ISSN 1330-3651 (Print), ISSN 1848-6339 (Online) https://doi.org/10.17559/TV-20240321001416
Original scientific paper

Cloud Computing Data Transmission Security Guarantee Model Based on Mod256-PSC Hybrid Encryption Algorithm

Jinming YUAN

Abstract: With the widespread application of cloud computing technology, the secure transmission of image data in cloud environments has become an important issue. Traditional image encryption techniques face challenges in dealing with large-scale and dynamic cloud computing environments, such as complex key management and insufficient encryption efficiency. To address these issues, this study proposes an innovative image encryption decryption algorithm that combines pixel sorting classification (PSC) method and block mod256 scrambling encryption (SE) technology, aiming to improve the security of image data transmission in cloud computing. Through empirical experiments, this study found that the newly proposed algorithm exhibited superior performance while maintaining image integrity. In comparison to existing technologies, the new technology has demonstrated an improvement in both peak signal-to-noise ratio (PSNR) and image size. Specifically, at lower data embedding rates, the average PSNR value of this algorithm ranged from 52 dB to 54 dB, and it exhibited high security ratings on different types of images. In addition, the algorithm also demonstrated strong robustness in resisting various attack paradigms in cloud computing systems. Although the algorithm proposed in this study has limitations in real-time processing, it provides a new approach for secure transmission of image data in cloud computing and valuable reference for future research. Future work will focus on optimizing the real-time processing capabilities of algorithms and further validating and expanding them in real-world cloud computing environments.

Keywords: cloud computing; data embedding; image encryption; network attack; pixel sorting

1 INTRODUCTION

The advent of cloud computing has facilitated the deployment of data and applications in cloud environments, offering convenience and economy to an ever-increasing number of enterprises and individuals [1, 2]. In the field of image processing, the application of cloud computing enables the storage and processing of a significant volume of image data, offering powerful capabilities [3]. Nevertheless, the transmission of data in the network and cloud storage also presents numerous security risks, with the secure transmission of image data emerging as a significant concern. To ensure the integrity, availability, and confidentiality of image data, it is crucial to study and apply efficient and reliable encryption techniques [4].

The existing image encryption technologies mainly rely on traditional symmetric and asymmetric encryption methods. Although symmetric encryption technology is widely popular due to its fast speed and simple algorithm, its application is limited by key management and distribution issues in large-scale and dynamic cloud computing environments. Although asymmetric encryption technology effectively addresses the challenge of key distribution, its efficiency in processing large amounts of image data is limited, which presents a challenge for cloud computing. Therefore, the paper aims to develop a new image encryption and decryption algorithm to improve the security performance of image encryption methods in cloud computing.

To fill this research gap, this study proposes a novel image encryption algorithm (IEA) based on hybrid encryption technology. This algorithm combines pixel sorting classification (PSC) method and block mod256 scrambling encryption (SE) technology, aiming to solve the security issues related to image data transmission in cloud computing [5]. This algorithm employs the inherent characteristics of image data for encryption, while also enhancing the flexibility and security of encryption through the introduction of modular encryption strategies [6].

The main contribution of this study lies in: Firstly, by combining PSC method and SE technology, a new hybrid encryption algorithm is proposed, which significantly improves the security and efficiency of encryption while maintaining image quality. Secondly, this study validates the effectiveness of the proposed algorithm through experiments and compares it with existing IEA. The results show that the algorithm exhibits superior performance in multiple indicators. Finally, this study provides new ideas and methods for the secure transmission of image data in cloud computing, which is of great significance for promoting the development of cloud computing security technology.

2 LITERATURE REVIEW

Image data in cloud computing transmission may face the risk of network attacks. Therefore, this paper analyzes the research results of previous researchers on image security encryption, providing some ideas for reference in this study. Yang Z. et al. believed that time delay systems could be utilized in the field of image encryption. Therefore, the author proposed a differential-order energy storage element time-delay system, designed an image encryption scheme based on this system, and analyzed some statistical characteristics. Digital simulation has verified the effectiveness of theoretical analysis and the security of image encryption schemes [7]. Zhang F. et al. proposed a novel 2D delayed complex logic mapping. This new mapping method extended the variables of traditional 2D logical mapping from real numbers to complex fields. Then the researchers constructed a color image encryption system on the grounds of this mapping method, which used bit-level permutation and one-time keys to improve computational speed and defend against selective plaintext attacks. The outcomes indicated that the encryption system exhibited a substantial key space and exemplary key sensitivity, with information entropy approaching optimal

values. Additionally, it demonstrated resilience to traditional cryptographic attacks. Zhang Q's team proposed a solution to enhance the transmission security and speed of multi-image content by addressing challenges such as large data volume, slow transmission rates, and low security during internet transmission. The study concentrated on resolving transmission and storage issues related to large-scale image data in cloud computing environments. It demonstrated the significance of hybrid encryption technology in improving transmission security and speed [8].

Wang X. et al. designed a chaotic IEA and introduced a composite key. Specifically, the author proposed a new scrambling method that randomly divided the pixels of a plaintext image into four blocks, performed different rounds of Arnold transformation on each block, and then combined the four blocks to generate a scrambling image [9]. Next, a composite key was designed, which generated the true key by filtering out a set of pseudo keys through a synchronously updated Boolean network. This key served as the initial value of a hybrid linear nonlinear coupled mapping lattice system for generating chaotic sequences. Last, the matrix semi-tensor product operation was utilized for chaotic sequences and scrambled images for generating encrypted images. The test results showed that compared to other encryption algorithms, the proposed algorithm was more secure and effective [10]. Due to the increased power function of RSA encryption, computation became cumbersome and time-consuming. Budati A. K. et al. proposed an improved Rivest Shamir Adleman algorithm. The test results on multiple image datasets showed that the designed algorithm had the optimal execution time, and the encrypted data possessed a high level of security protection [11]. Xu L. et al. designed a new IEA that used the Zigzag algorithm to scramble pixel positions. The test results showed that the designed algorithm could enhance the security of image encryption results. The encryption speed did not significantly increase compared to traditional methods [12].

In conclusion, although some encryption algorithms have been developed for the purpose of transmitting images and graphics, there is no specific IEA designed for the specific type of image in question. In cloud computing, the transmission of images presents a unique set of challenges. Each image has its own data characteristics, and the implementation of targeted encryption measures can significantly enhance the security of image encryption.

3 METHOD

The Internet has led to the widespread use of cloud computing applications. In terms of image processing, consumers have gradually accepted the method of encrypting images and uploading them to the cloud for management [13-15]. Nevertheless, data stored in the cloud remains susceptible to theft, manipulation, and other forms of exploitation. This study aims to design a model that guarantees the security of image transmission in cloud computing. The model combines the PSC method with mod256 block SE technology. The core of this model is the image data encryption and decryption algorithm.

3.1 Plaintext Image Information Encryption Algorithm Based on the PSC Prediction

In a cloud computing environment, the primary concern is the security of the network. Consequently, it is imperative to devise a rational encryption algorithm to guarantee the security, integrity, and reliability of data. Firstly, the image data encryption and decryption algorithm in the cloud computing image data transmission security guarantee model is designed. Due to the significant differences in the structure and content of plaintext and ciphertext information in the image, the two are treated separately and appropriate encryption algorithms are designed for each [16, 17]. The image plaintext information encryption algorithm contains two aspects. The first is to use the designed PSC prediction method to predict image pixels, and the second is to embed additional data (AD) and restore the image. Firstly, it designs an image pixel prediction process based on the PSC prediction method by classifying the images. The images are divided into three categories, namely images containing four, three, and two domains. The following will provide a detailed explanation of the three types of images. A 256-level grayscale image with a size of $M \times N$ will be divided into pixel blocks with a size of 4×4. Taking Fig. 1 as an example, the prediction principle of pixels is explained. As shown in Fig. 1, the four-pixel blocks in the middle after division are predicted based on the four adjacent pixel blocks from the top, bottom, left, and right. The pixel blocks at edges and corners are predicted on the basis of the three or two adjacent pixel blocks. This method can fully utilize surrounding pixels [18].

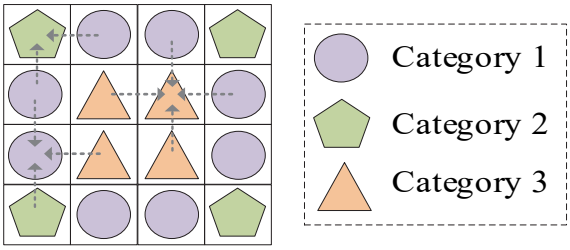

Figure 1 Pixel block classification prediction display

The calculation process of the PSC prediction method is designed subsequently. For an image block containing n pixels, the pixels are sorted in ascending order. This study uses n_L, n_H, and n_R to represent the number of elements in sets L, H, and R, where each set represents a class of pixels. The pixel block $\{x(1), x(2), .., x(n)\}$ is sorted in ascending order and becomes $\{h(1), h(2), .., h(n)\}$. During the initialization process, it sets $L = \{h(1)\}$, $R = \{h(n)\}$, $i = 1$, $j = n$, $n_L = 1$, and $n_R = 1$. Then, the classification process is carried out according to Eq. (1).

$$\begin{cases} h(i) \in L, i = i + 1, \text{if } h(i) - h(1) \le EL \text{ and } i \le j \le n \\ h(j) \in R, j = j - 1, \text{if } h(n) - h(j) \le EL \text{ and } i \ge j \ge 1 \end{cases} \quad (1)$$

The EL parameter in Eq. (1) is the maximum value of the prediction error interval (PEI) to determine the

maximum value of the AD PEI, while *i* and *j* are utilized for pixel classification counting. After the classification is completed, the remaining pixels will form the set *H*. When predicting pixel values, different prediction methods are applied based on the characteristics of different sets. For the pixels in set *L*, its predicted value is the maximum value in the set as max(*L*). For the pixels in set *R*, the predicted value is the minimum value in the set as min(*R*).

For the pixels in set *H*, it first determines whether the difference between max(*H*) and max(*L*) is greater than *EL*, and then predicts the pixels in set *H* on the basis of the judgment results. The specific prediction process of pixels in set *H* is shown in Eq. (2).

$$f(i)=\begin{cases}\max(L), \text{if } 1\le i\le nH, \max(H)-\max(L)\le EL\\ \max(L)+EL, \text{if } 1\le i\le nH, EL<\max(H)-\max(L)<2EL\\ \max(L)-EL, \text{if } 1\le i\le nH, \max(H)-\max(L)>2EL\\ \max(L), if\ i=nH\end{cases} \tag{2}$$

In Eq. (2), $f(i)$ is the predicted value of pixel *i*. The PSC method is used to predict the four domain pixels in the case, as shown in Fig. 1. The order of adjacent pixels $\{x_1,x_2,x_3,x_4\}$ sorted by the PSC method is $\{c_1,c_2,c_3,c_4\}$, and the prediction operation is performed according to Eq. (3).

$$x'=\begin{cases}c_1-(EL+1), \text{if } x\le c_1 \text{ and } |x-c_1|>EL\\ \lfloor (c_2+c_3)/2 \rfloor, if\ c_1<x<c_4\\ c_4, if\ x>c_4 \text{ and } x-c_4\le EL\\ c_4+(EL+1), \text{if } x\ge c_4 \text{ and } x-c_4>EL\\ c_1, \text{if } x\le c_1 \text{ and } |x-c_1|\le EL\end{cases} \tag{3}$$

In Eq. (3), x'. represents the predicted pixel value. Similarly, the prediction method for edge pixels can be obtained, as shown in Eq. (4).

$$x'=\begin{cases}c_1-(EL+1), \text{if } x\le c_1 \text{ and } |x-c_1|>EL\\ c_2, \text{if } c_1<x<c_3\\ c_3, \text{if } x>c_3 \text{ and } x-c_3\le EL\\ c_3+(EL+1), \text{if } x\ge c_3 \text{ and } x-c_3>EL\\ c_1, \text{if } x\le c_1 \text{ and } |x-c_1|\le EL\end{cases} \tag{4}$$

The prediction method for corner pixels is shown in Eq. (5).

$$x'=\begin{cases}c_1-(EL+1), \text{if } x\le c_1 \text{ and } |x-c_1|>EL\\ \lfloor (c_1+c_2)/2 \rfloor, \text{if } c_1<x<c_2\\ c_2, \text{if } x>c_2 \text{ and } x-c_2\le EL\\ c_2+(EL+1), \text{if } x\ge c_2 \text{ and } x-c_2>EL\\ c_1, \text{if } x\le c_1 \text{ and } |x-c_1|\le EL\end{cases} \tag{5}$$

Next is to embed AD. Firstly, the second and third-class pixels are used to predict the first-class pixels, and data embedding is added to obtain the modified first-class pixels. Then it performs the same operation on the second and third types of pixels using the first type of pixels to obtain the modified second and third types of pixels. The above description is a rotating embedding model for pixel classification, which simultaneously preserves predicted values and hides AD. The calculation process of embedding data is as follows: For the pixel $x(i,j)$ in the image, an appropriate adjacent pixel based on its position within the block is selected, and then the PSC prediction method is used to obtain the predicted result $x'(i,j)$ value. The next step is to calculate the prediction error $Pe(i,j)$ according to Eq. (6).

$$Pe(i,j)=x(i,j)-x'(i,j) \tag{6}$$

Then, on the grounds of the range of prediction error, the embedding operation of AD is performed, and the calculation method is shown in Eq. (7). Embedding AD into the three types of pixels can obtain an image G containing the AD.

$$g(i,j)=\begin{cases}x(i,j)-(EL+1), \text{if } Pe(i,j)<-EL\\ x(i,j)+Pe(i,j)-b, \text{if } -EL\le Pe(i,j)\le 0\\ x(i,j)+Pe(i,j)+b, \text{if } 0\le Pe(i,j)\le EL\\ x(i,j)+(EL+1), \text{if } Pe(i,j)>EL\end{cases} \tag{7}$$

In Eq. (7), *b* represents the extracted AD. AD extraction method is redesigned, using the PSC prediction method to predict pixels, extracting AD, and restoring images. To ensure the accuracy of the extracted data, it is extracted in the order of the third, second, and first-class pixels. The pixel prediction during AD extraction is consistent with that during embedded data. However, due to the changes in predicted pixel values after data embedding, the resulting predicted values may differ from the original predicted values, leading to recovery errors. Therefore, when extracting AD, various pixels are also operated according to Eqs. (3), (4), and (5), but the maximum value of pixels is changed to $EL+1$ before prediction. Then its predicted pixels vary in $EL+1$ steps within the value range to improve prediction accuracy. After obtaining the accurate $x'(i,j)$, Eq. (8) is used to calculate the prediction error Pe'.

$$Pe'(i,j)=g(i,j)-x'(i,j) \tag{8}$$

Considering that the range of AD values reaches $[-EL,EL]$ as well as the maximum pixel change value reaches $EL+1$. If the prediction error of the extracted AD is within the range $[-2EL-1,2EL+1]$, it indicates that pixel *g* contains *b*. *b* is calculated according to Eq. (9).

$$b=\begin{cases}0, \text{if } Pe' \bmod 2=0\\ 1, \text{if } Pe' \bmod 2=1\end{cases} \tag{9}$$

Finally, it corrects g to obtain the original pixel x, as shown in Eq. (10).

$$x=\begin{cases} g=(EL+1), \text{if } Pe'<-2EL-1 \\ x'+\text{fix}\left(Pe'-b/2\right), \text{if } 0\le Pe'\le 2EL+1 \\ x'+\text{fix}\left(Pe'-b/2\right), \text{if } -2EL-1\le Pe'\le 0 \\ g-(EL+1), Pe'>2EL+1 \end{cases} \tag{10}$$

At this point, the encryption method for plaintext image data has been designed, and the overall calculation process is shown in Fig. 2.

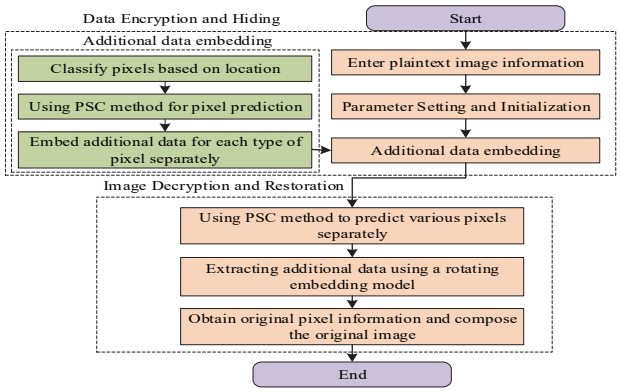

Figure 2 Calculation process of plaintext image data encryption method based on the PSC prediction

3.2 PSC-Based Reversible Encryption for Ciphertext Images

The encryption algorithm of the image data security model designed above for cloud computing systems is not suitable for processing ciphertext images. Therefore, a new encryption algorithm for ciphertext image transmission is designed, and the core of this algorithm is still the PSC method. The designed ciphertext IEA contains image encryption and decryption, AD hiding, AD extraction, and image restoration steps.

Firstly, the paper designs the image encryption and decryption part of the algorithm, considering that the reversible information hiding method in the ciphertext IEA is the prediction error histogram translation, and AD needs embedding in the encrypted image. Therefore, it is essential for ensuring the correlation and security between the encrypted data and the original data, so choosing the block mod256 block SE method is the most appropriate. In the AD hiding step, to accurately extract AD, auxiliary information such as the final embedding position and number of embedding layers of the AD are required. Therefore, AD hiding contains two. The first is the reversible information hiding algorithm using a hybrid PSC prediction method for image embedding and AD processing. The second part is overflowing handling. To save auxiliary information, the encrypted image E will be divided into two parts according to rows, A and B. The former is used to save auxiliary information, and the latter is used to embed AD. When hiding AD, the least significant bit (LSB) of some pixels in A and the AD form the payload data P, and the auxiliary information replaces the LSB hidden in A with bits. The adaptive embedding process for embedding AD is shown in Fig. 3. In Fig. 3, the first B part of P is first divided into 4 × 4-pixel blocks with no overlap between them. Then, P is embedded into B through the plaintext IEA designed above, and L is used to record the embedding layers of the payload data P. Then it sets L according to pixel classification, treating each type of pixel as a layer during the setting process. In the calculation of hidden AD, end is used to record the position of the last hidden load data.

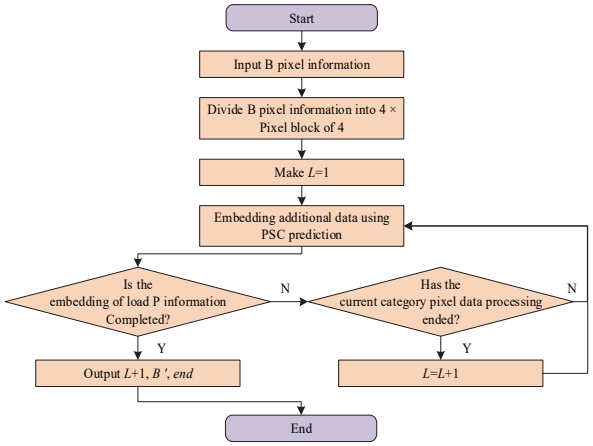

Figure 3 Adaptive embedding process

This study redesigns the overflow processing steps, and after completing adaptive information hiding, there is a possibility of pixel overflow in the area where the payload data is hidden. At this point, corresponding measures need to be taken for section B'. B' represents a B-pixel block embedded with AD. Overflowing pixels need to be restored before load data extraction, so they must be moved in consistent units. To embed multiple layers, it is necessary to determine the unit of movement on the ground of the number of embedded layers L. Since the image pixels in this study are divided into three categories, $k=L/3$ represents the number of times each type of pixel needs to be embedded, and $n=L\%3$ represents the category of pixels that have been embedded multiple times. If $n=0$, it means that the number of times each type of pixel embeds information is equal, and the overflow pixel movement m_0 is calculated according to Eq. (11).

$$m_0=k\cdot(EL+1) \tag{11}$$

If $n=1$ or $n=2$ indicates that the first or first two types of pixels are embedded with more payload data than other types, then the required movement m_{1_2} of the overflowing pixels is calculated according to Eq. (12).

$$m_{1\_2}=(k+1)\cdot(EL+1) \tag{12}$$

The recording process of the specific overflow location diagram *map* is described in Eq. (13).

$$map=\begin{cases} 0, \text{if } g<0 \\ 1, \text{if } g>255 \end{cases} \tag{13}$$

In Eq. (13), g is the encrypted image pixel containing AD. Then it performs overflow processing, as shown in Eq. (14).

$$g' = \begin{cases} g + k \cdot (EL+1), \text{if } g < 0, n = 0 \\ g + (k+1) \cdot (EL+1), \text{if} < 0, n \neq 0 \\ g - k \cdot (EL+1), \text{if } g > 255, n = 0 \\ g - (k+1) \cdot (EL+1), \text{if } g > 255, n \neq 0 \end{cases} \quad (14)$$

In Eq. (14), g' is the pixel that has been processed for overflow. After obtaining the overflow location of the *map* graph, it is compressed using arithmetic encoding. At this point, all auxiliary information for extracting load data and restoring images has been obtained. After obtaining auxiliary information, the information is hidden in the lowest LSB bit of Part *A* pixel through the bit replacement method. However, it is necessary to place the number of rows in section *A* in the top 5 bits for the receiving end to extract the payload data and obtain a complete encrypted image.

After receiving an encrypted image containing AD at the receiving end, the first step is to obtain the number of rows in the *A* part from the first 5 bits, and then divide the image into two parts: *A* and *B*. Then it extracts auxiliary information *L*, *EL*, and overflow location maps from the lowest LSB bit in the *A* section. After obtaining the overflow location map, it uses arithmetic encoding to obtain the *map*. Then, *k* and *n* are calculated using *L*, and overflow recovery is performed on the *B* part according to the positions of 0 and 1 in the *map* graph to obtain the B' part of the encrypted image that originally contained AD. The recovery process can refer to Eq. (15), where g' is the pixel with AD added and g'' is the restored pixel.

$$g'' = \begin{cases} g' + k \cdot (EL+1), \text{if } map = 0, n = 0 \\ g' - (k+1) \cdot (EL+1), \text{if } map = 0, n \neq 0 \\ g' + k \cdot (EL+1), \text{if } map = 1, n = 0 \\ g' + (k+1) \cdot (EL+1), \text{if } map = 1, n \neq 0 \end{cases} \quad (15)$$

Then it extracts the load data from the B' section. Due to the multi-layer information hiding in the image, it is necessary to start extracting the load data from the last layer when extracting information. The pixel type of the last layer can be determined by n: $n = 0$, 1, 2, and the last layer corresponds to the third, first, and second types of pixels. Then it performs load data extraction. Starting from the W layer, after each extraction of a type of pixel, *L* will decrease by 1 until *L* decreases to 0, marking the end of the load data extraction process and obtaining *B* pixel information. Especially when dealing with layer *L*, once the load data extraction is completed for *end* pixels, the extraction of that layer is considered complete.

After completing all load data extraction, the lowest LSB bit of Part *A* is obtained from the load data. Next, it uses a bit replacement method to restore the *A* part, and then combines the *A* and *B* parts to obtain the original encrypted image *E*. Then it reversely executes the encryption process of the ciphertext image designed earlier to decrypt the image. PSC can effectively utilize the correlation between pixels for prediction, improve encryption efficiency, and enhance the efficiency and concealment of data hiding. The mod256 block SE disrupts the correlation between pixels, making it difficult for attackers to extract useful information from the ciphertext. Consequently, the integration of the PSC method's data embedding efficiency with the mod256 encryption's robust security properties can be employed to enhance the overall security and resilience of the system. In summary, the overall flowchart of the image data encryption algorithm designed for this study, which combines PSC prediction and block mod256 block SE (Mod256_PSC), is shown in Fig. 4.

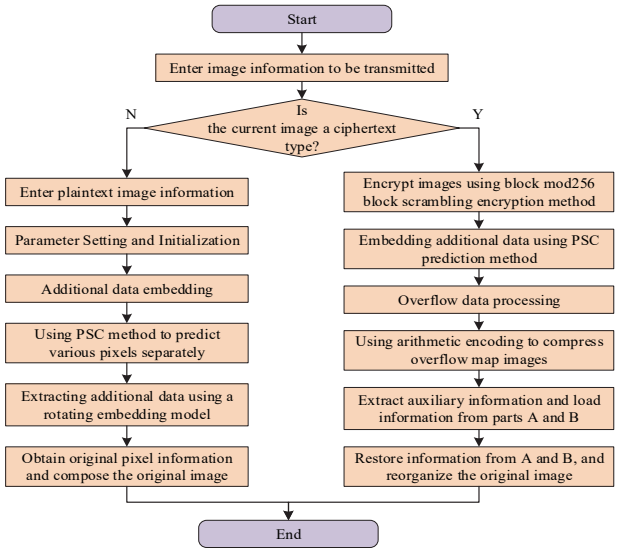

Figure 4 Image cloud computing transmission encryption algorithm based on the hybrid encryption technology

To optimize the model effect, the study uses Bayesian optimization to adjust the system parameters. The posterior distribution of the objective function is established by Gaussian process regression. Thereafter, the acquisition function is employed to balance the exploration and development and to select the next assessment point. This method has a limited number of iterations, is rapid, and can robustly identify the global optimal solution for non-convex problems. By rationally designing the neural network architecture and setting the search space of hyper-parameters, Bayesian optimization can significantly improve the performance of the model.

3.3 Mod256_PSC Model Performance Test Experimental Setup

To test the security performance, computational overhead, and decryption image quality of the cloud computing image data transmission security assurance model integrated with IEA designed for this study, a testing experiment is currently needed. For this purpose, the study selects SE, DCT, DWT, and standard AES encryption algorithms as the control group for performance comparison with Mod256-PSC. To ensure the fairness and comparability of the experiment, the IEA designed using MATLAB 2018 software deployment is used, and the algorithms are compared. The software and hardware

environment for this experiment includes Windows 10 Professional Edition, 16 GB of running memory, and Intel 7-8700 CPU. In the experiment, a dataset is constructed using Lena images, baboon images, Barbara images, and chili pepper images, as well as 1338 images from an uncompressed color image database (UCID). The first four images are shown in Fig. 5.

(a) Peppers (b) Barbara

(c) Lena (d) Baboon

Figure 5 Content of four test images

The UCID image is randomly divided into a training set and a testing set in a 7:3 ratio. These datasets contain images of various sizes and complexities to test the scalability of the algorithm. For Mod256-PSC, after multiple experiments and adjustments, the following hyper-parameter settings have been determined: number of encryption rounds, 8 rounds, key length, 256 bits, encryption block size, and 64 × 64 pixels. The prediction error ratio, graph length, AD embedding rate, peak signal-to-noise ratio (*PSNR*), prediction accuracy, computational complexity, and security score are selected as evaluation indicators. Among them, the prediction error ratio is the ratio of the absolute sum of errors to the absolute sum of all actual values. The graph length is the length of the image after encryption. The AD embedding rate is the ratio of the number of embedded bits to the total number of pixels. The formula for calculating the *PSNR* is shown in Eq. (16).

$$PSNR = 20 \times \log_{10}(\frac{Max_I}{\sqrt{MSE}}) \tag{16}$$

In Eq. (16), Max_I represents the maximum value of image point color and *MSE* represents the mean square error. The prediction accuracy is the ratio of the correctly predicted quantity to the total quantity. Computational complexity refers to the spatial resources required for algorithm operation. The security score represents the system's ability to resist attacks. Then, the scalability testing, image quality evaluation, and security testing are conducted. To evaluate the scalability of the algorithm, the study selects images of different sizes for encryption and decryption. From small icons to large high-definition images, the efficiency and stability of algorithms are observed in processing different amounts of data. During the experiment, the time required for encryption and decryption of each algorithm is recorded, and the computational complexity of each algorithm is calculated based on this. By comparison, Mod256-PSC shows advantages in computational efficiency. Finally, to evaluate the security of the algorithm, a series of security attack tests are conducted and the success rate of the attacks is recorded as the basis for security scoring.

4 RESULT

As the Mod256_PSC IEA is based on the PSC pixel prediction method, it is first necessary to determine the parameter scheme that can optimize the performance of the PSC pixel prediction method. The statistical results of the prediction error ratio of the PSC pixel prediction method in four color images are shown in Fig. 6. The horizontal and vertical axes in Fig. 6 demonstrate parameter values and prediction error ratios, respectively. The line style is used to distinguish between test images. In Fig. 6, as the parameter *EL* increases, the prediction error of the PSC prediction method for these four images shows a monotonic increasing trend compared to the data, but the growth amplitude gradually decreases. For example, for Lena images, when the parameters are 1 and 2, the corresponding prediction error ratios are 0.62 and 0.68, with an increase of 0.06. When the parameters are 7 and 8, the prediction error ratios are 0.87 and 0.88, respectively,

increasing by 0.01. This is because the error of PSC pixel prediction is concentrated around the 0 point, and the further away from the 0 point, the smaller the corresponding total error. Therefore, when the parameters are too high, the improved prediction error ratio is limited.

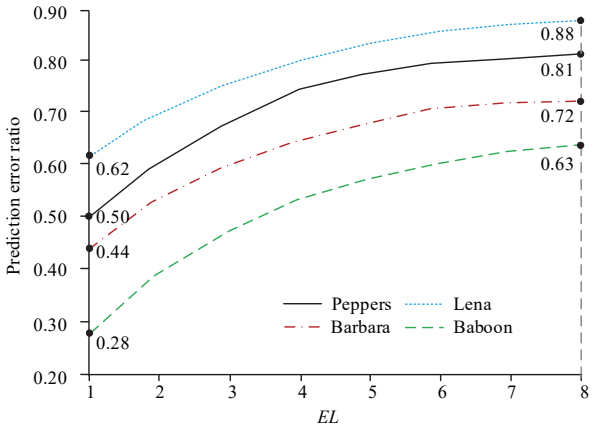

Figure 6 Prediction error ratio of PSC pixel prediction method in four color images

The maximum AD embedding rate of four images are compared under different *EL* parameter values, and the statistical outcomes are shown in Tab. 1. Tab. 1 shows that as the value of the *W* parameter increases, the maximum AD embedding rate of each image gradually decreases. For example, when the parameters are 1 and 8, the average data embedding rates of the four-color map are 1.27 and 0.59. This is because as *EL* increases, the length of the overflow location map also increases. Considering the conclusions in Fig. 6 and Tab. 1, the *EL* parameter is selected as 4 for subsequent experiments.

Table 1 Maximum AD Embedding rate of PSC pixel prediction method in four color images

EL parameter	Lena	Baboon	Barbara	Peppers	Mean value
1	1.78	0.94	0.95	1.41	1.27
2	1.71	0.81	0.92	1.27	1.18
3	1.59	0.69	0.89	1.14	1.08
4	1.43	0.53	0.82	1.08	0.97
5	1.35	0.41	0.81	0.92	0.87
6	1.23	0.30	0.78	0.78	0.77
7	1.11	0.20	0.75	0.64	0.68
8	1.02	0.11	0.73	0.51	0.59

This study tests the PSNR values of the designed PSC pixel prediction method and other common pixel prediction methods under different AD embedding rates. The statistical outcomes are shown in Fig. 7. In Fig. 7, GAN represents a generative adversarial network, LSTM represents a long short-term memory neural network, and AEPC represents an adaptive experimental pixel by pixel classification algorithm. The black solid line represents the maximum and minimum curves of the PSNR data points for each algorithm. Fig. 7 shows that regardless of the type of image data, the higher the data embedding rate, the smaller the corresponding image PSNR. However, under the same conditions, the average PSNR of the PSC prediction method designed this time is higher than that of other pixel prediction methods.

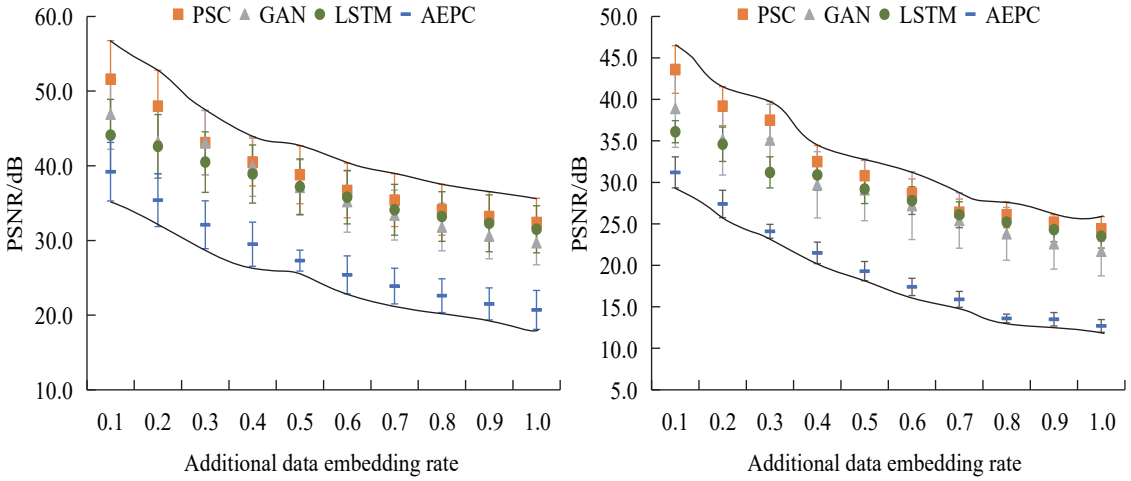

Figure 7 PSNR of each pixel prediction method under different AD embedding rates

The *map*-plot size of each pixel prediction method is compared under different data embedding rates, and the statistical outcomes are shown in Fig. 8. The meaning of the sub-graph and the horizontal axis in Fig. 8 are consistent with Fig. 7, while the vertical axis represents the corresponding size of the *map* graph. Fig. 8 shows a positive correlation between the data embedding rate and the size of the *map*-image for each pixel prediction method. Under the same conditions, the *map*-plot size of the PSC method designed this time is lower than that of the comparison method. During the process of increasing the embedding rate of AD from 0.1 to 0.9 using the PSC method, the size of the *map*-graph varies from 476 to 8054.

After comparing the decrypted image quality of various encryption and decryption algorithms, PSNR is still used as the evaluation indicator, and the statistical outcomes are shown in Fig. 9. To improve the accuracy of statistical results, each experimental scheme is repeated five times, and the curve in Fig. 9 shows the polynomial fitting line of the data. Fig. 9 shows that as the embedding rate of AD increases, the more information the image is encrypted, resulting in lower quality after decryption. For

example, for the Mod256_PSC IEA designed this time, when the AD embedding rate reaches 0.1, its mean PSNR in four independent images and the UCID dataset is 52 dB and 54 dB, respectively. However, when the data embedding rate increases to 0.7, the corresponding data decreases to 46 dB and 40 dB. Under the same AD embedding rate conditions, the Mod256_PSC IEA designed this time has the highest mean PSNR.

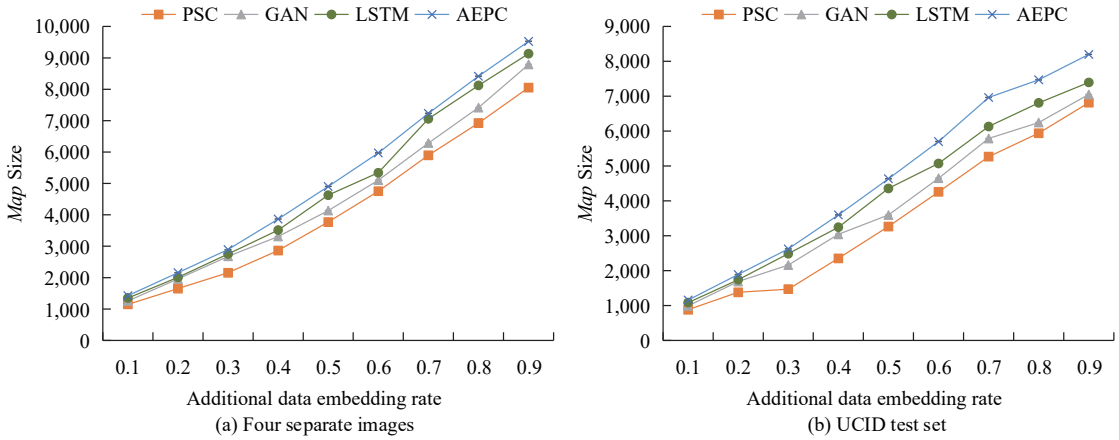

Figure 8 Size of *map* images for each pixel prediction method under different AD embedding rates

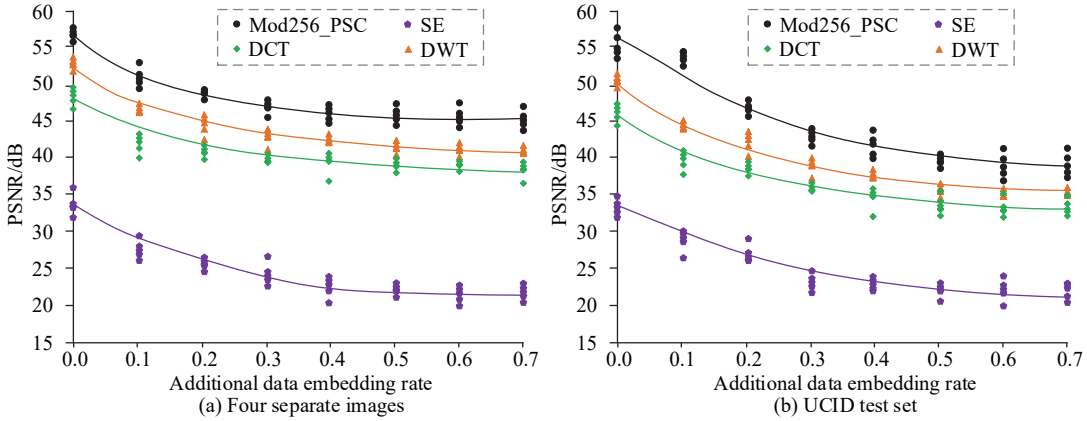

Figure 9 Decrypted image quality under different AD embedding rates

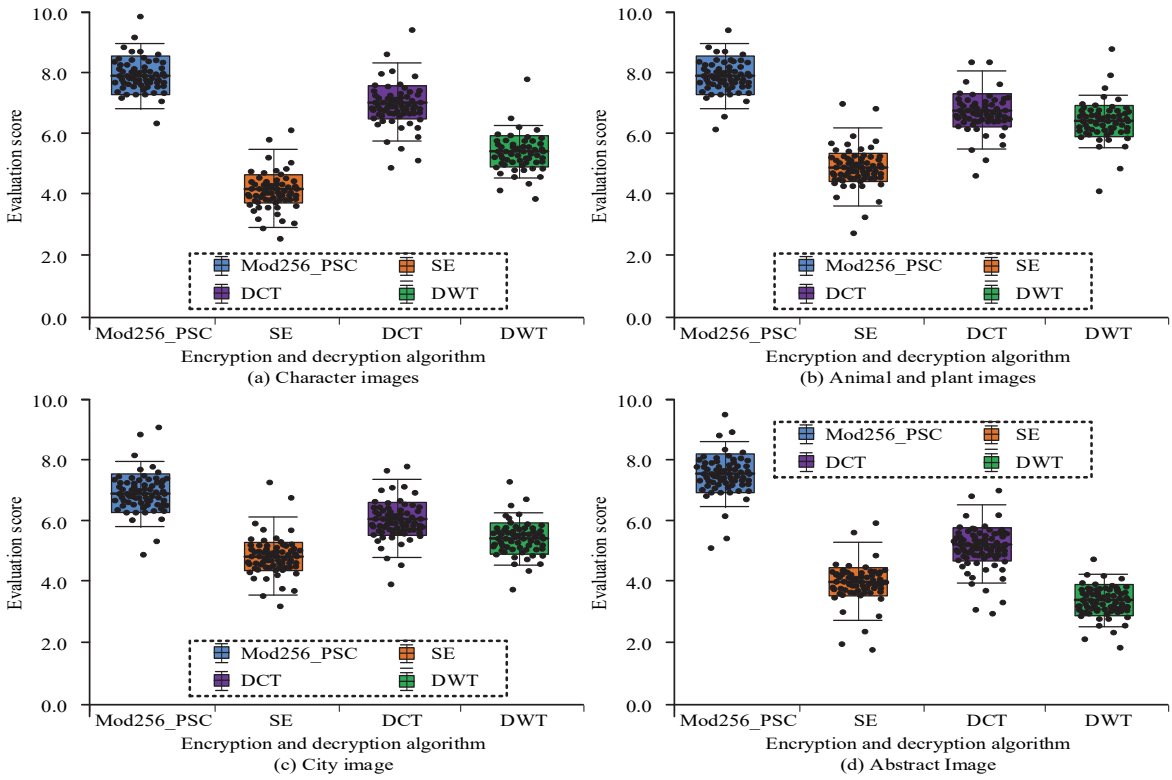

Figure 10 Security performance evaluation of image category dimension

Finally, the image data protection capabilities of various cloud computing security models are compared. To ensure reliability while reducing experimental workload, the subjective evaluation method is employed to assess the data protection capability of the algorithm, considering objective indicators such as a very low attack success rate and the need for repeated experiments. It invites 55 domestic and foreign experts in cloud computing encryption and image security to evaluate various cloud computing security models from multiple perspectives, and each evaluation is scored on a ten-point scale. These experts have doctorates in fields such as cryptography, computer security, and image processing, have extensive work experience, and hold professional certifications in related fields. The higher the score, the better the experts believe the security performance of this item is. The evaluation results of each algorithm from the image category are calculated, as shown in Fig. 10. In Fig. 10, each sub-graph represents different image types, and the vertical axis represents the expert's evaluation score. Fig. 10 shows that the median safety scores of experts in characters, animals and plants, cities, and abstract images are 7.8 points, 8.0 points, 6.9 points, and 7.6 points, respectively, which are higher than the comparison algorithm.

Next, the security evaluation results of expert members on different types of simulation attacks faced by each algorithm are compared, as shown in Tab. 2. Tab. 2 shows the average score of the expert group. Tab. 2 shows that the average score of the Mod256_PSC image encryption and decryption algorithm designed on various types of cloud computing system attacks ranges from 8.5 to 8.9 points, which is significantly higher than other comparative models. At the same time, it has been proven that Mod256-PSC has good robustness.

Table 2 Security performance evaluation of attack type dimension

Attack type	Mod256_PSC	SE	DCT	DWT
Man in the middle attack	8.6	6.4	7.1	7.9
Distributed Denial of Service Attacks	8.5	5.3	7.4	8.1
Remote File Inclusion Attack	8.7	5.9	7.2	8.2
Fragment Crushing Attack	8.6	4.8	7.8	8.0
Image grabbing attack	8.5	6.7	7.5	7.9
Image tampering attacks	8.8	7.2	7.4	8.0
Image deletion attack	8.9	5.8	7.1	8.1

Finally, to further validate the performance of the designed hybrid encryption technology, the asynchronous updating Boolean network encryption algorithm based on chaos (ABNEA) [19], fast IEA based on an improved 6-D chaotic system (FEEABICS) [20], and IEA based on 2D Lorenz and Logistic systems (IEA-TDLL) [20] were studied. The computational complexity, scalability, prediction accuracy, image quality, and security were compared. At the same time, through t-test, the *P*-value were calculated after comparing the introduced method with Mod256-PSC to verify the difference. The significance test standard was set to 0.05. If $P < 0.05$, it indicates that the difference is statistically significant, and if $P > 0.05$, it indicates that the difference is not statistically significant and comparable. The results are shown in Table 3. From Tab. 3, the *P*-values after *t*-test using the introduced method and Mod256-PSC were both less than 0.05, indicating that the difference between the two groups was statistically significant. The computational complexity of the designed Mod256-PSC was 3.2 × 106OP/s, which was lower than the other three algorithms. The scalability, prediction accuracy, and image quality were 90%, 93.5%, and 42.8, respectively, which were significantly higher than other algorithms. The success rate of the attack was 2.1%, which was 3.2%, 1.6%, and 4.4% lower than ABNEA, FEEABICS, and IEA-TDLL, respectively. The above results proved that the comprehensive performance of Mod256-PSC was good.

Table 3 Comprehensive performance evaluation of different algorithms

Algorithm / Metrics	Computational complexity (OP/s)	Scalability / %	Prediction accuracy / %	Image Quality (PSNR)	Attack success rate / %	*P*
Mod256_PSC	3.2×10^6	90	93.5	42.8	2.1	/
ABNEA	4.5×10^6	75	89.0	39.5	5.3	< 0.05
FEEABICS	3.8×10^6	80	91.2	41.0	3.7	< 0.05
IEA-TDLL	5.1×10^6	70	87.6	38.2	6.5	< 0.05

5 DISCUSSION

In this study, an encryption and decryption algorithm for cloud computing image data transmission is developed based on hybrid encryption technology, combined with the PSC prediction method and mod256 block SE technology [20]. The algorithm aims to improve the security performance of image transmission in cloud computing environments. The original intention of this study is to address the issues of low efficiency and inconvenient key management in traditional image encryption techniques for secure image transmission in cloud computing systems, while ensuring a balance between encryption depth and transmission efficiency.

Through in-depth analysis of the experimental results, it can be concluded that the essence and significance of this study lie in the following two points: The first point is that the PSC method can fully utilize the characteristics of the image itself for pixel prediction, effectively reducing distortion after embedding AD [21, 22]. The second point is that the mod256 block SE method enhances the reversibility and complexity of the algorithm and improves its anti-attack ability. The combination of these two enables the algorithm designed in this study to ensure image quality while greatly improving security and stability, meeting the current security requirements for cloud computing data transmission. The above conclusion can be drawn from the fact that the average score of the image encryption and decryption algorithm designed in this study on various types of cloud computing system attacks ranges from 8.5 to 8.9 points, which is significantly

higher than other comparative encryption and decryption algorithms.

Compared to previous research results, the algorithm designed in this study achieved significant improvements in PSNR and image security rating. Especially in areas such as image deletion attacks and image tampering attacks, Mod256_PSC has demonstrated superior defense capabilities. The average scores of the designed algorithm on image deletion attacks and image tampering attacks were 8.9 and 8.8, respectively, which were higher than other comparison algorithms. The research results of Mansouri A et al. showed that their designed encryption algorithm had a poor ability to cope with image tampering attacks, which was related to the computational structure of their designed algorithm [23]. The achievement of these results can be attributed to two key factors: the efficient pixel classification and prediction ability of the PSC prediction method, and the innovative application of the mod256 block scrambling method. In addition, compared to the previous research, the design method significantly enhances the stability of the model while ensuring the image quality, which highlights the new breakthrough in the study of image encryption.

The main reason for the good performance of the research results is that the design of the PSC prediction method fully utilizes the inherent correlation of images, while the mod256 block SE method introduces more uncertainty while ensuring the reversibility of the algorithm, enhancing the anti-attack ability.

At the same time, although the paper mainly focuses on the encrypted transmission of image data in cloud computing environment, Mod256_PSC has certain universality. The hybrid encryption technique employed in the study integrates predictive methods and block scrambling techniques, enabling both approaches to be effective in addressing diverse data types. Among them, the prediction approach is capable of leveraging the intrinsic properties of the data and enhancing the encryption efficiency. Conversely, the block scrambling technology serves to enhance the reversibility and anti-attack capability of the algorithm. Therefore, the results of this study can not only be used in the encryption transmission of image data, but also have potential application prospects in other types of data and applications.

However, there are also some limitations to this study. Firstly, although the proposed algorithm has shown excellent performance in experiments, its complexity is high and may not be suitable for applications with high real-time requirements [24]. Secondly, the testing in this study is mainly based on theoretical models and simulation experiments, which may differ from the complex situations in real cloud computing environments. The actual application effect still needs further verification.

Overall, the image encryption and decryption algorithm proposed in this study not only has theoretical innovation, but also the experimental results support its practicality and effectiveness. In the cloud computing environment, by combining PSC prediction method and mod256 block SE technology, the designed algorithm can effectively solve the problems of low image transmission efficiency and inconvenient key management of traditional image encryption technology, which has important practical significance and potential application. The designed algorithm adopts hybrid encryption technology, which can effectively improve the encryption efficiency when processing large-scale image data sets, and reduce the computing cost effectively while having good scalability. Future work will focus on further optimizing the real-time processing capability of algorithms and conducting testing and verification on real cloud computing platforms. At the same time, it is also necessary to consider extending this algorithm to other types of data encryption transmission testing to meet a wider range of security needs. Future work will focus on extending the designed algorithm to other data types for encrypted transmission testing to meet broader information security needs.

6 CONCLUSION

This paper proposed a novel hybrid encryption algorithm for secure image transmission in cloud computing environments. The algorithm integrated PSC prediction and block mod256 SE to enhance the security and efficiency of image encryption. Experimental results on various image datasets demonstrated the superiority of the proposed method in terms of PSNR, image quality, and security performance compared to existing methods. The proposed algorithm achieved a good balance between security and efficiency, making it a promising solution for secure image transmission in cloud computing. Expert evaluations further validated the effectiveness of the proposed method in defending against various types of attacks in cloud computing systems. The main contributions of this study lie in the innovative integration of PSC and block mod256 SE, as well as the comprehensive evaluation of the proposed algorithm's performance against state-of-the-art methods. However, the algorithm's real-time processing capability and performance in real-world cloud computing scenarios need further investigation. Future research should focus on optimizing the computational efficiency of the algorithm, integrating it with other security mechanisms, and extending its application to other data types. The proposed hybrid encryption algorithm has the potential to promote the adoption and trustworthiness of cloud computing services by providing a robust and efficient solution for secure data transmission.

7 REFERENCES

[1] Daoui, A., Karmouni, H., Ogri, O. E., Sayyouri, M., & Qjidaa, H. (2022). Robust image encryption and zero-watermarking scheme using SCA and modified logistic map. *Expert Systems with Applications*, *190*(Mar), 116193.1-116193.26. https://doi.org/10.1016/j.eswa.2021.116193

[2] Hu, W. & Dong, Y. (2022). Quantum color image encryption based on a novel 3D chaotic system. *Journal of Applied Physics*, *131*(11), 114402.1-114402.13.

[3] Sang, Y., Sang, J., & Alam, M. S. (2022). Image encryption based on logistic chaotic systems and deep autoencoder. *Pattern Recognition Letters*, *153*(Jan), 59-66. https://doi.org/10.1016/j.patrec.2021.11.025

[4] Erkan, U., Toktas, A., Toktas, F., & Alenez, F. (2022). 2D eπ-map for image encryption. *Information Sciences*, *589*(5560), 770-789. https://doi.org/10.1016/j.ins.2021.12.126

[5] Xingyuan, W., Cheng, L., & Donghua, J. (2021). A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT. *Information Sciences*, *574*(1), 505-527. https://doi.org/10.1016/j.ins.2021.06.032

[6] Wang, X., Yang, J., & Guan, N. (2021). High-sensitivity image encryption algorithm with random cross diffusion based on dynamically random coupled map lattice model. *Chaos Solitons & Fractals*, *143*(5), 110582.1-110582.19. https://doi.org/10.1016/j.chaos.2020.110582

[7] Yang, Z., Liang, D., Ding, D., & Hu, Y. B. (2021). Dynamic behavior of fractional-order memristive time-delay system and image encryption application. *Modern Physics Letters B*, *35*(16), 2150271.1-2150271.22. https://doi.org/10.1142/S0217984921502717

[8] Zhang, F., Zhang, X., Cao, M., Ma, F., & Li, Z. (2021). Characteristic Analysis of 2D Lag-Complex Logistic Map and Its Application in Image Encryption. *IEEE Multimedia*, *28*(4), 96-106. https://doi.org/10.1109/MMUL.2021.3080579

[9] Zhang, Q., Han, J., & Ye, Y. (2021). Multi-image encryption algorithm based on image hash, bit-plane decomposition and dynamic DNA coding. *IET Image Processing*, *15*(4), 885-896.

[10] Wang, X. & Gao, S. (2020). Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network. *Information Sciences*, *539*(9), 195-214. https://doi.org/10.1016/j.ins.2020.06.030

[11] Budati, A. K., Snv, G., Cherukupalli, K., Kumar, A. P., & Moorthy, V. K. (2021). High speed data encryption technique with optimized memory based RSA algorithm for communications. *Circuit World*, *47*(3), 269-273. https://doi.org/10.1108/CW-10-2020-0282

[12] Xu, L. & Zhang, J. (2022). A Novel four-Wing chaotic system with multiple attractors based on hyperbolic sine: Application to image encryption. *Integration*, *32*(13), 313-331. https://doi.org/10.1142/S0218127422501917

[13] Hafsa, A., Gafsi, M., Malek, J., & Machhout, M. (2021). FPGA Implementation of Improved Security Approach for Medical Image Encryption and Decryption. *Scientific Programming*, *2021*(Pt.1), 6610655.1-6610655.20. https://doi.org/10.1155/2021/6610655

[14] Kanwal, S., Inam, S., Cheikhrouhou, O., Kinza, M., Atef, Z., & Habib, H. (2021). Analytic Study of a Novel Color Image Encryption Method Based on the Chaos System and Color Codes. *Complexity*, *2021*(Pt.19), 5499538.1-5499538.19. https://doi.org/10.1155/2021/5499538

[15] Gupta, M. D. & Chauhan, R. K. (2021). Secure image encryption scheme using 4D-Hyperchaotic systems based reconfigurable pseudo-random number generator and S-Box. *Integration*, *81*(Nov), 137-159. https://doi.org/10.1016/j.vlsi.2021.07.002

[16] Li, Z., Peng, C., Tan, W., & Li, L. (2021). An Effective Chaos-Based Image Encryption Scheme Using Imitating Jigsaw Method. *Complexity*, *2021*(Pt.6), 8824915.1-8824915.18. https://doi.org/10.1155/2021/8824915

[17] Mansouri, A. & Wang, X. (2021). A novel one-dimensional chaotic map generator and its application in a new index representation-based image encryption scheme. I*nformation Sciences*, *563*(8), 91-110. https://doi.org/10.1016/j.ins.2021.02.022

[18] Hidayat, I., Ali, M., & Arshad, A. (2022). Machine Learning-Based Intrusion Detection System: An Experimental Comparison. *Journal of Computational and Cognitive Engineering*, *2*(2), 88-97.

[19] Gao, S. (2023). Asynchronous Updating Boolean Network Encryption Algorithm. *IEEE Transactions on Circuits and Systems for Video Technology*, *33*(8), 4388-4400. https://doi.org/10.1109/TCSVT.2023.3237136

[20] Chen, H., Bai, E., Jiang, X., & Wu, Y. (2022). A Fast Image Encryption Algorithm Based on Improved 6-D Hyper-Chaotic System. *IEEE Access*, *10*, 116031-116044. https://doi.org/10.1109/ACCESS.2022.3218668

[21] Li, T., Du, B., & Liang, X. (2020). Image Encryption Algorithm Based on Logistic and Two-Dimensional Lorenz. *IEEE Access*, *8*, 13792-13805. https://doi.org/10.1109/ACCESS.2020.2966264

[22] Zheng, B., Qiu, Z., & Yang, J. (2022). A Novel Fingerprint Encryption Based on Image and Feature Mosaic. *Tehnički vjesnik*, *29*(6), 1914-1922. https://doi.org/10.17559/TV-20220302094719

[23] Yu, G., Zhao, Y., Cui, Z., & Zuo, Y. (2021). A QPSO Algorithm Based on Hierarchical Weight and Its Application in Cloud Computing Task Scheduling. *Computer Science and Information Systems*, *18*(1), 189-212. https://doi.org/10.2298/CSIS200223033Y

[24] Arul Jothi, S. & Venkatesan, R. (2023). A Deep Learning Approach for Efficient Anomaly Detection in WSNs. International Journal of Computers Communications & Control, *18*(1), 1-30. https://doi.org/10.15837/ijccc.2023.1.4756

Contact information:

Jinming YUAN
(Corresponding author)
Department of information engineering,
Jincheng Institute of Technology,
Jincheng, Shanxi, 048026, China
E-mail: yjm230714@163.com