Hindawi
Advances in Mathematical Physics
Volume 2021, Article ID 7986300, 10 pages
https://doi.org/10.1155/2021/7986300

Research Article

Security Analysis of Image Scrambling Cipher Based on Compound Chaotic Equation

Luoyin Feng

Georgia Institute of Technology, Washington 98119, USA

Correspondence should be addressed to Luoyin Feng; luoyinfeng@gatech.edu

Received 17 August 2021; Revised 28 August 2021; Accepted 30 August 2021; Published 20 September 2021

Academic Editor: Miaochao Chen

As digital image has become one of the most important forms of expression in multimedia information, the security of digital image has become a concern. Because of its large amount of data and high redundancy, there are many security hidden dangers in ordinary image encryption methods. Aiming at the problems of low flexibility and poor anti-interference of traditional image scrambling technology, this paper proposes to select the scrambling diffusion encryption structure in the process of chaotic digital image encryption, which can produce relatively better encryption performance than single scrambling and diffusion scrambling. The composite chaotic operation used in this paper masks the distribution characteristics of chaotic subsequences. Based on the composite chaotic mapping model, the image scrambling password under the two-dimensional chaotic equation is established by scrambling the image in space and frequency domain. Several rounds of experiments show that the algorithm has a large scrambling scheme, further expands the key space of Arnold algorithm, and effectively resists the common computer brute force attack cracking and image decryption cracking methods such as exhaustive, differential attack and known plaintext attack. The improved encryption algorithm can realize the key avalanche effect, is very sensitive to the initial key and has high key security performance, and solves the security problem in the process of image transmission. Several performance syntheses show that the algorithm has high security performance and is suitable for image encryption scheme.

1. Introduction

With the rapid development and progress of science and technology and information network, the application of network and multimedia technology and computer technology had played a more and more important role in today's life. The early text data information had been replaced by vivid and intuitive multimedia information. Among them, digital images were used in people's daily life, biological application, and medical information. Military remote sensing images and other aspects had played an important role [1]. With the popularity of network cloud and network, the computing processing level of computer was accelerated. The use of digital image processing showed more obvious advantages in network and media channel transmission. First, it had high transmission efficiency, is fast and convenient, is easy to process and receive, and could realize communication transmission anytime and anywhere. Secondly, it improved the communication rate and carried a large amount of information. Therefore, as a faster way of information expression, digital image had affected all aspects of people's life. In order to ensure the security of digital image transmission, we must study various image information security technologies and have enough ability to ensure the security of images.

Digital image scrambling technology was the most studied image encryption measure in recent years [2]. This image encryption technology was independent, and its scrambling method would not produce redundant information, which was especially suitable for encrypting large images [3], so as to improve the security of image transmission to a certain extent. Image scrambling technology was used as the preprocessing of information hiding, which interferes with the gray distribution of secret information and makes it more like noise added to image files. At present, great progress had been made in the research of scrambling and encryption algorithm for gray image. Compared with the classical

asymmetric key DES and AES cryptosystem [4] and the symmetric key RSA cryptosystem, there were some problems in digital image encryption. Firstly, the digital image had a large amount of information storage. The uncompressed $256 * 256$ 8-bit gray image needed to occupy 0.5 mbit of data. The classical encryption system took too much time and had poor real-time performance compared with encryption. Secondly, digital image information could not be in the form of continuous coding like text information, and the redundancy between pixels was high. Therefore, the classical key system was difficult to meet the requirements of digital image information encryption. In recent years, experts and scholars had proposed many image encryption schemes based on chaos theory. The commonly used image scrambling algorithms include Arnold transform, Hilbert transform, magic square transform, Fibonacci transform, and affine transform [5]. However, the simple encryption algorithm of one-dimensional chaotic system had insufficient key space, and it was easy to identify chaotic system by using phase space reconstruction method, which had been proved to be low security [6]. Due to the good statistical and topological characteristics of chaotic system, it had begun to become an important frontier of image encryption research. However, chaotic encryption algorithm was still in the stage of model research and discussion, and there were still many problems to be solved in practice.

The scheme proposed in this paper was based on the composite chaotic system of two chaotic systems. The composite chaotic system maintained the chaotic characteristics of all subsystems, could produce a wider parameter set with good chaotic effect than one-dimensional chaos, and had a more complex iterative control chaotic system, which was much more complex than the dynamic behavior of a single subsystem [7], so the security performance of the algorithm was higher. In classical digital image encryption, the preprocessing sequence generated by chaotic key and exclusive or operation of plaintext image could speed up the efficiency of encryption and produce good encryption effect. A large number of experimental studies showed that the encryption structure of scrambling and diffusion in the process of chaotic digital image encryption could produce relatively better encryption performance than single scrambling and diffusion scrambling [8].

Based on the above analysis, the chapters of this paper would be arranged as follows: the second section of this paper would analyze the research status of existing image security algorithms and lead to the broad application space of chaos theory in image encryption algorithms; in the third section, the image scrambling cipher and its decoding algorithm would be constructed based on the composite chaotic equation; the fourth section of this paper showed a series of simulation experiments. After the transformation key information was encrypted, the ciphertext image was completely destroyed, which proved that it had strong key sensitivity; The histogram distribution of the ciphertext was uniform, which indicated that the ciphertext had the characteristics of antistatistical analysis; the correlation between the scrambled ciphertext image pixels was close to zero, which showed that the ciphertext image encrypted by this system had good correlation characteristics, and the above characteristics could well reflect the security of this algorithm.

2. Related Work

Nowadays, there were mainly two ways to protect image security: one was to scramble or distribute the digital image to be protected according to the basic idea and application principle of cryptography so that the image did not seem to include any meaningful content [9]. The second was to hide the image that needs to be protected into another image that did not need to be protected, so as to protect the hidden image, and the image that did not need to be protected would not change greatly. This technology was called information hiding and camouflage technology in digital image processing, including digital watermarking [10]. Researchers have proposed many scrambling algorithms from the perspective of changing image pixel position and pixel value, such as Arnold, Fibonacci, bit plane, gray code, and m sequence.

Now, the first image scrambling technology had attracted more and more attention of researchers and users. In image encryption technology, digital image scrambling technology [11] was very important. Generally speaking, the effect of image scrambling is better. As the secret information hidden in the carrier information, the stronger the antidetection ability was, the higher the hiding ability was. At the beginning, digital image scrambling technology only scrambled the image position space [12], but today, for digital images, only scrambling the image position could not meet our needs. Therefore, people continued to study on this basis and find that in addition to scrambling in the spatial domain of digital images (including color space and position space), the scrambling process could also be carried out in the frequency domain of the digital image. This discovery made people further improve the implementation of digital image technology.

Applying chaos theory to image encryption, Robert A.J. Matthews first proposed a chaotic stream cipher scheme based on deformed logistic map in 1989. The evolution of chaotic encryption could be divided into three processes. Firstly, chaotic synchronization was used in the process of communication security. Secondly, it was directly used for plaintext encryption of digital images. Finally, encryption was carried out in combination with the scrambling and replacement principles proposed by modern cryptography. Various chaotic encryption models were evolved. Kaur et al. proposed an algorithm based on fractional Hartley transform and chaotic permutation [13]; Kumar et al. used the chaotic dynamic system of pixel shuffle enhancement based on three-dimensional matrix to encrypt color images [14]; Zhang et al. cited the linear hyperbolic chaotic system of partial differential equation to generate pseudorandom high-sensitivity sequence stream for scrambling and replacement operation of image encryption [15].

Compared with one-dimensional chaotic mapping, high-dimensional control system could produce larger key space [16]. Secondly, the motion trajectories of each plane were more complex, with large dissipation, and the generated random sequence was close to uniform distribution

[17]. Then, the generated chaotic sequence was properly processed as a key stream, which could directly encrypt the image with good real-time performance. Finally, because of its better dynamic nonlinear characteristics, it had high security in the field of cryptography and was widely used in digital image encryption.

3. Design of Image Scrambling Cipher Algorithm Based on Compound Chaotic Equation

3.1. Constructing Compound Chaotic Equation. Logistic mapping was a simple nonlinear regression dynamic model. The mapping model was known from

$$x_{n+1} = \mu x_n(1 - x_n), \quad x_n \in (0, 1),\ \mu \in (0, 4]. \tag{1}$$

The logistic model would follow μ. The change of value produces different performance [18]. Whether the system was in a chaotic state still needs to meet the limitations of certain initial parameter conditions. In the development process of chaotic dynamics, the research showed that when $\mu \in (3.56994567, 4)$, the system experienced period doubling bifurcation state and finally entered chaotic state. The sequence generated by the mapping was unpredictable [19], aperiodic and nonconvergent, and was very sensitive to the bifurcation parameters and the initial value of the system. Figure 1 shows that the initial value of logistic system was $x_0 = 0.5$ and the branch parameters $\mu = 3.98$ and $\mu = 3.9800000001$. The sequence distribution diagram generated by 100 iterations of the system at 3.98 billion 1 showed that the sequence distribution was unpredictable and in an aperiodic state.

Let $x_i = f_q(x_{i-1})$, $q = 0, 1, \cdots, k$ be a group of discrete chaotic dynamical systems defined on $[0, 1]$. For any sequence, $R = (r_1, r_2, r_3, \cdots) \in \{0, 1, \cdots, k\}^{\infty}$, $i = 1, 2, \cdots$, $r_i = 0, 1, \cdots$, was the composite system of the iterative system under sequence R, R was the composite sequence, and $x_i = f_q(x_{i-1})$, $q = 0, 1, \cdots, k$ was the subsystem.

The algorithm formed a composite chaotic mapping model: the initial condition $x \in (0, 1)$ of the system was a part of the key, and the iterative trajectory of the system was determined by q_i and x_0. R_j was a nonlinear transformation mechanism, which changed the floating-point numbers between $(0, 1)$ into a set $\{0, 1\}$, that is, $R_j : (0, 1) \longrightarrow \{0, 1\}$, the nonlinear transformation formula here was that j was a part of the key, and its size was generally determined by the number n of decimal precision reserved by the iterative function value x [20], and $j \ll n/\log_{10}2$ was the ciphertext encrypted by the C_i composite chaotic system. The encryption expression of composite chaotic system based on logistic mapping was

$$c_i = \left\lfloor \left((2^{q_i} - 1) + (-1)^{q_i} \sqrt{|2x_i - 1|} \right) * 2^j \right\rfloor \bmod 2. \tag{2}$$

The decryption expression was

$$q_i = \mathrm{xor}\left(c_i, \left(2^j \sqrt{|2x_i - 1|} \right) \bmod 2 \right). \tag{3}$$

In formulas (2) and (3), q_i took 0 or 1, which was the chaotic subsequence, that was, the plaintext information, j was determined by the decimal precision reserved by the iterative function value x, $j < <n/\log_{10}2$.

3.2. Scrambling Cipher Based on Compound Chaotic Equation. Firstly, the chaotic sequences $\{x_1(i)\}$, $\{x_2(i)\}$, $\{x_3(i)\}$ were constructed by using the known keys: $(u_1, x_1(0))$, $(u_2, x_2(0))$, $(u_3, x_3(0))$ through the LTS, LSS, and TSS composite chaotic mapping systems. Where $i = 1, 2, 3, \cdots 2 * M * N$, MN were the total number of pixel rows and columns of the original color image and RGB color separation image, respectively. $M * N$ random numbers before and after the chaotic sequence were selected to obtain $\{L_1(i)\}$, $\{L_2(i)\}$, $\{L_3(i)\}$, $\{O_1(i)\}$, $\{O_2(i)\}$, and $\{O_3(i)\}$, for scrambling and diffusion of RGB color components in plaintext.

The number sent by the source is x, and the corresponding bits of the number x and the research sequence y are modulo added, respectively, to obtain the sequence x_j. At this time, the x_j sequence has lost the meaning of the original information. Even if the encrypted sequence is transmitted in the channel, even if it is eavesdropped by others, if the sequence y is not known, the digital X carrying the original information cannot be solved, so as to play the role of encryption, Assuming that there is no bit error in the channel transmission process, sequence e reaches the receiving end and performs modulo binary addition with sequence y to restore the original digital X. The encrypted pseudorandom sequence was constructed:

$$x(i) = \mathrm{mod}\left(256, \mathrm{floor}\left(\sum x_j(i) \times 10^{15} \right) \right). \tag{4}$$

In order to eliminate chaotic jitter, considering the transient effect of chaos [21], $M * N$ sequence values were selected from $x(i)$ starting from the k-th sequence value to obtain $M * N$-dimensional pseudorandom sequence matrix, $k < M * N$. It could be seen that the pseudorandom matrix only depended on the original initial key control parameters and K value.

In this paper, let the size of the original image I (this paper takes the 256 gray level image as the research object) be $M * N$ (M was the number of row pixels of image I and N was the number of column pixels of image I), $I(i, j)$ represent the gray value of the j column element in the i row of the image, and the scrambled image was B and the size was $M * N$. The scrambling cipher based on the composite chaotic equation is shown in Figure 2, and the algorithm flow was as follows:

Step 1. Read in a gray image I and display it, enter the key, take the key as the seed, and select an initial state.

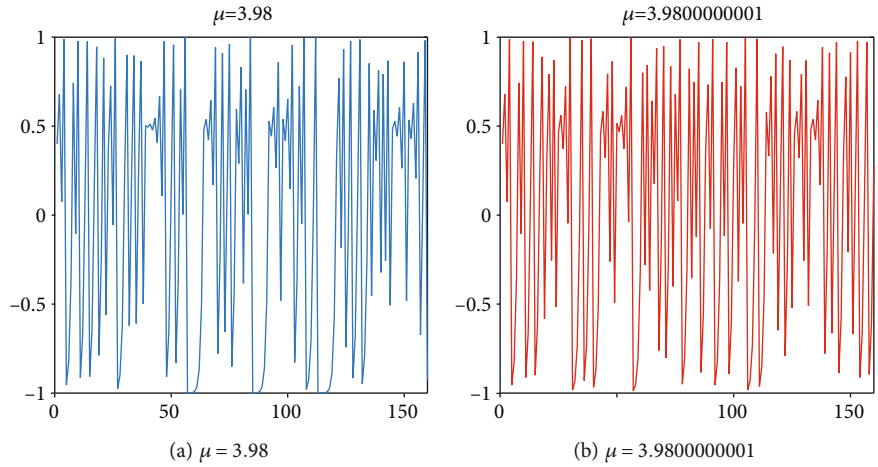


Figure 1: The sequence distribution diagram generated by 100 iterations of the system.

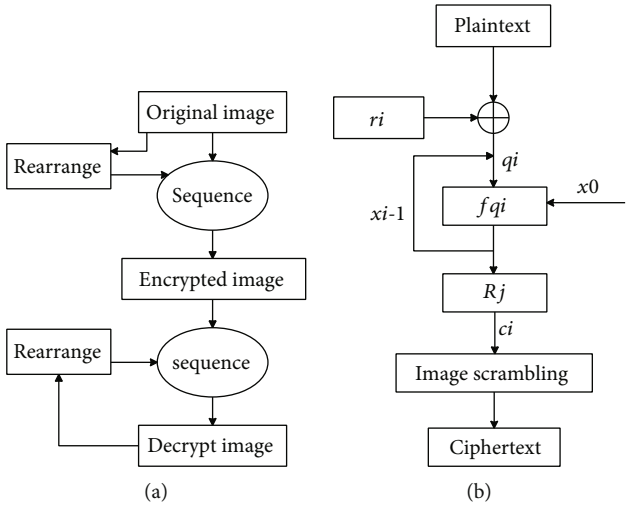


Figure 2: (a) The detailed implementation principle flowchart of image scrambling password. (b) Digital image encryption based on compound chaotic and image scrambling.

Step 2. Generate an $n * n$ random term matrix B display, then convert the B matrix into row vector C, arrange the C row vector from small to large into sequence D, and record the sequence number in the sequence.

Step 3. Convert the I matrix generated by the gray image into row vector E, and then, put the pixel values in row vector E into a row vector m in the order of sequence D.

Step 4. Convert the row vector m into a matrix. Finally, the scrambled image was output.

The restoration of scrambled image was the inverse process of image scrambling. Corresponding to the above scrambling algorithm, the specific operation steps were described as follows:

Step 1. Decrypt according to formula (3), generate a matrix, and save the decrypted image.

Step 2. Read in the image information, input the key, take the key as the seed, and select an initial state.

Step 3. Establish an empty matrix, put the pixel position of the scrambled image back to the position of the original image, that is, the inverse transformation of scrambling Step 3, and finally output the restored image.

In order to test the damage degree of the scrambling algorithm to the correlation of adjacent pixels of the image, all adjacent pixel pairs in the horizontal direction, all adjacent pixel pairs in the vertical direction, and some adjacent pixel pairs in the diagonal direction were randomly selected from the image [22], and the correlation coefficients of adjacent pixels were quantitatively calculated with the following formula:

$$\begin{aligned} E(x) &= \frac{1}{N}\sum_{i=1}^{N} x_i, \\ D(x) &= \frac{1}{N}\sum_{i=1}^{N} [x_i - E(x)]^2, \\ \mathrm{Conv}(x,y) &= \frac{1}{N}\sum_{i-1}^{N} [x_i - E(x)][y_i - E(y)], \\ \gamma_{xy} &= \frac{\mathrm{Conv}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}. \end{aligned} \tag{5}$$

In the above, x and y, respectively, table the pixel values of two adjacent pixels in the image and γ_{xy} was the correlation coefficient of two adjacent pixels of the image.

3.3. Decoding Algorithm of Scrambling Key S_{eq}. Create $m = \lceil \log_{256}(HW) \rceil$ plaintext gray images $I_l = \{I_l(t,j)\}_{t=1,j=1}^{HW}$ $(l = 1, 2, \cdots, m)$. According to the selected plaintext attack, the corresponding ciphertext image was $C_l = \{C_l(t,j)\}_{t=1,j=1}^{HW}$ $(l = 1, 2, \cdots, m)$. In addition, the one-dimensional sequence corresponding to I_l was $M_l = \{M_l(i)\}_{i=1}^{HW}$ $(l = 1, 2, \cdots, m)$

Input: $m = \lceil \log_{256}(HW) \rceil$, $I_1, I_2, \cdots, I_m, Q(0), R(HW+1)$, $l = 1, 2, \cdots, m$
Output: S_{eq}
For $l = 1$ to m do
$C_1 \longleftarrow \text{Fun\_Encrypt}(I_l)$;
$M_l \longleftarrow F(I_l)$;
$R_l \longleftarrow G^{-1}(C_l)$;
End for
$P_l \longleftarrow \text{zeros}(1, HW)$;
$P_l(1) \longleftarrow R_l(2) \oplus R_l(1) \oplus Q(0)$;
$P_l(HW) \longleftarrow R(HW+1) \oplus R_l(HW-1) \oplus D_{\text{eq}}(HW-1)$
For $i = HW - 1$ to 2 do
$P_l(\text{i}) \longleftarrow R_l(i+1) \oplus R_l(i-1) \oplus D_{\text{eq}}(i-1)$
End for
$P_{\text{index}} \longleftarrow \sum_{l=1}^{m} P_l \times 256^{l-1}$
$M_{\text{index}} \longleftarrow \sum_{l=1}^{m} M_l \times 256^{l-1}$
$S_{\text{eq}} \longleftarrow \text{compare}(P_{\text{index}}, M_{\text{index}})$;
Return S_{eq}.

Algorithm 1

and $M_l = F(I_l)$; the one-dimensional diffusion encryption sequence corresponding to C_l was $P_l = \{P_l(i)\}_{i=1}^{HW}$ $(l = 1, 2, \cdots, m)$ and $R_l = G^{-1}(C_l)$; the one-dimensional scrambling encryption sequence corresponding to M_l is $P_l = \{P_l(i-1)\}_{i=1}^{HW}$ $(l = 1, 2, \cdots, m)$ and $P_l(i) = f_{S_{\text{eq}}}(M_l(i))$. By substituting D_{eq} and R_l into $R(i) = R(i+1) \oplus (\sum_{k=1}^{i-1} \oplus D_{eq}(k))(\sum_{k=1}^{i} \oplus P(k))$ as known conditions, we could get

$$R_l(i) = R_l(i+1) \oplus \left(\sum_{k=1}^{i-1} \oplus D_{\text{eq}}(k)\right)\left(\sum_{k=1}^{i} \oplus P_l(k)\right). \quad (6)$$

According to formula (6),

$$\left(\sum_{k=1}^{i} \oplus P_l(k)\right) = R_l(i+1) \oplus R_l(i) \oplus \left(\sum_{k=1}^{i-1} \oplus D_{eq}(k)\right), \quad (7)$$

where $i = HW, HW-1, \cdots, 3, 2$; $l = 1, 2, \cdots, m$.

Then, $P_l(i)$ $(i = HW, \cdots, 4, 3; l = 1, 2, \cdots, m)$ was obtained according to the differential attack.

In formula (7), $i-1$ was used to replace i, i.e., $i \longleftarrow i-1$ to obtain

$$\left(\sum_{k=1}^{i-1} \oplus P_l(k)\right) = P_l(i) \oplus R_l(i-1) \oplus \left(\sum_{k=1}^{i-2} \oplus D_{\text{eq}}(k)\right), \quad (8)$$

where $i = HW+1, HW, \cdots, 3$; $l = 1, 2, \cdots, m$.

XOR (7) and (8) to obtain

$$P_l(i) = R_l(i+1) \oplus R_l(i-1) \oplus D_{\text{eq}}(i-1), \quad (9)$$

where $i = HW, HW-1, \cdots, 4, 3$; $l = 1, 2, \cdots, m$.

Note that the serial number i in formula (9) should be equal to the intersection of the serial number $i = HW, HW-1, \cdots, 3, 2$ in formula (7) and the serial number $i = HW+1, HW, \cdots, 4, 3$ in formula (8), so the serial number in formula (9) was $i = HW, HW-1, \cdots, 4, 3$.

Substituting $i = 1$ and $i = 2$ into formula (9), XOR can be obtained:

$$P_l(2) = R_l(3) \oplus R_l(1) \oplus D_{\text{eq}}(1). \quad (10)$$

Note that (10) had been included in (9), so only (9) needs to be considered, and the original serial number i in (9) was modified to $i = HW, HW-1, \cdots, 3, 2$.

Combine $P_1, P_2, \cdots, P_m$ into one-dimensional permutation encryption sequence P_{index} to obtain

$$P_{\text{index}}(i) = \lim_{m \longrightarrow \infty} \sum_{l=1}^{m} M_l(i) \times 256^{l-1}. \quad (11)$$

Similarly, combining $M_1, M_2, \cdots, M_m$ into one-dimensional sequence M_{index} could obtain

$$M_{\text{index}}(i) = \lim_{m \longrightarrow \infty} \sum_{l=1}^{m} M_l(i) \times 256^{l-1}, \quad (12)$$

where $i = 1, 2, \cdots, HW$. By comparing the position difference between P_{index} and M_{index} with the same pixel value, the equivalent scrambling key S_{eq} used for position scrambling could be solved. The algorithm for deciphering the equivalent scrambling key S_{eq} was as follows.

3.4. Improved Image Encryption Scheme. The overall encryption scheme of this paper is shown in Figure 3:

Diffusion processing is to hide the information of any plaintext pixel in as many ciphertext pixels as possible without changing the pixel position. The original image chaotic encryption algorithm included four parts: key parameter selection, replacement, forward diffusion, and reverse

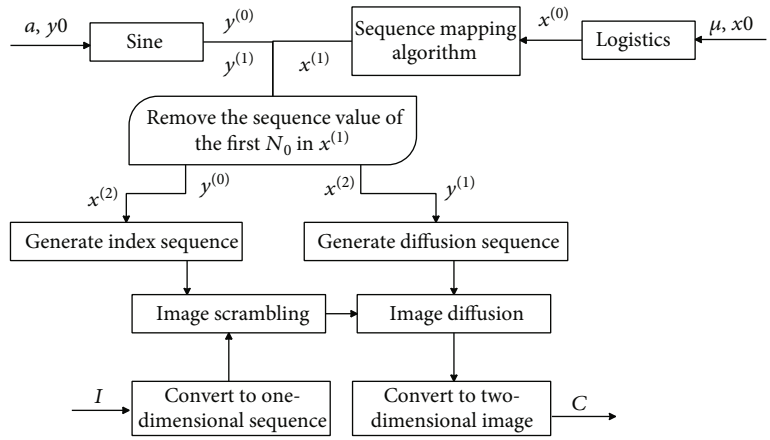


Figure 3: Block diagram of chaotic encryption algorithm of the original image.

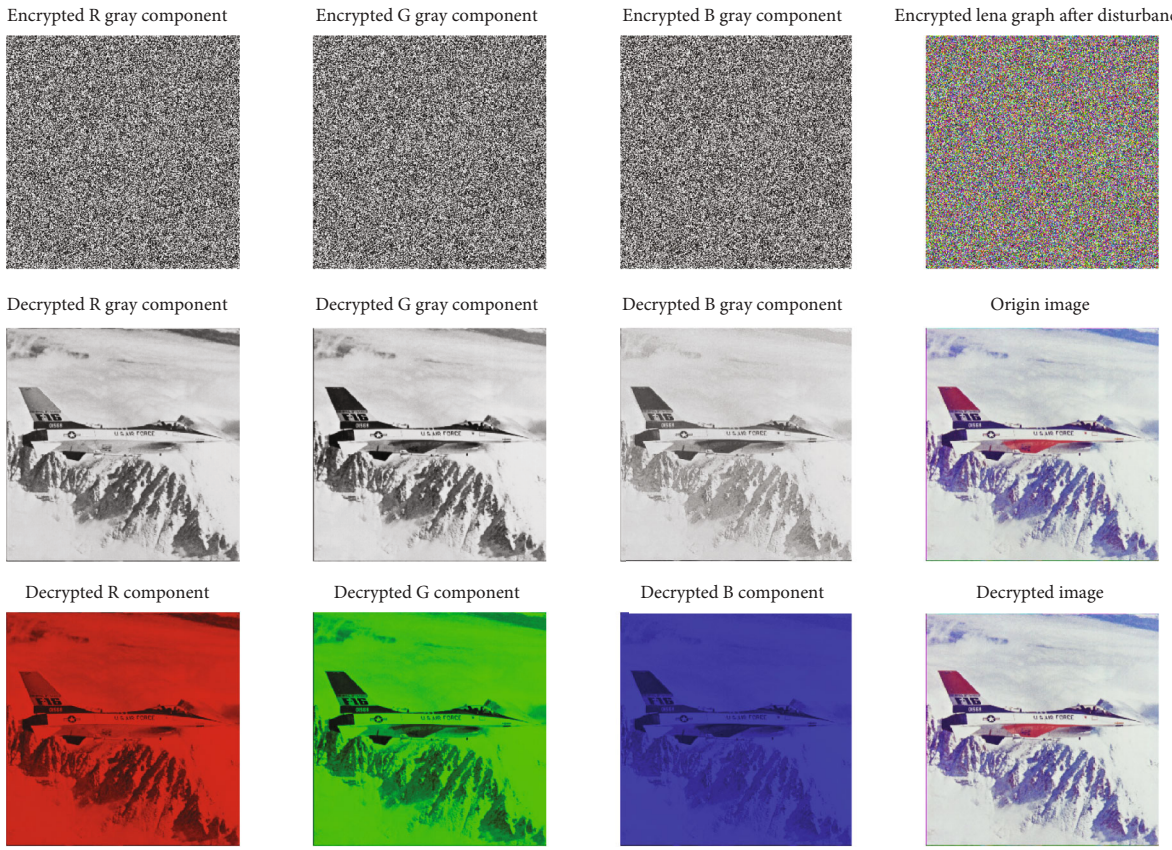


Figure 4: Airplane ciphertext component image.

diffusion [23], as shown in Figure 3. μ, x_0, α, and y_0 were the key, $x^{(0)}$ was the chaotic sequence generated by logistic mapping, $x^{(1)}$ was the uniformly distributed chaotic sequence generated after the conversion of $x^{(0)}$ by sequence mapping algorithm, $x^{(2)}$ was the chaotic sequence generated after removing the first N_0 sequence values in $x^{(1)}$, $y^{(0)}$ and $y^{(1)}$ were the chaotic sequence generated by sine mapping, S was the one-dimensional index sequence, D was a one-dimensional diffusion sequence, I was a two-dimensional plaintext gray image, M was a one-dimensional sequence corresponding to I, P was a one-dimensional displacement encryption sequence corresponding to m, q was a one-dimensional forward diffusion encryption sequence corresponding to P, R was a one-dimensional reverse diffusion encryption sequence corresponding to Q, and C was a two-dimensional ciphertext image corresponding to R. Note that the dimensions of I and C were $H \times W$. The dimensions of S, D, M, P, Q, and R were all $1 \times HW$, where h was the height of plaintext gray image, W was the width of plaintext gray image, and $N_0 = 200$.

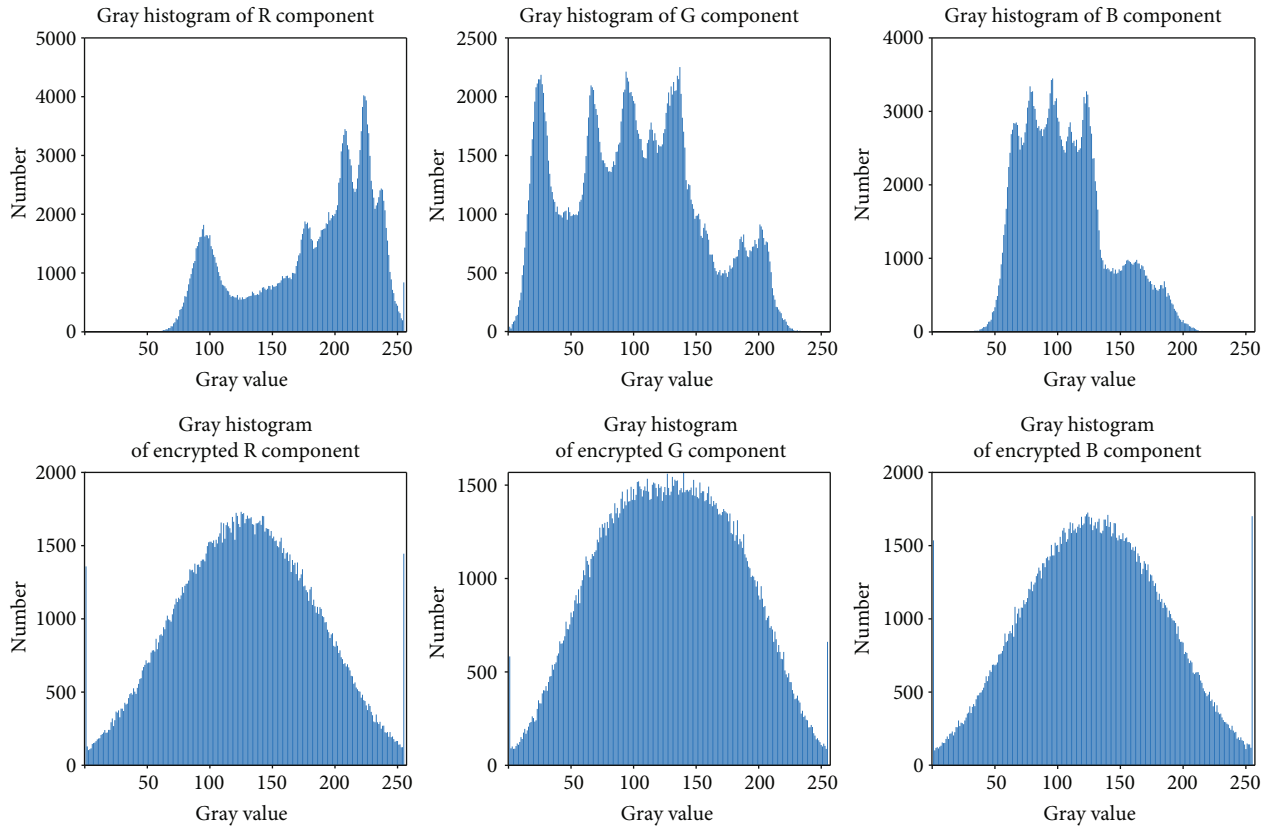


Figure 5: Histogram of each color component of airplane plaintext image and ciphertext image.

Table 1: Correlation coefficients of adjacent pixels of plaintext and ciphertext.

	Plaintext	Ciphertext	Origin image
Horizontal direction	0.9713	0.0034	0.5001
Vertical direction	0.9864	0.0051	0.4998
Diagonal direction	0.9448	0.0109	0.5000

4. Results and Safety Analysis

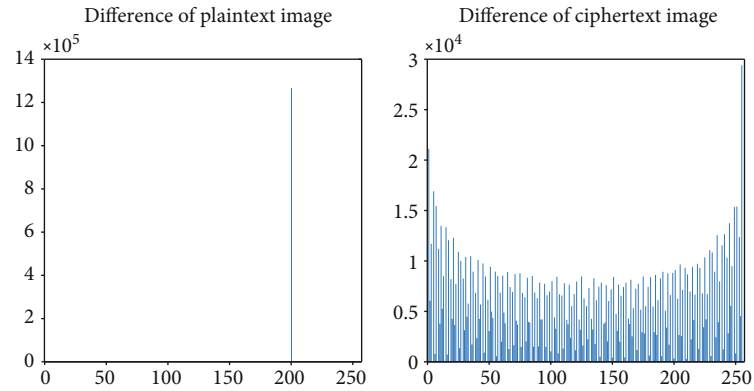
4.1. Experimental Simulation Results. The simulation experiment in this paper ran on Lenovo v460 notebook equipped with MATLAB r2019b, sets the initial key parameters $u_1 = 3.9875$, $x_1(0) = 0.3948$, $u_2 = 2.58902$, $x_2(0) = 0.927394$, $u_3 = 0.289335$, $x_3(0) = 0.927394$, and $k = 1000$, and selects the $256 * 256 * 256$ pixel true color standard test airplane image as the plaintext image. The clear ciphertext component image and decrypted image after a single round of encryption by the improved algorithm are shown in Figure 4, and the histogram of each color component of plaintext image and ciphertext image is shown in Figure 5.

Looking at Figures 4 and 5, it could be seen that the encrypted airplane color image was confused in terms of subjective vision, and the useful information about the plaintext cannot be obtained from the plaintext information. On the other hand, from the gray histogram before and after encryption, it could be seen that the gray distribution of R, G, and B components of airplane after encryption was uniform, which could effectively resist statistical analysis attacks.

Table 1 lists the results of correlation coefficients calculated in three directions. It could be seen from the data that the correlation between adjacent pixels of plaintext image was very good, while the correlation between adjacent pixels of encrypted image, whether horizontal, vertical, or diagonal, was close to 0. It showed that the adjacent pixels of the encrypted ciphertext were completely scrambled.

A good encryption algorithm should be sensitive to plaintext and key. The dependence of ciphertext on key can be verified by calculating the correlation coefficient between two images. The difference is that X_j and Y_j represent the pixel value of ciphertext image encrypted with different keys, and N is the number of pixels contained in the image. According to the definition of ciphertext sensitivity to key, if the encryption method has sensitive dependence on the key, the results obtained by encrypting the same image with a small difference key should be very different, that is, it has small correlation.

4.2. Evaluation and Analysis of Differential Attack. After the original image was encrypted by the encryption algorithm, the ciphertext image must be able to hide the general outline of the original image and hide the secret information of the original image, which was not easy to be attacked and leaked. Such encryption algorithm could have sufficient security. Generally, the security evaluation index would be analyzed and judged by the size of the key space, whether it could resist the exhaustive analysis of keys with a very large amount of data and whether it could withstand the



(a) Difference of plaintext image (b) Difference of ciphertext image

Figure 6: Histogram of each color component of Lena plaintext image and ciphertext image.

Table 2: Average values of NPCR and UACI in 100 tests.

	NPCR	UACI
R component	99.915%	42.381%
G component	99.391%	42.496%
B component	99.410%	42.381%

brute force cracking of high-speed computing of computers at this stage. In addition, the key sensitivity could also analyze the advantages and disadvantages of the encryption algorithm used and whether it could resist the common image decryption and cracking methods such as exhaustive and differential attacks.

The initial values of the two systems were used as the key, which was expressed by double precision real numbers accurate to 15 digits after the decimal point. The key space of the algorithm was $1015 \times 1015 \times 1015 \times 1015 \times 1015 = 1075 \approx 2249$, so the cryptosystem was sufficient to resist the exhaustive attack under the existing hardware conditions [24].

A good algorithm should be highly sensitive to plaintext, that is, any small change in plaintext image would produce great changes in ciphertext image. Figure 6(a) shows that the value 118 of $I(80, 82)$ in the plaintext image was changed to the difference of 119 plaintext image. It could be seen from Figure 6(b) that small changes in the plaintext image led to huge changes in the ciphertext image. It could be seen that writing text was very sensitive to plaintext, and this scheme could effectively resist known plaintext attacks.

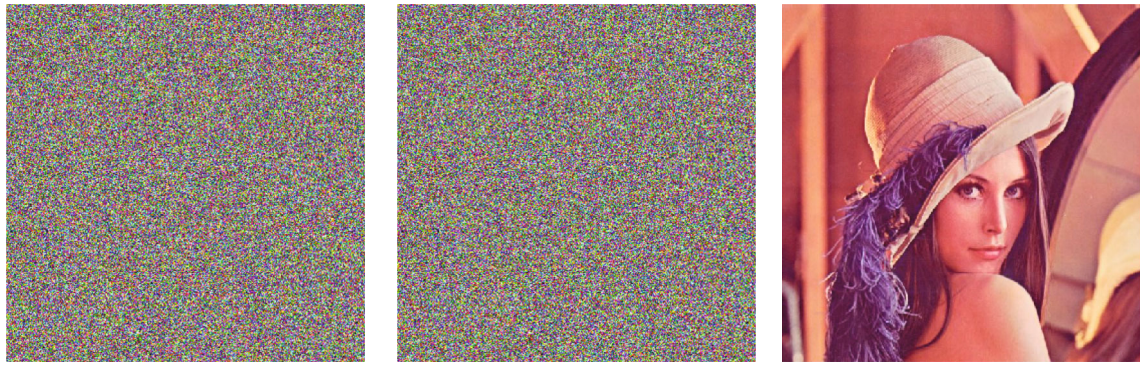
The effect of plaintext resistance to difference could also be measured by using pixel change rate NPCR and change intensity UACI value. In the chosen-plaintext attack, the adversary has the ability to obtain the encryption of any plaintext (s) of its choice. It then attempts to determine the plaintext that was encrypted to give some other ciphertext. Changing any numerical information of plaintext image randomly, if the encrypted ciphertext image changes greatly, it could resist differential attack. Otherwise, the encryption algorithm did not have enough resistance to differential attacks.

In order to verify the antidifferential attack ability of the algorithm, this paper randomly selected the pixel value $p(R)$ at the position of Lena color R component (I, J) to be encrypted, changed the small change mod $(P(R) + 1, 256)$, selected the same key for encryption, compared the encrypted images C1 and C2 before and after changing the pixels, and obtained the NPCR and UACI values. In order to avoid the contingency of the simulation experiment, repeat the experiment for 100 times to obtain the average value. The NPCR and UACI of each primary color component after experiment are shown in Table 2.

It could be seen from the data analysis in Table 2 that the NPCR and UACI values of each component of Lena ciphertext color image were connected with the recent expected values, indicating that the improved algorithm could effectively resist differential attacks.

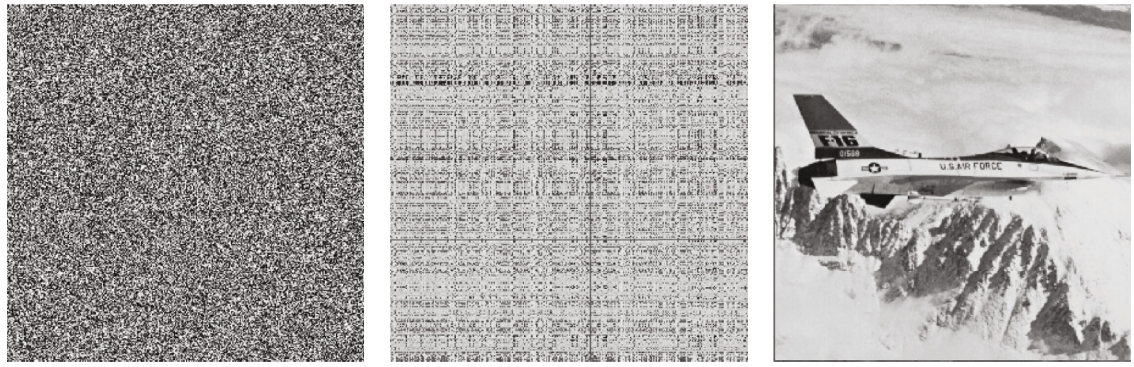
4.3. Key Space and Sensitivity Analysis. In order to verify the key sensitivity of the improved algorithm and then verify the effect of key avalanche effect, the ciphertext image should be able to change greatly after encrypting the key information by small transformation. By changing the initial key, the original encryption scheme was improved μ_1 to make minimal disturbance $\mu_1 + 10^{-15}$ to obtain the encrypted image before and after disturbance. Next, we selected the images before and after disturbance encryption for comparative analysis. As could be seen from Figure 7, the original error key decrypted image after disturbance was very different from the original Lena color image, and the original image information cannot be recovered. Therefore, the improved algorithm was very sensitive to the initial key and had high key security performance. It was verified that the improved encryption algorithm could realize the key avalanche effect and achieve good results.

In the improved algorithm proposed in this chapter, the art encryption times of each component and the control parameters of hyperchaotic system were selected as the key. The key $K = [x_0, y_0, z_0, w_0, a, b, c, d]$. If the calculation accuracy of the encryption system could reach 10^{14}, the size of the algorithm key space was at least 10^{84}, which further expands the key space of Arnold algorithm and could resist the brute force attack of computer. In order to verify the key sensitivity of the improved algorithm, x_0 of the original encryption scheme was minimally disturbed by changing



(a) Encrypted Lena graph after disturbance (b) Decrypted Lena graph of wrong key (c) Decrypted Lena graph of correct key

Figure 7: Decryption diagram of wrong key.



(a) Small deviation encryption diagram (b) Error key decryption image (c) Decrypt the image correctly

Figure 8: Key sensitivity analysis.

the initial key, and the cameraman encrypted image before and after the disturbance was obtained. Next, we selected the images before and after disturbance encryption for comparative analysis.

As could be seen from Figure 8, the original initial error key decrypted image after disturbance was very different from the original cameraman gray image, and the original image information cannot be recovered. Therefore, the improved algorithm was very sensitive to the initial key and had high key security performance.

5. Conclusion

Aiming at the defects of one-dimensional chaotic encryption, an improved encryption method was proposed. The image scrambling password was encrypted based on the composite chaotic equation, which enhances the security of the scheme. The ciphertext had the characteristics of uniform distribution in the whole value space, and the adjacent pixels had a correlation of approximately 0. The key space of this algorithm was large. The key was based on the initial value of two chaotic systems. The key space was 2249, which was equivalent to the binary 249-bit key, which was enough to resist the exhaustive attack under the existing conditions. In addition, the introduction of auxiliary key not only expanded the key space but also made the key related to the original image. The encryption scheme was sensitive to plaintext and increased the difficulty of decoding. In the encryption scheme, there was a correlation between pixel position scrambling and pixel value replacement, that was, multiple rounds of iterations were carried out for the two encryption steps, and each round of iteration would carry out position scrambling and pixel value replacement so that the key stream was not only related to the initial value of the chaotic system but also related to the plaintext, which enhances the ability to resist known plaintext attacks. Experimental results and theoretical analysis showed that this scheme had stronger ability to resist exhaustive attack, statistical attack, and known plaintext attack and had high security and good cryptographic characteristics.

Data Availability

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

Conflicts of Interest

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 paper.

References

[1] E. Hasanzadeh and M. Yaghoobi, "A novel color image encryption algorithm based on substitution box and hyper-chaotic system with fractal keys," *Multimedia Tools and Applications*, vol. 79, no. 11-12, pp. 7279–7297, 2020.

[2] A. Sahasrabuddhe and D. S. Laiphrakpam, "Multiple images encryption based on 3D scrambling and hyper-chaotic system," *Information Sciences*, vol. 550, pp. 252–267, 2021.

[3] U. Arshad, M. Khan, S. Shaukat, M. Amin, and T. Shah, "An efficient image privacy scheme based on nonlinear chaotic system and linear canonical transformation," *Physica A: Statistical Mechanics and its Applications*, vol. 546, p. 123458, 2020.

[4] J. K. P. Alegro, E. R. Arboleda, M. R. Pereña, and R. M. Dellosa, "Hybrid Schnorr RSA and AES cryptosystem," *International Journal of Scientific and Technology Research*, vol. 8, no. 10, pp. 1777–1781, 2019.

[5] N. Jiang, W. Y. Wu, and L. Wang, "The quantum realization of Arnold and Fibonacci image scrambling," *Quantum Information Processing*, vol. 13, no. 5, pp. 1223–1236, 2014.

[6] D. Banavath and S. Tadisetty, "A novel image self-adaptive encryption algorithm based on composite chaotic systems," *International Journal of Electronics Engineering (IJEE)-CS Journals*, vol. 9, no. 1, pp. 160–164, 2017.

[7] K. Aditya, A. K. Mohanty, G. A. Ragav, V. Thanikaiselvan, and R. Amirtharajan, "Image encryption using dynamic DNA encoding and pixel scrambling using composite chaotic maps," *IOP Conference Series: Materials Science and Engineering*, vol. 872, no. 1, article 012045, 2020.

[8] B. Yosefnezhad Irani, P. Ayubi, F. Amani Jabalkandi, M. Yousefi Valandar, and M. Jafari Barani, "Digital image scrambling based on a new one-dimensional coupled sine map," *Nonlinear Dynamics*, vol. 97, no. 4, pp. 2693–2721, 2019.

[9] B. Mondal, P. Kumar, and S. Singh, "A chaotic permutation and diffusion based image encryption algorithm for secure communications," *Multimedia Tools and Applications*, vol. 77, no. 23, pp. 31177–31198, 2018.

[10] A. Mohanarathinam, S. Kamalraj, G. K. D. Prasanna Venkatesan, R. V. Ravi, and C. S. Manikandababu, "Digital watermarking techniques for image security: a review," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 8, pp. 3221–3229, 2020.

[11] A. Khan and P. Trikha, "Compound difference anti-synchronization between chaotic systems of integer and fractional order," *SN Applied Sciences*, vol. 1, no. 7, p. 757, 2019.

[12] S. Subashanthini and M. Pounambal, "A new venture to image encryption using combined chaotic system and integer wavelet transforms," *International Journal of Cloud Computing*, vol. 10, no. 1/2, pp. 43–69, 2021.

[13] G. Kaur, R. Agarwal, and V. Patidar, "Color image encryption scheme based on fractional Hartley transform and chaotic substitution–permutation," *The Visual Computer*, 2021.

[14] M. Kumar, S. Kumar, M. K. Das, S. Singh, and R. Budhiraja, "Chaotic dynamical systems based image encryption model," in *2017 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 93–98, Jeju, 2017.

[15] Y. Zhang, D. Xiao, Y. Shu, and J. Li, "A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations," *Signal Processing Image Communication*, vol. 28, no. 3, pp. 292–300, 2013.

[16] L. S. Jahanzaib, P. Trikha, and D. Baleanu, "Analysis and application using quad compound combination anti-synchronization on novel fractional-order chaotic system," *Arabian Journal for Science and Engineering*, vol. 46, no. 2, pp. 1729–1742, 2021.

[17] S. N. Lagmiri, N. Elalami, and J. Elalami, "Three dimensional chaotic system for color image scrambling algorithm," *International Journal of Computer Science and Information Security*, vol. 16, no. 1, pp. 8–20, 2018.

[18] G. Dursun, F. Özer, and U. Özkaya, "A new and secure digital image scrambling algorithm based on 2D cellular automata," *Turkish Journal of Electrical Engineering & Computer Sciences*, vol. 25, no. 5, pp. 3515–3527, 2017.

[19] A. S. Yadav and S. Kumar, "Comparative analysis of digital image watermarking based on DCT, DWT and SVD with image scrambling technique for information security," in *2018 International Conference on Computational and Characterization Techniques in Engineering & Sciences (CCTES)*, pp. 89–93, Lucknow, India, 2018.

[20] B. Mondal, N. Biswas, and T. Mandal, "A comparative study on cryptographic image scrambling," in *Proceedings of the Second International Conference on Research in Intelligent and Computing in Engineering*, pp. 261–268, Jamshedpur, India, 2017.

[21] A. J. Mansor, H. N. Abdalla, and H. T. Ziboon, "Digital image scrambling using chaotic systems based on FPGA," in *2018 Third Scientific Conference of Electrical Engineering (SCEE)*, pp. 19–24, Baghdad, Iraq, 2018.

[22] M. Arora and M. Khurana, "Secure image encryption technique based on jigsaw transform and chaotic scrambling using digital image watermarking," *Optical and Quantum Electronics*, vol. 52, no. 2, p. 59, 2020.

[23] E. E. Mahmoud, L. S. Jahanzaib, P. Trikha, and M. H. Alkinani, "Anti-synchronized quad-compound combination among parallel systems of fractional chaotic system with application," *Alexandria Engineering Journal*, vol. 59, no. 6, pp. 4183–4200, 2020.

[24] N. Prajapati, A. Khan, and D. Khattar, "On multi switching compound synchronization of non identical chaotic systems," *Chinese Journal of Physics*, vol. 56, no. 4, pp. 1656–1666, 2018.