixel matrix. Subsequently, Arnold transformation is applied, iterating 100 times to further disrupt the image structure, ensuring a high level of diffusion and complexity. The proposed method demonstrates superior performance with an average pixel change rate (NPCR) of 0.9982 and a normalized average change intensity (NACI) of 0.3654, significantly increasing resistance to differential attacks. The encrypted images exhibit higher information entropy and effectively mask the original data, although at the cost of extended encryption time due to the dual scrambling process. The study concludes that the combined use of Henon mapping and Arnold transformation not only strengthens encryption against various attacks but also introduces a novel approach to image encryption, with potential for further optimization to enhance efficiency in handling larger images. This advancement is crucial for protecting privacy and ensuring data integrity in the transmission and storage of images, particularly in the face of evolving cyber threats.

INDEX TERMS Image encryption, algorithm combination, Henon mapping, Arnold transformation, chaotic system.

I. INTRODUCTION

The security of data transmission [1], [2] has become a key issue in the current digital information age, as data can be easily stolen in an open network environment. Due to the widespread use of mobile and Internet, a large amount of image data is transmitted and shared, which may contain commercial secrets and private information [3], [4], and these data must be properly protected. Traditional encryption algorithms can encrypt text data in a complex way [5], [6], but these algorithms have problems when encrypting multimedia data, which can cause a significant decline in image quality and make image decryption more challenging. The image encryption process [7], [8] requires a certain degree of secrecy and randomness.

Image encryption [9], [10] serves as a crucial safeguard during image data transmission, ensuring that the content remains unaltered and confidential. This process not only preserves the integrity of the image data but also fortifies its security and privacy by preventing any form of tampering or deletion. Image encryption [11], [12] is pivotal in today's digital information landscape, offering protection against various digital attacks while maintaining data integrity and safeguarding image privacy and security. To enhance the security

The associate editor coordinating the review of this manuscript and approving it for publication was Yizhang Jiang.

of image transmission, Zhang and Zhang [15] introduced a multi-image encryption algorithm that leverages bit plane and chaos principles. This algorithm employs an XOR (exclusive OR) operation on both chaotic and scrambled images, demonstrating robust resistance to statistical and brute force attacks. Similarly, Maazouz et al. [16] proposed a chaotic system, utilizing its state variables to devise a new replacement matrix, which was then integrated into an image encryption Feistel network. Liu et al. [17] conducted an in-depth analysis of two image encryption algorithms for first-order time-lag systems, enabling efficient retrieval of equivalent keys from known plaintext images and their corresponding cipher images. While these studies have significantly enhanced the security of image data during transmission, they are not without limitations. These algorithms often suffer from compromised security, computational inefficiency, and degradation in image quality when applied in real-world scenarios. The role of image encryption in preserving privacy and ensuring data integrity cannot be overstated. Although the chaos-based Feistel network algorithm offers promising resistance to attacks, there remain challenges related to security, efficiency, and image quality that warrant further research and refinement.

Henon mapping [18], [19] is a method for generating chaotic sequences with randomness and unpredictability. This chaos enhances the randomness of the encryption algorithm, thus improving its effectiveness. Henon mapping [20], [21] is a nonlinear dynamic system with strong nonlinear properties, which makes the encryption process more complicated. This complexity increases the difficulty for potential attackers to break the encryption, thereby enhancing the security of the algorithm. Arnold Transform [22] is an out-of-order operation that changes the position of image pixels. This operation can sufficiently confuse the spatial structure of the image and randomize the pixel position of the encrypted image. This increases the complexity and security of the encryption algorithm. Abdul-Kareem and Al-Jawher [23] designed a new color image encryption technique that utilizes multiple wavelet transforms, Arnold transforms, and two chaotic systems. This technique has high key sensitivity and the ability to resist multiple attacks. Shrivastava et al. [24] combined the wavelet transform with the Arnold transform to generate an encrypted image with additional variable flexibility, making it more suitable for secure transmission. Although the image encryption algorithm using Henon mapping [25] and Arnold transform [26] has achieved some achievements, the research of combining these two methods is still lacking.

In this paper, the randomness of the encryption algorithm is increased by combining Henon mapping and Arnold transformation, so as to improve the security and efficiency of image encryption. Images of eight animals were collected and converted into grayscale images to simplify the encryption process. The parameters of Henon mapping are set to $a = 1.4$ and $b = 0.3$, causing all pixels in the image to be scrambled. On this basis, Arnold transform is applied to further disrupt the image. Compared with the independent Henon mapping and Arnold transform, the proposed algorithm shows better performance, with the average pixel change rate (NPCR) of 0.9982 and the normalized average change intensity (NACI) of 0.3654. The encrypted images generated by this algorithm have higher information entropy, but require longer encryption time. The novelty of this study is that a new image encryption algorithm is proposed by combining Henon mapping and Arnold transform. By integrating these two scrambling methods, the randomness of the encryption algorithm is significantly enhanced, and the security of the image is greatly improved. This provides a new method for image encryption.

II. OPTIMIZATION METHODS FOR IMAGE ENCRYPTION ALGORITHMS

A. IMAGE COLLECTION AND PREPROCESSING

During network transmission and storage, image data is vulnerable to unauthorized access, theft and tampering. Image encryption can effectively protect the privacy and integrity of images and ensure the safe transmission and storage of data. Image encryption prevents illegal copying or piracy of images, protects the copyright and commercial interests of the original images, and upholds the rights of image creators.

The image data collected on the Internet platform is shown in Figure 1.

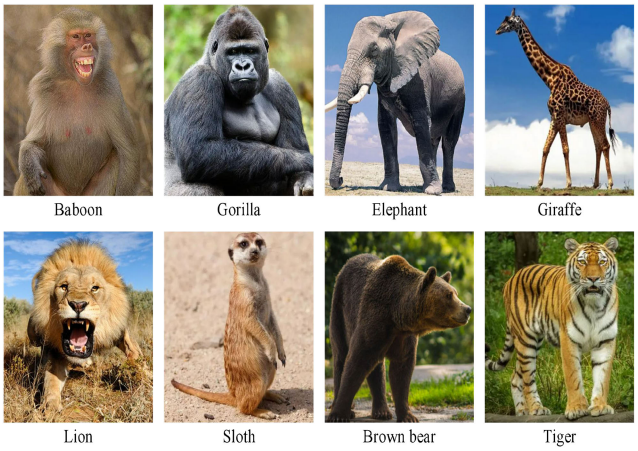

FIGURE 1. Original image data.

Figure 1 shows the collected image data, all of which are animal images, including 8 types of animal images. Image encryption can ensure that image data is not tampered with or damaged during transmission and storage, and maintain data integrity.

The collected images are subjected to grayscale conversion, reducing the dimensionality of the images and simplifying the processing of encryption algorithms. Image grayscale conversion [27], [28] is the process of converting color images into grayscale images. In grayscale images, the value of each pixel represents the brightness of that pixel. The formula for grayscale transformation of images is

expressed as:

$$H = 0.299 \times R + 0.587 \times G + 0.114 \times B \tag{1}$$

The result of grayscale transformation of the image is shown in Figure 2.

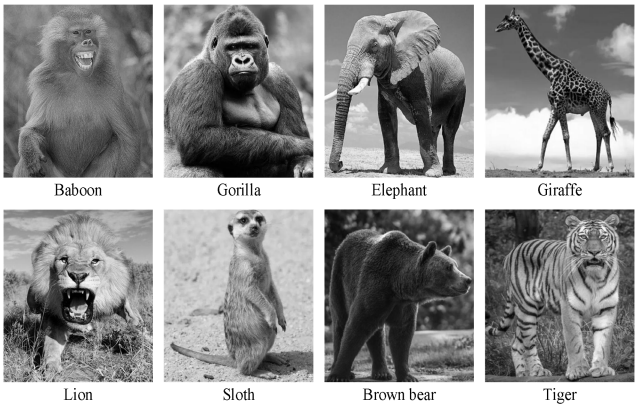

FIGURE 2. Results of image grayscale transformation.

Grayscale conversion converts color images into grayscale images, removes color information, simplifies image representation, and reduces data complexity. Compared to color images, grayscale images have lower computational complexity, so the processing speed of grayscale images is faster in image processing and analysis.

B. HENON MAPPING ENCRYPTION

Chaotic systems refer to a type of dynamic system that is nonlinear, deterministic, and sensitive depending on initial conditions. Chaotic systems have a high degree of nonlinearity and randomness, which can be utilized to enhance the confusion of image encryption algorithms. Using chaotic mapping or chaotic sequences to scramble image pixels makes the encrypted image difficult to analyze and crack [29], [30], [31].

The Henon mapping [33], [34], [35] is a simple but chaotic two-dimensional dynamical system, represented by:

$$\begin{cases} x_{n+1} = y_n + 1 - a \cdot x_n^2 \\ y_{n+1} = b \cdot x_n \end{cases} \tag{2}$$

In Formula 2, a and b are both parameters of the Henon mapping, where a is 1.4 and b is 0.3. The trajectory of the mapping can be obtained through iterative calculation. In the Henon mapping, the parameters a=1.4 and b=0.3 are chosen based on the chaotic properties they produce, ensuring that the mapping has good chaotic behavior, thereby enhancing the randomness and security of the image encryption algorithm.

The Henon mapping [36], [37] is a nonlinear dynamical system, which leads to the complexity and unpredictability of the mapping trajectory. The trajectory of Henon mapping is very sensitive to the initial conditions. Minor initial value changes result in significant differences in the mapping trajectory, exhibiting the butterfly effect of chaotic systems.

The Henon mapping bifurcation is illustrated in Figure 3.

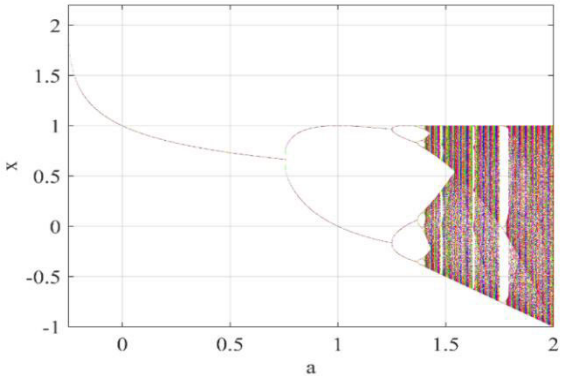

FIGURE 3. Henon mapping bifurcation.

The horizontal axis in Figure 3 indicates the parameter a of the Henon mapping, and the vertical axis indicates the trajectory points of the Henon mapping. By adjusting the value of parameter a, different behaviors of the trajectory point x in the Henon mapping can be observed, including periodicity, chaos, etc. When parameter a takes different values, the bifurcation phenomenon of trajectory point x can be observed, that is, the stability of the mapping changes, thus forming a bifurcation structure.

The grayscale image to be encrypted is converted into a two-dimensional pixel matrix, with an image size of N×M. The initial seed point (x_0, y_0) is set as the initial conditions for Henon mapping. Each pixel (x_i, y_i) in the image is scrambled. (x_i, y_i) is substituted into Formula 2 for scrambling:

$$\begin{cases} x_{i+1} = y_i + 1 - a \cdot x_i^2 \\ y_{i+1} = b \cdot x_i \end{cases} \tag{3}$$

By using Henon mapping to obtain the scrambled result, (x_{i+1}, y_{i+1}) is mapped back to the pixel matrix of the image, and the grayscale values of the original pixels are copied to the new pixel positions to ensure that the content of the image does not change. Scrambling is repeated and iterated until all pixels have completed the shuffling operation.

C. ARNOLD TRANSFORMATION ENCRYPTION

Arnold transformation [38], [39] is a classic image scrambling operation that changes the structure of an image by permeating and mapping its pixels, increasing the diffusion and security of encryption algorithms. The formula for Arnold transformation is expressed as:

$$\begin{cases} x' = (2x + y) \ mod \ N \\ y' = (x + y) \ mod \ N \end{cases} \tag{4}$$

In Formula 4, (x', y') is the pixel coordinates after Arnold transformation. By iteratively applying Arnold transformation, the image is subjected to multiple scrambling operations, increasing the randomness and obfuscation of the

encryption algorithm. The essence of scrambling is the mapping of new and old positions. The scrambling principle in Arnold transformation is shown in Figure 4.

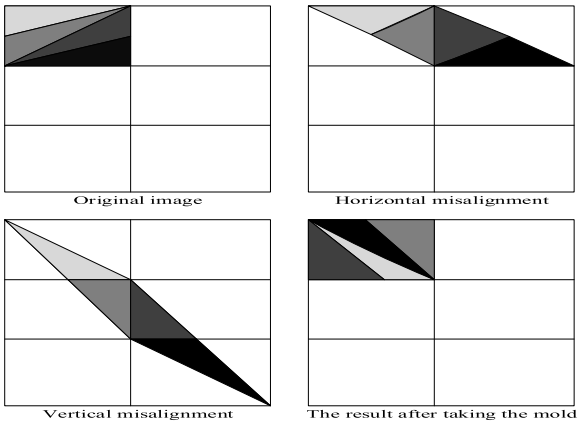

FIGURE 4. Scrambling principle in Arnold transformation.

Figure 4 shows the scrambling principle in Arnold transformation, which involves performing horizontal misalignment on the original image and vertical misalignment on the basis of horizontal misalignment. Finally, the image is modeled to obtain the transformed image.

The result of Arnold transformation is shown in Figure 5.

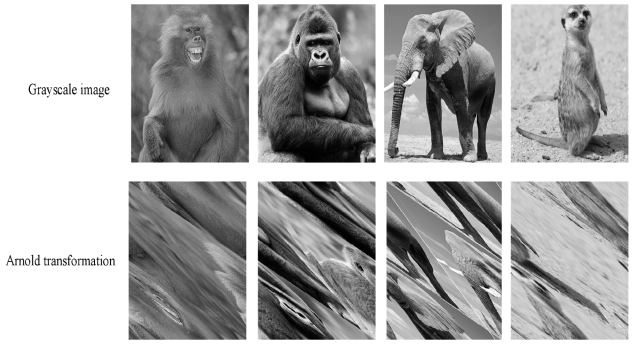

FIGURE 5. Results of Arnold transformation.

Figure 5 shows the result of Arnold transformation, and the difference between the transformed image and the original image is very large. The Arnold transformation disrupts the spatial structure of an image by scrambling the pixel positions, resulting in changes in the pixel positions of the original image.

The process of combining Henon mapping and Arnold transformation is shown in Figure 6.

The image to be encrypted is encrypted using the Henon map, generating a chaotic sequence. The pixels of the image are scrambled to enhance the randomness of the encryption algorithm. The image is encrypted by mapping it with Henon and then encrypting it using the Arnold transform, which further messes up the image. Through the decryption process, the image information is gradually restored to ensure the correct restoration of the original image.

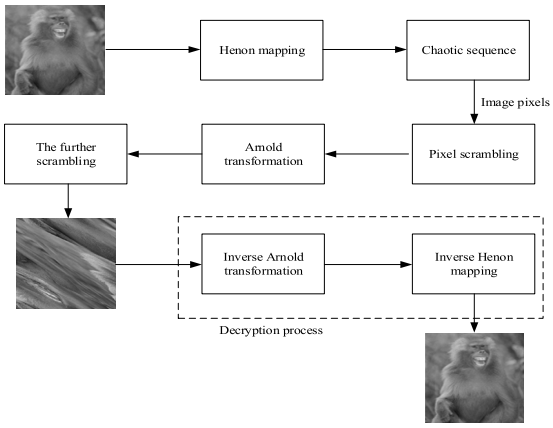

FIGURE 6. Combination process of Henon mapping and Arnold transformation.

Henon mapping and Arnold transformation are applied to image encryption and increased security by spreading pixels. Henon maps introduce a chaotic feature that randomly scrambles image pixels, making it difficult for attackers to backinfer the original image. Arnold transform changes the image structure by permutation and mapping, increases the complexity of encryption, and further improves the security of encryption. The combination of these theories makes encryption stronger and more resistant to attacks.

The Henon map generates a chaotic sequence through nonlinear dynamics, which is used to disrupt the image pixel matrix. In the Henon map, the parameters a and b control the chaotic characteristics of the mapping, and the generated sequence has high randomness, making the pixel position of the image unpredictable. This chaotic sequence effectively disrupts the initial structure of the image by iteratively scrambling the position of each pixel. Then, the Arnold transform further destroys the image structure. By repeatedly permuting and mapping the pixel positions of the image, the Arnold transform makes the spatial structure of the image more complex and chaotic. Its iterative process continuously changes the pixel positions, enhancing the obfuscation of the encrypted image, ensuring that the encrypted image is difficult to recover or analyze.

D. IMAGE DECRYPTION

Through the reverse Henon mapping algorithm, the encrypted image pixels are restored to the original image pixels. After the inverse Arnold transformation and inverse Henon mapping, the original image before encryption can be obtained.

The Arnold transformation matrix is:

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \tag{5}$$

The inverse matrix of matrix A is represented as:

$$A^{-1} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \tag{6}$$

The inverse Arnold transformation matrix is applied to the pixel coordinates of the encrypted image to achieve the inverse Arnold transformation.

The Henon mapping is a nonlinear dynamical system, and the inverse Henon mapping is achieved through numerical iteration. Assuming the pixel coordinate of the encrypted image is set to (x_0, y_0), the numerical iteration method is used to solve for the next point (x_{n+1}, y_{n+1}), so that (x_{n+1}, y_{n+1}) is restored to the original point (x_0, y_0) after forward Henon mapping.

III. PERFORMANCE EVALUATION OF IMAGE ENCRYPTION

During image transmission and storage, data may be subject to unauthorized access or attacks, such as eavesdropping, tampering, or interception. Image encryption can ensure the security of image data during transmission and storage, preventing data leakage or damage [40], [41]. The collected images of 8 animals are subjected to grayscale processing.

Using a combination of Henon mapping and Arnold transformation for image encryption, the parameters a is set to 1.4 and b to 0.3 in the Henon mapping. The Henon mapping and Arnold transformation are iterated 100 times each, and the inverse Arnold transformation and inverse Henon mapping are used for decryption. The grayscale image is used as the plaintext image, and the plaintext image is subjected to encryption/decryption testing. The effect of encryption/decryption is shown in Figure 7.

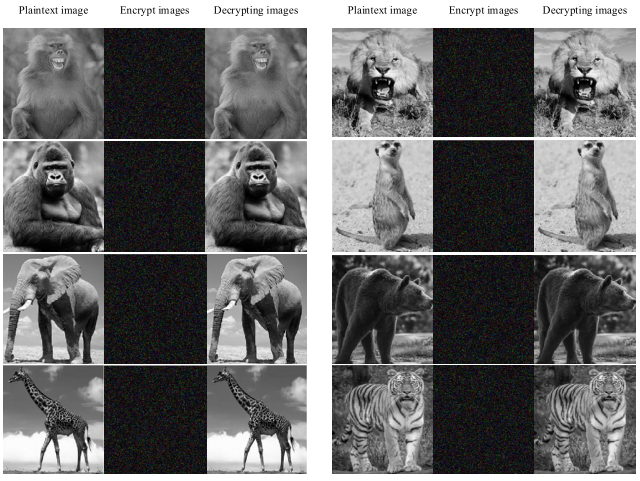

FIGURE 7. Effect of encryption/decryption.

Figure 7 shows plaintext images, encrypted images, and decrypted images. Visually, plaintext images are very similar to decrypted images, and there is a significant difference between encrypted and plaintext images. Encrypted images can effectively mask plaintext image information.

The objective of image encryption is to enhance the security of images. This study integrates Henon mapping and Arnold transformation for the purpose of encrypting images.In the conducted experiment, we established the parameters of the Henon mapping as a=1.4 and b=0.3, while the number of iterations for the Arnold transformation was set at 100. The chosen images were uniformly sized at 256×256 pixels, encompassing diverse scenes and contents. During the encryption procedure, each image underwent 100 iterations of both the Henon mapping and Arnold transformation. The control variables were meticulously selected to ensure the consistency and comparability of the experimental results.In the conducted experiment, a diverse range of animal images were chosen to ensure both representativeness and diversity.

The experiment was repeated multiple times to yield reliable results. The parameters for the Henon map were set at a=1.4 and b=0.3, with the iteration count set at 100. Similarly, the Arnold transformation was iterated 100 times. The histogram variance, adjacent pixel correlation, anti-differential cryptanalysis capability, and information entropy of the images before and after encryption were compared to evaluate the effectiveness of the encryption process.The variance of the histogram is represented as:

$$var(U) = \frac{1}{n^2} \sum_{i=0}^{n} \sum_{j=0}^{n} \frac{1}{2} (u_i - u_y)^2 \tag{7}$$

The adjacent pixel correlation is calculated as:

$$R_{xy} = \frac{E((x - E(x))(y - E(y)))}{\sqrt{D(x)}\sqrt{D(y)}} \tag{8}$$

The NPCR formula for differential attack resistance analysis based on number of pixels change rate and normalized average change intensity is:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{N \times M} \tag{9}$$

The calculation formula for NACI is:

$$NACI = \sum_{i,j} \frac{|Q_1(i,j) - Q_2(i,j)|}{255 \times N \times M} \tag{10}$$

In Formula 10, Q_1 and Q_2 represent plaintext grayscale images and encrypted grayscale images, respectively.

NPCR and NACI are key indicators to evaluate the effectiveness of image encryption algorithms. NPCR measures the ratio of pixel changes between the plaintext image and the ciphertext image. The higher the value, the greater the sensitivity of the encryption algorithm to small changes in plaintext and the ability to resist differential attacks. The calculation method is to count the differences in pixel values of the plaintext and ciphertext images and take the average value. NACI measures the average intensity of changes in image pixel values, and evaluates the encryption effect by calculating the change amplitude of each pixel in the plaintext and ciphertext images. The higher the NACI value, it means that the encrypted image has experienced more significant changes at the pixel level, thereby improving the security and attack resistance of the algorithm. Together, these two indicators reflect the performance of the encryption algorithm in protecting the security and effectiveness of image data.

The calculation formula for information entropy is:

$$H(X) = -\sum_{i=0}^{n} P(x_i) log_2 P(x_i) \quad (11)$$

Information entropy measures the complexity and uncertainty of information in an image. A high entropy value indicates that the image data is more random and complex. In image encryption, a higher information entropy means that the encrypted image is difficult to predict or recover, which enhances the security of encryption. Information entropy close to the theoretical maximum value indicates that the encryption process effectively scrambles the pixel values, thereby improving the ability to resist attacks.

In order to comprehensively consider the encryption effect of Henon mapping combined with Arnold transformation, the encryption speed of the algorithm is also evaluated, and the time required for encryption is analyzed by changing the size of the image. The experiment compares the encryption algorithm combining Henon mapping with Arnold transformation with a single Henon mapping and Arnold transformation [42], [43], [44].

In the experiment, animal images were collected and processed in gray scale. Then, the image encryption is carried out by combining Henon mapping and Arnold transform with parameters of a=1.4 and b=0.3, and each algorithm is iterated 100 times. The histogram variance, adjacent pixel correlation, anti-differential cryptanalysis, information entropy and encryption time of the images before and after encryption are evaluated. Repeat the experiment to get reliable results.

Encryption time is a key factor in evaluating the performance of encryption algorithms and directly affects their usability in real-time applications. Long encryption time may cause delays and affect user experience, which is especially important in real-time video surveillance or online communications. Optimizing encryption time can ensure the timeliness and efficiency of data transmission and improve the overall responsiveness of the system. For resource-constrained devices, the long encryption process may exceed their processing capabilities and reduce the practicality of the application. Therefore, security and efficiency must be considered when designing encryption algorithms.

To address the computational complexity and scalability of the algorithm in high-resolution images, efficiency is improved by optimizing code implementation, parallel computing, or hardware acceleration. In addition, simplifying the obfuscation process and reducing the number of iterations can also help reduce the computational burden, thereby achieving effective processing of high-resolution images.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

Following the encryption process utilizing the Henon mapping and Arnold transformation, we conducted a series of experiments to evaluate the effectiveness of our algorithm. The experiments were carried out on a standard PC environment equipped with an Intel Core i7 processor, 64GB of RAM, and running on Windows 10 operating system. The images used in our experiments were of varying dimensions, ranging from 256 × 256 to 1024 × 1024 pixels, to simulate different scenarios of image transmission and storage.

A. RESULTS OF HISTOGRAM VARIANCE

Histogram variance is an important measure of image encryption security, which reflects the distribution of pixel intensities in an image. A high variance implies a uniform distribution of pixel values and a higher degree of randomness in the encrypted image, thus increasing the difficulty of cracking. In this study, the approach aims to improve the security of image encryption by combining Henon mapping and Arnold transform.The nonlinear dynamics introduced by Henon mapping and the pixel position rearrangement of Arnold transform work together to increase the complexity and randomness of the encryption process. Experiments will evaluate the effect of the proposed algorithm on histogram variance to demonstrate its effectiveness in resisting statistical attacks and protecting the privacy of image data.The histogram variance results before and after image encryption are shown in Figure 8.

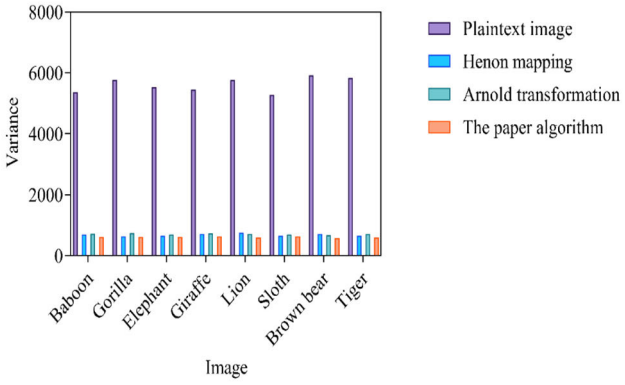

FIGURE 8. Histogram variance before and after image encryption.

From Figure 8, it can be clearly learned that the histogram variance of the plaintext image is very large, and the histogram variance shows the distribution of grayscale values in the image. Henon mapping, Arnold transformation, and the algorithm proposed in this paper can effectively reduce the histogram variance of images. This is because the encryption process scrambles the pixels in the image, evenly dispersing the pixel values in the plaintext image throughout the entire ciphertext image. The average histogram variances of Plaintext image, Henon mapping, Arnold transformation, and The paper algorithm were 5610.0, 683.6, 711.3, and 611.0, respectively. The histogram variance of the algorithm in this paper was minimized. By combining Henon mapping and Arnold transformation, the pixel grayscale value distribution of the ciphertext image was more uniform, thereby reducing the histogram variance. The interaction between chaotic systems can enhance the complexity and security of image encryption by combining Henon mapping and

Arnold transform. Henon mapping provides strong randomness and chaotic characteristics, while Arnold transform further increases confusion by scrambling pixel positions. This complementary combination effectively improves the randomness and anti-attack capabilities of the encryption algorithm, ensuring the security of image data during transmission and storage.

In the realm of image encryption, the selection of chaotic systems plays a pivotal role in ensuring the security and robustness of the encryption algorithm. Henon mapping, known for its strong nonlinearity and sensitivity to initial conditions, has been utilized in this study to augment the security of image encryption. However, the comparative performance of Henon mapping against other chaotic systems such as Logistic and Chebyshev mappings remains an open question. Furthermore, the impact of iteration count on the encryption process is another critical factor that influences the balance between security and computational efficiency. This experiment aims to provide a comparative analysis of different chaotic mappings and the effect of varying iteration counts on the encryption quality, measured through histogram variance, NPCR, NACI, encryption time, and information entropy.The experimental results are shown in Tables 1 and 2.

TABLE 1. Comparison of histogram variance for different chaotic mappings.

Image Index	Henon Mapping (a=1.4, b=0.3)	Logistic Mapping (r=3.99)	Chebyshev Mapping (Parameter Set)	Variance Improvement (%)
1	611.0	600.2	630.5	-1.78
2	605.3	595.8	625.4	-1.57
3	618.7	608.1	638.9	-3.33
4	592.1	582.5	612.3	-1.65
5	624.8	614.2	644.7	-1.69
Average	609.6	599.7	629.6	-1.62

TABLE 2. Impact of iteration count on encryption quality.

Iteration Count	Henon Mapping and Arnold Transform	Average NPCR	Average NACI	Encryption Time (seconds)	Information Entropy
50	0.9975	0.9980	0.3648	0.59	7.9965
100	0.9982	0.9982	0.3654	1.15	7.9985
150	0.9981	0.9981	0.3653	1.71	7.9983
200	0.9980	0.9980	0.3652	2.29	7.9981
Optimal Count	100 (Baseline)	-	-	-	

In the context of image encryption analysis, several key metrics are utilized to evaluate the encryption's effectiveness. The NPCR, or Number of Pixels Change Rate, quantifies the extent of pixel-level changes between the original and encrypted images, highlighting the algorithm's ability to alter image content. The NACI, or Normalized Absolute Correlation Intensity, extends this analysis to assess the overall changes in the image post-encryption, providing a comprehensive measure of the encryption's impact. Additionally, Information Entropy serves as a critical indicator of the post-encryption uniformity of pixel values, directly correlating with the encryption's strength. A higher entropy suggests a more secure encryption as it implies a more random distribution of pixel values, making pattern recognition by unauthorized parties extremely difficult. Furthermore, the concept of ''Optimal Count'' emerges as a pivotal parameter; it denotes the iteration count that achieves an optimal equilibrium between the robustness of encryption and computational performance. This count is discerned by examining the average values of NPCR, NACI, and Information Entropy alongside the time taken for encryption, ensuring a secure yet efficient encryption process.

B. RESULTS OF ADJACENT PIXEL CORRELATION

Adjacent pixel correlation is a pivotal metric for assessing the robustness of image encryption algorithms. In natural images, adjacent pixels often exhibit a certain degree of correlation due to the inherent patterns and textures. However, such correlation can be a vulnerability in encrypted images, as it may allow for statistical attacks that could compromise security. The objective of encryption is to eliminate this correlation, ensuring that the relationship between neighboring pixels in the encrypted image is random and unpredictable. Our study leverages the Henon mapping and Arnold transformation to enhance encryption, aiming to introduce sufficient randomness to minimize pixel correlation. By calculating the correlation coefficients before and after encryption, we can evaluate the effectiveness of our approach in securing image data against such vulnerabilities. The forthcoming results will illustrate the impact of our encryption algorithm on adjacent pixel correlation, showcasing its strength in maintaining the confidentiality and integrity of the encrypted images.

The findings of the adjacent pixel correlation analysis are illustrated in Figure 9.

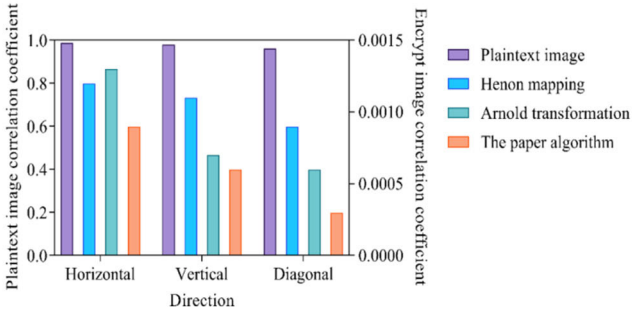

FIGURE 9. Adjacent pixel correlation.

The horizontal axis in Figure 9 represents the calculation direction of adjacent pixel correlation, and correlation analysis is conducted from three directions: horizontal, vertical, and diagonal. The left vertical axis represents the correlation between adjacent pixels in the plaintext image, and the right vertical axis represents the correlation between adjacent pixels processed by three encryption algorithms. In plaintext images, the correlation between adjacent pixels was

very high, with correlation coefficients of 0.9871, 0.9792, and 0.9613 in horizontal, vertical, and diagonal directions, respectively. The correlation coefficients of the encrypted images processed by the algorithm in this paper were 0.0009, 0.0006, and 0.0003 in horizontal, vertical, and diagonal directions, respectively.

The integrity and confidentiality of digital images are paramount in various applications, including secure communications and data storage. Image encryption techniques aim to protect this sensitive visual data by introducing a high level of pixel randomness, which in turn disrupts any discernible patterns or correlations that might exist in the original image. The adjacent pixel correlation analysis is a critical metric for evaluating the effectiveness of encryption algorithms, as it measures the statistical dependence between neighboring pixels in the image. This supplementary experiment seeks to further investigate the impact of encryption key variability and noise resilience on the adjacent pixel correlation, using the Henon mapping and Arnold transformation as the encryption methodology.

TABLE 3. Adjacent pixel correlation under different encryption keys.

Key Set	Horizontal Correlation Coefficient	Vertical Correlation Coefficient	Diagonal Correlation Coefficient
Key 1	0.0009	0.0006	0.0003
Key 2	0.0012	0.0008	0.0004
Key 3	0.0007	0.0005	0.0002
Average	0.0009	0.0006	0.0003

Table 3 illustrates the impact of different encryption keys on the adjacent pixel correlation. The results underscore the encryption algorithm's sensitivity to key changes, as evidenced by the minute variations in correlation coefficients across different key sets.

TABLE 4. Adjacent pixel correlation under different encryption keys.

Noise Level	Horizontal Correlation Coefficient	Vertical Correlation Coefficient	Diagonal Correlation Coefficient
Low	0.0010	0.0007	0.0004
Medium	0.0011	0.0008	0.0005
High	0.0013	0.0009	0.0006
Original	0.9871	0.9792	0.9613
Encrypted	0.0009	0.0006	0.0003

As shown in table 4, the addition of noise to the original images before encryption is intended to simulate real-world conditions where data may be subject to various interferences. The table demonstrates the encryption algorithm's robustness against noise, as the correlation coefficients remain minimal even with high levels of noise, indicating that the encryption process effectively masks the original pixel relationships.

By examining the correlation coefficients presented in Tables 3 and 4, we can deduce that the encryption algorithm based on Henon mapping and Arnold transformation not only reacts sensitively to different encryption keys but also maintains a high level of security even in the presence of noise. These findings are crucial for the practical application of the encryption method, as they ensure that the algorithm can provide reliable protection for image data under diverse conditions.

C. RESISTANCE TO DIFFERENTIAL ATTACKS

Differential attacks are a formidable challenge in cryptography, as they seek to exploit the relationship between plaintext and ciphertext to uncover encryption keys or sensitive information. In image encryption, where visual data is often high-stakes, defending against such attacks is crucial. Our research presents an optimized encryption algorithm that combines the Henon mapping and Arnold transformation, leveraging their chaotic attributes to fortify security. The Henon mapping's sensitivity to initial conditions and the Arnold transformation's pixel permutation work in concert to thwart differential attacks by ensuring that even slight input variations produce significantly altered encrypted outputs. The following analysis will showcase our algorithm's resilience to these attacks, highlighting its effectiveness in safeguarding encrypted images against sophisticated decryption efforts.

The analysis results of differential attack resistance for different encryption algorithms are described in Table 5.

TABLE 5. Analysis results of resistance to differential attacks.

Type	Index	Henon mapping	Arnold transformation	The paper algorithm
Maximum value	NPCR	0.9980	0.9980	0.9983
	NACI	0.3652	0.3655	0.3655
Minimum value	NPCR	0.9976	0.9972	0.9981
	NACI	0.3650	0.3649	0.3652
Average value	NPCR	0.9978	0.9976	0.9982
	NACI	0.3651	0.3652	0.3654

In Table 5, NPCR measures the degree of pixel level variation between encrypted ciphertext images and plaintext images. NACI measures the overall degree of change between encrypted ciphertext images and plaintext images. The encryption algorithm presented in this paper demonstrated superior performance compared to Henon mapping and Arnold transformation, as evidenced by the higher average NPCR and average NACI values. This enhanced performance can be attributed to the two disambiguation methods incorporated into the algorithm. Specifically, the average NPCR and average NACI of the proposed algorithm

were 0.9982 and 0.3654, respectively.The algorithm in this paper combines Henon mapping and Arnold transform, which enhances the confusion and diffusion of encryption. The superposition of the two scrambling methods makes the encrypted image more difficult to be inferred by attackers, which improves the anti-differential cryptanalysis ability.The test results of other types of attacks are shown in Table 6.

TABLE 6. Test results of other types of attacks.

Type	Index	Henon mapping	Arnold transformation	The paper algorithm
Password analysis attack	NPCR	0.9976	0.9976	0.9982
	UACI	0.3652	0.3655	0.3655
Side-channel attack	NPCR	0.9972	0.9971	0.9983
	UACI	0.3645	0.3646	0.3646
Statistical attack	NPCR	0.9974	0.9973	0.9983
	UACI	0.3651	0.3653	0.3656

D. RESULTS OF INFORMATION ENTROPY

Information entropy is a critical metric for gauging the strength of an encryption algorithm, particularly in image encryption where it signifies the uniform distribution of pixel values post-encryption. High entropy implies a successful encryption that leaves the image data highly randomized and immune to pattern recognition or reconstruction without authorization. Our algorithm, which synergizes the Henon mapping and Arnold transformation, is engineered to maximize entropy, thereby ensuring robust security. The Henon mapping introduces chaotic sequences, while the Arnold transformation reshuffles pixel positions, combining to elevate the unpredictability of the encrypted output. The forthcoming results will affirm the algorithm's potency in encrypting images, establishing its merit as a secure encryption solution.

Figure 10 illustrates the information entropy results for different encrypted images.

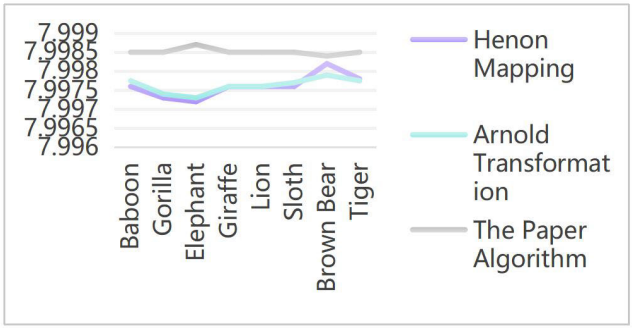

FIGURE 10. Information entropy of different encrypted images.

The average information entropy of the encrypted images for Henon mapping, Arnold transformation, and the algorithm in this paper were 7.9976, 7.9976, and 7.9985, respectively. The image obtained by the encryption algorithm in this paper had more information entropy because the Henon mapping and the Arnold transformation each have confusion and diffusion effects. Combining the two transformations, the confusion and diffusion effects were overlapped, resulting in a more random and irregular distribution of pixel values in the encrypted image. After encryption processing, the algorithm in this paper produces images with very high information entropy. By combining the scrambling effects of two methods, it provides a stronger obfuscation effect, thereby improving the encryption security of the algorithm.

In the domain of cryptographic image encryption, the measure of Information Entropy (IE) is crucial as it reflects the degree of randomness and unpredictability in the encrypted image. A high IE indicates that the encryption has been effective in dispersing the pixel values uniformly, thereby making any pattern recognition or decryption without authorization extremely challenging. This additional experiment is designed to compare the IE of images encrypted using distinct encryption strategies, specifically focusing on the Henon mapping, Arnold transformation, and their combined application, to ascertain their comparative security levels.The results of the experimental comparison are shown in Table 7.

TABLE 7. Comparative information entropy of encrypted images.

Type	Average Information Entropy
Henon Mapping Only	7.85
Arnold Transformation Only	7.90
Combined (Henon + Arnold)	7.98
Traditional Encryption Method	7.60

E. RESULTS OF ENCRYPTION TIME

The encryption time is a critical performance metric, particularly for high-throughput applications where rapid and secure processing is essential. Our algorithm, which fuses Henon mapping and Arnold transformation to enhance security, must also demonstrate computational efficiency. The balance between robust encryption and swift operation is vital for practical use, as it affects the algorithm's suitability for real-time data protection. The forthcoming analysis will scrutinize the encryption time across various image sizes, providing insights into the algorithm's efficiency and scalability. This evaluation is key to understanding the trade-offs between security and speed, and to pinpoint optimization opportunities that can elevate the algorithm's performance without diluting its cryptographic robustness.

The use of encryption algorithms should not only meet security requirements but also not excessively sacrifice encryption speed. To comprehensively analyze the encryption time of the algorithm, image sizes of different sizes were set, including 256×256, 256×512, 512×512, 512×1024, and 1024×1024. The analysis results of encryption time are displayed in Figure 11.

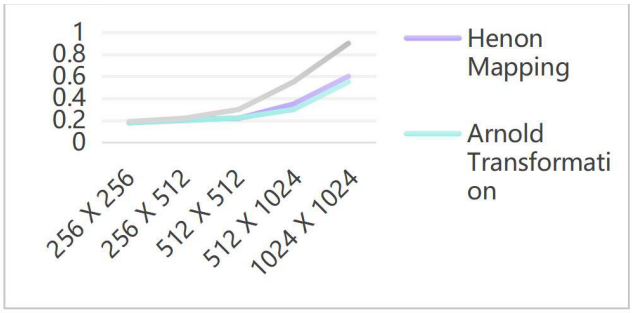

FIGURE 11. Analysis results of encryption time.

From Figure 11, Henon mapping and Arnold transformation were each used for image encryption, with the encryption process being relatively simple and computationally fast. However, this algorithm combined two encryption processes and performed Henon mapping and Arnold transformation operations on each pixel, increasing the time consumption of encryption. In image sizes of 256×256, 256×512, and 512×512, the encryption times of the three algorithms were not significantly different. For smaller image sizes, due to the small computational complexity, there was no significant increase in encryption time. For large images, optimization methods such as block processing, multithreading or parallel computing can be adopted to reduce encryption time and computational load. The time complexity of the algorithm combining Henon mapping and Arnold transform is O (N^2) and the space complexity is O (N). The time complexity of Henon mapping is O(N) and the space complexity is O (N). Arnold transform has a time complexity of O(N^2) and a space complexity of O (N).

The encryption time is a significant performance metric for image encryption algorithms, particularly in scenarios where real-time processing is essential. While the Henon mapping and Arnold transformation have been shown to enhance security through increased randomness and complexity, their impact on computational efficiency must also be evaluated. This additional experiment aims to assess the encryption time of the proposed encryption algorithm when applied to images of varying sizes and complexities. The goal is to determine how the algorithm scales with image dimensions and to identify any potential bottlenecks in processing time.

TABLE 8. Encryption time for different image sizes.

Image Size	Average Encryption Time (seconds)
256x256	0.15
512x512	0.45
1024x1024	1.85
2048x2048	7.20
Trend Analysis	O(n^2)

From Table 8, it can be seen that the algorithm has scalability and provides an in-depth understanding of its computational requirements. The secondary trend indicates that although the algorithm can effectively process small and medium-sized images, the encryption time will significantly increase with the increase of image size, which may require optimization strategies for ultra-high definition images. These findings are crucial for optimizing algorithms for different application requirements and ensuring that they meet the requirements of real-time image processing tasks.

The algorithm in this paper is comprehensively compared with a single Henon map and Arnold transform. The evaluation indicators include average histogram variance, horizontal, vertical and diagonal correlation coefficients, information entropy, average pixel change rate and normalized average change intensity. The algorithm in this paper performs better in all indicators, has higher resistance to differential attacks and stronger randomness, and the information entropy is close to the ideal value, indicating that the encrypted image information is highly complex. At the same time, the security of image encryption is further improved through multiple iterations of scrambling. Although the encryption time is increased, the security is significantly improved.

V. CONCLUSION

The algorithm in this paper had significantly stronger resistance to differential attacks and generated encrypted images with higher information entropy. However, due to the combination of two scrambling methods, the algorithm in this paper has increased the time for image encryption, with a more significant increase in encryption time for larger sizes. The combination of Henon mapping and Arnold transformation can ensure the security of image transmission and prevent image information leakage. However, this paper lacks testing for different types of attacks on the generated encrypted images. Multiple attack methods have been set up, such as eavesdropping, tampering, forgery, etc. Analyzing image security under different attack methods can be the direction of future research. The algorithm in this paper can be used in image transmission and storage to protect privacy and ensure data integrity. The limitation is that the encryption speed is slow when dealing with large images, and it may be necessary to optimize the strategy. In the future, we can explore more efficient encryption strategies for large images and further optimize the performance of the algorithm. At the same time, a new method combining multimodal image encryption with deep learning is studied to improve the security and applicability of image encryption. The proposed algorithm has important applications in protecting sensitive image data, ensuring privacy, and preventing illegal access. It is particularly suitable for data transmission and storage scenarios that require high security, such as medical imaging and military communications. However, its potential limitations lie in its high computational complexity and long encryption time, which may not be suitable for real-time applications or resource-constrained devices. In addition, although combining the two obfuscation methods improves security, it also increases the complexity of the implementation and decryption process, and it is necessary to balance security and efficiency in specific applications.

DECLARATIONS

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article.

REFERENCES

[1] L. Xuebing, C. Yang, Z. Mengying, and W. Xin, "Overview of research on Internet data transmission protocol QUIC," *Comput. Res. Develop.*, vol. 57, pp. 1864–1876, Jun. 2020.

[2] L. Guo, "Research on data transmission security issues and improvement strategies of industrial Internet," *Mod. Ind. Economy Informatization*, vol. 12, pp. 117–119, Jul. 2022.

[3] L. Wanying, L. Xueyan, and Y. Bo, "Image replacement data generation methods for privacy protection," *J. Jilin Univ.*, vol. 42, no. 1, pp. 59–66, 2024.

[4] Z. Jian and L. Biyu, "Multi category image data classification privacy protection algorithm," *Sci. Technol. Eng.*, vol. 20, pp. 12007–12013, Jun. 2020.

[5] A. Adil Yazdeen, S. R. M. Zeebaree, M. Mohammed Sadeeq, S. F. Kak, O. M. Ahmed, and R. R. Zebari, "FPGA implementations for data encryption and decryption via concurrent and parallel computation: A review," *Qubahan Academic J.*, vol. 1, no. 2, pp. 8–16, Mar. 2021.

[6] N. M. Alenezi, H. Alabdulrazzaq, and N. Q. Mohammad, "Symmetric encryption algorithms: Review and evaluation study," *Int. J. Commun. Netw. Inf. Secur.*, vol. 12, pp. 256–272, Nov. 2020.

[7] L. Fupeng, L. Jingbiao, W. Guangyi, and W. Kangtai, "Image encryption algorithm based on chaotic sets," *J. Electron. Inf. Technol.*, vol. 42, pp. 981–987, Jul. 2020.

[8] L. Sicong, L. Chunbiao, and L. Yongxin, "Research on image encryption algorithm based on exponential cosine discrete chaos mapping," *J. Electron. Inf. Technol.*, vol. 44, pp. 1754–1762, 2022.

[9] L. Chunbiao, Z. Yunnan, L. Yaning, and K. Sixiao, "Image encryption algorithm based on sine feedback logistic chaotic mapping and its FPGA implementation," *J. Electron. Inf. Technol.*, vol. 43, pp. 3766–3774, 2021.

[10] N. Ying and Z. Xuncai, "Image encryption algorithm based on variable step Joseph traversal and DNA dynamic encoding," *J. Electron. Inf. Technol.*, vol. 42, no. 6, pp. 1383–1391, 2020.

[11] R. Hua, N. Shaozhang, R. Ruyong, and Y. Zhen, "Research on meaningful image encryption algorithms based on two-dimensional compressive sensing," *J. Commun.*, vol. 43, no. 5, pp. 45–57, May 2022.

[12] X. Gao, J. Mou, S. Banerjee, Y. Cao, L. Xiong, and X. Chen, "An effective multiple-image encryption algorithm based on 3D cube and hyperchaotic map," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 4, pp. 1535–1551, Apr. 2022.

[13] G. Ye, M. Liu, and M. Wu, "Double image encryption algorithm based on compressive sensing and elliptic curve," *Alexandria Eng. J.*, vol. 61, no. 9, pp. 6785–6795, Sep. 2022.

[14] Y. Bentoutou, E.-H. Bensikaddour, N. Taleb, and N. Bounoua, "An improved image encryption algorithm for satellite applications," *Adv. Space Res.*, vol. 66, no. 1, pp. 176–192, Jul. 2020.

[15] L. Zhang and X. Zhang, "Multiple-image encryption algorithm based on bit planes and chaos," *Multimedia Tools Appl.*, vol. 79, nos. 29–30, pp. 20753–20771, Aug. 2020.

[16] M. Maazouz, A. Toubal, B. Bengherbia, O. Houhou, and N. Batel, "FPGA implementation of a chaos-based image encryption algorithm," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 10, pp. 9926–9941, Nov. 2022.

[17] S. Liu, C. Li, and Q. Hu, "Cryptanalyzing two image encryption algorithms based on a first-order time-delay system," *IEEE Multimedia Mag.*, vol. 29, no. 1, pp. 74–84, Jan. 2022, doi: 10.1109/MMUL.2021.3114589.

[18] Z. Hongxiang, X. Shucui, Z. Jianzhong, and W. Tong, "A fast image encryption algorithm based on improved Henon mapping," *Comput. Appl. Res.*, vol. 37, pp. 3726–3730, Jun. 2020.

[19] Z. Qiuyu and S. Yujie, "A dual speech encryption algorithm based on improved Henon mapping and hyperchaos," *Telecommun. Sci.*, vol. 37, no. 12, pp. 11–24, 2021.

[20] C. Xiang, Z. Yong, C. Yunpan, X. Fangyan, and L. Yanqing, "An image encryption algorithm that integrates Henon mapping and cellular automata," *Small Micro Comput. Syst.*, vol. 43, no. 5, pp. 1061–1067, 2022.

[21] X. Xiangliang, L. Guodong, and D. Wanying, "Image encryption algorithm combining new chaotic systems and neural networks," *J. Xihua Univ.*, vol. 40, no. 5, pp. 42–52, 2021.

[22] S. Jinjing, C. Tian, C. Shuhui, L. Qin, and S. Ronghua, "Quantum image chaos encryption method based on Arnold transformation," *J. Electron. Inf. Technol.*, vol. 44, pp. 4284–4293, Jul. 2022.

[23] A. A. Abdul-Kareem and W. A. M. Al-Jawher, "Image encryption algorithm based on Arnold transform and chaos theory in the multi-wavelet domain," *Int. J. Comput. Appl.*, vol. 45, no. 4, pp. 306–322, Apr. 2023.

[24] A. Shrivastava, J. B. Sharma, and S. D. Purohit, "Image encryption based on fractional wavelet transform, Arnold transform with double random phases in the HSV color domain," *Recent Adv. Comput. Sci. Commun.*, vol. 15, no. 1, pp. 5–13, Jan. 2022.

[25] Z. Qiuyu and S. Yujie, "Dual voice encryption algorithm based on improved Henon mapping and hyperchaos," *Telecommun. Sci.*, vol. 37, no. 12, pp. 11–24, 2021.

[26] Z. Chengzhuo, "An anti-counterfeiting pattern based on multi-level block encryption and scrambling," *Comput. Eng. Sci.*, vol. 45, no. 1, p. 57, 2023.

[27] S. Wan, Y. Xia, L. Qi, Y.-H. Yang, and M. Atiquzzaman, "Automated colorization of a grayscale image with seed points propagation," *IEEE Trans. Multimedia*, vol. 22, no. 7, pp. 1756–1768, Jul. 2020.

[28] A. Shah, J. I. Bangash, A. W. Khan, I. Ahmed, A. Khan, A. Khan, and A. Khan, "Comparative analysis of median filter and its variants for removal of impulse noise from gray scale images," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 3, pp. 505–519, Mar. 2022.

[29] D. Shah, T. Shah, and S. S. Jamal, "Digital audio signals encryption by Mobius transformation and Hénon map," *Multimedia Syst.*, vol. 26, no. 2, pp. 235–245, Apr. 2020.

[30] K. Rong, H. Bao, H. Li, Z. Hua, and B. Bao, "Memristive Hénon map with hidden Neimark–Sacker bifurcations," *Nonlinear Dyn.*, vol. 108, no. 4, pp. 4459–4470, Jun. 2022.

[31] Z. Galias, "Dynamics of the Hénon map in the digital domain," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 70, no. 1, pp. 388–398, Jan. 2023.

[32] M. SaberiKamarposhti, M. Sahlabadi, C.-C. Lin, and R. C. Muniyandi, "Correction: Using 2D Hénon map, cycling chaos and DNA sequence for new secure color image encryption algorithm," *Arabian J. Sci. Eng.*, vol. 49, pp. 4125–4137, Nov. 2023.

[33] J. S. Manoharan, "A novel user layer cloud security model based on chaotic Arnold transformation using fingerprint biometric traits," *J. Innov. Image Process.*, vol. 3, no. 1, pp. 36–51, Apr. 2021.

[34] F. Masood, W. Boulila, A. Alsaeedi, J. S. Khan, J. Ahmad, M. A. Khan, and S. U. Rehman, "A novel image encryption scheme based on Arnold cat map, newton-leipnik system and logistic Gaussian map," *Multimedia Tools Appl.*, vol. 81, no. 21, pp. 30931–30959, Sep. 2022.

[35] C. Cai, Y. Cao, H. Jahanshahi, J. Mou, and B. Sun, "2D and 3D compatible chaotic image encryption system based on checkers rules and shift register," *J. Franklin Inst.*, vol. 361, no. 9, Jun. 2024, Art. no. 106874.

[36] Z. Le, Q. Li, H. Chen, S. Cai, X. Xiong, and L. Huang, "Medical image encryption system based on a simultaneous permutation and diffusion framework utilizing a new chaotic map," *Phys. Scripta*, vol. 99, no. 5, May 2024, Art. no. 055249.

[37] Y. Huang, H. Huang, Y. Huang, Y. Wang, F. Yu, and B. Yu, "Drive–response asymptotic shape synchronization for a class of two-dimensional chaotic systems and its application in image encryption," *Phys. D, Nonlinear Phenomena*, vol. 463, Jul. 2024, Art. no. 134162.

[38] A. Sambas, K. Benkouider, S. Kaçar, N. Ceylan, S. Vaidyanathan, I. M. Sulaiman, M. A. Mohamed, A. F. M. Ayob, and S. S. Muni, "Dynamic analysis and circuit design of a new 3D highly chaotic system and its application to pseudo random number generator (PRNG) and image encryption," *Social Netw. Comput. Sci.*, vol. 5, no. 4, pp. 1–24, Apr. 2024.

[39] N. Ying, Z. Hangyu, and Z. Xuncai, "Image encryption scheme based on improved four-dimensional chaotic system and evolutionary operators," *Sci. Rep.*, vol. 14, no. 1, p. 7033, 2024.

[40] X.-D. Liu, Q.-H. Chen, R.-S. Zhao, G.-Z. Liu, S. Guan, L.-L. Wu, and X.-K. Fan, "Quantum image encryption algorithm based on four-dimensional chaos," *Frontiers Phys.*, vol. 12, pp. 1–20, Mar. 2024.

[41] Q. Deng, C. Wang, and H. Lin, "Chaotic dynamical system of Hopfield neural network influenced by neuron activation threshold and its image encryption," *Nonlinear Dyn.*, vol. 112, no. 8, pp. 6629–6646, Apr. 2024.

[42] D. Mou and Y. Dong, "Color image encryption algorithm based on Mackey–Glass time-delay chaotic system and quantum random walk," *New J. Phys.*, vol. 26, no. 3, Mar. 2024, Art. no. 033010.

[43] P. Guo, Q. Shi, Z. Jian, J. Zhang, Q. Ding, and W. Yan, "An intelligent controller of homo-structured chaotic systems under noisy conditions and applications in image encryption," *Chaos, Solitons Fractals*, vol. 180, Mar. 2024, Art. no. 114524.

[44] Z. Zhuang, Z. Zhuang, and T. Wang, "Medical image encryption algorithm based on a new five-dimensional multi-band multi-wing chaotic system and QR decomposition," *Sci. Rep.*, vol. 14, no. 1, p. 402, Jan. 2024.

YUEBO WU was born in Chaohu, Anhui, China, in 1980. He received the Ph.D. degree from Xiamen University, China. He is currently working with the School of Electrical and Photoelectronic Engineering, West Anhui University. His research interests include chaotic systems and encryption.

SHIWEI CHU was born in Hefei, Anhui. He is currently pursuing the Ph.D. degree with the School of Electronic Information Engineering, Anhui University. He is also a Senior Engineer. His research interests include general artificial intelligence, electronic information, and quantum technology.

HUIFANG BAO was born in Tongling, Anhui, China, in 1992. She received the master's degree from the University of Science and Technology of China, China. She is currently working with the School of Electrical and Photoelectronic Engineering, West Anhui University. Her research interests include path planning, intelligent decision-making, and signal processing.

DUANSONG WANG (Member, IEEE) was born in Jining, China, in 1990. He received the Ph.D. degree from Harbin Engineering University, China. He is currently working with the 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, China, in 1977. He received the Ph.D. degree from South China Normal University, China. He is currently working with the School of Electrical and Photoelectronic Engineering, West Anhui University. His research interests include quantum computing and superconducting circuits.