Hindawi
Mathematical Problems in Engineering
Volume 2022, Article ID 9076305, 9 pages
https://doi.org/10.1155/2022/9076305

Research Article

Research on Multilevel Chaotic Image Encryption Algorithm Based on Optical Processing Technology

Guangli Li[1] **and Muhammad Talha**[2]

[1]*Department of Computer and Information Engineering, Hebei Petroleum Vocational and Technical University, Chengde 067000, China*
[2]*Department of Computer Science, Superior University Lahore, Lahore, Pakistan*

Correspondence should be addressed to Muhammad Talha; talhashoaibt@yahoo.com

Received 20 April 2022; Revised 16 May 2022; Accepted 19 May 2022; Published 31 May 2022

Academic Editor: Naeem Jan

A multilevel chaotic image encryption solution based on optical processing technology is proposed to solve the difficulties of poor security and slow picture processing performance in the present avatar encryption method. The security key is created by collecting and categorising the features of multilevel chaotic pictures combined with optical processing technology. As a result, the original picture data are crystal clear and accurate. The increase in image processing security will help in simplifying and speeding the multilevel chaotic picture enrcryption process. As a result of these findings, researchers discovered that the multilevel chaotic picture encryption method based on optical processing technology is more secure in the application process, can perform image encryption faster, and improves the efficiency and accuracy of image processing overall.

1. Introduction

Artificial intelligence and big data have become more commonplace in people's daily lives during the last several years. Groups and even whole nations may be accessed via massive data. The information conveyed by a color picture is much more readily understood than a sound [1]. People like to convey information and express themselves via visuals. Information expressed in this manner has grown to be one of the most extensively used and significant forms of communication globally. In addition to politics and economics, it may be used in domains such as education and entertainment. Unauthorized access to and viewing sensitive picture data are not permitted in some study domains, such as the military, medical, or legal, for fear of compromising national security [2]. Because of its intrinsic information hiding properties, it is hard to overlook the advantages of chaos in image encryption. Compared to the traditional electrical chaotic system, the vertical cavity surface emitting laser is the most extensively used semiconductor laser.

In contrast to electrical chaos, the optical chaos formed by it is faster, has a larger bandwidth, has less loss, and is more complicated. A brief introduction to chaos theory is offered and a technique for encrypting pictures using chaos. Several essential cryptographic concepts are also presented simultaneously, followed by a comparison of their connections. Following that, several chaotic image encryption techniques and algorithms are shown. The optical processing technique is the basis for a multilayer chaotic picture encryption scheme. The suggested high-dimensional Z-matrix map offers favourable qualities such as a lengthy period and varying number of periods for various dimensions compared to current image encryption maps. Because of this, the matrix map is a good choice for picture encryption. The suggested high-dimensional Z-matrix mapping may be used to encrypt and degrade images. This research offers an optical processing-based multilevel chaotic image encryption method for picture degradation encryption. It then examines the practical application prospects of the degradation algorithm presented by experimentation and comparison. In the realm of picture information encryption, optical chaos's unique properties provide significant benefits and a wide range of potential applications. As a result, this work investigates an optical chaos-based multi-image compression and encryption technique. Below is a list of the most important findings from this study [3]. In this article, two connected vertical cavity surface emitting lasers are used to construct a secure communication system that produces optical chaos. The system's exterior disruption is caused via mutual injection. The outputs of many lasers may be synchronised by adjusting the laser settings. Chaos may be seen in light output from the laser after synchronisation. The encryption and decryption key may be formed from such a signal in the picture encryption process. There is a theoretical underpinning for both processes, and this article simulates two VCSELs using this theoretical framework. Various metrics, including simulation data, demonstrate their effectiveness.

2. Research on Multilevel Chaotic Image Encryption Algorithm

2.1. Multilevel Chaotic Image Feature Acquisition Algorithm Based on Optical Processing Technology. Duffieux has successfully implemented the Fourier optical transform in the optical field. The basic idea behind the Fourier transform is to convert a signal from time domain (or spatial domain) to frequency domain, allowing an optical image to be expressed not only by light intensity, amplitude, or transmittance but also by spatial domain, which can be interpreted by spatial frequency distribution and change [4]. Lens has Fourier transform characteristics, so lens is often used in optical encryption system, which is the basis of optical information processing. Next, the Fourier transform properties of the lens are analyzed in detail at three different positions of the object (in front of the lens, behind the lens, and close to the lens). The Fourier transform properties of the lens are shown in Figure 1.

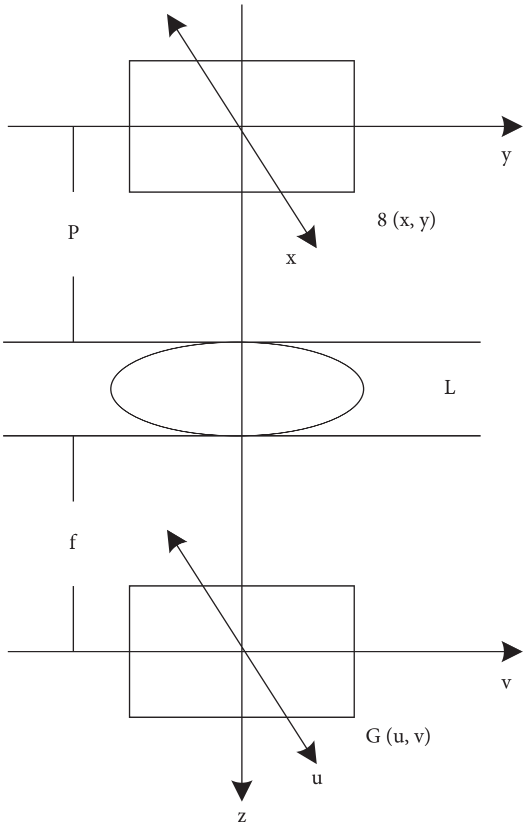

Figure 1: Fourier transform properties of lens.

Since then, Fourier optics has developed into an indispensable part of modern optics and has gradually evolved into an important mathematical tool in information science. $G\ (x)$ is a periodic function, and we assume that its period is $t = 1/F$. When this function satisfies the Dirichlet condition, the series form of the periodic function can be expanded by exponential periodic system, trigonometric function system, or other orthogonal function system. The exponential Fourier series describing the distribution of the function in the form of mathematical expression can be written as follows:

$$Ag(x) = \sum_{n=-\infty}^{\infty} G_n \exp(j2\pi n f x),$$
$$G_n = \frac{1}{T}\int_{T/2}^{-T/2} g(x)\exp(-j2\pi n f x)\mathrm{d}x. \tag{1}$$

When a signal is not a periodic signal, we can regard it as a periodic signal whose period t tends to infinity. When the signal's period is infinity, the spectral line interval of the signal will tend to infinity, and the discrete spectrum will evolve into a continuous spectrum. To better analyze the spectral characteristics when the signal is aperiodic, a concept spectral density is introduced:

$$G(jw) = \lim_{T\longrightarrow\infty}\frac{G_n}{1/T} = \lim_{T\longrightarrow\infty} G_n T. \tag{2}$$

It reflects the spectrum value on the unit frequency band. According to the Fourier series of function distribution, when the period t tends to infinity, the spectral line interval tends to infinity. Therefore, the continuous spectrum v can be expressed instead of the discrete spectrum 2π and can be expressed as follows:

$$G(jw) = \lim_{T\longrightarrow\infty} G_n T = \int_{-\infty}^{\infty} g(x)\exp(-jwx)\mathrm{d}x,$$
$$g(x) = \frac{1}{2\pi}\int_{-\infty}^{\infty} G(jw)\exp(jwx)\mathrm{d}w. \tag{3}$$

Therefore, $G(jwx)$ is actually the four transform function of the main signal G(X). Fourier will help to transform the original function of each pair of Fourier transform. Fourier transform is generally complex, and $G\ ()$ is a complex function, which can be expressed as follows:

$$G(jw) = |G(jw)| \exp(j\varphi(w)) = R(w) + jX(w), \tag{4}$$

where $R(w)$ is the amplitude spectrum of the signal, which is the real part of the complex number; $X(w)$ is the phase spectrum of the signal, which is the imaginary part of the complex number. For the two-dimensional function $g(x, y)$, if the function is integrable in its whole plane and the Dirichlet condition has been satisfied, the definition of its two-dimensional Fourier transform $G(u, v)$ can be expressed as follows:

$$G(u, v) = \int\int_{-\infty}^{\infty} \exp[-j2\pi(ux + vy)] \mathrm{d}x\mathrm{d}y = FT\{g(x, y)\}, \tag{5}$$

where FT is expressed as Fourier transform. $G(u, v)$ is the expression of the function $g(x, y)$ in the frequency domain, is its Fourier spectrum function, and is also a two-dimensional function with independent variables u and v. Similarly, the process of inverse Fourier transform is the transformation from spectral function to spatial domain original function. The inverse Fourier transform is expressed in IFT as follows:

$$\begin{aligned} g(x, y) &= \int\int_{\infty}^{\infty} G(u, v) \exp[j2\pi(ux + vy)] \mathrm{d}u\mathrm{d}v \\ &= IFT\{G(u, v)\}. \end{aligned} \tag{6}$$

The above formula can form mutually transformed Fourier transform pairs, ux and vy are conjugate variables, and u and v are the spatial frequencies of $G(u, v)$ in the x-axis direction and Y-axis direction respectively, which are different expressions of the same physical quantity in the spatial domain and time domain. Therefore, in order to simulate the properties of the light field output by two mutually injected lasers, we must first write the rate equation expression of the two lasers:

$$\begin{aligned} \frac{\mathrm{d}N_{1,2}}{\mathrm{d}t} &= \gamma_n\left(\mu - N_{1,2}\left(1 + \left|E_{1,2}^x\right|^2 + \left|E_{1,2}^y\right|^2\right)\right) - j\gamma_n n_{1,2}\left(E_{1,2}^y E_{1,2}^{x^*} - E_{1,2}^x E_{1,2}^{y^*}\right), \\ \frac{\mathrm{d}n_{1,2}}{\mathrm{d}t} &= -\gamma_s n_{1,2} - \gamma_n n_{1,2}\left(\left|E_{1,2}^x\right|^2 + \left|E_{1,2}^y\right|^2\right) - j\gamma_n N_{1,2}\left(E_{1,2}^y E_{1,2}^{x^*} - E_{1,2}^x E_{1,2}^{y^*}\right). \end{aligned} \tag{7}$$

In the above expression, the subscripts of 1 and 2 represent the labels of the two lasers, the superscripts of x and y refer to the polarization square of the output light field, γ_n represents the normalized input current, γ_n represents the mismatch between the output light field frequencies of the two lasers and represents the spin counter rotation rate, and $n_{1,2}$ represents the intensity of the joint injection light field between laser 1 and laser 2, $N_{1,2}$ refers to the injection time when two lasers inject light fields with the same intensity into each other, ξ_1, ξ_2 represent the center frequency of mcsl1 and mcsl2, respectively, $\overset{1,2}{G}$ represents the noise introduced in the process of laser spontaneous emission, and the remaining parameters are shown and explained in the previous section:

$$\begin{aligned} G_{1,2}^x &= \sqrt{\frac{v_{sp}}{2}}\left(\sqrt{N_{1,2} + n_{1,2}}\,\xi_1 + \sqrt{N_{1,2} - n_{1,2}}\,\xi_2\right), \\ G_{1,2}^y &= -j\sqrt{\frac{v_{sp}}{2}}\left(\sqrt{N_{1,2} + n_{1,2}}\,\xi_1 - \sqrt{N_{1,2} - n_{1,2}}\,\xi_2\right), \end{aligned} \tag{8}$$

where v_{sp} represents the spontaneous emission rate. The multilevel chaotic image encryption algorithm based on optical processing technology needs to decompose the image module and encrypt the subimage with different key parameters to improve the security and periodicity of the output key sequence. The improvement of the encryption algorithm is mainly divided into the following four steps:

Step 1. Input the original image file, which can be expressed in the form of matrix W and encryption times T.

Step 2. Input the initial conditions, generate a random sequence from the chaotic map, and deal with it appropriately, so as to obtain the chaotic sequence of natural number.

Step 3. Encrypt the image using the diffusion function.

Step 4. Improve the encryption algorithm of chaotic mapping for the input parameters to get the parameters again.

Step 5. Repeat steps 2 and 4 until time t to obtain the output encrypted image file.

2.2. Optimization of Multilevel Chaotic Image Encryption Steps. The turbidity principle-based picture encrypting technique is described. The key generates a long enough bubble pure sequence, and the position transformation matrix and gray transformation matrix are built from the sea turbidity sequence [5]. The plaintext picture is then repeatedly interacted with the position transformation matrix and gray transformation matrix to produce the effect of image pixel position replacement and pixel value scrambling, and the ciphertext image is the ultimate output [6]. The image encryption process based on the principle of chaos is shown in Figure 2.

The frame flow of the proposed color multi-image compression and encryption based on optical chaos is shown in Figure 3.

In this framework, optical chaos is not only embedded in compressed sensing but also embedded in optical technology (the optical technology used here is a double random phase mask based on fractional Fourier transform). The

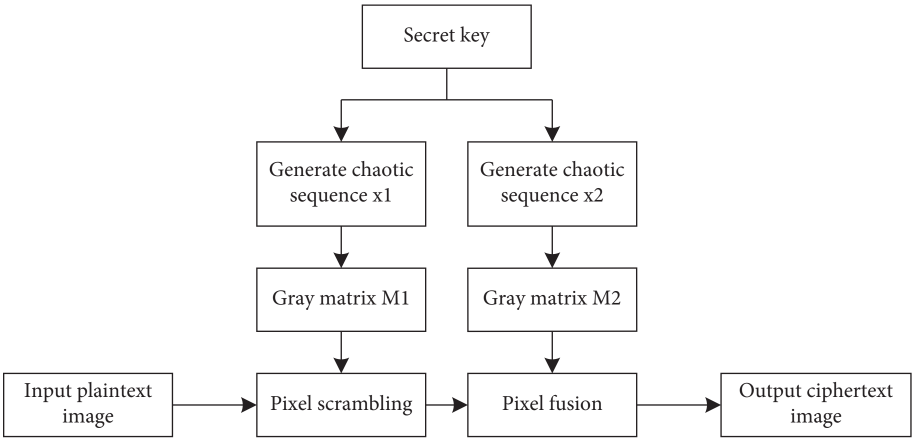

Figure 2: Image encryption process based on chaos principle.

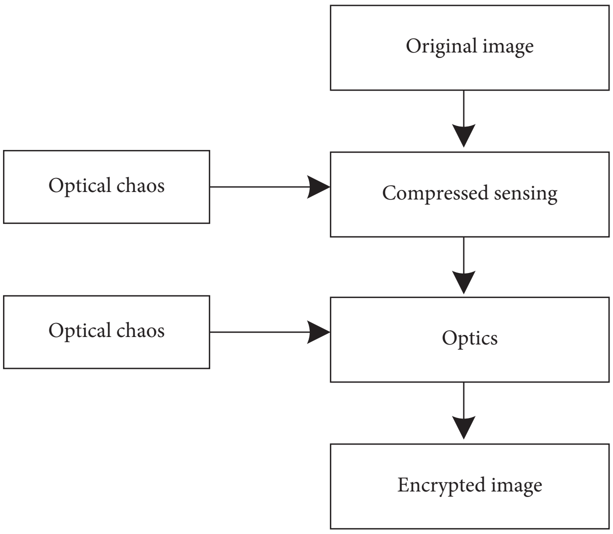

Figure 3: Frame flow of color multi-image compression and encryption based on optical chaos.

Table 1: Cryptanalysis methods.

Attack form	Attacker gets content
Ciphertext-only attack	Encryption algorithm itself Get no part of ciphertext The ciphertext information selected by yourself and the corresponding plaintext generated by the key
Clear text attack	Get no part of ciphertext Encryption algorithm itself The plaintext information selected by yourself and the corresponding ciphertext generated by the key
Known plaintext attack	Encryption algorithm itself Get some ciphertext
Ciphertext-only attack	One or more ciphertext pairs The ciphertext information selected by yourself and the corresponding plaintext generated by the key Get no part of ciphertext

Table 2: Relationship and difference between chaos and cryptosystem.

Compare	Chaos	Cryptosystem
Contact	Number of iterations	Number of encryption rounds
	Restricted by starting conditions	Controlled by key
	Sensitive to parameters and start conditions	Changing statistical relationships through scrambling and diffusion
Difference	Phase space on real number set	Phase space on finite integer set
	There are no evaluation and performance indicators	There are relatively complete evaluation and performance indicators

original image is first measured by compressed sensing based on optical chaotic system, and the measured part of Hadamard matrix is further applied [7]. Then, the final compressed encrypted image is encrypted based on the double random phase mask of optical chaotic system. In the encryption process, the encryption algorithm and key are the most important to prevent the encryption system from being damaged. Therefore, the security of encryption depends entirely on the key [8]. To find vulnerabilities, attackers also have many cryptanalysis methods, as listed in Table 1.

It can be seen from the table that ciphertext-only attack is the most difficult to attack because of the least available information [9]. The relationship and difference between chaos theory and cryptography are listed in Table 2.

If only the above improvements are made for the original algorithm, the security will be greatly improved. However, to achieve good scrambling and diffusion effect, multiple rounds (number of rounds $n > 42$) of encryption are required, which does not meet the needs of image encryption in practical application. The reason is that the scrambling effect of this algorithm only depends on the scrambling stage, and the diffusion effect only depends on the diffusion stage. To achieve a good encryption effect with fewer encryption rounds, simple operations (such as table lookup

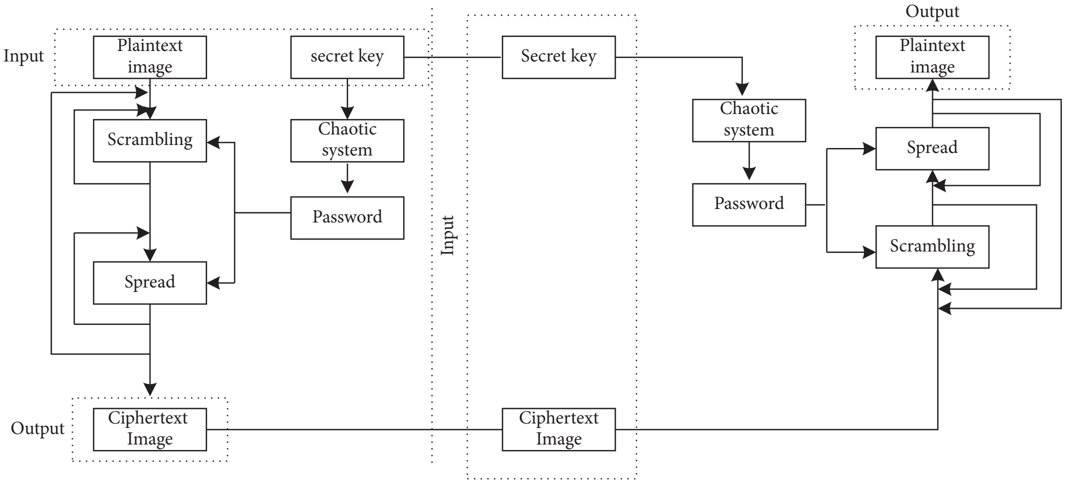

Figure 4: Schematic diagram of encryption and decryption of chaotic digital image cryptosystem.

and XOR) are added to the algorithm framework [10]. In improving this encryption algorithm, two simple XOR operations (XOR) are introduced before and after the scrambling stage, while the other operation steps are not changed. Thus, in the first stage, the scrambling of pixel positions and the replacement of pixel values are carried out simultaneously, while the pixel transformation in the second stage also increases the effect of diffusion. The result of this improvement is that the diffusion effect depends not only on the diffusion stage but also on the scrambling stage [11]. Therefore, the same encryption effect can be achieved with less encryption rounds, but the encryption time has been greatly reduced. For these two XOR operations, the first XOR operation is to operate the previous processed pixel value and the current plaintext pixel value (the order is from top to bottom and from left to right). The first pixel is XOR with a fixed key value, and the last processed pixel is XOR with (2,2) pixels. The operation steps are basically the same for the second XOR operation, except that the pixel values are carried out pixel by pixel from left to right and from top to bottom [12]. The following equation gives the basic structure of two XOR operations:

$$
\begin{gathered}
\begin{cases}
v^{r}_{1,1} = \mathrm{bitxor}\left(p^{r}_{1,1}, S\right), \\
v^{r}_{i,j} = \mathrm{bitxor}\left(p^{r}_{i,j}, v^{r}_{i,j-1}\right),
\end{cases} \\
\begin{cases}
v^{c}_{1,1} = \mathrm{bitxor}\left(\mathrm{Per}\left[v^{r}_{1,1}\right], S^{*}\right), \\
v^{c}_{i,j} = \mathrm{bitxor}\left(\mathrm{Per}\left[v^{r}_{i,j}\right], v^{c}_{i-1,j}\right),
\end{cases} \\
v_{2,2} = \mathrm{bitxor}\left(v^{c}_{2,2}, v^{c}_{N,N}\right),
\end{gathered}
\tag{9}
$$

where p is the current plaintext pixel, V is the pixel value after the first XOR processing, V is the pixel value after scrambling and the second XOR processing, S is key fixed values controlled by the user, Per is the scrambling operation before the second XOR processing, and v_2 is the final pixel value after the processing of (2,2) points (where $<n.0 < j5m$. The above simple XOR operation can effectively change the encrypted pixel value of each pixel in the image and achieve a good diffusion effect [13]. Therefore, this structure is very conducive to image encryption. The multilevel chaotic image encryption system based on chaotic system belongs to the symmetric key cryptosystem because it has the same key in encryption and decryption. The encryption and decryption diagram of the cryptographic system is shown in Figure 4.

As can be seen from the figure, the encryption system inputs the plaintext image and key and outputs the ciphertext image through the encryption algorithm [14]. The encryption aspect sends the key to the decryption aspect through the secret channel (in most cases, it is realized utilizing the public key cryptosystem) and transmits the ciphertext image to the decryption aspect through the public channel. In the decryption system, the key and ciphertext image are input, and the decrypted image is output through the decryption algorithm. The restored plaintext can be output only when the key is correct [15].

2.3. Implementation of Chaotic Image Encryption. From the structure of chaotic image encryption, the encryption structure of chaotic image encryption algorithm can be roughly divided into scrambling operation encryption structure, diffusion operation encryption structure, scrambling diffusion operation encryption structure, and diffusion scrambling operation encryption structure. Common chaotic maps include logistic, Henon, and baker maps [16]. Security analysis may assess the image encryption algorithm's security performance. To assess the security performance of the chaotic picture encryption technique, the ciphertext generated by the chaotic image encryption algorithm may be attacked using some attack methods. A guaranteed security chaotic picture encryption system should have modest correlation between neighbouring pixels and a uniform histogram distribution to successfully withstand other assaults. The key design process, security assessment system, and performance analysis system of conventional cryptography theory are quite developed when compared to the traditional cryptography theory. However, due to the short development time of chaotic encryption system, there is no standard and unified criterion for evaluating chaotic encryption algorithm [17]. The common standards used to evaluate the security performance of chaotic image encryption algorithms are gray histogram index, adjacent pixel correlation index, key sensitivity index, key space index, average pixel correlation index, and differential attack. The adjacent pixel correlation refers to the similar characteristics between the gray values of adjacent pixels of the image. An attacker can crack the adjacent pixel values around the pixel point through the pixel value of one of the image pixels [18]. The image pixel position rearrangement method is usually used to encrypt the image to avoid this situation. In this way, the correlation between adjacent pixels of the image is disrupted, and the attacker cannot crack any data information of adjacent pixels around a pixel from the pixel value of a pixel in the image. The calculation formula is as follows:

$$\begin{aligned} r_{xy} &= \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)} \cdot \sqrt{D(y)}}, \\ \operatorname{cov}(x, y) &= \frac{1}{N} \sum_{i=1}^{N} \left(\left(x_i - E(x) \right) \left(y_i - E(y) \right) \right), \\ E(x) &= \frac{1}{N} \sum_{i=1}^{N} x_i, \\ D(x) &= \frac{1}{N} \sum_{i=1}^{N} \left(x_i - E(x) \right)^2. \end{aligned} \tag{10}$$

In the above formula, $\operatorname{cov}(x, y)$ represents the correlation function of pixel values, $E(x)$ represents the mean, and $D(x)$ represents the mean square deviation. Before the image is encrypted, its histogram is irregular and uneven. Under this condition, some image information can be obtained [19]. If the image is encrypted, the gray histogram of the image is relatively flat and uniform distribution, which proves that the scrambling effect of the image encryption algorithm is better. On the contrary, it shows that the scrambling effect of the algorithm is not very obvious; that is, the security of the encryption algorithm is not high [20]. In image, it is assumed as the total number of image pixels which represent the number of pixels of the K gray level. The formula is as follows:

$$P(r_k) = \frac{n_k}{N}, \tag{11}$$

where P_i can reflect the frequency in the image. Therefore, the distribution characteristics of the gray value of an image can be obtained through the histogram. For analyzing an image, the image gray histogram is a convenient and fast tool [21]. The formula for calculating the histogram value and the variance formula for calculating the histogram are as follows:

$$\begin{aligned} U &= \sum_{i=1}^{255} P_i, \\ \partial^2 &= \sum_{i=1}^{255} P_i (i - u)^2. \end{aligned} \tag{12}$$

According to the above XOR operation principle, each $P(I, J)$ and $B(I, J-1)$ are XOR operated in order to obtain $P(I, J)$. $B(I, J)$ is obtained by operating according to the above position exchange principle. After all XOR and transposition operations are completed, $B(m, n)$ is obtained. B is the image after scrambling the original image. The cross conversion of chaotic images is shown in Figure 5.

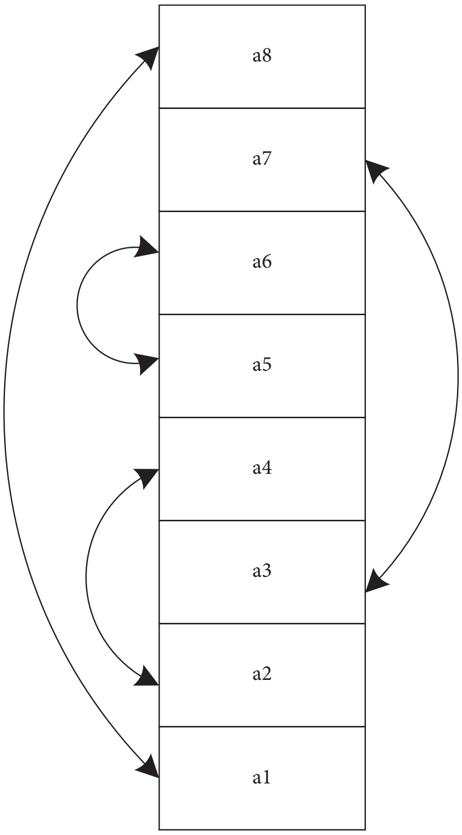

Figure 5: Schematic diagram of chaotic image cross transposition.

The design of chaotic image encryption algorithm generally follows the following steps: when the security requirement of encrypted image is relatively low and the speed of encryption and decryption is relatively fast, a simple low dimensional chaotic system can be selected as the encryption system. If the image has a high demand for encryption security, it will help in high demand of chaotic mapping system as the main key. In selecting the key, we can choose the combination of internal key and external key and select multiple encryption keys, which can ensure that the key space is relatively large, the encryption effect is good, and can resist the attack of exhaustive method; Encryption and decryption are two different process. The pixel position scrambling operation and pixel value diffusion operation are carried out on the original image to encrypt the image through the selected chaotic mapping system. The decryption process is the reverse process of encryption. *Step 4*: it will help to evaluate the encryption security. After encrypting the original image, the ciphertext is obtained. The encryption index analyzes the security of ciphertext image encryption effect and the speed of encryption and decryption.

Table 3: Comparison of correlation coefficient values of adjacent pixels before and after image encryption.

Direction	Horizontal correlation coefficient	Vertical correlation coefficient	Diagonal correlation coefficient
Original image	0.93658	0.95685	0.90868
Original image 1	−0.00268	−0.00685	0.00658
Original image 2	−0.00438	−0.00468	−0.00258
Original image 3	0.00165	0.00109	−0.00168
Original image 4	0.00265	−0.00198	0.00015

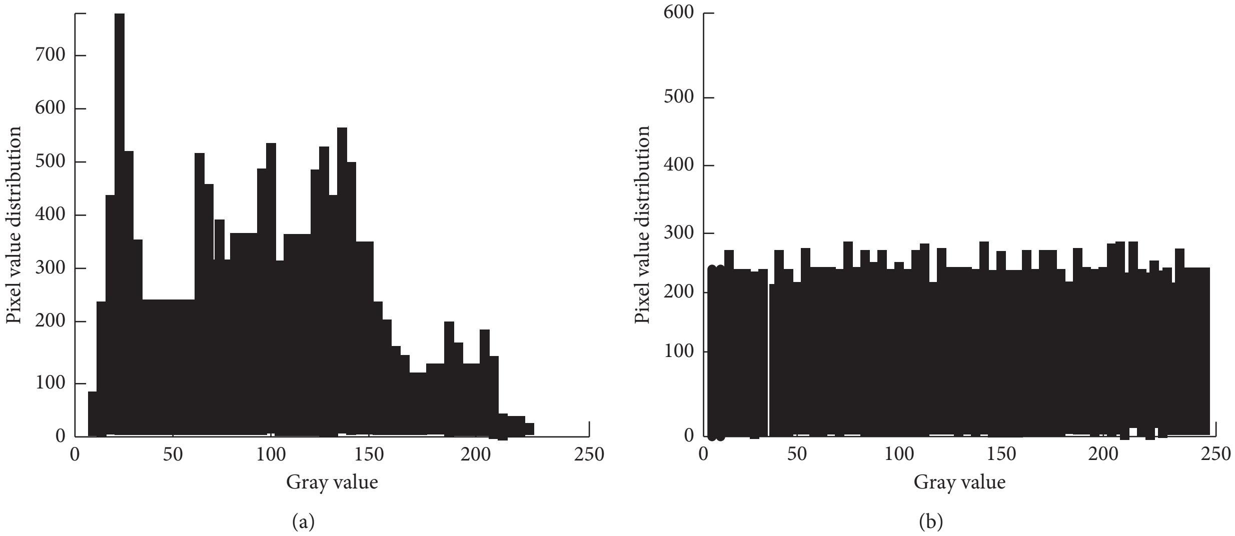

Figure 6: Image histogram comparison detection results. (a) Lena original histogram. (b) Lena ciphertext histogram.

3. Analysis of Experimental Results

In VC++ 6.0 programming environment, the simulation experiment of encryption and decryption of a gray image is carried out by using the multilevel chaotic image encryption algorithm based on optical processing technology. The parameters of setting the key are as follows: the correct decryption password is $x_0 = 0.6$; the traditional key is $a = 20$ and $B = 40$; the key of multilevel chaotic image encryption algorithm based on optical processing technology is $M = 5$, $n = 8$, $u = 11$, $v = 5$, and $f = 50$. The encryption key of the image is 8739 bits and the space is $28739 \approx 10328$. At this time, the space of the key must be strong to resist brute force attacks to ensure the accuracy of the experiment. The multilevel chaotic image encryption algorithm based on optical processing technology decomposes the original image into modules and sets the mapping equation for different parameters (a, b):

$$\begin{aligned}\operatorname{cov}(a,b) &= E(a - E(a))(b - E(b))\\ &= \frac{1}{N}\sum_{i=1}^{N}(a_i - E(a))(b_i - E(b)),\end{aligned} \tag{13}$$

Where E is the pixel and N is considered as the total parameter of chaotic region control. Because the chaotic mapping system's starting value is chosen at random and the initial value's selection range is broad, the initial value is particularly sensitive to the sequence's setting. Read the complete image information and digitise the increase in periodic cycle feature of the key output. This will help to increase the sequence for the enhancement of standard multilevel chaotic image encryption. After the original image is encrypted by the algorithm proposed in this section, four encrypted ciphertext subgraphs can be obtained. The correlation coefficient values of adjacent pixels in the horizontal, vertical, and diagonal directions of the original image and ciphertext subgraph are listed in Table 3.

Table 4: Comparison between two kinds of digital encrypted images.

Project	Original image	Traditional digital encryption image	Digital image encryption based on chaotic mapping
Horizontal direction	0.9812	0.3587	0.1358
Vertical direction	0.9578	0.0763	0.0886
Diagonal direction	0.9435	0.0268	0.0135

Different key pairs are used for the images of each submodule, so that the system has high confidentiality and will not be easily attacked by the outside world. By distributing the gray value of each pixel information of the image, the image gray histogram can be obtained, and the histogram's statistical correlation between images can be seen intuitively. The experimental results are shown in Figure 6.

The image histogram can intuitively reflect the difference between before encryption and after encryption. The pixel values before encryption are unevenly distributed and easy to be decoded. In contrast, the pixels after encryption are evenly distributed and completely cover up the distribution of the original image, which greatly increases the difficulty of decoding the protected image. To summarise, this algorithm has an unsettling impact. The initial tests are carried out to validate the rationale of the enhanced multilayer chaotic picture encryption technique based on optical processing technology. The diagram shows that even if the key is Y or X parameter changes slightly, the picture before encryption cannot be reliably recovered. We will make full sue of sensitivity of chaotic map for the digital improvement of the security of map encryption algorithm. The adjacent digital images in the original image are highly correlated. The correlation of adjacent digital images is reduced to avoid image scrambling, and the ability to resist attacks is greatly enhanced. About 100 pairs of pixel parameters are selected from the original and encrypted images and tested from horizontal, vertical, and diagonal directions. The test results are listed in Table 4.

It can be seen from the table that the digital encrypted image based on the improved algorithm of optical processing technology has slightly higher pixels in the vertical direction compared with the traditional digital encrypted image. Whether from the perspective of vision or the scrambling of image orientation, the improved digital image based on optical processing technology is better than the traditional digital encrypted image. It is concluded that the improved encryption algorithm can increase the key's space and improve the encrypted image's security performance. The viewing effect of the image is also very good, and the time is greatly shortened, which can fully meet the real-time requirements.

4. Conclusion

In multimedia information security research, secure digital picture transmission and storage have been a hot subject. Unfortunately, ergodicity, pseudorandomness, and sensitivity to beginning circumstances are chaos features. As a result, individuals use chaos to create multilevel chaotic image encryption. Image encryption technology is a game-changing advancement that has addressed several tough research challenges. The picture encryption techniques based on three chaotic maps are investigated in this study.

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 conflicts of interest.

References

[1] Y. Xian and X. Wang, "Fractal sorting matrix and its application on chaotic image encryption," *Information Sciences*, vol. 547, no. 5, pp. 1154–1169, 2021.

[2] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Information Sciences*, vol. 480, no. 6, pp. 403–419, 2019.

[3] J. C. Dagadu, J. Li, and E. O. Aboagye, "Medical image encryption scheme based on multiple chaos and DNA coding," *International Journal on Network Security*, vol. 21, no. 1, pp. 83–90, 2019.

[4] Q. Shen, W. Liu, Y. Lin, and Y. Zhu, "Designing an image encryption scheme based on compressive sensing and non-uniform quantization for wireless visual sensor networks," *Sensors*, vol. 19, no. 14, pp. 3081–3085, 2019.

[5] W. H. Alshoura, Z. Zainol, J. S. Teh, and M. Alawida, "A new chaotic image watermarking scheme based on SVD and IWT," *IEEE Access*, vol. 8, pp. 43391–43406, 2020.

[6] Z. M. Z. Muhammad and F. Ozkaynak, "Security problems of chaotic image encryption algorithms based on cryptanalysis driven design technique," *IEEE Access*, vol. 7, pp. 99945–99953, 2019.

[7] X. Wang, S. Gao, L. Yu et al., "Chaotic image encryption algorithm based on bit-combination scrambling in decimal system and dynamic diffusion," *IEEE Access*, vol. 7, pp. 103662–103677, 2019.

[8] J. Gayathri and S. Subashini, "An efficient spatiotemporal chaotic image cipher with an improved scrambling algorithm driven by dynamic diffusion phase," *Information Sciences*, vol. 489, no. 5, pp. 227–254, 2019.

[9] W. Feng, Y. G. He, H. M. Li, and C.-L. Li, "Cryptanalysis of the Integrated Chaotic Systems based image encryption algorithm," *Optik*, vol. 186, no. 8, pp. 449–457, 2019.

[10] K. A. K. Patro and B. Acharya, "An efficient dual-layer cross-coupled chaotic map security-based multi-image encryption system," *Nonlinear Dynamics*, vol. 104, no. 3, pp. 2759–2805, 2021.

[11] M. Alawida, A. Samsudin, J. S. Teh, and R. S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption," *Signal Processing*, vol. 160, no. JUL, pp. 45–58, 2019.

[12] A. Broumandnia, "The 3D modular chaotic map to digital color image encryption," *Future Generation Computer Systems*, vol. 99, no. 11, pp. 489–499, 2019.

[13] T. Wang, L. Song, M. Wang, and Z. Zhuang, "A novel image encryption algorithm based on parameter-control scroll chaotic attractors," *IEEE Access*, vol. 8, pp. 36281–36292, 2020.

[14] R. Zhao, Y. Zhang, X. Xiao, and X. R. Ye, "TPE2: three-pixel exact thumbnail-preserving image encryption," *Signal Processing*, vol. 183, no. 6, Article ID 108019, 2021.

[15] B. Vaseghi, S. Mobayen, S. S. Hashemi, and A. Fekih, "Fast reaching finite time synchronization approach for chaotic systems with application in medical image encryption," *IEEE Access*, vol. 9, pp. 25911–25925, 2021.

[16] R. B. Krishnan, N. R. Kumar, and N. R. Raajan, "An approach for attaining content confidentiality on medical images through image encryption with steganography," *Wireless Personal Communications*, vol. 23, no. 3&4, pp. 1–17, 2021.

[17] A. Firdous, A. U. Rehman, and M. M. Saad Missen, "A gray image encryption technique using the concept of water waves, chaos and hash function," *IEEE Access*, vol. 9, pp. 11675–11693, 2021.

[18] M. Yildirim, "DNA encoding for RGB image encryption with memristor based neuron model and chaos phenomenon," *Microelectronics Journal*, vol. 104, no. 5, Article ID 104878, 2020.

[19] J. Khan, J. P. Li, B. Ahamad, and S. A. Parveen, "SMSH: secure surveillance mechanism on smart healthcare IoT system with probabilistic image encryption," *IEEE Access*, vol. 8, pp. 15747–15767, 2020.

[20] G. Kaur, R. Agarwal, and V. Patidar, "Color image encryption scheme based on fractional Hartley transform and chaotic substitution-permutation," *The Visual Computer*, vol. 38, no. 3, pp. 1027–1050, 2021.

[21] S. Wang, "Simulation of multi-feature contrast enhancement method for digital media images," *Computer Simulation*, vol. 37, no. 4, p. 178, 2020.