A New Thumbnail Preserving Encryption Scheme

Jie Zhang*
School of Software, Henan University
104754201738@henu.edu.cn

Zhihua Gan
School of Software, Henan University
gzh@henu.edu.cn

Yang Yang
School of Software, Henan University
zhangjie567@henu.edu.cn

Wenbin Jiang
School of Software, Henan University
972759079@qq.com

Xin He
School of Software, Henan University
hx_henu@126.com

Xiuli Chai
School of Artificial Intelligence, Henan University
chaixiuli@henu.edu.cn

ABSTRACT

Cloud services can store a large number of images, but cannot protect the security of user privacy. The traditional image encryption scheme improves the privacy security, but reduces the visibility of the image, which makes the image invisible in the cloud service. To maintain both cloud storage security and visual usability, Tajik et al. proposed a thumbnail preserving encryption (TPE) scheme so that the encrypted image is presented as a low-resolution version of the plaintext image. However, this scheme only scrambles and replaces pixels, and has low security. Aiming at the problem of low security of this method, this paper proposes a new thumbnail preserving encryption scheme (New-TPE). The plaintext image information is used as part of the key to construct the correlation between the encryption process and the plaintext image; The optimal random value is selected from multiple random values and is added to the pixel value replacement process, which increases the degree of variation of pixel values before and after the replacement and reduces the correlation between adjacent pixels; The simulated annealing idea is introduced to select the optimal scrambling sequence within the range; A displacement function scrambling method is proposed to reduce the correlation between adjacent pixels. The experimental results show that the proposed scheme has higher security and a better balance between image privacy and security.

CCS CONCEPTS

• **Security and privacy**; • **Database and storage security**; • **Data anonymization and sanitization**;

KEYWORDS

Thumbnail preserving encryption (TPE), Image privacy, Usability, Cloud storage security, Image encryption

*Corresponding author

ICAIP 2022, November 18–20, 2022, Zhanjiang, China

ACM ISBN 978-1-4503-9715-5/22/11…$15.00
https://doi.org/10.1145/3577117.3577145

ACM Reference Format:
Jie Zhang, Zhihua Gan, Yang Yang, Wenbin Jiang, Xin He, and Xiuli Chai. 2022. A New Thumbnail Preserving Encryption Scheme. In *2022 6th International Conference on Advances in Image Processing (ICAIP 2022), November 18–20, 2022, Zhanjiang, China.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3577117.3577145

1 INTRODUCTION

In the current Internet era, people use electronic devices to generate a large number of images every day and upload them to cloud services [1-2]. Although cloud services bring us convenience, it is difficult to guarantee the security of user information. Mainstream cloud service providers such as Facebook and iCloud have experienced user privacy photo leakage or unauthorized abuse of user images, which proves that we must find some ways to improve the security of personal privacy. Some scholars suggest using traditional encryption schemes to encrypt images [3-6], so as to ensure the security of personal privacy. However, traditional encryption methods make the ciphertext image noise-like. When uploaded to the cloud service, it will lose visual availability.

In order to solve these problems, some scholars proposed encryption schemes which can keep the thumbnail unchanged. The ciphertext images generated by these schemes protect personal privacy while retaining some information of the original image. Users can identify the plaintext images they need through ciphertext images similar to low-quality plaintext images [7]. For example, Wright et al. proposed an thumbnail preserving encryption (TPE) [8]. In this scheme, the image was divided into blocks and scrambled in each block to achieve the encryption effect. However, since only the position of the pixel value is changed before and after the encryption operation, and the pixel value is not changed, the security of the encryption scheme is not high, and it cannot resist the known-plaintext attack (KPA) and chosen-plaintext attack (CPA). In 2017, Marohn et al. proposed an approximate TPE [9]. In this scheme, two encryption methods are proposed, which are the least significant bit (LSB) and dynamic range preserving encryption (DRPE). LSB scheme uses stream cipher encryption to change the pixel value of the image. The encrypted image is similar to the thumbnail of the plain image, but is not completely consistent and cannot be decrypted losslessly. In the DRPE scheme, the plaintext image is first partitioned, and then the pixel values are replaced according to the maximum and minimum pixel values in each block. The scheme also cannot completely preserve the thumbnail of the plain image, and there is a possibility of decryption failure. Later, Zhang

et al. proposed a high-fidelity thumbnail preserving ecryption (HF-TPE) [10]. Compared with Marohn's scheme, HF-TPE improves the availability of ciphertext, but reduces the security of ciphertext image. In 2019, Tajik et al. proposed an ideal thumbnail preserving encryption (Ideal-TPE) [11]. However, there is no relationship between the encryption key and the plaintext image, which cannot resist CPA and KPA. Moreover, only simple pixel value replacement and scrambling are performed on the image, and the security of the ciphertext image is difficult to guarantee. Besides, Zhao et al. proposed a three-pixel thumbnail preserving encryption (3px-TPE) [12], which improves the encryption performance in each iteration, but the encryption time is a little long and the overall efficiency is low.

Inspired by the above studies, this paper proposes a new thumbnail preserving encryption scheme (New-TPE). The main contributions of this scheme are as follows:

(1) A New-TPE is proposed. The scheme can make the thumbnail of the encrypted image consistent with the thumbnail of the plaintext image.
(2) The length, width and average pixel value of the plaintext image are used as part of the key to encrypt the image. The association between plaintext image and encryption process is constructed.
(3) Random values need to be added in the process of changing the pixel values, so we propose a method to select the desired random values.
(4) The displacement function is proposed for the dislocation process.

The remainder of this article is as follows. Section 2 introduces the related theoretical knowledge, including Logistic chaotic map, Chen chaotic system, pixel value replacement algorithm and simulated annealing arithmetic. Section 3 describes the process of encryption algorithm and decryption algorithm. The experimental results are analyzed in Section 4. Section 5 is the conclusion, which further summarizes the work of this paper.

2 PRELIMINARIES

2.1 Logistic chaotic map and Chen chaotic system

Since one-dimensional Logistic chaotic map and three-dimensional Chen chaotic system have good random effects [13], they are very suitable for image encryption algorithm. Logistic chaotic map is a relatively simple nonlinear system, also known as the insect population model and expressed by Eq. (1), where the parameter u is the control parameter. When $3.569945627 \leq u \leq 4$, the system is in a chaotic state.

$$w_{n+1} = uw_n(1 - w_n). \tag{1}$$

Chen chaotic system is expressed by Eq. (2). When the control parameters $a = 35,\ b = 8\ /\ 3,\ c = 28$, the chaotic system will be in a chaotic state, and the chaotic sequence with good effect can be generated.

$$\begin{cases} x_{n+1} = -ax_n + ay_n, \\ y_{n+1} = (c - a)x_n + cy_n - x_n z_n, \\ z_{n+1} = x_n y_n - bz_n. \end{cases} \tag{2}$$

2.2 Pixel value replacement algorithm

Tajik et al. proposed a pixel value replacement algorithm that keeps the sum unchanged [11]. Each replacement is operated with two pixels as a group. For example, when replacing pixels in the encryption process, the operation is performed by the following Eq. (3)[11],

$$\begin{cases} a' = \mathrm{mod}((a + r), (sum + 1)), (sum \leq 255) \\ a' = 255 - \mathrm{mod}((a + r), (511 - sum)), (sum > 255) \\ b' = sum - a'. \end{cases} \tag{3}$$

where a and b are the original pixel values, a' and b' are the replaced pixel values, sum is the sum of a and b, r is the random value, $\mathrm{mod}(m, s)$ is the modular operation, and the sum of pixel values remains unchanged before and after the operation.

2.3 Simulated annealing arithmetic

Metropolis et al. proposed the idea of simulated annealing (SA) [14], which is a probabilistic algorithm. The operation process of the SA algorithm is as follows:

Firstly, generate a new solution using the generate function, and this new solution should be in the range of solution space. Secondly, calculate the difference of the objective function between the new solution and the current solution. Thirdly, judge whether to use new solutions. Finally, after judgment, decide whether to use the new solution instead of the current solution, and the first iteration process is over. In this way, complete multiple rounds of judgment, and ultimately select the optimal solution within the scope.

3 THE PROPOSED ENCRYPTION ALGORITHM AND DECRYPTION ALGORITHM

3.1 Encryption algorithm

The detailed steps for image encryption are shown below.

Step 1: Pre-processing.

Suppose the image size of the original image is $M \times N$, and the original image is chunked with each chunk of size $b \times b$ ($b < N$ and $b < M$), and each chunk is encrypted separately using the subsequent steps.

The initial value of the chaotic sequence is generated using the SHA 256 function. A 256-bit hash string is produced after inputting a random length information to it, and it is an irreversible string transformation. The password plus the length, width and pixel average of the plaintext image are used as input to the SHA256 function, and the resulting 256-bit key H is divided into 64 sub keys, each with a length of 4 bits, and represented as $H = h_0, h_1, h_2, h_3 \cdot \cdot\cdot, h_{63}$. Then define the parameter x', y', z', w'. $x' = 1,\ y' = 2,\ z' = 3,\ w' = 4$ is set in this algorithm and x_1, y_1, z_1, w_1can be calculated by Eq. (4).

$$\begin{cases} x_1 = x' + (h_0 \oplus \cdots \oplus h_{15})/256, \\ y_1 = y' + (h_{16} \oplus \cdots \oplus h_{31})/256, \\ z_1 = z' + (h_{32} \oplus \cdots \oplus h_{47})/256, \\ w_1 = \mathrm{mod}(w' + (h_{48} \oplus \cdots \oplus h_{63})/256, 1). \end{cases} \tag{4}$$

The above obtained x_1, y_1, z_1 are substituted into Chen chaotic system as the initial values, and w_1 is inputted into the Logistic map as the initial value. After iterating them $M \times N \times 3 \times 5 + 1000$ times, the first 1000 elements are discarded to obtain four groups of chaotic

sequences $x(i), y(i), z(i), w(i)$ with length of $(M \times N \times 15)$.Then the above obtained chaotic sequence is quantized using Eq. (5).

$$\begin{cases} X(i) = F(\mathrm{mod}(x(i) \times 10^{14}, M \times N)) + 1, \\ Y(i) = F(\mathrm{mod}(y(i) \times 10^{14}, M \times N)) + 1, \\ Z(i) = F(\mathrm{mod}(z(i) \times 10^{14}, M \times N)) + 1, \\ W(i) = F(\mathrm{mod}(w(i) \times 10^{14}, M \times N)) + 1. \end{cases} \tag{5}$$

where $F(u)$ is the $floor(u)$ function, and the nearest integer that is less than or equal to u can be returned.

According to Eq. (6), the two different sequences are subtracted to obtain the random sequences L_1, L_2, L_3, andL_4.

$$\begin{cases} L_1(i) = X(i) - Y(i), \\ L_2(i) = Y(i) - Z(i), \\ L_3(i) = Z(i) - W(i), \\ L_4(i) = W(i) - X(i). \end{cases} \tag{6}$$

Step 2: Change pixel value while keeping the sum of the pixel values unchanged

The color plaintext image is divided into three channels R, G, and B, and the pixel values of $b \times b$-sized blocks in each channel are replaced. In the replacement process, two-pixel values are selected in turn, and the pixel values are replaced by Eq. (3).

When replacing, an array with length n is selected from the random sequence, and then the number closest to the average of the sum of the two-pixel values is selected from the array as the random number, then use this random number and pixel value for the following operation.

Step 3: Pixel position scrambling operation based on SA

The function of scrambling operation is to change the position of pixels. Therefore, based on the idea of SA, the following processes are established in this subsection.

1) Setting the objective function. The objective function is to calculate the number of pixels whose positions are moved before and after scrambling.
2) Setting the displacement function. The displacement function refers to using three random sequences to move the position of three pixels in the scrambling process. For example, the sequence that needs to be scrambled is ' 123456789 ', the first random sequence is ' 762134851 ', the second random sequence is ' 651349732 ', and the third random sequence is ' 495138921 '. When the first scrambling is carried out, the first element ' 7 ' of the first random sequence, the first element ' 6 ' of the second random sequence, and the first element ' 4 ' of the third random sequence are selected as the exchange targets. The seventh element in the scrambling sequence is moved to the sixth position, the sixth element is moved to the fourth position, and the fourth element is moved to the seventh position. The new sequence ' 123657489 ' is obtained. In this way, the subsequent scrambling is completed.
3) Setting the decision function. The decision function is used to determine whether to use new solutions instead of the current solution. If the new solution is superior to the current solution, that is, when the objective function of the new solution is greater than that of the current solution, the new solution is used to replace the current solution. If the objective function of the new solution is less than or equal to the objective function of the current solution, *Pr* and Pt are calculated according to Eq. (7), and when *Pr* is greater than *Pt*, the new solution is used instead of the current solution, otherwise the current solution is still used.

$$\begin{cases} Pr = \exp(-dE/L) \\ Pt = \exp(-1/L) \end{cases} \tag{7}$$

where dE is the difference between the objective function of the sequence before and after scrambling. L is the length of generating chaotic sequence, and the length of L increases with the number of iterations in the iteration process.

In this algorithm, L_1, L_2, and L_3 are used to scramble the R channel, L_2, L_3, and L_4 are used to shuffle the G channel, and L_3, L_4, and L_1 are used to scramble the B channel. The decision function is used to determine whether the conditions are met, and Steps 2 and 3 are executed many times. The end condition is that the objective function reaches the maximum value $(M \times N \times 3)$, or the cycle of executing Steps 2 and 3 reach 100 times.

After performing the above steps, image encryption process is completed.

3.2 Decryption algorithm

Step 1: Using the same key as the encryption process, the same random sequence is obtained after preprocessing.

Step 2: The inverse of the scrambling operation is performed on the ciphertext image to recover the pixel positions.

Step 3: The inverse operation of the pixel value replacement operation is performed on the ciphertext image whose pixel positions have been recovered, so that the ciphertext image is recovered to the plaintext image.

The image decryption process is completed.

4 EXPERIMENTAL RESULT ANALYSIS

This section takes the Lena image with resolution of 512×512 as an example for experimental analysis. Experimental simulation platform is as: CPU: AMD Ryzen 74800H with Radeon Graphics, 2.90 GHz; Operating system: Windows 10; Programming tool: Matlab2016a.

4.1 Analysis of encryption effect

The experiments in this section focus on analyzing the thumbnails of ciphertext images with different chunk sizes. In Fig. 1, (a) is the plaintext image and (b) to (i) are ciphertext images with chunk sizes of 4, 8, 16, 32, 64, 128, 256, and 512. From Fig. 1, we can see that as the chunk size becomes larger, the ability of the ciphertext image to hide information becomes stronger, while the visual usability of the ciphertext image becomes lower. When the chunking is very small, the ciphertext image is very close to the plaintext image and exposes too much information, so the visual usability is higher, but the security is lower. When the chunk size is the same as the plaintext image size, both the ciphertext image and the traditional encrypted image present a noise-like image, and the ciphertext image is more secure, but less practical. Users can select the block size for the encrypted image before uploading it to the cloud to balance the privacy and security of the encrypted image.

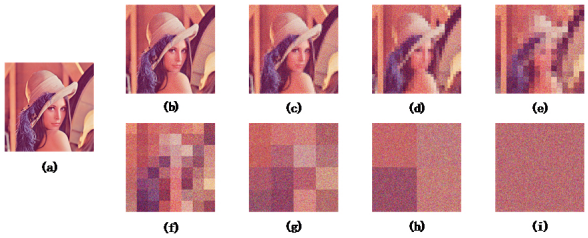

Figure 1: Lena ciphertext images

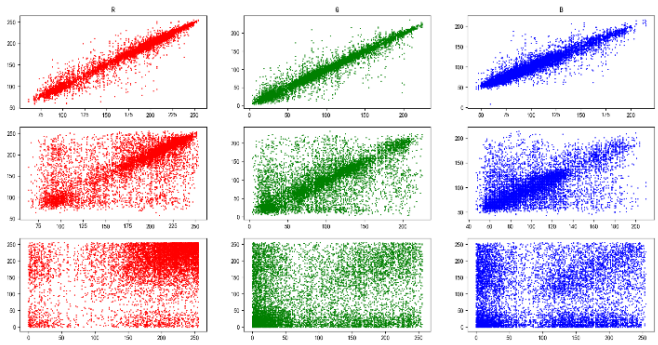

Figure 2: Correlation analysis of adjacent pixels

4.2 Analysis of peak signal-to-noise ratio

Peak signal-to-noise ratio (PSNR) is an objective standard to measure image distortion and noise level. The smaller the PSNR value of the ciphertext image compared with the plaintext image, the greater the distortion of the ciphertext image, the greater the gap between the ciphertext image and the plaintext image, and the better the encryption effect of the ciphertext image. In this section, we first analyze the PSNR of ciphertext image and plaintext image under different block sizes, and where LSB (i) represents the inversion pixel bit i in the algorithm.

The PSNR values of ciphertext images and plaintext images obtained by different algorithms are shown in Table 1, where the bold numbers represent the optimal PSNR values obtained by different algorithms for the same chunk size. As the chunk size becomes larger, the PSNR value of the ciphertext image tends to decrease, which means the difference between the ciphertext image and the plaintext image tends to become larger. When comparing TPE, HF-TPE, LSB(1), LSB(2), LSB(3) and Ideal-TPE under different chunk sizes, the PSRN of New-TPE ciphertext image is the smallest, which represents the largest gap between the obtained ciphertext image and the plaintext image. The PSRN value of DRPE cipher image is 29.3734 dB when the chunk size is 64×64, the PSNR value of New-TPE cipher image is slightly larger than the result of DRPE. The PSNR values of New-TPE ciphertext images at other chunk sizes are smaller than the results of DRPE. In summary, the security of cipher image obtained by New-TPE algorithm is better than TPE, HF-TPE, LSB(1), LSB(2), LSB(3) and Ideal-TPE, and better than DRPE in some chunk sizes, so the cipher image has higher security.

4.3 Analysis of correlation analysis between adjacent pixels

Adjacent pixel correlation analysis refers to the analysis of two or more correlated elements to measure the correlation between adjacent pixels [15]. There is a high correlation between adjacent pixels in the image. Usually, the size of the adjacent pixel value can be derived from a pixel value. The process from plaintext image to ciphertext image is to break the correlation to defend statistical attacks. Therefore, the lower the correlation between adjacent pixels is, the higher the security of ciphertext image is.

Fig. 2 gives the neighboring pixel correlation graphs of Lean plaintext image and ciphertext image with different encryption schemes when the chunk size is 32. Each row from top to bottom shows the adjacent pixel correlation maps for the original, TPE encryption scheme [8] and New-TPE encryption scheme, respectively. From the figure, it can be seen that there is a strong correlation between the neighboring pixels of the plaintext image. Compared with the TPE algorithm, the pixel distribution in the adjacent pixel correlation analysis graph of the ciphertext image obtained by the New-TPE algorithm is more uniform, so the anti-attack performance of the New-TPE algorithm is higher than that of the [8].

4.4 Analysis of information entropy

Information entropy is a measure of the random degree of the signal source, which can be used to measure the randomness of the ciphertext image. The measurement method calculates the change

Table 1: PSNR values between ciphertext image and plaintext image (unit: dB)

Scheme	Block size			
	8×8	16×16	32×32	64×64
TPE [8]	63.0723	55.4116	49.4038	43.5887
HF-TPE [10]	36.6960	35.3735	33.6757	31.4485
DRPE [9]	51.5384	42.1398	34.2109	29.3734
LSB(1) [9]	36.8869	36.0038	34.9894	33.7939
LSB(2) [9]	38.3148	37.2580	35.8805	34.1565
LSB(3) [9]	38.2979	37.2621	35.9019	34.1366
Ideal-TPE [11]	36.4060	35.3179	34.0939	32.4155
New-TPE	35.6244	34.2794	32.7255	30.5980

Table 2: Information entropy analysis results

Schemes	Block size				
	8×8	16×16	32×32	64×64	128×128
TPE[8]	7.7500	7.7500	7.7500	7.7500	7.7500
HF-TPE[10]	7.7651	7.7651	7.7651	7.7651	7.7651
DRPE[9]	7.7497	7.6786	7.5047	7.3434	7.3007
Ideal-TPE[11]	7.9156	7.9243	7.9373	7.9556	7.9698
New-TPE	7.8172	7.8179	7.8173	7.8176	7.817

degree of each gray level pixel in each color channel. If the pixel distribution is more uniform, the ciphertext image is more resistant to statistical attacks. In general, the more regular the system, the more information the ciphertext image leaks and the smaller its information entropy. On the contrary, the higher the security of ciphertext image, the greater its information entropy. The ideal value of information entropy of three-channel color image is 8. When the information entropy is closer to the ideal value, the pixel distribution of ciphertext image is more uniform, and the security of ciphertext image is higher. We use the calculation method in [16] to calculate the information entropy.

It can be seen from Table 2 that the ciphertext image information entropy of New-TPE scheme is the maximum compared with TPE, HF-TPE, and DRPE schemes under different block sizes. Compared with Ideal-TPE scheme, ciphertext image information entropy gotten by New-TPE scheme is slightly lower, but the difference is not big. In summary, the ciphertext image of New-TPE scheme is evenly distributed, has high security, and can effectively resist statistical attacks.

4.5 Analysis of execution time

In this section, we use the Lena image with a size of 512×512 as the original image The original Lena images were made into thumbnails of sizes 4, 8, 16, 32, 64, 128, 256 and 512, and the encryption times of these images were analyzed using different encryption algorithms. As shown in Fig. 3, where New-TPE is the algorithm of this paper, 1 round was iterated during the test. Ideal-TPE [11] is the algorithm proposed by Tajik et al. Since there is a selection process with 100 cycles in the algorithm of this paper, the algorithm was iterated for 100 rounds during the testing process. 3px -TPE [12] is the algorithm proposed by Zhao et al, in which the test is iterated for 1 round.

As can be seen from Fig. 3, the encryption time is longer when the image size increases. The 3px-TPE algorithm has a time complexity of $O(ns^3)$, where n represents the number of image elements, s represents the number of images containing encryption units, and the encryption units are in groups of three pixels, so the encryption time increases sharply as the plaintext image gets larger. The encryption times of Ideal-TPE algorithm and New-TPE algorithm are close for image sizes of 4×4, 8×8, 16×16 and 32×32. When the image size is 128×128, 256×256 and 512×512, the encryption efficiency of New-TPE algorithm is higher than that of Ideal-TPE algorithm. As shown above, the encryption efficiency of New-TPE algorithm is better than that of Ideal-TPE algorithm and 3px -TPE algorithm.

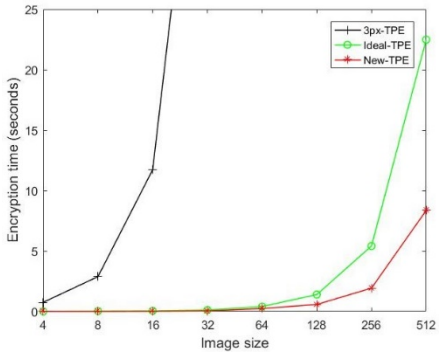

Figure 3: Analysis of encryption time of different algorithms (unit: s)

5 CONCLUSION

In this paper, we propose a new New-TPE. In this scheme, the plaintext image information is first used as part of the key to establish the association between the plaintext image and the key. Next, a suitable random value is selected to operate with the original pixel value, and this operation is performed to change the pixel value. Finally, SA and displacement function scrambling method are added in the image scrambling process to improve the ciphertext image security. The scheme generates a ciphertext image with certain security, and the ciphertext image is similar to the low-resolution plaintext image, which provides some visual usability. The experimental and analysis results show that the scheme can correctly perform encryption and decryption operations, and has higher security than other algorithms. The speed of this encryption algorithm is relatively slow. When there are too many encrypted images, the encryption time will be very long. Therefore, in future research, encryption time should be reduced.

REFERENCES

[1] Carrington D. How many photos will be taken in 2021?[EB/OL]. Mylo, 2021. (2021). https://blog.mylio.com/how-many-photos-will-be-taken-in-2021-stats/.
[2] Tierney M, Spiro I, Bregler C, *et al.* Cryptagram: Photo privacy for online social media[C]//Proceedings of the first ACM conference on Online social networks. 2013: 75–88.
[3] Wei D, Jiang M. A fast image encryption algorithm based on parallel compressive sensing and DNA sequence[J]. Optik, 2021, 238: 166748.
[4] Huo D, Zhu Z, Wei L, *et al.* A visually secure image encryption scheme based on 2D compressive sensing and integer wavelet transform embedding[J]. Optics Communications, 2021, 492: 126976.
[5] Roy S, Shrivastava M, Rawat U, *et al.* IESCA: an efficient image encryption scheme using 2-D cellular automata[J]. Journal of Information Security and Applications, 2021, 61: 102919.

[6] Wang X, Liu C, Xu D, *et al.* Image encryption scheme using chaos and simulated annealing algorithm[J]. Nonlinear Dynamics, 2016, 84(3): 1417-1429.
[7] Gregory R L. Knowledge in perception and illusion[J]. Philosophical Transactions of the Royal Society B: Biological Sciences, 1997, 352(1358): 1121-1128.
[8] Wright C V, Feng W, Liu F. Thumbnail-preserving encryption for JPEG[C]//Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security. 2015: 141-146.
[9] Marohn B, Wright C V, Feng W, *et al.* Approximate thumbnail preserving encryption[M]//Proceedings of the 2017 on Multimedia Privacy and Security. 2017: 33-43.
[10] Zhang Y, Zhao R, Xiao X, *et al.* HF-TPE: High-fidelity thumbnail-preserving encryption[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2021, 32(3): 947-961.
[11] Tajik K, Gunasekaran A, Dutta R, *et al.* Balancing Image Privacy and Usability with Thumbnail-Preserving Encryption[J]. IACR Cryptol. ePrint Arch., 2019, 2019: 295.
[12] Zhao R, Zhang Y, Xiao X, *et al.* TPE2: Three-pixel exact thumbnail-preserving image encryption[J]. Signal Processing, 2021, 183: 108019.
[13] Li Y, Tang W K S, Chen G. Generating hyperchaos via state feedback control[J]. International Journal of Bifurcation and Chaos, 2005, 15(10): 3367-3375.
[14] Wikipedia, https://en.wikipedia.org/wiki/Simulated_annealing.
[15] Chai X, Zheng X, Gan Z, *et al.* Exploiting plaintext-related mechanism for secure color image encryption[J]. Neural Computing and Applications, 2020, 32(12): 8065–8088.
[16] Wang X, Guan N. A novel chaotic image encryption algorithm based on extended Zigzag confusion and RNA operation[J]. Optics & Laser Technology, 2020, 131: 106366.