EAI Endorsed Transactions
on Scalable Information Systems

Research Article EAI.EU

A novel color image encryption method using Fibonacci transformation and chaotic systems

Chunming Xu[1,*]

[1]School of Mathematics and Statistics, Yancheng Teachers University, China

Abstract

INTRODUCTION: With the rapid proliferation of image data in networks, safeguarding image data has become an urgent and challenging task, wherein image encryption technology plays a pivotal role. This paper explores color image encryption algorithms and proposes a novel method aimed at enhancing the security and efficacy of image encryption.
OBJECTIVES: This study aims to effectively integrate information from different channels of color images to enhance the effectiveness of pixel decomposition-based image encryption algorithms. Additionally, it employs two different algorithms, Fibonacci matrix transformation and XOR diffusion operations, to modify pixel values, thereby enhancing the effectiveness of image encryption. Various metrics are utilized to analyze the encryption performance and compare it with existing image encryption algorithms.
METHODS: The pixel values of the R, G, and B channels of color images, each originally represented with 8 bits, are first divided into two integers ranging from 0 to 15, which are then merged into a new data matrix. Subsequently, multiple rounds of permutation are applied to the transformed matrix. Then, the Fibonacci transformation matrix is applied to further alter the values of the permuted matrix elements. Finally, XOR diffusion operations are executed to obtain the encrypted image.
RESULTS: Experimental results demonstrate that the proposed method achieves favorable outcomes across various image encryption metrics. The algorithm not only inherits advantages similar to those of bit-based image encryption techniques but also effectively integrates information from each channel of color images, thereby enhancing operational feasibility and security.
CONCLUSION: This study provides new insights and solutions for improved color image encryption, expectedly applicable in domains such as information concealment and data protection.

Received on 18 03 2024; accepted on 18 06 2024; published on 22 07 2024

Keywords: Image Encryption; Pixel Decomposition; Fibonacci transformation; Image Scrambling; Chaotic System.

doi:10.4108/eetsis.5452

1. Introduction

In today's information age, network data is experiencing exponential growth in various forms such as text, audio, images, and videos, becoming crucial foundations for scientific research, business decisions, and societal development. However, with the rapid increase in data volume and the ease of data exchange, cybersecurity issues are increasingly prominent[1–4]. Safeguarding personal privacy, national security, and commercial confidentiality poses not only technical challenges but also necessitates concerted efforts from governments, enterprises, and individuals to implement multi-layered preventive measures to ensure data integrity and confidentiality. Image data holds an increasingly significant position in networks, facilitated by the widespread adoption of smart devices enabling effortless generation and sharing of large quantities of images. These images encompass personal records as well as critical information in domains such as medical imaging, satellite imagery, and security monitoring. Consequently, protecting the security and privacy of image data has emerged as a pivotal aspect of contemporary cybersecurity efforts. These factors have prompted researchers to delve deeply into image encryption technologies to ensure the security and

*Corresponding author. Email: ycxcm@126.com

integrity of images during transmission, storage, and processing, thereby meeting the security requirements of image data in the digital age [5–7].

The objective of image encryption is to transform and manipulate image data using cryptographic methods and algorithms, rendering it into an unintelligible format to prevent unauthorized access or tampering by third parties. These algorithms typically involve rearranging pixels, confusing them, or performing mathematical operations, thereby maintaining the structural integrity of the image while making the encrypted content difficult to identify or revert to its original form. This security measure not only applies to safeguarding personal privacy but also provides critical protection for the transmission and storage of sensitive information [8–10].

Traditional encryption methods like Data Encryption Standard (DES)[11], Advanced Encryption Standard (AES)[12], Rivest Shamir Adleman (RSA)[13], and Elliptic Curve Cryptography (ECC)[14] are optimized for encrypting textual data. Image data, being two-dimensional, large-scale, and rich in redundancy, differs significantly in structure and nature from traditional textual data. This unique combination of visual perception, contextual relevance, and diversity renders traditional encryption algorithms unsuitable for image encryption.

Chaos, a dynamic behavior marked by complexity, unpredictability, and sensitivity, exhibits traits like unpredictability, sensitivity to initial conditions, aperiodicity, fractal structure, and specific statistical properties. These characteristics make chaos an intriguing and complex phenomenon with extensive research and application potential across fields like science, mathematics, and engineering. Chaos has found widespread application in image encryption[15–17]. By integrating chaotic sequences with image data, highly random encrypted images can be generated. This approach offers strong resistance against statistical analysis and cryptographic attacks but necessitates precise parameters and initial conditions for decryption.

So far, researchers have proposed many different chaotic image encryption algorithms, such as those based on Zigzag transformations[18, 19], Josephus transformation[20, 21], Arnold transformation[22, 23], etc. Many image encryption algorithms are based on pixel-level. In recent years, bit-level image encryption methods have attracted the attention of researchers because they can change pixel values as well as the location of pixels within the image. To date, many bit-level image encryption algorithms have been proposed[24–26]. However, bit-level image encryption algorithms are more complex to implement compared to pixel-level image encryption. In light of this, the literature[27] proposes an image encryption algorithm based on pixel decomposition that not only has the advantages of bit-level image encryption but also has relatively reduced complexity. However, when encrypting color images, it encrypts the R, G, B three components separately, without considering the effective fusion between different channel pixels. Regarding this, this paper combines image pixel decomposition with Fibonacci transformation and chaotic sequences to propose a new image encryption algorithm. This algorithm not only has the advantages of bit encryption algorithms but also allows for better integration of pixels from different image channels.

The remainder of this paper is organized as follows: Section 2 provides a review of fundamental knowledge. Section 3 introduces the proposed image encryption scheme. Section 4 presents the experimental results and the security of the presented method. Finally, Section 5 concludes this paper.

2. Fundamental Knowledge

2.1. Chaotic systems

Recently, Dong presented a three dimensional chaotic system: a novel three dimensional chaotic system which has a hidden attractor and coexisting attractors and is described by the following mathematical expression[28]:

$$\begin{cases} \dot{x_1} = a(x_2 - x_1) \\ \dot{x_2} = cx_1 - x_1x_3 \\ \dot{x_3} = -bx_3 + x_1x_2 - d \end{cases} \tag{1}$$

where x_1, x_2, x_3 are state variables, and a, b, c, d are system parameters. When the system parameters are $a = 35, b = 3, c = 35, d = 10$, the chaotic system (1) exhibits complex chaotic behavior. In addition, it has a higher value of the largest Lyapunov exponent than the original Chen chaotic system. The state space plots for system (1) when $(a, b, c, d) = (35, 3, 35, 10)$ and the initial values are $(x0, y0, z0) = (1, 1, 1)$ are shown in Figure 1. From Figure 1, it can be seen that the system has unpredictable and complex dynamic behavior, making it more suitable for image encryption problems.

2.2. Image Pixel Decomposition

The main idea of image pixel decomposition is to break down each 8-bit image pixel value into two 4-bit binary numbers, and then convert them into two integers ranging between 0 to 15[27]. For instance, if the pixel value of the image is 105, first convert it into the binary sequence 01101001, then divide it into two binary sequences of length 4, which are 0110 and 1001, and further convert them into two decimal numbers, 6 and 9. Similarly, we can provide the inverse transformation of the pixel decomposition process. For example, if there are two adjacent elements, 6 and

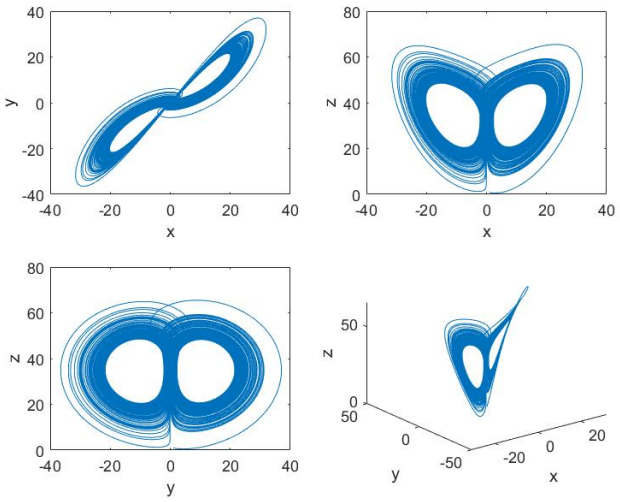

Figure 1. Typical dynamical behaviors of the chaotic system.

9, first convert them into binary numbers 0110 and 1001, respectively. By concatenating 0110 and 1001, we obtain an 8-bit binary number 01101001, which can be further converted into the decimal number 105.

Assuming the image's width is M and height is N, we can transform it into an $M \times 2N$ matrix through pixel decomposition. As for color images, since they have three components: R, G, and B, we can decompose and reassemble them to obtain a matrix of size $3M \times 2N$.

2.3. Fibonacci Matrices

Fibonacci sequence is a recursive sequence defined based on the following mathematical expression:

$$F(n) = F(n-1) + F(n-2) \tag{2}$$

where $F(1)$ and $F(2)$ are both equal to 1 and n is a positive integer greater than 2. The Fibonacci matrix is a generalization based on the Fibonacci sequence[29]. It is defined as follows:

$$W_n = \begin{bmatrix} F(n+1) & F(n) \\ F(n) & F(n-1) \end{bmatrix}. \tag{3}$$

where $F(n)$ is the Fibonacci sequence. The inverse matrix W_n^{-1} of W_n is:

$$W_n^{-1} = \begin{bmatrix} F(n-1) & -F(n) \\ F(-n) & F(n+1) \end{bmatrix}. \tag{4}$$

When multiplying a data matrix B with matrix W_n, it can replace the element values of the matrix B. When decrypting, we can multiply the encryption matrix with W_n^{-1}.

3. The Encryption Method

The proposed encryption algorithm consists of three stages. The first stage involves decomposing and scrambling the image pixels; the second stage performs a Fibonacci transformation operation; the third stage is an XOR diffusion process to obtain the final ciphered image. The structure of the encryption algorithm is shown in Figure 2.

Assume that the size of the color plain image P is $M \times N \times 3$, where M and N are the height and width of the image, respectively. Denote the color components of red, green and blue of P as P_R, P_G and P_B, respectively. The specific steps of the proposed encryption algorithm are described as follows:

3.1. Generation of the chaotic encryption sequences

Using the relevant information of plaintext images to generate the initial state value of the chaotic system, which will enhance the correlation between the proposed encryption algorithm and plaintext information. In this paper, the plaintext image P will be used as the input data of the SHA256 function to generate a 256-bit hash key. Then, this 256-bit hash key will be divided into 32 decimal numbers with each group containing 8 bits, and represented by K as:

$$K = k_1, k_2, \cdots, k_{32} \tag{5}$$

The initial values x_0, y_0, z_0 of the chaotic system (1) is calculated utilizing the following equations:

$$\begin{cases} x_0 = \frac{1}{256}(k_1 \oplus k_4 \oplus \cdots \oplus k_{28}) \\ y_0 = \frac{1}{256}(k_2 \oplus k_5 \oplus \cdots \oplus k_{29}) \\ z_0 = \frac{1}{256}(k_3 \oplus k_6 \oplus \cdots \oplus k_{30}) \end{cases} \tag{6}$$

In addition, we also calculate two integer values T_1 and T_2:

$$\begin{cases} T_1 = (k_{31} \oplus k_{32}) \mod 5 + 50 \\ T_2 = 2 * (abs(k_{31} * k_{32}) \mod 6 + 2) \end{cases} \tag{7}$$

which are the number of scrambling rounds and the order of the Fibonacci matrix, respectively.

3.2. Matrix scrambling

The primary objective of scrambling is to disrupt the spatial correlation between adjacent elements and conceal the original visual information. The scrambling process involves the following steps:

(1) Decompose each element of the image to transform the image of size $M \times N$ into a data matrix of size $M \times 2N$, with elements being integers between 0 and 15. For a color image, we can separately transform its R, G, B components P_R, P_G and P_B and then combine them into a $3M \times 2N$ data matrix P_1.

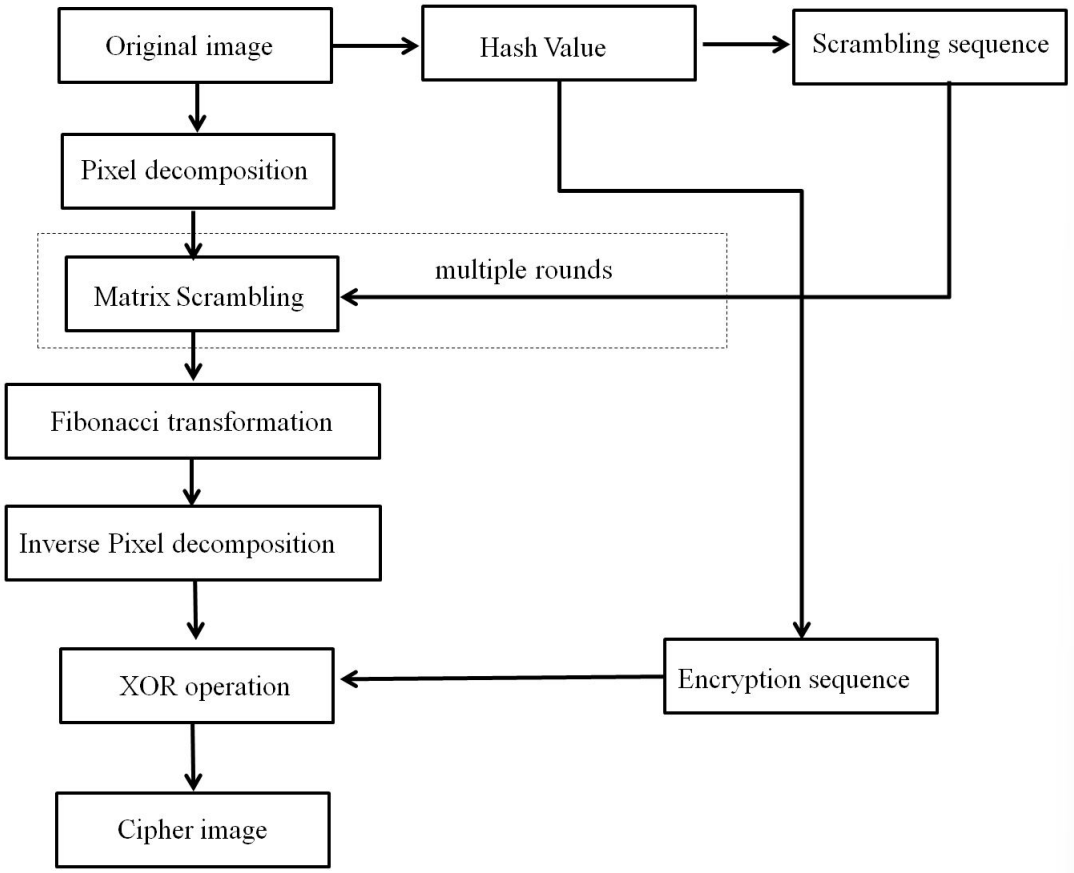

Figure 2. Flow chart of the image encryption algorithm.

(2) Iterate system (1) $2000 + L$ times with the initial values x_0, y_0, z_0 and then remove the former 2000 values so that three chaotic sequences s_1, s_2, s_3 of length L are gotten, where $L = max\{3M, 2N\}$. Calculate two sequences v_1, v_2 which will be used in the following scrambling process with s_1, s_2, s_3 by

$$\begin{cases} v_1 = floor(|(s_1 + s_2)(2001 : 2000 + T_1 * 3M)| \\ \times 10^{10} \mod 2N) \\ v_2 = floor(|(s_2 + s_3)(2001 : 2000 + T_1 * 2N)| \\ \times 10^{10} \mod 3M) \end{cases} \tag{8}$$

(3) The elements of matrix P_1 are scanned using v_1 and v_2 to change their positions.

The specific algorithm is shown in Algorithm 1. Where, circshift is a circular shift function. Through matrix scrambling, not only the correlation among pixels is disrupted, but the effective fusion of the elements from the different R, G, and B components is also achieved. Additionally, due to the change in positional relationships between adjacent elements, if an inverse pixel decomposition transformation is applied, a matrix different from the original image pixel matrix will be obtained.

Algorithm 1: Matrix scrambling

Input: matrix P_1; vectors v_1 and v_2
Result: Scrambled matrix P_2

initialization;
for k=1:T_1 **do**
  $m_1 = v_1((k-1) * 3M + 1 : k * 3M)$;
  $m_2 = v_2((k-1) * 2N + 1 : k * 2N)$;
  for i=1:$3M$ **do**
    $P_1(i,:) = circshift(P_1(i,:), [0, m_1(i)])$
  end
  ;
  for i=1:$2N$ **do**
    $P_1(:,i) = circshift(P_1(:,i), [m_2(i), 0])$
  end
  ;
  P_2=P_1;
end
return P_2

3.3. Fibonacci Matrix transformation

Calculate the Fibonacci matrix of order T_2 and use it to scramble the object matrix P_2. The specific algorithm is shown in Algorithm 2.

Algorithm 2: Fibonacci Matrix transformation

Input: matrix P_2;Fibonacci matrix W_n
Result: Scrambled matrix P_3

initialization;
for $i = 1 : 2 : 3M$ **do**
  for $j = 1 : 2 : 2N$ **do**
    $A = \begin{bmatrix} P_2(i,j) & P_2(i,j+1) \\ P_2(i+1,j) & P_2(i+1,j+1) \end{bmatrix}$;
    $M = W_n * A$;
    $P_3(i,j) = M(1,1)$;
    $P_3(i,j+1) = M(1,2)$;
    $P_3(i+1,j) = M(2,1)$;
    $P_3(i+1,j+1) = M(2,2)$;
  end
end
return P_3

After applying the Fibonacci matrix transformation, we obtain a new matrix P_3. Through the Fibonacci matrix transformation, the values of the elements will be further altered.

3.4. Pixel diffusion

Do the iteration system (3) $2000 + M * N$ times with the parameters x_0, y_0, z_0 and then remove the former 2000 values so that three chaotic sequences x_s, y_s, z_s of length $M * N$ are gotten. Calculate three sequences m_1, m_2, m_3 which will be used in the following encryption process with x_s, y_s, z_s by

$$\begin{cases} m_1 = |x_s| \times 10^{15} \mod 256 \\ m_2 = |y_s| \times 10^{15} \mod 256 \\ m_3 = |z_s| \times 10^{15} \mod 256 \end{cases} \tag{9}$$

Merging the neighboring elements within matrix P_3 to create matrix P_4 via the inverse process of pixel decomposition, with matrix P_3 having dimensions $3M$ by $2N$ and matrix P_4 having dimensions $3M$ by N. Furthermore, we split the matrix P_4 into three vectors V_R, V_G, V_B each with dimensions $M * N$. We perform a diffusion operation on V_R, V_G, V_B with the sequences m_1, m_2, m_3 to further alter the pixel values. The specific method is as follows:

$$\begin{cases} C_R(1) = V_R(1) \oplus (mod(V_R(L) + V_G(L) + V_B(L)), 256) \\ \oplus m_1(1) \\ C_G(1) = V_G(1) \oplus (mod(V_R(L) + V_G(L) + V_B(L)), 256) \\ \oplus m_2(1) \\ C_B(1) = V_B(1) \oplus (mod(V_R(L) + V_G(L) + V_B(L)), 256) \\ \oplus m_3(1) \end{cases} \tag{10}$$

and

$$\begin{cases} C_R(i) = V_R(i) \oplus (mod(C_R(i-1) + C_G(i-1) + C_B(i-1)), \\ 256) \oplus m_1(i) \\ C_G(i) = V_G(i) \oplus (mod(C_R(i-1) + C_G(i-1) + C_B(i-1)), \\ 256) \oplus m_2(i) \\ C_B(i) = V_B(i) \oplus (mod(C_R(i-1) + C_G(i-1) + C_B(i-1)), \\ 256) \oplus m_3(i) \end{cases} \tag{11}$$

where $2 \le i \le M * N$.

Transform C_R, C_G, C_B into matrix forms and combine them to demonstrate the encrypted color image C.

4. The Decryption Method

The decryption process is the inverse of the encryption process. It mainly includes the following steps:

Step(1) : Perform an XOR transformation on the three components of the cipher image C.

Step(2) : Perform image pixel decomposition on the matrix obtained from Step (1) and combine it into a 3M*2N matrix.

Step(3) : Apply the Fibonacci inverse transform and the inverse scrambling operation to the matrix obtained from Step (2).

Step(4) : Carry out the inverse image pixel decomposition transform on the matrix obtained from Step (3) and further combine it to form the original plaintext image.

5. Tests and Analysis of the Proposed Scheme

In the experiment, three standard color test images with a size of $256 \times 256 \times 3$ were used. They are Airplane, Lena and Peppers. Figure 3 shows the encrypted and decrypted images corresponding to the plaintext images.

From Figure 3, it can be observed that the encrypted ciphertext images appear as a disordered, snowflake-like noise images. Therefore, the encrypted images effectively conceal the information of the original plaintext images. Furthermore, the decrypted images are identical to the original images, indicating the effectiveness of the decryption algorithm.

5.1. Key space analysis

In encryption systems, the size of the key space is a crucial factor. The larger the key space, the more effectively it can prevent brute-force attacks. The size of the key space is mainly determined by factors such as the parameters and initial values of the key. The key space of the proposed algorithm consists of nine parameters $(a, b, c, d, x_0, y_0, z_0, T_1, T_2)$, which are the initial values of the chaotic system parameters, the control parameter of the chaotic system, the iteration

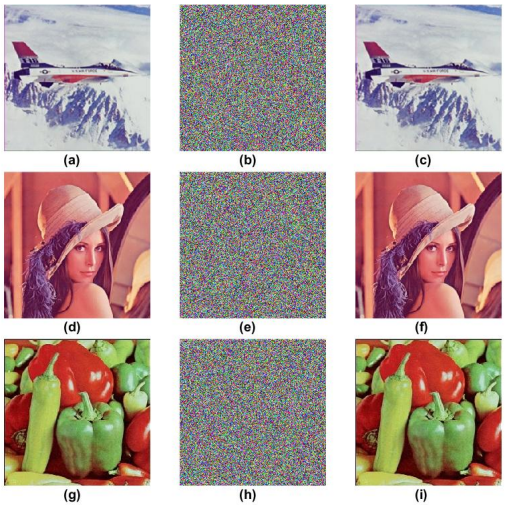

Figure 3. The experimental results of the encrypted images. (a) Plaintext Airplane. (b)Ciphertext of Airplane. (c) Decryption of Airplane. (d) Plaintext Lena. (e)Ciphertext of Lena. (f) Decryption of Lena. (g) Plaintext Peppers. (h)Ciphertext of Peppers. (i) Decryption of Peppers.

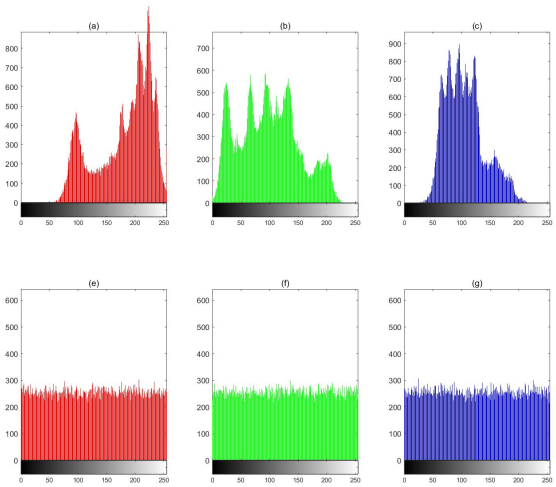

Figure 4. Histograms of Lena in red, green, and blue. Histograms of original and corresponding encrypted images in rows 1 and 2, respectively.

count T_1 of the permutation operation and the order of T_2 the Fibonacci matrix. Assuming that each parameter is represented with double precision up to 15 decimal places, the key space of the encryption algorithm is more than 10^{105}, that is approximately 2^{348}. So the key space of the encryption system far exceeds the suggested 2^{100}. Therefore, this algorithm has a sufficiently large key space, and the proposed method can effectively resist brute-force attacks.

5.2. Histogram analysis

The histogram gives a representation of the distribution of pixel values in a digital image, specifically the count of pixels for each grayscale level. If the histogram of an image is evenly distributed, attackers will be unable to glean meaningful information from the statistical analysis of grayscale values. Figure 4 display the grayscale histograms of the plaintext Lena image and its corresponding encrypted image in R, G, B channels. As Figure 4 reveals, the grayscale distribution of the plaintext image is uneven, making it susceptible to statistical attacks. Conversely, the histogram of the encrypted image appears flat, indicating effective concealment of the plaintext information.

5.3. Correlation analysis

For a plaintext image, the pixel values vary continuously in a two-dimensional plane, leading to strong correlations between adjacent pixels in both horizontal and vertical directions. To effectively encrypt the image, the correlation between adjacent pixels must be minimized, making the pixel values unpredictable. Formula(12) can be used to calculate the correlation coefficient between adjacent pixels in an image[30]:

$$r_{xy} = \frac{\sum_{i=1}^{N}((x_i - E(x))(y_i - E(y)))}{\sqrt{(\sum_{i=1}^{N}(x_i - E(x))^2)(\sum_{i=1}^{N}(y_i - E(y))^2)}} \tag{12}$$

$$E(x) = \sum_{i=1}^{N} x_i \tag{13}$$

$$E(y) = \sum_{i=1}^{N} y_i \tag{14}$$

where x_i and y_i are gray-level values of the selected adjacent pixels, and N is the number of sample pixels.

To assess the correlation between adjacent pixels in both the plaintext and encrypted images, we randomly selected 5000 pairs of adjacent pixels from the R, G, and B channels in both the original and encrypted images. We then calculated the correlation using Formula(12). Table 1 details the specific correlation coefficient values. Additionally, Figure 5 and Figure 6 illustrate the distribution of correlation between adjacent pixels in the plaintext and encrypted image of Lena, respectively. By comparing Figure 5 and Figure 6, it becomes evident that the adjacent pixels in the plaintext image exhibit high correlation, whereas the correlation between adjacent pixels in the encrypted image approaches zero. This suggests that the encryption algorithm effectively reduces correlation, demonstrating strong decorrelation capabilities.

Table 1. Correlation coefficients of the R,G and B components of the plaintext color image of Peppers

Image	Color	Plain Image			Cipher Image		
		H	V	D	H	V	D
Airplane	R	0.9519	0.9484	0.9052	0.0206	-0.0191	0.0225
	G	0.9598	0.9562	0.9223	-0.0029	0.0218	0.0002
	B	0.9421	0.9274	0.8869	0.0002	-0.0101	0.0184
Lena	R	0.9428	0.9709	0.9195	0.0001	-0.0105	-0.0176
	G	0.9435	0.9709	0.9219	-0.0005	-0.0013	0.0094
	B	0.8982	0.9466	0.8641	0.0091	-0.0029	0.0076
Peppers	R	0.9365	0.9358	0.8886	-0.0099	-0.0007	0.0052
	G	0.9694	0.9718	0.9474	0.0275	-0.0099	0.0154
	B	0.9343	0.9390	0.8908	0.0085	0.0020	-0.0122

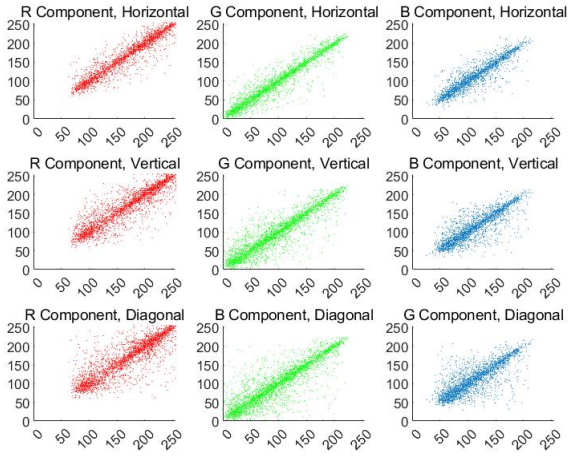

Figure 5. Correlation distributions of plaintext Lena image in each direction.

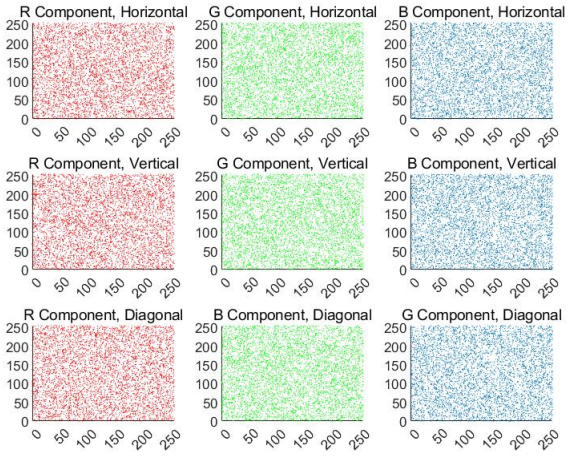

Figure 6. Correlation distributions of encrypted Lena image in each direction.

5.4. Information entropy analysis

Information entropy measures the randomness and disorder within information. A higher entropy for the encrypted image indicates greater randomness and subsequently higher security. The formula for calculating information entropy is provided by [31] as:

$$H(m) = -\sum_{i=0}^{255} P(m_i) \log_2 P(m_i) \tag{15}$$

In this equation, m_i refers to the $i-th$ gray level in a digital image, and $P(m_i)$ represents the probability of m_i.

For color images, we can calculate the information entropy for each of the R, G, and B components separately. The specific calculation results are shown in Table 2. As can be seen from Table 2, the information entropies of the encrypted images are all very close to the ideal value of 8, indicating that the algorithm exhibits good randomness and security.

5.5. Analysis of differential attack resistance

The ability to resist differential attacks is a key metric for gauging the efficacy of image encryption. This metric is typically evaluated using two standards: the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI)[32]. The NPCR calculates the percentage of pixel value alterations in the encrypted image resulting from random modifications to any pixel in the unencrypted

Table 2. Information entropy for color images

Image	Plain Image			Cipher Image		
	R	G	B	R	G	B
Airplane	6.8072	6.8738	6.3298	7.9976	7.9970	7.9971
Lena	7.2763	7.5834	7.0160	7.9974	7.9974	7.9972
Peppers	7.4200	7.6644	7.1570	7.9971	7.9968	7.9964

image. In contrast, UACI provides a measure of the specific extent of these changes. To compute NPCR and UACI for two images, we can use the following formulas:

$$NPCR = \frac{\sum_{ij} D_{ij}}{W \times H} \times 100\% \tag{16}$$

$$UACI = \frac{1}{W \times H} \frac{\sum_{ij} (C_1(i,j) - C_2(i,j))}{255} \times 100\% \tag{17}$$

where $C_1(i,j)$ and $C_2(i,j)$ are the encrypted images for the plain images and D_{ij} is defined by

$$D_{ij} = \begin{cases} 0 & \text{if } C_1(i,j) = C_2(i,j) \\ 1 & \text{if } C_1(i,j) \neq C_2(i,j) \end{cases} \tag{18}$$

The theoretical values for NPCR and UACI are 99.609375% and 33.463541%, respectively.

Table 3 displays the NPCR and UACI values for each image's R, G, and B components. Notably, these values align closely with the theoretical standards, underscoring the algorithm's exceptional resistance to differential attacks.

5.6. Performance comparison with other methods

To further substantiate the effectiveness of the proposed method, this study compares it with the other three image encryption techniques reported in [27], [33] and [34]. The evaluation metrics include entropy, NPCR, UACI, and correlation coefficient analysis. The detailed data are presented in Table 4.

According to the data displayed in Table 4, our method outperforms the results from literature [27], indicating that the fusion method we proposed for the R, G, B channels can enhance the image encryption effect. Additionally, the performance of our encryption method is competitive when compared with the methods in literature [33] and [34], demonstrating the efficacy of the proposed method.

6. Conclusions

In this study, based on the concept of image pixel decomposition, combined with the Fibonacci transformation matrix and chaotic sequence, we propose a novel image encryption algorithm. The security assessment of this technique proves its robustness and effectiveness. The main advantages of the paper are as follows:

(1) Similar to bit-based image encryption algorithms, the method proposed in this paper decomposes pixels into smaller units and applies scrambling operations, thereby enhancing the complexity and effectiveness of the encryption process. Moreover, compared to bit-based approaches, the implementation of this method is more convenient and efficient for image encryption.

(2) Many conventional image encryption algorithms rely solely on simple operations like XOR diffusion to alter pixel values. In contrast, the method proposed in this paper incorporates both XOR diffusion and Fibonacci matrix transformation, which jointly modify pixel values more effectively to conceal sensitive image information. The introduction of the Fibonacci matrix not only increases the randomness of the encryption process but also enhances the algorithm's resilience against cryptographic analysis, ensuring the security and reliability of the encrypted images.

(3) Unlike traditional methods that individually encrypt the R, G, and B channels of color images, the method proposed in this paper integrates these three channel components effectively, enabling their mutual influence and synergy. This comprehensive encryption strategy significantly enhances the overall security of encrypted images. Therefore, this method is more suitable for protecting and transmitting color images, offering new insights and approaches for research and practice in the field of digital image security.

From the experimental results, the proposed method shows good performance and is a relatively effective image encryption algorithm.

Acknowledgments

The authors would like to express their sincere gratitude to the anonymous reviewers for their insightful feedback. This work is partially supported by the Jiangsu Higher Education Institutions of China (Grant No.23KJA120004).

References

[1] Yin J, Tang M, Cao J, S, et al. Knowledge-Driven Cybersecurity Intelligence: Software Vulnerability Coexploitation Behavior Discovery. IEEE Transactions on Industrial

Table 3. NPCR and UACI results for color images

Image	NPCR			UACI		
	R	G	B	R	G	B
Airplane	0.9960	0.9964	0.9958	0.3365	0.3363	0.3366
Lena	0.9961	0.9962	0.9962	0.3358	0.3349	0.3354
Peppers	0.9962	0.9959	0.9958	0.3347	0.3351	0.3349

Table 4. Performance comparison with other methods of the Lena image

Index	Color	Ref.[33]	Ref.[34]	Ref.[27]	Proposed
Horizontal Correlation	R	-0.0137	0.0071	0.0220	0.0001
	G	-0.0246	-0.0005	-0.0323	-0.0005
	B	-0.0137	-0.0029	0.0092	0.0091
Vertical Correlation	R	-0.0237	0.0009	-0.0122	-0.0105
	G	-0.0170	-0.0034	-0.0175	-0.0013
	B	0.0023	0.0045	0.0300	-0.0029
Diagonal Correlation	R	0.0109	0.0026	-0.0347	-0.0176
	G	-0.0133	-0.0034	0.0123	0.0094
	B	-0.0013	0.0008	0.0053	0.0076
NPCR(%)	R	99.61%	99.63%	99.59%	99.61%
	G	99.61%	99.63%	99.61%	99.62%
	B	99.61%	99.62%	99.62%	99.62%
UACI(%)	R	33.47%	33.50%	33.34%	33.58%
	G	33.48%	33.56%	33.53%	33.49%
	B	33.47%	33.53%	33.49%	33.54%
Information entropy	R	7.9892	7.9971	7.9969	7.9974
	G	7.9898	7.9971	7.9972	7.9974
	B	7.9899	7.9973	7.9976	7.9972

Informatics. 2023, 19(4) : 5593-5601.
[2] You M, Yin J, Wang H, et al. A knowledge graph empowered online learning framework for access control decision-making. World Wide Web. 2023, 26: 827–848.
[3] Dharmaraj R Patil, Tareek M Pattewar. Majority voting and feature selection based network intrusion detection system. EAI Endorsed Transactions on Scalable Information Systems. 2022, 9(6), 2022: e6.
[4] Venkateswaran N, Prabaharan S P. An efficient neuro deep learning intrusion detection system for mobile adhoc networks. EAI Endorsed Transactions on Scalable Information Systems. 2022, 9(6), 2022: e7.
[5] Yan S H, Li L, Gu B X, et al. Design of hyperchaotic system based on multi-scroll and its encryption algorithm in color image. Integration. 2023, 88: 203-221.
[6] Qu G, Meng X, Yin Y. Optical color image encryption based on Hadamard single-pixel imaging and Arnold transform. Optics and Lasers in Engineering. 2021, 137(20) : 106392.
[7] Wang X, Su Y. Image encryption based on compressed sensing and DNA encoding. Signal Processing Image Communication. 2021, 12: 116246.
[8] Naim M, Pacha A A, Serief C. A novel satellite image encryption algorithm based on hyperchaotic systems and Josephus Problem. Progress in space research. 2021, 67(7) : 2077-2103.
[9] Zhang X, Wang L, Wang Y, et al. An image encryption algorithm based on hyperchaotic system and variable-step josephus problem. International Journal of Optics. 2020, 4:1-15.
[10] Gao H, Wang X Y. An image encryption algorithm based on dynamic row scrambling and ZigZag transform. Chaos, Solitons and Fractals. 2021, 147(6) :110962.

[11] Diffie W, Hellman M E. Exhaustive Cryptanalysis of the NBS Data Encryption Standard. IEEE Computer. 1977, 10(6) :74-84.
[12] Stinson D R. Cryptanalysis of the AES: A Brief Survey. Journal of Cryptology. 2002, 15(2) :143-158.
[13] Rivest R L., Shamir A, Adleman L M. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM. 1978, 21(2) : 120-126.
[14] Smart N P. The discrete logarithm problem on elliptic curves of trace one. Journal of Cryptology. 2004, 17(3) :143-145.
[15] Huang H, Cheng D. 3-image bit-level encryption algorithm based on 3D nonequilateral arnold transform and hyperchaotic system. Security and Communication Networks. 2020,7:1-13.
[16] Dong H, Bai E, Jiang X Q . Color image compression-encryption using fractional-order hyperchaotic system and DNA coding. IEEE Access. 2020, 8:163524-163540.
[17] Wang X Y, Wang X L , Teng L, et al. Lossless embedding: A visually meaningful image encryption algorithm based on hyperchaos and compressive sensing. Chinese Physics B. 2023, 2: 020503.
[18] Wang X Y, Guan N N. A novel chaotic image encryption algorithm based on extended Zigzag confusion and RNA operation. Optics and Laser Technology. 2020, 131 (11):106366.
[19] Xu X, Feng J. Research and implementation of image encryption algorithm based on zigzag transformation and inner product polarization vector. IEEE International Conference on Granular Computing. San Jose, California, USA, 2010:556-561.
[20] Wang X Y, Sun H H. A chaotic image encryption algorithm based on improved Joseph traversal and cyclic shift function Optics and Laser Technology. 2020, 122 (2): 105854.
[21] Guo Y, Shao L P, Yang L . Bit-level image encryption algorithm based on Josephus and Henon chaotic map. Application Research of Computers. 2015, 32 (4): 1131-1137.
[22] Singh P, Yadav A K, Singh K. Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition. Optics and Lasers in Engineering. 2017, 91 (4):187-195.
[23] Chen L F, Zhao D M, Ge F. Image encryption based on singular value decomposition and Arnold transform in fractional domain. Optics Communications. 2013, 291: 98-103.
[24] Xiong G Q, Cai Z C, Zhao S F. A bit-plane encryption algorithm for RGB image based on modulo negabinary code and chaotic system. Digital Signal Processing. 2023, 141(9):104153.
[25] Wu J H, Liao X F, Yang B. Cryptanalysis and enhancements of image encryption based on three-dimensional bit matrix permutation. Signal Processing. 2018, 142 (7):292-300.
[26] Zhang W , Hai Y, Zhao Y L, et al. Image encryption based on three-dimensional bit matrix permutation. Signal Process. 2016, 118(1):36-50.
[27] Xu C, Zhang Y. Image encryption based on pixel decomposition. International Journal of Network Security. 2024, 26(4): 686-693.
[28] Dong C W. Dynamic analysis of a novel 3D chaotic system with hidden and coexisting attractors:offset boosting, synchronization, and circuit realization. Fractal and Fractional. 2022, 6(10):547. .
[29] Liang Z Y, Qin Q X, Zhou C J. An image encryption algorithm based on Fibonacci Q-matrix and genetic algorithm. Neural Computing and Applications. 2022, 34: 19313–19341.
[30] Zhou S , Qiu Y., Wang X, et al. Novel image cryptosystem based on new 2d hyperchaotic map and dynamical chaotic s-box. Nonlinear dynamics. 2023, 111: 9571-9589.
[31] Wang J, Zhi X, Chai X, et al. Chaos-based image encryption strategy based on random number embedding and DNA-level self-adaptive permutation and diffusion. Multimedia Tools And Applications. 2021, 80(4) : 1-36.
[32] Hosny K M, Kamal S T, Darwish M M. Novel encryption for color images using fractional-order hyperchaotic system. Journal of Ambient Intelligence and Humanized Computing. 2022, 13(2) : 973-988.
[33] Wu X J , Wang K S, Wang X Y , et al. Color image dna encryption using nca map-based cml and one-time keys. Signal Process. 2018, 148 (7) : 272–287.
[34] Malik M G A, Bashir Z , Iqbal N, et al. Color image encryption algorithm based on hyper-chaos and DNA computing. IEEE Access. 2020, 8: 88093–88107.