A color image encryption algorithm for expert detection system based on composite chaotic sequences

Z. Li [1]
[1] *School of Forensic Science and Technology, Criminal Investigation Police University of China, 110854, China, Shenyang, Huanggu District, Tawan Street, 83*

Abstract

With the development of the Internet, the amount of information carried in images is gradually increasing, and image encryption algorithms for data transmission have been developed. The conventional composite chaotic sequence encryption algorithm has the problem of too long convergence speed when applied to images, which can lead to the risk of information leakage in the image. To address this issue, this study first applies chaotic attractors to improve composite chaotic sequences and enhance the search domain of their Leia Index. At the same time, the Arnold transform technology is introduced into the expert monitoring system, and the two systems are fused to generate a fusion algorithm for color image encryption. Finally, the study conducts experiments on the Differ dataset to verify the effectiveness and superiority of the fusion algorithm, and compares it with three algorithms such as artificial fish schools. The image encryption times of the four algorithms are 6 s, 16 s, 29 s, and 33 s respectively, indicating that the fusion algorithm has the highest encryption speed. When facing exhaustive attacks, the image information damage degrees of the four algorithms are 0.014, 0.051, 0.172, and 0.184, respectively. The experimental results show that the proposed algorithm can effectively resist differential attacks and exhaustive attacks, and is suitable for encrypting color images.

Keywords: composite chaotic sequence, expert detection system, color image encryption, chaotic attractor, Leia index, Arnold transformation.

Citation: Li Z. A color image encryption algorithm for expert detection system based on composite chaotic sequences. Computer Optics 2025; 49 (1): 95-102. DOI: 10.18287/2412-6179-CO-1457.

Introduction

Against the backdrop of the rapid development of the information terminal industry, the use of images for information transmission is becoming increasingly popular, which has great convenience for people's lifestyles [1, 2]. Due to the large amount of privacy information of residents contained in images, research on image information confidentiality is equally important in the context of the simultaneous development of the information theft industry. Composite Chaotic Sequence (CCS) has the ability to scramble pixels and has been developed in the research of image encryption [3]. However, this method is only applicable to low chromaticity images, and for color images, the convergence speed of CCS cannot meet the confidentiality requirements. The experts' approach to this is to introduce a chaotic attractor (CA) and change its Leia Index (LI). This method can effectively improve the encryption speed and is sufficient to deal with differential attacks. But the exhaustive attack targets encrypted images, and this method cannot repair the information loss of the attacked images [4]. To address this issue, this study inserted Arnold Transformation (AT) into Expert Detection (ED) and generated a fusion algorithm (LCS-AED) with it. The main content of the study can be divided into four parts. The first part mainly analyzes and summarizes the current applications of CCS. The second part introduces the methods of using CAs and introduces them into CCS. The third part conducts simulation experiments on the Differ dataset. The last part analyzes and compares the performance of this model with traditional models, and points out the shortcomings that still exist in the research. The practical significance of this study is to provide a powerful encryption algorithm for color images to cope with various attack methods, with intention to effectively protect image information and thereby safeguard residents' privacy.

1. Related works

In the encryption algorithms of color images, research is widely distributed internationally. Song et al. believed that independent chaotic parameters have transient effects and other issues, so they proposed a brand new chaotic system (S-L-F). Their system was sensitive to initial values and has a maximum entropy of 0.95, indicating that it was suitable for image encryption. In response to the problem of poor practicality of traditional multi image encryption schemes, they adopted image recombination for multi image encryption. After testing, their ciphertext images could effectively resist differential attacks. The experimental results showed that their algorithm had high security [5]. Chen et al. fused dynamic DNA encoding and chaos to generate a fusion algorithm for color image encryption. They used three neuron scores as the birth device for chaotic sequences, and this initial value was generated using five parameters and ordinary images. They proposed a new 3D projection obfuscation method to obfuscate the three pigments red, green, and blue. Finally, they used XOR to ensure the security of encryption. The experimental outcomes indicated that their algo-

rithm was superior in encryption ability and could resist conventional attack methods [6]. Hassan et al. also developed color image encryption algorithms based on DNA encoding and chaos. They defined that the initial value was generated by a five parameter external key and associated the external key with the discrete step size. They set a larger key space and increase the sensitivity of the algorithm. In addition, they randomly placed the red, green, and blue pixels and diffused the image information. Their research findings indicated that their algorithm had good confidentiality performance and could effectively face differential attacks [7]. To protect digital images, Huang et al. encrypted the images into white noise images. They derived two one-dimensional chaotic maps and designed a two-dimensional chaotic system. They used the proposed chaotic mapping to scramble the original image using the generated chaotic sequence, and then used the chaotic sequence to obfuscate it. The simulation results showed that their proposed algorithm was effective and reliable [8].

With the continuous development of attack methods, relying solely on CCSs to protect information is slightly insufficient, and ED has gradually entered the vision of many scholars. Shen et al. believed that the technical challenge of collaborative labeling systems lied in information explosion, which made it difficult to quickly obtain expert information. Therefore, they proposed ED and recommendation models based on label semantics. They first improved the aggregation hierarchical clustering, then proposed a community ED algorithm to identify community experts, and finally proposed an expert recommendation algorithm based on collaborative filtering algorithm. They conducted experiments on real datasets, and the experimental findings denoted that their model had better performance than the benchmark method [9]. Zhang et al. mined association data based on expert systems to accelerate the establishment of rule bases. They proposed anomaly detection methods for building systems and used association rules to associate anomalies with normal operations. Then, they would develop an expert system based on the established rule base. They applied the proposed method to actual refrigeration units, and experimental results expressed that their method could successfully detect abnormal operating modes and multiple unknown abnormal operations [10]. Zhang et al. proposed an image encryption algorithm based on chaotic mapping for stacking 2D and 1D chaotic sequences. Firstly, they used integer keys to generate the initial values of chaotic sequences, and they used external key sequences to generate logical matrices. Then, they used diffusion structures for the encryption process and chaotic sequences for scrambling. To improve encryption, they analyzed several typical numerical experiments and scrambled image blocks using chaotic sequences. The experimental results indicated that their image encryption system had security [11].

Through the research of numerous experts and scholars, it has been found that research on color image encryption algorithms is very popular, but there is still little research linking ED technology to it. This study groundbreaking introduces ED technology into conventional image encryption algorithms and establishes a composite system based on image information protection.

2. Design and research of ED system based on CCS in color image encryption

CCS is a common nonlinear system in which the flowing elements are called CAs. To design high-quality algorithms for color image encryption, this study first improves the CCS, then integrates it with the ED system, and explores its application effect in color image encryption.

2.1. Establishment of an encryption system integrating CCSs with ED

Conventional CCSs have the problem of unfixed convergence speed in the same direction during operation [12]. To reduce the probability of this situation occurring, this study introduces the LI in the CA to characterize the motion of the chaotic oscillator. Research sets the correlation between the value of LI and the system dimension, and assumes a variable initial sphere in space.A method for calculating the LI is established, as shown in Formula (1).

$$LI = \lim_{t\to\infty} t^{-1} \times \ln \frac{r_t}{r_0}. \tag{1}$$

In Formula (1), the original shape radius of the variable initial ball is denoted as r_0, and after a time interval of t, the radius of the ball at this time is expressed as r_t. The r_t in the LI can represent the degree of chaos in CCS, and its value is positively correlated with the volume of the chaotic sequence. When a CCS with LI is working, the system's tangent transformation is determined by the vector of the modulus operation. There are two working states of LCS, as shown in Fig. 1.

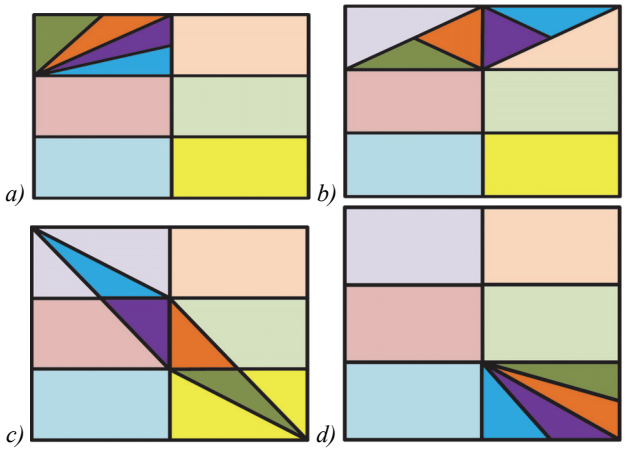

Fig. 1. Working state of LCS under different conditions: primitive chaotic sequence (a), transverse transformation (b), normal transformation (c), transformed system (d)

Fig. 1 describes the operation of LCS, where Fig. 1(a) is the original chaotic sequence. When the result of the modulo operation is linear, LCS adopts a lateral transformation, as shown in Fig. 1(b). Otherwise, it uses the normal transformation method shown in Fig. 1(c) [13]. Finally, the LCS is transformed into a CCS in a staggered state, as shown in Fig. 1(d). The converted LCS contains a large number of compressed signals, and their density is reduced using Formula (2).

$$\begin{cases} \theta = \alpha x \\ y = \beta x = \gamma\theta \end{cases}. \tag{2}$$

In Formula (2), the compressed and sparse signals are represented by x, θ, and α represents the dilution rate of the signal during the process. y is the predicted value at the end of dilution, with β and γ representing the slope of the signal before and after dilution, respectively [14]. The two are closely related to dilution time, so the study introduces the compression measurement method into the source signal to reduce the running time of the process. The introduction method is as follows Formula (3).

$$\left[1-\delta(k)\right]\times\|x\|_2^2 \le \|Ax\|_2^2 \times\left[1+\delta(k)\right]\times\|x\|_2^2. \tag{3}$$

In Formula (3) above, the size of the arrangement during signal segmentation is denoted as A, and the set of distances between signals is represented by $\delta(k)$. When the measured value $\delta(k)$ is constant, the dynamic formula of A can be determined, as shown in Formula (4).

$$B_{n+1} = uB_n \times\left(1-B_n\right). \tag{4}$$

In Formula (4), the randomly selected signal is represented by B_n; its next signal is denoted as B_{n+1}; the dynamic relationship between the two is denoted as u. It is a constant that takes a value on [3.57, 4]. The use of Formula (4) can reflect the motion law of the signal. Although this method has a wide range of values, it still has weak confidentiality performance when facing high-intensity differential attacks [15]. To enhance the confidentiality performance of the system, the ED section is introduced in the study. ED is a system that mimics the planning process of experts and has multiple ways of thinking, as shown in Fig. 2.

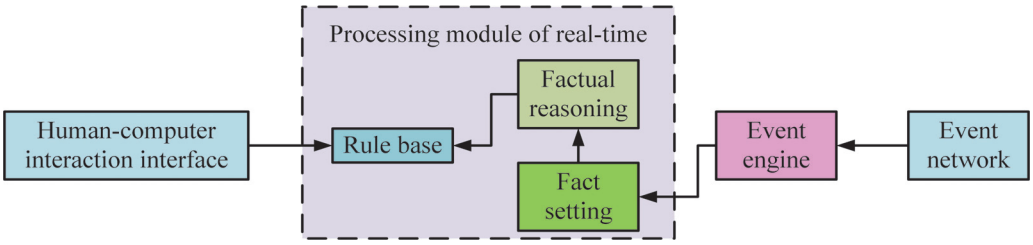

Fig. 2. The processing of ED

Fig. 2 shows the process of ED, including human-computer interaction, event import, and real-time processing. During the event import process, the engine will split the type, origin, and port of the event, as well as the target location and interface. The results obtained from this step can be used for computation to output events that match the components of the event inference machine. However, due to the large amount of data transported in this process, it is more dangerous than the event splitting part [16]. To achieve effective data protection, this study adds AT to it, as shown in Formula (5).

$$\begin{bmatrix} \chi_{n+1} \\ \varepsilon_{n+1} \end{bmatrix} = \begin{bmatrix} \iota & p \\ q & pq+\iota \end{bmatrix} \times \begin{bmatrix} \chi_n \\ \varepsilon_n \end{bmatrix} \times mid_n. \tag{5}$$

In Formula (5), the randomly selected data nodes are denoted as χ_n; their adjacent nodes are represented by χ_{n+1}; their coordinates are denoted as $\varepsilon_n, \varepsilon_{n+1}$. Through the control of p, q, these nodes are limited to a certain range. ι is a correction constant used in the control process to prevent abnormal events from jumping out. mid_n is the calculation of node area, which is related to the range of events. The use of ED after AT can limit the range of LCS values. For the encryption of two-dimensional events in LCS, event nodes can be marked with coordinates, as shown in Formula (6) below.

$$\begin{cases} \kappa_{i+1} = \nu\lambda_\kappa\kappa_i \times\left(1-\kappa_i\right)+o\mu_i \\ \mu_{i+1} = \nu\lambda_\mu\mu_i \times\left(1-\mu_i\right)+o\kappa_i \end{cases}. \tag{6}$$

In Formula (6) above, the initial coordinates of the event point are denoted as o, and the two axis coordinates at time i are represented by κ_i and μ_i, respectively. At this time, the event parameters of both are denoted as $\lambda_\kappa, \lambda_\mu$. The event coordinates at the next moment are denoted as κ_{i+1}, μ_{i+1}, and the transformation rules between the two depend on the correlation between the events. The study uses v to represent them. Optimizing LCS using AED can generate LCS-AED and obtain the optimized encryption method, as shown in Fig. 3.

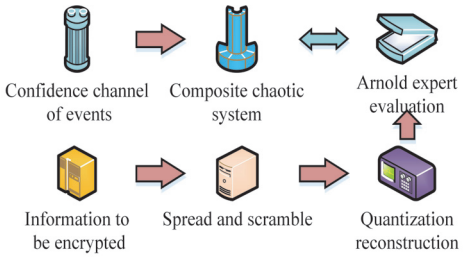

Fig. 3. Encryption flow chart of LCS-AED

Fig. 3 shows the encryption process of LCS-AED. After being processed separately by LCS and AED, the level of

confidentiality of the information has been greatly improved. In this process, the degree of information diffusion and confusion depends on the initial level of confusion, and the relationship between the two follows Formula (7).

$$\begin{cases} \dfrac{dc}{dt} = \varpi \times (j - c) \\ \dfrac{dj}{dt} = rc - gc - j \end{cases}. \tag{7}$$

In Formula (7), the event after diffusion scrambling and the initial event are recorded as j, c respectively, and the diffusion time is represented by t. The scaling of the diffusion process is denoted as ϖ, while r and g represent the system parameters of LCS and AED, respectively. The use of LCS-AED can not only keep conventional information confidential, but also occupy an important position in image encryption.

2.2. Model construction based on fusion system LCS-AED and color image encryption

For the encryption of color images, conventional encryption methods face the problem of a large amount of information, due to the excessive variety of pixels in color images. To enhance the work adaptability of the encryption algorithm, this study extends the information contained in the secret key, as shown in Formula (8). This method not only optimizes the sensitivity of LCS-AED to color images, but also effectively resists differential attacks from spoilers, occupying an important position in the research of plaintext image encryption algorithms [17].

$$KEY = \left\{ \sum_{i=1}^{n} key_i \,\middle|\, n \in [1, 64] \right\}. \tag{8}$$

In Formula (8), the set of keys is denoted as KEY, where the elements are represented by key_i. From Formula (8), this study divides the secret key score into 64, so the key solving types are composed of 2^{64} key solving types. For the decryption of a system, the high sensitivity of the system determines its security, that is, an error in decryption represents the loss of image information. The decryption measures of this encryption method are shown in Formula (9), and in order to ensure fast encryption of the system, the method used in this study is XOR operation [18].

$$\begin{cases} \theta_0 = (key_1 \times key_2 \times \ldots \times key_{16}) / (2^{16}) \\ \vartheta_0 = (key_{17} \times key_{18} \times \ldots \times key_{32}) / (2^{16}) \\ X_0 = (key_{33} \times key_{34} \times \ldots \times key_{48}) / (2^{16}) \\ Y_0 = (key_{49} \times key_{50} \times \ldots \times key_{64}) / (2^{16}) \end{cases}. \tag{9}$$

In Formula (9), θ_0, ϑ_0 mean the event coordinates before decryption, and the event coordinates after decryption are recorded as X_0, Y_0. This method targets pixels, which have three types during the encryption process: red, green, and blue. When LCS-AED encrypts these pixels, the regularity between the source color image encodings is disrupted, and the encrypted image can only be restored with the corresponding key. Due to its strong resistance to exhaustive attacks, the decryption process of the designed image in this study is shown in Fig. 4 [19].

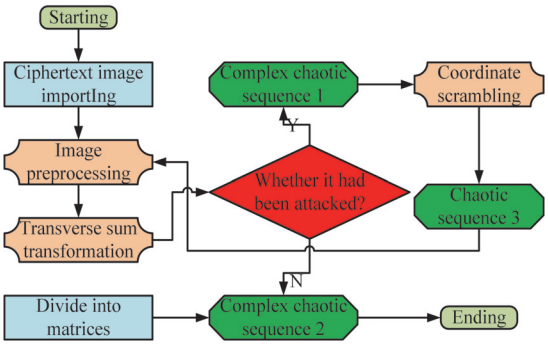

Fig. 4. Decryption flow chart of images to deal with exhaustive attacking

Fig. 4 shows the proposed method for countering exhaustive attacks. From Fig. 4, the process of adding attack determination to the existing LCS-AED fusion system is studied. When facing exhaustive attacks, LCS-AED will transfer image information into a CCS. Due to its strong uncertainty, this sequence can effectively target exhaustive attacks. During the operation of the algorithm, the attacked image will be reassigned using the following Formula (10).

$$\begin{cases} \mathrm{mod}(\rho, l) = uuf + \{\rho, l\} \\ \mathrm{mod}(\sigma, l) = uut + \{\sigma, l\} \end{cases}. \tag{10}$$

In Formula (10) above, the modulo operation is denoted as mod( ), which is a method of evading exhaustive attacks; ρ, σ express the image coordinates under attack; uuf, uut are the response constant for exhaustive attacks, and they take values in CCSs. In the image, the labeled pixels are represented by l, which also represents a sequence to prevent information loss. After encountering exhaustive attacks on encrypted images, a portion of the information in the image will be lost. To explore the importance of this part of information, the correlation between pixels in the image is studied and calculated to determine the degree of information damage, as shown in Formula (11).

$$\begin{cases} cur(Pi, Xe) = Lo^{-1} \times (Pi_i - E_{Pi}) \times (Xe_i - E_{Xe}) \\ E_{Pi} = Lo^{-1} \times \sum_{i=1}^{Lo} Pi_i \\ D_{Pi} = Lo^{-1} \times \sum_{i=1}^{Lo} (Pi_i - E_{Pi})^2 \end{cases}. \tag{11}$$

In Formula (11), $cur(Pi, Xe)$ denotes the degree of information loss between adjacent pixels; Pi, Xe are the randomly selected two adjacent pixels; the total pixels in the image are recorded as $L0$; E_{Pi} and D_{Pi} represent the loss in the horizontal and vertical directions of the pixels, respectively. When the information loss value is too high, the information carrying capacity of pixels decreases,

which represents a successful attack [20]. To increase information protection efforts, this study aims to reduce the correlation between pixels, as shown in Formula (12).

$$\Delta H = \sum_{i=1}^{Lo} \varsigma_i \lg\left(2\times\varsigma_i\right). \tag{12}$$

In Formula (12) above, the degree of information confusion between pixels is denoted as ΔH, and pixels with additional information are represented using ς_i. Adopting this method can not only fully decode encrypted images with the correct key, but also enhance its confusion towards exhaustive attackers. There are keys with different sensitivities in the key space, and they can all behave independently when decoding images. Due to the fact that small differences in the secret key can also have a significant impact on the decoding results, the study introduces a destructive method of CCSs, which involves scrambling pixels in the event of a key error, as shown in Figure 5.

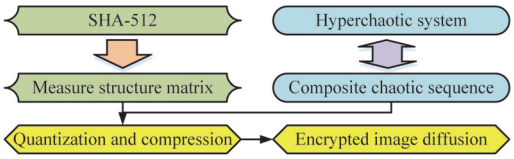

Fig. 5. Protecting process of CCS to image

For LCS-AED encrypted images, the key of the image is dynamically transformed to enhance the security of the image. After the chaotic sequence in Fig. 5 is destroyed, although the image information becomes scattered, the total amount of information carried by pixels remains unchanged, meaning that the damaged image can be repaired. To fully preserve image information, this study introduces discrete wavelet functions into the LCS-AED process, as shown in Formula (13).

$$\begin{aligned}&\tau_t\left(\ell,\Omega\right)=\left|\mho_0\right|^{-0.5}\times\tau\left[\left(t-\Omega\mho_0\upsilon_0\right)/\mho_0{}^t\right]=\\&=\left|\mho_0\right|^{-0.5}\times\tau\left(t\mho_0{}^{-t}-\Omega\upsilon_0\right).\end{aligned} \tag{13}$$

In Formula (13), the parameters of pixels in the horizontal and vertical directions are denoted as $\mho, \upsilon$, ℓ, and Ω respectively, representing the discretized values of the two. τ is a conditional parameter in the discrete process, which is related to the degree of pixel loss. During the discretization process, the information in the pixels is rearranged to obtain the original information. Through this rearrangement method, the final pixel information obtained can be guaranteed to be complete, as shown in Formula (14).

$$F\left(t\right)=C\times\sum_{-\infty}^{0}\sum_{0}^{+\infty}C\left(\ell,\Omega\right)\times\tau_t\left(\ell,\Omega\right). \tag{14}$$

In Formula (14), the information ratio between the damaged pixel and the repaired pixel is denoted as C. The information obtained through formula (14) can be retained intact, which belongs to one-dimensional information. Due to the fact that color images belong to two-dimensional information, the complete information ultimately needs to be converted in the following way (15).

$$\begin{cases}\omega_{i,j}=\psi\times\tau_t\left(i\right)F\left(j\right)\\ \xi_{i,j}=\zeta\times Xe_iE_{Xe}\end{cases}. \tag{15}$$

In Formula (15), ω and ξ express the recovered information in both directions, and ψ,ξ is the conditional parameter of their recovery process, whose value is related to the total image information.

3. Practical verification of the encryption model LCS-AED in color images

To verify the encryption effect of LCS-AED, this study conducted experiments on the Differ dataset. This dataset contains images under differential attack and exhaustive attack, with a total of 1000 images of both types. Due to the different sharpness of images in the dataset, research was conducted on various sharpness images to verify the application effect of the model.

3.1. Analysis of the effect of LCS-AED on images under differential attack

During the experiment, due to the limited amount and types of data on the Differ dataset, this study divided them equally into two groups. The image clarity in these two sets of data was similar and could be considered as the same dataset. Before the experiment, equipment selection and parameter determination were first conducted, as shown in Tab. 1.

Tab. 1. Experimental parameters and equipment selection of LCS-AED model

Device type	Operating parameters or software
2D-LASM parameter	0.618
AT	1,3,150
Composite chaotic system	9,168,2-195,-5
Size of the image	512*512
Operating system	Windows XP
Central processing unit	Corei7-5500U GPU
Data set	Differ
Language	Easy Chinese
Execution method	Matlab R2023c
System memory	8.0T*2
Method of encryption	LCS-AED
Main frequency	50~60 Hz

For the LCS-AED algorithm, it involves steps such as graying out images and pixel distortion when encrypting color images. In these steps, the attack timing of differential attack will have a significant impact on the confidentiality of the encrypted image. To mitigate this impact, this study conducted experiments on the convergence time of the LCS-AED encryption algorithm and compared it with the experimental results of the Harris Hawks Optimization (HHO) algorithm, Spotted hyena (SH) algorithm, and Artificial Fish Swarm (AF) algorithm. The experimental results are shown in Fig. 6.

Figure 6 compares the encryption time of four algorithms. From Fig. 6*a*, for image encryption with high clarity, LCS-AED achieved a stable encryption time of 6 seconds when running to the 203rd image. This time was the

shortest among the four encryption algorithms, with HHO, SH, and AF algorithms having encryption times of 16 s, 29 s, and 33 s, respectively. Although the encryption time of images with high blurriness was significantly longer than that of clear images, LCS-AED still had the fastest encryption speed of 11 seconds. The encryption algorithm proposed in the study had the highest efficiency after equal training. To verify the superiority of the system, this study conducted experiments on the energy loss of the algorithm. The experimental results are shown in Fig. 7.

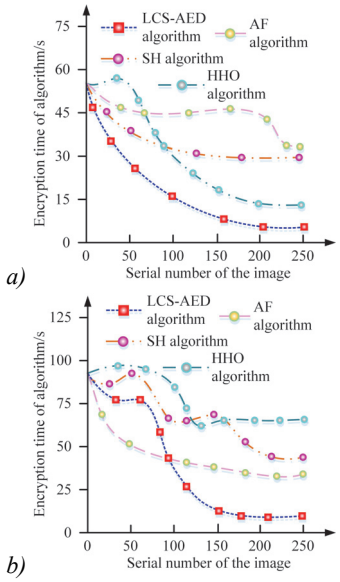

Fig. 6. Comparison of convergence time of four encryption algorithms: high-definition pictures (a), blurred pictures (b)

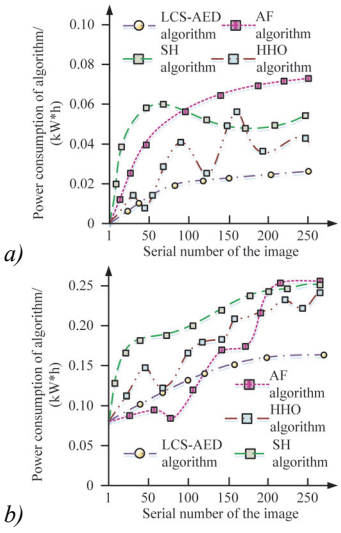

Fig. 7. Comparison chart of energy consumption of four encryption algorithms: high-definition pictures (a), blurred pictures (b)

Fig. 7 is the comparison ofthe energy consumption of four encryption algorithms during operation. From Fig. 7*a*, after encryption of 121 images, the energy loss of the LCS-AED algorithm tended to stabilize, reaching 0.020 kW×h per image. This loss was the lowest among the four algorithms, with the power consumption of the other three algorithms being 0.041, 0.048, and 0.069 kW×h. Due to the low resolution of blurry images, their energy loss during encryption was significantly higher than that of clear images. The algorithm proposed in the study still had the lowest energy loss under these conditions, at 0.148 kW×h. The LCS-AED algorithm was the most environmentally friendly under the same working conditions.

3.2. Application effectiveness of LCS-AED in encrypted images faced with exhaustive attacks

Among common attack methods, differential attack targets the image encryption process. Exhaustive attack is different. It will decode the encrypted image. At this point, image information not only suffers from loss, but also leaks when the encryption method is not advanced enough. To explore the effectiveness of algorithms in dealing with exhaustive attacks, this study conducted experiments on the degree of information loss in images and the degree of information repair after attacks, and set the experimental environment as shown in Table 2.

Tab. 2. Parameter setting and experimental environment of the algorithm in the face of exhaustive attack

Device type	Operating parameters or software
Data set	Differ
Language	Easy Chinese
Method of decryption	LCS-AED
LI	0.427
Size of the image	512*512
Central processing unit	Corei8-5521U GPU
Main frequency	50~60 Hz
Operating system	Windows 8+
AT	1,3,150
Floppy disk memory	512 GB
Discrete conditional parameter	0.054
Execution method	Matlab R2023c

When the destructor uses exhaustive attacks as an image parsing method, the exhaustive attack arranges the pixels of the image and decodes them by recombining them. When pixels are rearranged, some information will collapse due to the destructive nature of exhaustive attacks on color images. This study analyzed the degree of information loss in color images and compares them with the experimental results of HHO, SH, and AF algorithms. The experimental results are plotted as shown in Fig. 8.

Fig. 8 shows the comparison of image information loss in the face of exhaustive attacks. From Fig. 8*a*, for images before the 23rd, the information loss of the AF algorithm was lower than that of LCS-AED. As the experiment continued, LCS-AED was already familiar with the attack method after attacking 136 images using the same attack method. At this point, the information loss of the image tended to stabilize, and the loss rate was the lowest among the four algorithms, which was 0.016. In the experiment in Fig. 8*b*, the information loss degrees of LCS-AED, HHO, SH, and AF algorithms were 0.014, 0.051, 0.172, and 0.184, respectively. When facing exhaustive

attacks, the image information protected by LCS-AED had the best retention. For lost information, encryption algorithms would repair it. This study conducted experiments on the information recovery process after an attack, and the experimental results are shown in Fig. 9.

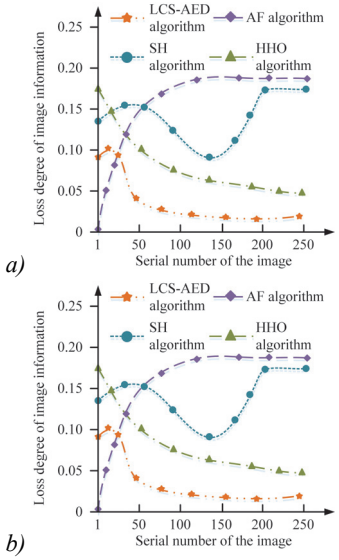

Fig. 8. Comparison chart of information lossing of four algorithms: high-definition pictures (a), blurred pictures (b)

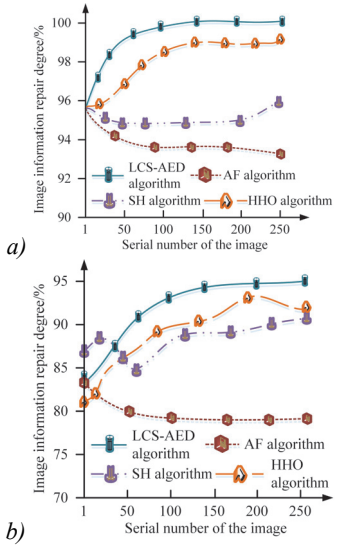

Fig. 9. The information recovery processing of four algorithms after attack: high-definition pictures (a), blurred pictures (b)

From Fig. 9, the experimental results for repairing clear images were better than those for blurry images. In the fuzzy image information restoration experiment shown in Fig. 9*b*, although the SH algorithm before image 48 had better experimental results than LCS-AED, LCS-AED had the best experimental results after that, with the best image information restoration level of 94.8 %. The experimental results of HHO, SH, and AF algorithms were 91.2 %, 89.7 %, and 79.4 %, respectively. LCS-AED had the highest information recovery for the same image. However, only a single experimental result could not demonstrate the authenticity of the LCS-AED algorithm. Therefore, 33 experiments were conducted on this dataset and a fitting diagram was drawn as shown in Figure 10.

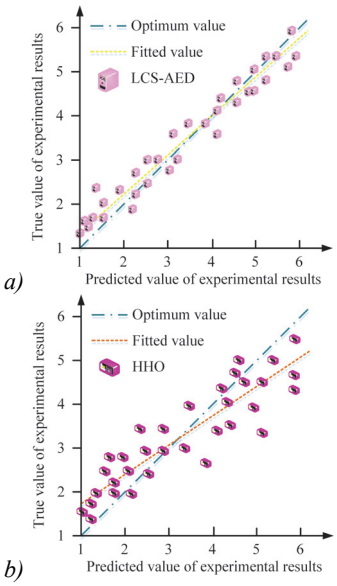

Fig. 10. Linear fitting diagram of 33 experiments between LCS-AED (a) and HHO Algorithm (b)

From Fig. 10, in 33 experiments, the linear fitting of LCS-AED was 0.9826, which was higher than the linear fitting of HHO algorithm. The experimental results denoted that the algorithm proposed in the study had superior encryption performance for colored images and had universality, which can be applied to the encryption of color images.

Conclusion

With the modernization of the information dissemination industry, encryption methods for color images have developed. To cope with the attack methods of saboteurs, this study improved CCS and ED using CAs and AT, respectively, and generated LCS-AED. The simulation experiments studied were conducted on the Differ dataset and compared with three algorithms: HHO, SH, and AF. For clear images, their encryption times were 6 s, 16 s, 29 s, and 33 s, respectively. For blurred images, the encryption times were longer, and the encryption times for the four algorithms were 11 s, 32 s, 48 s, and 63 s, respectively. LCS-AED has the best encryption performance when facing the same image. For the energy consumption performance of the system, the power consumption of LCS-AED, HHO, SH, and AF were 0.020, 0.041, 0.048, and 0.069 kW×h, respectively. After the same work, LCS-AED had the highest energy utilization rate. After facing exhaustive attacks, the information loss degrees of the four algorithms were 0.016, 0.021, 0.034, and 0.060, respectively. Under the same attack conditions, LCS-AED had the best protection effect on image information. For image information restoration, their degree of information restoration was 99.7%, 98.6%, 95.9%, and 93.2%, respectively. LCS-AED retained the most information in the image after the attack.

The experimental results expressed that the LCS-AED encryption algorithm had high efficiency and universality, and was suitable for encryption of color images. But this study only focused on differential and exhaustive attacks, and attack methods included differential and integral attacks. Faced with an increasing number of attack methods, this type of research is equally important and will gradually be carried out in future research.

Acknowledgements

The research was supported by the Special Project of Basic Work for Strengthening Police with Science and Technology of the Ministry of Public Security, Project number: No. 2020GABJC03; Basic Scientific Research Projects of Education Department in 2023, Project number: No. JYTZD2023146 and Guangdong Provincial Forensic Science of Evidence Materials (Nantian) Engineering Technology Research Center Open Projects Fund, Project number: ETRC202404.

References

[1] Jani KK, Anand A, Srivastava S, Srivastava R. Automatic abnormality detection system for capsule endoscopy. J Inf Sci Eng 2020; 36(5): 955-966. DOI: 10.6688/JISE.202009_36(5).0001.

[2] Monte DCS, Ornaghi JHL, Ornaghi FG, Monticeli FM, Voorwald HJC, Cioffi MOH. Effect of different stacking sequences on hybrid carbon/glass/epoxy composites laminate: Thermal, dynamic mechanical and long-term behavior. J Compos Mater 2020; 54(6): 731-743. DOI: 10.1177/00219983198685.

[3] Margabandu S, Subramaniam SK. Influence of fiber stacking sequences and matrix materials on mechanical and vibration behavior of jute/carbon hybrid composites. World J Eng 2021; 19(5): 639-651. DOI: 10.1108/WJE-01-2021-0008.

[4] Guo Y, Mustafaoglu Z, Koundal D. Spam detection using bidirectional transformers and machine learning classifier algorithms. J Comput Cogn Eng 2022; 2(1): 5-9. DOI: 10.47852/bonviewJCCE2202192.

[5] Song X, Xu D, Li G, Xu W. Multi-image reorganization encryption based on SLF cascade chaos and bit scrambling. J Web Eng 2021; 20(4): 1115-1130. DOI: 10.13052/jwe1540-9589.20410.

[6] Chen L, Yin H, Yuan L, Lopes AM, Machado JAT, Wu R. A novel color image encryption algorithm based on a fractional-order discrete chaotic neural network and DNA sequence operations. Front Inform Techn El 2020; 21(6): 866-879. DOI: 10.1631/FITEE.1900709.

[7] Hassan MH, Elsayed SK, Kamel S, Rahmann C, Taha IBM. Developing chaotic Bonobo optimizer for optimal power flow analysis considering stochastic renewable energy resources. Int J Energ Res 2022; 46(8): 11291-11325. DOI: 10.1002/er.7928.

[8] Huang H, Yang S, Ye R. Efficient symmetric image encryption by using a novel 2D chaotic system. IET Image Process 2020; 14(6): 1157-1163. DOI: 10.1049/iet-ipr.2019.0551.

[9] Shen M, Wang J, Liu O, Wang H. Expert detection and recommendation model with user-generated tags in collaborative tagging systems. J Database Manage 2020; 31(4): 24-45. DOI: 10.4018/JDM.2020100102.

[10] Zhang C, Zhao Y, Zhou Y, Zhang X, Li T. A real-time abnormal operation pattern detection method for building energy systems based on association rule bases. Build Simul-China 2022; 15(1): 69-81. DOI: 10.1007/s12273-021-0791-x.

[11] Zhang Y, Zhao J, Zhang B. An image encrypting algorithm based on 1D and 2D logistic chaotic systems. Int J Embed Syst 2022; 15(1): 34-43. DOI: 10.1504/IJES.2022.122057.

[12] Liu W, Khalil AM, Basheer R, Kin Y. Prediction system for diagnosis and detection of coronavirus disease-2019 (COVID-19): A fuzzy-soft expert system. CMES-Comp Model Eng 2023; 135(3): 2715-2730. DOI:10.32604/cmes.2023.024755.

[13] Oslund S, Washington C, So A, Chen T, Ji H. Multiview robust adversarial stickers for arbitrary objects in the physical world. J Comput Cogn Eng 2022; 1(4): 152-158. DOI: 10.47852/bonviewJCCE2202322.

[14] Saha I, Dang EK, Svatunek D, Houk KN, Harran PG. Computational generation of an annotated gigalibrary of synthesizable, composite peptidic macrocycles. P Natl A Sci 2020; 117(40): 24679-24690. DOI: 10.1073/pnas.2007304117.

[15] Kaboglu C, Eken TY, Yurekturk Y. Impact performances and failure modes of glass fiber reinforced polymers in different curvatures and stacking sequences. J Compos Mater 2022; 56(7): 1123-1138. DOI: 10.1177/00219983211059.

[16] Genç MS, Özkan R. Optimum layer sequence analysis for composite blade using ACP-FSI model. Int J Sust Aviat 2021; 7(4): 354-371. DOI: 10.1504/IJSA.2021.119693.

[17] Rajappan RJ, Kondampatti KT. A composite framework of deep multiple view human joints feature extraction and selection strategy with hybrid adaptive sunflower optimization-whale optimization algorithm for human action recognition in video sequences. Comput Intell-US 2022; 38(2): 366-396. DOI: 10.1111/coin.12499.

[18] Školáková P, Badri Z, Foldynová TS, Ryneš J, Šponer J, Fojtová M, Fajkus J, Marek R, Vorlíčková M, Mergny JL, Trantírek L. Composite 5-methylations of cytosines modulate i-motif stability in a sequence-specific manner: Implications for DNA nanotechnology and epigenetic regulation of plant telomeric DNA. BBA-Gen Subjects 2020; 1864(9): 129651-129651. DOI: 10.1016/j.bbagen.2020.129651.

[19] Ünver M, Olgun M, Türkarslan E. Cosine and cotangent similarity measures based on Choquet integral for Spherical fuzzy sets and applications to pattern recognition. J Comput Cogn Eng 2022; 1(1): 21-31. DOI: 10.47852/bonviewJCCE2022010105.

[20] Sahbaz KN, Karaduman Y. Effect of stacking sequence on the mechanical properties of non-interlaced multiaxial jute yarn/epoxy composites. J Compos Mater 2022; 56(13): 2083-2094. DOI: 10.1177/0021998322109058.

Author's information

Zhen Li was born in Shenyang, Liaoning, P.R. China, in 1980. He received the master's degree from Shenyang University of Technology, P.R. China. Now, he worked in Criminal Investigation Police University of China. His research interests include questioned documents examination, digital image processing and information security. E-mail: *lizhen_wjjyjsx@126.com.*

Received: November 08, 2023. The final version – April 07, 2024.