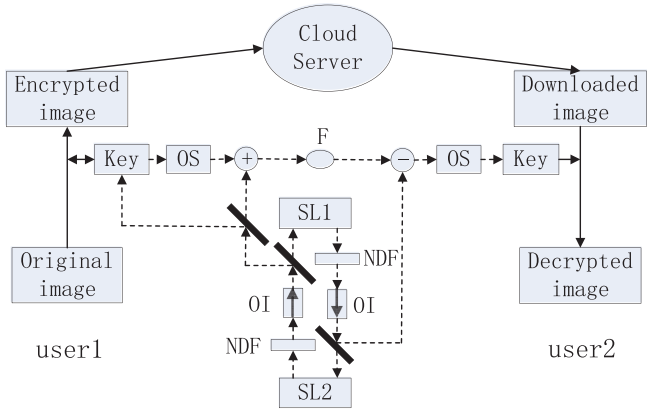
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Exploiting Optical Chaos for Color Image Encryption and Secure Resource Sharing in Cloud

Volume 11, Number 3, June 2019

Lili Li
Yiyuan Xie
Yuzhu Liu
Bocheng Liu
Yichen Ye
Tingting Song
Yushu Zhang
Yong Liu



DOI: 10.1109/JPHOT.2019.2919576
1943-0655

Exploiting Optical Chaos for Color Image Encryption and Secure Resource Sharing in Cloud

Lili Li,[1] Yiyuan Xie ,[1,2] Yuzhu Liu,[1] Bocheng Liu,[1] Yichen Ye,[1] Tingting Song,[1] Yushu Zhang,[3] and Yong Liu[2]

[1]School of Electronics and Information Engineering, Southwest University, Chongqing 400715, China
[2]School of Optoelectronic Information, University of Electronic Science and Technology of Chengdu, Sichuan 611731, China
[3]School of Information Technology, Deakin University, Geelong, Vic 3125, Australia

DOI:10.1109/JPHOT.2019.2919576

Manuscript received January 11, 2019; revised May 23, 2019; accepted May 24, 2019. Date of publication May 28, 2019; date of current version June 11, 2019. This work was supported in part by the 863 program of China under Grant 2015AA016304, in part by the National Natural Science Foundation of Chongqing City under Grant Nos.cstc2016jcyjA2002, in part by the Postdoctoral Science Foundation of China under Grant Nos.2016M590875, and in part by the Fundamental Research Funds for the Central Universities under Grant XDJK2018B012. Corresponding author: Yiyuan Xie (e-mail:yyxie@swu.edu.cn).

Abstract: Cloud as a developing technology provides convenient services to sharing and usage of images resource, but brings a threat to images security and privacy authentication. Optical chaos possess distinct superiority for image secure sharing, therefore, based on two mutually coupled semiconductor lasers (MC-SL1 and MC-SL2), we theoretically propose a color image encryption system for secure resource sharing and introduce a watermarking method for images privacy authentication in cloud. In our paper, after achieving chaos synchronization under proper parameters, two MC-SLs are used to transmit encryption/decryption key space generated by chaotic signal of MC-SL1 and user's key. We carry out digital watermarking and encryption of a color image before secure resource sharing in cloud. On the other side of cloud, we make some tests for decryption of color image by received key space and watermark extraction. Meanwhile, we discuss security performance of color image encryption/decryption and key space transmission process, and analyze secure resource sharing of color image in cloud.

Index Terms: Cloud, chaos synchronization, image encryption, optical chaos, watermark, semiconductor lasers (SLs).

1. Introduction

As one of the most authoritative technologies in the IT industry, cloud technology exhibits many advantages such as large scale, virtualization, processing data remotely, low cost, providing sharing services to users on demand basis [1]–[3], and therefore has potential applications in IT industry, business and academia, especially the data storage and sharing in cloud services [4]–[6]. With the rapid development of cloud technology, the amount of information over cloud technology especially the multimedia files like images or video are growing exponentially. In recent years, images storage and sharing in cloud have attracted much attention. Consequently, related studies on the images

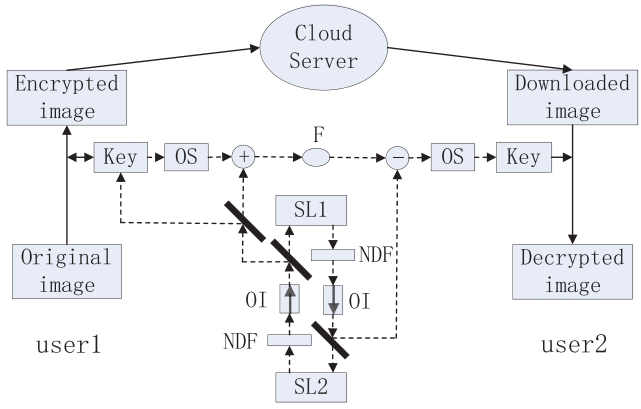


Fig. 1. The structure diagram of the proposed color image encryption system in cloud.

storage and sharing, especially color image, have been reported based on the different methods theoretically and experimentally. However, it also brings about great trouble to the security of image and other multimedia files in cloud. Actually, many image encryption methods have been put forward since mid-1990s [7]. There are some traditional encryption algorithms such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and RSA [8], but with the growing demand for applications, they are no longer appropriate for image encryption due to the redundancy and special storage format, high-volume data and so on [9]. Therefore, since the first chaotic cryptograph proposed by Matthews in 1989 [10], the application of chaotic map on image encryption has entered people's sight for their properties due to its merits, including ergodicity and sensitive dependence on initial parameters, complex dynamics behaviors and real number field properties [11], [12]. Recently, many image encryption algorithms using chaotic maps have been carried out, for instance, three-dimensional (3D) cat map, logistic map, the double Chaos and so on [13]–[15].

Compared to traditional electrical chaos, optical chaos produced by semiconductor laser (SL) has a bevy of outstanding qualities, including higher bandwidth and complexity, low power consumption and better compatibility with long-distance communication [16], therefore has broad applications, for example, optical chaos can generate high-speed random number, make information memory device, and it can be useful for chaotic radar ranging and chaos secure communication [17]–[20], especially image encryption and resource secure sharing in cloud [21]. Actually, we have achieved gray-scale image encryption and transmission using optical chaos based on point-to-point (P2P) communications [22]. However, color image encryption and secure resource sharing studies in cloud using optical chaos generated by SL are still scarce.

To the best of our knowledge, we first present a color image encryption system using optical chaos generated by two mutually coupled SLs (MC-SL1 and MC-SL2) for secure resource sharing in cloud, and introduce a watermarking method for images privacy authentication in cloud. In this paper, we embed a binary image into a color image firstly, and analyze chaos synchronization performance of two MC-SLs and transmission security of key space generated by chaotic output of MC-SL1 and user's key. Secondly, we present color image encryption process using Josephus traversing map and Logistic map. Thirdly, we explain other users' employment for the encrypted color image in cloud. Lastly, we make some security analyses on the proposed encryption algorithm and system.

2. Theory Analysis

The structure diagram of the proposed color image encryption system in cloud is illustrated in Fig. 1. As can be seen from the diagram, the proposed system mainly consists of user1, user2,

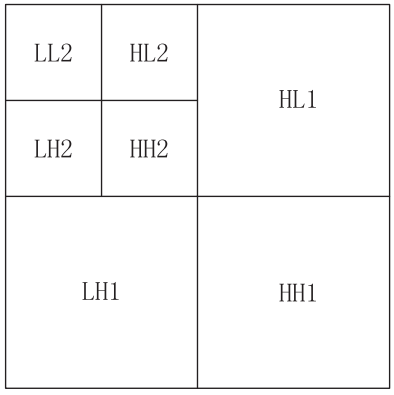


Fig. 2. The decomposition diagram of two levels DWT.

cloud server and key space transmission module. In user1, a binary watermark is embedded into a color image based on discrete wavelet transform (DWT), and the watermarked color image is shuffled and diffused by using Josephus traversing map and Logistic map respectively, in this case, the encrypted color image can be uploaded to cloud server for secure resource sharing. In key space transmission module, two MC-SLs are mutually injected unidirectionally by optical isolators (OI), and neutral density filters (NDF) can change the injection rates. For MC-SL1, 2, their outputs are divided into two parts, the transmission part of chaotic signal is injected into another MC-SL through fiber, and the other part is used to generate and transmit key space with user1's key. In addition, the other users (i.e., user2) can download the encrypted color image, and use received key space for decrypting the color image. Furthermore, user2 can extract the watermark from the decrypted color image for privacy authentication.

2.1 A Watermarking Method Based on Discrete Wavelet Transform (DWT)

DWT is an analysis method about time-frequency signal, which makes an image be decomposed into subimages at different space and frequencies [23], [24]. Therefore, DWT has been paid close extensive attention for its application in image processing. In this paper, we introduce a watermarking method employing DWT for image privacy authentication. As shown in Fig. 2, after three matrices R, G and B is extracted from an original color image, the matrice R is first decomposed into four subbands denoted LL1, LH1, HL1, and HH1 at level 1 in the DWT domain by two levels wavelet decomposition, where LL1 stands for low-frequency subband, and LH1, HL1, HH1 represent high-frequency subbands. In addition, the LL1 subband further is decomposed to obtain level 2 of decomposition (i.e., LL2, LH2, HL2, and HH2), and a binary watermark is embedded into low-frequency subband LL2.

Here, the performance of the watermarking method can be validated by Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) [22]:

$$MSE = \frac{1}{W \times H} \sum_{i=1}^{W-1} \sum_{j=1}^{H-1} (I_W(i,j) - I(i,j)) \tag{1}$$

$$PSNR = 10 \times \log_{10} \left(\frac{255^2}{MSE} \right) \tag{2}$$

where W and H is the size of color image, $I_W(i,j)$ is the pixels of the watermarked color image, and $I(i,j)$ is the pixels of the original color image. The smaller the value of MSE is and the higher the value of PSNR is, the better the performance is.

2.2 Generation and Transmission of Key Space Using Optical Chaos Generated by Two MC-SLs

We use two MC-SLs to generate optical chaos and transmit encryption/decryption key space. For numerical simulations of outputs of two MC-SLs, based on the spin-flip model (SFM) [25], [26], the rate equations for the two MC-SLs can be indicated as:

$$\frac{dE_{1,2}^{x,y}}{dt} = k(1+i\alpha)((N_{1,2}-1)E_{1,2}^{x,y} \pm in_{1,2}E_{1,2}^{y,x}) \pm (-\gamma_a - i\gamma_p)E_{1,2}^{x,y} + \eta_{2,1}E_{2,1}^{x,y}(t-\tau_{2,1})e^{-i2\pi(f\tau_{2,1}-\Delta ft)} + F_{1,2}^{x,y} \tag{3}$$

$$\frac{dN_{1,2}}{dt} = \gamma_n(\mu - N_{1,2}(1+|E_{1,2}^{x}|^2+|E_{1,2}^{y}|^2)) - i\gamma_n n_{1,2}(E_{1,2}^{y}E_{1,2}^{x}{}^* - E_{1,2}^{x}E_{1,2}^{y}{}^*) \tag{4}$$

$$\frac{dn_{1,2}}{dt} = -\gamma_s n_{1,2} - \gamma_n n_{1,2}(|E_{1,2}^{x}|^2+|E_{1,2}^{y}|^2) - i\gamma_n N_{1,2}(E_{1,2}^{y}E_{1,2}^{x}{}^* - E_{1,2}^{x}E_{1,2}^{y}{}^*) \tag{5}$$

where the superscripts 1 and 2 represent MC-SL1 and MC-SL2, and the symbols x and y represent for x polarization component (x-PC) and y polarization component (y-PC). E stands for the slowly varying complex component of the field, N expresses the total carrier inversion of SLs, n accounts for the difference of carrier number between the spin-up and spin-down radiation channels, k and α represent the delay inversion of optical field and the line-width enhancement factor, γ_s and γ_n is the spin-flip relaxation intensity and the decay intensity of the parameter, γ_a and γ_p are the linear dichroism and birefringence. μ accounts for the normalized injection current. $\eta_{1,2}$ and $\tau_{2,1}$ are the injection strength and the injection time from MC-SL1 to MC-SL2 and from MC-SL2 to MC-SL1, respectively. f is the central frequency of the MC-SLs, Δf the mismatching of f between MC-SL1 and MC-SL2. And the spontaneous emission noises are described as the following formulas [27]:

$$F_{1,2}^{x} = \sqrt{\beta_{sp}/2}\left(\sqrt{N_{1,2}+n_{1,2}}\xi_1 + \sqrt{N_{1,2}-n_{1,2}}\xi_2\right) \tag{6}$$

$$F_{1,2}^{y} = -i\sqrt{\beta_{sp}/2}\left(\sqrt{N_{1,2}+n_{1,2}}\xi_1 - \sqrt{N_{1,2}-n_{1,2}}\xi_2\right) \tag{7}$$

where ξ_1 and ξ_2 are independent Gaussian white noise, and β_{sp} is the spontaneous emission rate.

The synchronization performance between MC-SL1, 2 is evaluated by the following formula:

$$C = \frac{\langle (I_i(t) - \langle I_i(t)\rangle)(I_j(t) - \langle I_j(t+\Delta t)\rangle)\rangle}{\langle |I_i(t) - \langle I_i(t)\rangle^2|\rangle^{1/2}\langle |I_j(t) - \langle I_j(t+\Delta t)\rangle^2|\rangle^{1/2}} \tag{8}$$

where i and j represents MC-SL1, 2, $I = |E|^2$ is the output intensity of the MC-SLs, and the range of time shift Δt is [−10 ns,10 ns]. The range of $|C|$ is [0, 1], and $|C| = 1$ represents the perfect and ideal synchronization performance.

In addition, the communication performance of the transmission is evaluated by Q-factor [28]:

$$Q = \frac{(\langle P_1\rangle - \langle P_2\rangle)}{\sigma_1 + \sigma_2} \tag{9}$$

where P_i is the mean power and σ is the corresponding standard deviation. Larger Q-factor indicate the better communication performance.

Furthermore, to accomplish secure encryption of the watermarked color image, the encryption/decryption keys should have close correlation with users. Here, the output of MC-SL1 can be transformed into pseudo random sequences, and twelve 8-bit long binary sequences (K_L) will be selected from the pseudo random sequence randomly. At the same time, the user's input key (K_C) is a string of characters which can be expressed as twelve 8-bit long binary sequences. Nevertheless, the parameters of the encryption/decryption algorithms should come from the key. Therefore, the key should be generated by a combination of K_L and K_C, and the generation process is described as follows:

Firstly, K_L and K_C are transformed into twelve binary sequences of 8 bits. To protect the key against opponent's attacks, we mix K_L and K_C by the XOR operation, i.e., $K_E = K_L \oplus K_C$, then the

six parameters of the color image encryption can be obtained by the following formulas:

$$\begin{aligned} S_1 &= round(((K_E(1) + K_E(2))/K) * M) \\ D_1 &= round(((K_E(3) + K_E(4))/K) * M) \\ S_2 &= round(((K_E(5) + K_E(6))/K) * M) \\ D_2 &= round(((K_E(7) + K_E(8))/K) * M) \\ L_i &= round(K_E(9) + K_E(10))/K \\ S &= round(((K_E(11) + K_E(12))/K) * 255) \end{aligned} \tag{10}$$

In addition, we use the chaos masking (CM) encryption schemeto transmit the key space generated by the chaotic output of MC-SL1 [29]–[31].

2.3 Color Image Encryption and Secure Resource Sharing in Cloud

Before the watermarked color image is uploaded to cloud server, we exploit Josephus traversing map, Logistic map and the "XOR plus mod" operation to encrypt the watermarked color image for its secure sharing. Actually, Josephus traversing map is derived from Josephus problem, and it can be used to shuffle the positions of the watermarked color image pixels [32]. However, the values of the image pixels are still unaltered, and it is possible that some crackers attack the Josephus traversing map encryption process. Therefore, we introduce Logistic map and the "XOR plus mod" operation to diffuse the values of the watermarked color image pixels for better encryption. The whole encryption process is shown as the following three steps:

First, we choose parameters S_1, D_1 for rows, S_2, D_2 for columns as the numbers of the starting point and the selection point of Josephus traversing map from key space. Meantime, we choose two control parameters for Logistic map and the "XOR plus mod" operation: L_i is a floating number in (0,1), and S is an integer.

Second, the watermarked color image is converted into three matrices R, G and B. Every 256 $\times$ 256 matrice is lined up as a sequence by rows, and the sequence gets different traversal orders through Josephus traversing map, then the new sequence is reshaped a new matrice. Furthermore, the new matrice is also lined up as a sequence by columns and the other steps follow the same procedure mentioned above, and the Josephus traverding map permutation process can be iterative for several times.

Third, the three new matrices are diffused by Logistic map and the "XOR plus mod" operation [33]–[35]:

Step 1: Use L_i as the initial value to compute the chaotic Logistic map:

$$x(i+1) = 4x(i)(1 - x(i)) \tag{11}$$

if the calculated value is within the interval (0.2, 0.8), then perform step 2; if not, iterate the map in (10) until the next value is within (0.2, 0.8). However, notice that 0.5 is an undesired point, it can stop the iterations of Logistic map, in this case, another L_i should be chose to restart the diffusion process.

Step 2: When a proper value is obtained from step 1, digitize the value as $\phi(k)$, and $\phi(k)$ is XOR-ed with the values of currently operated pixel $I(i)$ and previously operated pixel in the new three matrices, shown in the following formula:

$$C(k) = \phi(i) \oplus \{[I(i) + \phi(i)] mod N\} \oplus C(i-1) \tag{12}$$

where $C(i-1)$ is the previously output cipher-pixel, $C(i)$ is the currently calculated cipher-pixel, and N is the color level of the three matrices R, G, B ($N = 256$). Here, we set the initial value of the currently operated pixel $I(0) = S$. After finishing the color image encryption, the performance of encryption algorithm can be measured by image entropy (H) and the correlation coefficient of

(a) (b) (c)

Fig. 3. The watermarking process of a binary image and a color image (a) a binary image, (b) an original color image, (c) the embedded color image.

pixels [13], [15]:

$$H = \sum_{i=0}^{k} P_i \log_2 \frac{1}{P_i} \tag{13}$$

$$E(x) = \frac{1}{N} \sum_{i=0}^{N} x_i$$

$$D(x) = \frac{1}{N} \sum_{i=0}^{N} (x_i - E(x))^2$$

$$C = \frac{E(x - E(x))(y - E(y))}{\sqrt{D(x)}\sqrt{D(y)}} \tag{14}$$

P_i is the probability of the ith grayscale, x and y are the values of the neighboring pixels in the matrices R, G, B of color image, respectively. Besides, the ideal value of H for the encrypted color image is 8.

In addition, after encrypting the watermarked color image, we outsource the image to the cloud for secure resource sharing.

2.4 Color Image Decryption and Watermark Extraction

For the other legal users, they can download the encrypted color image and use received key space to decrypt the watermarked color image. The decryption of the encrypted watermarked color image is the inverse transform of Josephus map, Logistic map and the "XOR plus mod" operation. Among them, the decrypted process of Logistic map is exhibited by the following formula:

$$I(k) = \{\phi(i) \oplus C(i) \oplus C(i-1) + N - \phi(i)\} \, mod N \tag{15}$$

In addition, based on DWT, we extract the watermark from the decrypted color image for the feasibility of image integrity authentication in cloud.

3. Numerical Simulation Results and Discussion

3.1 The Watermarking of a Color Image

As described in theory analysis, we select a binary image whose size is 50×20 as a watermark, and the watermark is embedded into low-frequency subband LL2 of the matrice R of a color image based on DWT, and the simulation results are shown in Fig. 3. It serves to perceive that the watermarked color image is almost the same as the original color image, simultaneously, the values of MSE and PSNR are 2.59 and 43.99, respectively, which illustrates the watermarking method has good performance.

TABLE 1
Parameters of the MC-SLs

Parameter	MC-SL1	MC-SL2
α	3	3
k	300 ns^{-1}	300 ns^{-1}
γ_s	50 ns^{-1}	50 ns^{-1}
γ_a	0.1 ns^{-1}	0.1 ns^{-1}
γ_p	10 ns^{-1}	10 ns^{-1}
γ_n	1 ns^{-1}	1 ns^{-1}
f	1.944×10^{14}	1.944×10^{14}
μ	2.7	2.7

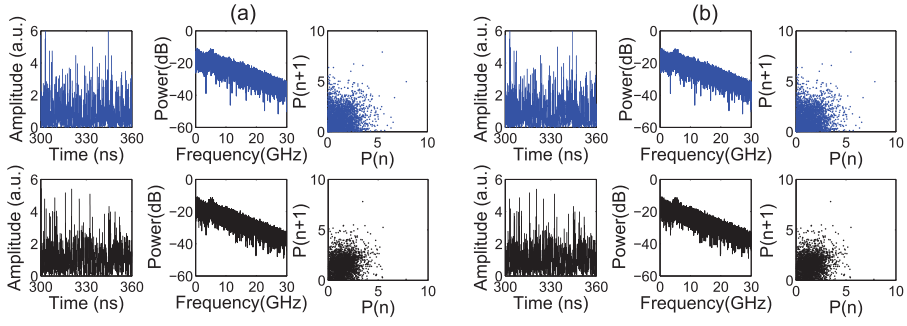


Fig. 4. Time series, power spectra and phase portraits of (a) MC-SL1, (b) MC-SL2 for x-PC and y-PC.

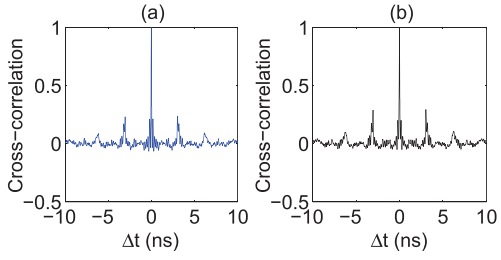


Fig. 5. Cross-correlation coefficient between MC-SL1 and MC-SL2 for (a) x-PC and (b) y-PC.

3.2 Generation and Transmission of Key Space Using Optical Chaos Generated by Two MC-SLs

For the MC-SLs, the rate equations (1)–(3) can be numerically solved by fourth-order Runge-Kutta algorithm. In the following generation and transmission of key space, the internal parameters of all the VCSELs are showed in Table 1.

Meanwhile, the values of some parameters are set becomingly: $\eta_{1,2} = 10$ ns^{-1} and $\tau_{1,2} = 3$ ns. Fig. 4 displays time series, power spectra and phase portraits of MC-SL1,2 for x-PC and y-PC, it is clear that the chaotic outputs of MC-SL1 and MC-SL2 have high bandwidth. What's more, as shown in Fig. 5, it is obvious that cross-correlation coefficient between MC-SL1 and MC-SL2 are nearly 1 at $\Delta t = 0$ ns, which proves two MC-SLs realize general synchronization. In this case, we convert key space to binary for convenient and secure transmission by optical fibers, and transmission results are shown in Fig. 6 by parts. From Fig. 6(a) and Fig. 6(b) we can see that the binary key space after transmission keeps almost unchanged, and Fig. 6(c) presents the eye diagram is clear and wide-open, where corresponding Q-factor is 9.368 and the BER is less than 4.22×10^{-20}, which

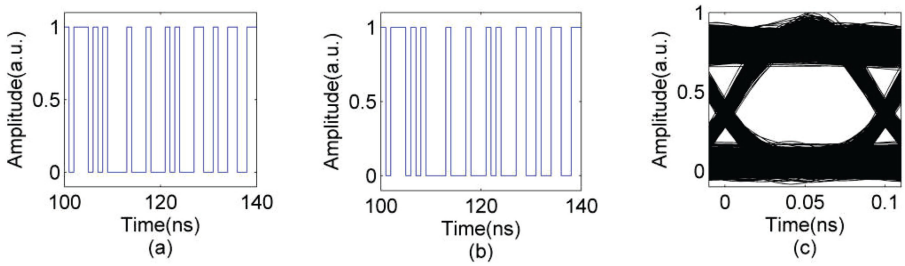


Fig. 6. Transmission and eye diagrams of key space by optical fibers partly (a) original binary key space, (b) received binary key space, (c) eye diagrams of transmission.

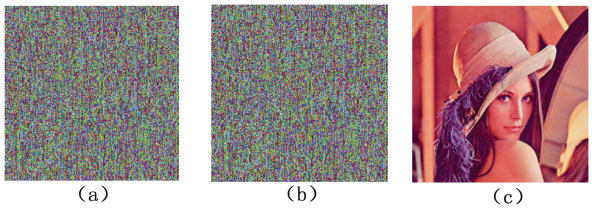


Fig. 7. Encryption/decryption and secure resource sharing of color image. (a) The encrypted color image. (b) The downloaded color image in cloud. (c) The decrypted color image.

Fig. 8. Extraction of the decrypted color image.

can well meet the requirement of transmission. Hence, the key space is transmitted safely through optical fibers for later image decryption.

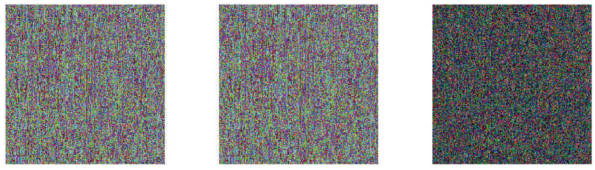
3.3 Encryption/Decryption of Color Image and Secure Resource Sharing in Cloud

Fig. 7(a) describes encryption result of the watermarked color image. Clearly, original color image is successfully encrypted, and the entropy (H) of encrypted color image is 7.9972, conveying the truth that the proposed encryption mechanism is perfect and valid as expected.

In addition, based on encryption of the watermarked color image, we achieve secure sharing in clouds. Fig. 7(b) and Fig. 7(c) is the encrypted color image downloaded from cloud and its decryption result using received key space, it is evident that the downloaded color image and original encrypted color image do not have great change in fact, and the decrypted color image is still clear and almost same as the original color image, which achieves the feasibility of secure resource sharing of the color image in cloud.

3.4 Watermark Extraction of The Decrypted Color Image

Due to privacy authentication of the watermarked encrypted color image, the watermark is recovered from the decrypted color image, shown in Fig. 8. The simulation result reveals there is almost no difference between the extracted watermark and original watermark, and their correlation coefficient is close to 1, therefore, the binary watermark embedded into the color image is extracted from the decrypted color image successfully.



(a) (b) (c)

Fig. 9. Encryption key sensitivity analysis (a) Encrypted color image: Key = 12345678901a, (b) Encrypted color image: Key = 12345678901b, (c) Difference image.

(a) (b) (c)

Fig. 10. Decryption key sensitivity analysis (a) Decrypted color image: Key = 12345678901a, (b) Decrypted color image: Key = 02345678901a, (c) Difference image.

4. Security Analysis

To study the security performance of the proposed encryption algorithm against some common security attacks, such as statistical attack, differential attack and brute-force attack, this section will analyze and discuss the security through some aspects.

4.1 Key Space and Sensitivity Analysis

First, a perfect encryption/decryption algorithm should have enough key space to fight brute-force attack. According to the above analysis to generation of key space, our encryption/decryption algorithm has four 16-bit long binary control parameters for Josephus traversing map and two 16-bit long binary control parameters for Logistic map. The key space size of possible combinations of control parameters S_1, D_1, S_2, D_2, L_i, S is $2^{6\times16} \approx 7.923 \times 10^{28}$. Therefore, the key space of the proposed algorithm is large enough to resist brute-force attack.

On the other hand, the key should have sensitivity in the encryption/decryption process. Here, we make test 1 and test 2 of user's encryption/decryption key sensitivity as follows:

Test 1: Set user's key to "12345678901a" and encrypt the watermarked color image. Then change one bit of the twelve key, like "12345678901b", and use the changed key to encrypt the watermarked color image again. Last compare difference between the two encrypted color image. All the results are shown in Fig. 9, Fig. 9(c) tells us that the color image encrypted by the key "12345678901a" has 99.6% of difference from the one encrypted by the key "12345678901b" although there is one bit change about the encryption key.

Test 2: Encrypt the watermarked color image by the key "12345678901a". Then decrypt the encrypted color image by the two key "12345678901a" and "02345678901a", respectively. Last compare difference between the two decrypted color image. Fig. 10 displays the simulation results, and it can be known that the two decrypted color image by the key "12345678901a" and "02345678901a" have 99.62% of difference.

The two tests above fully testify that the key has excellent sensitivity in the encryption and decryption process.

4.2 Histograms and Correlation Analysis

The histograms of a color image show the chances of the pixels at different intensity values [8], [38], and correlation coefficients of two adjacent pixels can reveal the randomness of a color image.

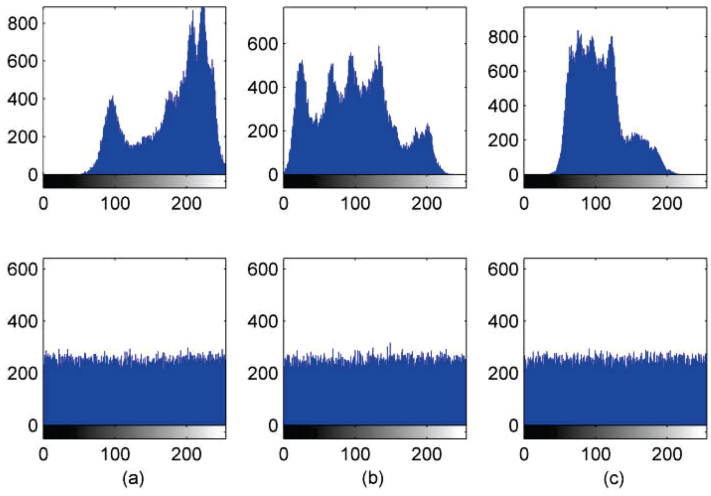


Fig. 11. Histogram of original embedded color image and the encrypted embedded color image (a) the matrice R, (b) the matrice G, (c) the matrice B.

TABLE 2
Correlation Coefficient Between Original and Encrypted Images

Correlation	Original image			Encrypted image		
	R	G	B	R	G	B
Horizontal	0.0267	0.0139	0.0144	0.9636	0.9361	0.9151
Vertical	0.0010	0.0028	0.0112	0.9606	0.9221	0.9133
Diagonal	0.0031	0.0009	0.0034	0.9216	0.8836	0.8540

In order to analyze the performance of the proposed encryption algorithm against statistical attack, we make security analysis based on the histograms of the encrypted color image and correlation coefficients of two adjacent pixels. Fig. 11 displays the histograms of original watermarked color image and the encrypted watermarked color image, the histogram of the encrypted color image is properly uniform, which is different from the uneven histogram of original color image. Table 2 is correlation coefficient of two vertically, horizontally and diagonally adjacent pixels in the original and encrypted color image, it is obvious that all the correlation coefficients dramatically decline and are close to 0 after being encrypted by the proposed encryption algorithm, which means a high randomness of the encrypted color image.

4.3 Differential Analysis

Generally speaking, it is possible for an attacker to change some pixels in an image, possibly affecting the final result. Here, to study the influence of one-pixel change on the encrypted image, we introduce two parameters: Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI). NPCR measures the percentage of pixels difference for two images, and UACI is the average intensity of differences between two images. Here, NPCR and UACI are given by the following formulas [36], [37]:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \tag{16}$$

$$UACI = \frac{1}{W \times H} \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\% \tag{17}$$

TABLE 3
NPCR and UACI of a Color Image

Component	NPCR	UACI
R	99.28%	50.1%
G	99.16%	49.83%
B	99.43%	45.46%

where W and H are the width and height of two image (i.e., C_1 and C_2), $C_1(i, j)$ and $C_2(i, j)$ is the pixel values of two images, D is an array that has a connection with $C_1(i, j)$ and $C_2(i, j)$. If $C_1(i, j)$ is equal to $C_2(i, j)$, $D(i, j)$ is 1, if not, $D(i, j)$ is 0.

According to the analysis above, we make a test for NPCR and UACI about the one-pixel change influence, the results are shown in Table 3. The values of NPCR and UACI is almost close to 100% and more than 30%, respectively, when original color image has one-pixel change. Namely, the proposed encryption algorithm has good performance against differential attack.

5. Conclusion

In summary, based on optical chaos generated by two SLs, we propose a color image encryption algorithm and system for secure resource sharing in cloud. In our system, we achieve high-quality chaos synchronization between two MC-SLs by changing injection rates and other variables, when the cross-correlation coefficients C between MC-SL1 and MC-SL2 are approximately 1 at $\Delta t = 0$ ns, then the two MC-SLs are used to transmit encryption/decryption key space generated by chaotic signal of MC-SL1 and user's key in 15 km fibers with wide-open eye diagrams and high Q-factor 9.368. In addition, due to privacy authentication of color image, we introduce a watermarking method based on DWT, and embed a binary image into a color image successfully, because the entropy H of the encrypted color image is 7.9972 and almost close to 8. Besides, we utilize Josephus traversing map and Logistic map to encrypt the watermarked color image for secure resource sharing. At the same time, we make some security analyses on the performance of the proposed encryption system against several attacks, such as key space and sensitivity analysis, histograms and correlation analysis, NPCR and UACI analysis, which illustrates the proposed encryption algorithm has efficient performance against several attacks. Lastly, we obtain the encrypted color image, and use received key space to decrypt the color image and extract the watermark successfully. Therefore, the proposed system can achieve color image encryption and secure resource sharing perfectly. We also hope our research will be significant for later researches on image encryption and the sharing technology of secure resources.

Acknowledgment

The authors wish to thank the anonymous reviewers for their valuable suggestions.

References

[1] M. Armbrust *et al.*, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, Apr. 2010.
[2] G. Brunette and R. Mogull, "Security guidance for critical areas of focus in cloud computing v2. 1," Cloud Security Alliance, Seattle, WA, USA, 2009, pp. 1–76.
[3] G. Q. Hu, D. Xiao, T. Xiang, S. Bai, and Y. S. Zhang, "A compressive sensing based privacy preserving outsourcing of image storage and identity authentication service in cloud," *Inf. Sci.*, vol. 387, pp. 132–145, May 2017.
[4] Z. H. Xia, X. H. Wang, L. G. Zhang, Z. Qin, X. M. Sun, and K. Ren, "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 11, pp. 2594–2608, Nov. 2016.
[5] H. Takabi, J. B. Joshi, and G. J. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE Secur. Privacy*, vol. 8, no. 6, pp. 24–31, Dec. 2010.

[6] L. F. Wei *et al.*, "Security and privacy for storage and computation in cloud computing," *Inf. Sci.*, vol. 258, no. 3, pp. 371–386, Feb. 2014.
[7] P. Rad, M. Muppidi, A. S. Jaimes, S. S. Agaian, and M. Jamshidi, "A novel image encryption method to reduce decryption execution time in cloud," in *Proc. 9th Annu. Int. Syst. Conf.*, Apr. 2015, pp. 478–482.
[8] S. Mazloom and A. M. Eftekhari-Moghadam, "Color image encryption based on coupled nonlinear chaotic map," *Chaos, Solitons Fractals*, vol. 42, no. 3, pp. 1745–1754, Nov. 2009.
[9] X. P. Wei, L. Guo, Q. Zhang, J. X. Zhang, and S. G. Lian, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system," *J. Syst. Softw.*, vol. 85, no. 2, pp. 290–299, Feb. 2012.
[10] R. Matthews, "On the derivation of a chaotic encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, Jan. 1989.
[11] L. Kocarev and G. Jakimovski, "Chaos and cryptography: from chaotic maps to encryption algorithms," *IEEE Trans. Circuits Syst.-I*, vol. 48, no. 2, pp. 163–169, Jul. 2001.
[12] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons Fractals*, vol. 21, no. 3, pp. 749–761, Jul. 2004.
[13] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image Vis. Comput.*, vol. 24, no. 9, pp. 926–934, Sep. 2006.
[14] X. Q. Fu, B. C. Liu, Y. Y. Xie, W. Li, and Y. Liu, "Image encryption-then-transmission using DNA encryption algorithm and the double Chaos," *IEEE Photon. J.*, vol. 10, no. 3, Jun. 2018, Art. no. 3900515.
[15] K. W. Wong, B. S. H. Kwok, and W. S. Law, "A fast image encryption scheme based on chaotic standard map," *Phys. Lett. A*, vol. 372, no. 15, pp. 2645–2652, Apr. 2008.
[16] G. G. Xu *et al.*, "Efficient power extraction in surface-emitting semiconductor lasers using graded photonic heterostructures," *Nature Commun.*, vol. 3, Jul. 2012, Art. no. 952.
[17] A. Argyris *et al.*, "Chaos-based communications at high bit rates using commercial fibre-optic links," *Nature*, vol. 438, no. 17, pp. 343–346, Nov. 2005.
[18] V. Annovazzi-Lodi, S. Donati, and A. Scire, "Synchronization of chaotic injected-laser systems and its application to optical cryptography," *IEEE J. Quantum Electron.*, vol. 32, no. 6, pp. 953–959, Jun. 1996.
[19] F. Y. Lin and J. M. Liu, "Chaotic radar using nonlinear laser dynamics," *IEEE J. Quantum Electron.*, vol. 40, no. 6, pp. 815–820, Jun. 2004.
[20] A. Uchida *et al.*, "Fast physical random bit generation with chaotic semiconductor lasers," *Nature Photon.*, vol. 2, no. 12, pp. 728–732, Nov. 2008.
[21] O. Graydon, "Optical encryption: Polarization keys," *Nature Photon.*, vol. 9, no. 3, Mar. 2015, Art. no. 141.
[22] Y. Y. Xie, J. C. Li, Z. F. Kong, Y. S. Zhang, X. F. Liao, and Y. Liu, "Exploiting optics chaos for image encryption-then-transmission," *J. Lightw. Technol.*, vol. 34, no. 22, pp. 5101–5109, Nov. 2016.
[23] T. R. Downie and B. W. Silverman, "The discrete multiple wavelet transform and thresholding methods," *IEEE Trans. Signal Process.*, vol. 46, no. 9, pp. 2558–2561, Sep. 1998.
[24] M. S. Hsieh, D. C. Tseng, and Y. H. Huang, "Hiding digital watermarks using multiresolution wavelet transform," *IEEE Trans. Ind. Electron.*, vol. 48, no. 5, pp. 875–882, Oct. 2001.
[25] J. Martin-Regalado, F. Prati, M. San Miguel, and N. B. Abraham, "Polarization properties of vertical-cavity surface-emitting lasers," *IEEE J. Quantum Electron.*, vol. 33, no. 5, pp. 765–783, May 1997.
[26] R. Al-Seyab, K. Schires, N. A. Khan, A. Hurtado, I. D. Henning, and M. J. Adams, "Dynamics of polarized optical injection in 1550-nm VCSELs: theory and experiments," *IEEE J. Sel. Topics Quantum Electron.*, vol. 17, no. 5, pp. 1242–1249, Sep. 2010.
[27] T. Deng, G. Q. Xia, and Z. M. Wu, "Broadband chaos synchronization and communication based on mutually coupled VCSELs subject to a bandwidth-enhanced chaotic signal injection," *Nonlinear Dyn.*, vol. 76, no. 1, pp. 399–407, Apr. 2014.
[28] L. Wang, Z. M. Wu, J. G. Wu, and G. Q. Xia, "Long-haul dual-channel bidirectional chaos communication based on polarization-resolved chaos synchronization between twin 1550 nM VCSELs subject to variable-polarization optical injection," *Opt. Commun.*, vol. 334, pp. 214–221, Jan. 2015.
[29] S. Sivaprakasam and K. A. Shore, "Signal masking for chaotic optical communication using external-cavity diode lasers," *Opt. Lett.*, vol. 24, no. 17, pp. 1200–1202, Sep. 1999.
[30] C. R. Mirasso, P. Colet, and P. García-Fernández, "Synchronization of chaotic semiconductor lasers: Application to encoded communications," *IEEE Photon. Technol. Lett.*, vol. 8, no. 2, pp. 299–301, Feb. 1996.
[31] J. Ohtsubo, "Chaos synchronization and chaotic signal masking in semiconductor lasers with optical feedback," *IEEE J. Quantum Electron.*, vol. 38, no. 9, pp. 1141–1154, Sep. 2002.
[32] D. S. Xiang and Y. S. Xiong, "Digital image scrambling based on Josephus traversing," *Comput. Eng. Appl.*, vol. 10, pp. 44–46, 2005.
[33] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image Vis. Comput.*, vol. 24, no. 9, pp. 926–934, Sep. 2006.
[34] L. Kocarev and G. Jakimoski, "Logistic map as a block encryption algorithm," *Phys. Lett. A*, vol. 289, no. 4, pp. 199–206, Oct. 2001.
[35] G. C. Wu and D. Baleanu, "Discrete fractional logistic map and its chaos," *Nonlinear Dyn.*, vol. 75, no. 1, pp. 283–287, Jan. 2014.
[36] X. C. Zhang, Z. Zhou, and Y. Niu, "An image encryption method based on the Feistel network and dynamic DNA encoding," *IEEE Photon. J.*, vol. 10, no. 4, Aug. 2018, Art. no. 3901014.
[37] S. L. Sun, "A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit level scrambling," *IEEE Photon. J.*, vol. 10, no. 2, Apr. 2018, Art. no. 7201714.
[38] T. Sivakumar and P. Li, "A secure image encryption method using scan pattern and random key stream derived from laser chaos," *Opt. Laser Technol.*, vol. 111, pp. 196–204, Apr. 2019.