ARM-Embedded Implementation of a Novel Color Image Encryption and Transmission System Based on Optical Chaos

Bo-Cheng. Liu,[1] Yi-Yuan. Xie,[1,2] Yu-Shu. Zhang,[3,4] Yi-Chen. Ye,[1] Ting-Ting. Song,[1] Xiao-Feng. Liao,[5] and Yong. Liu[2]

[1]*School of Electronic 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, Victoria 3125, Australia*
[4]*College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China*
[5]*School of Computer Science, Chongqing University, Chongqing 400044, China*

Manuscript submitted ??. This work was supported by the Natural Science Foundation of Chongqing City under Grant Nos. cstc2016jcyjA0581, by the Postdoctoral Science Foundation of China under Grant Nos. 2016M590875, by the Fundamental Research Funds for the Central Universities under Grant XDJK2018B012. Corresponding author: Y. Y. Xie (e-mail: yyxie@swu.edu.cn).

Abstract: Cloud servers are very suitable for sharing and storing image data and meanwhile it is confronted with many security and privacy problems. Optical chaos and hardware implementation of image encryption possess distinct superiorities in secret image sharing. Hence, combining the advantages of advanced reduced instruction set computer machine (ARM)-embedded platform Exynos4412 model, together with vertical-cavity surface emitting laser (VCSEL) subject to positive optoelectronic feedback (POEF), a novel color image encryption and transmission system is experimentally realized and appraised. We investigate the dynamic behaviors of the VCSEL and obtain the chaotic output. An analog to digital conversion (ADC) module is utilized for optical chaos data acquisition. The improved gravity model and the double sine map are exploited to encrypt the image, and the encrypted image is securely shared by cloud services. The user can download the encrypted image and decrypt it by the hardware board. The experiment results reveal that the system has an excellent resistance to common attacks. Compared to the numerical simulation, our hardware implementation for such a color image encryption and transmission system is formidable to actualize, but we successfully implemented and tested in a real-world environment. By comparing experimental and simulation results, the consistent results are found. Therefore, in the case of similar encryption effect, the user's information privacy protection in the actual industrial or commercial systems can be securely guaranteed on our hardware platform.

Index Terms: ARM-embedded implementation, optical chaos, VCSEL, image encryption.

1. Introduction

Cloud technology has brought great changes to our daily life, due to substantial advantages such as high utilization efficiency of resources, low cost, and high privacy protection [1], [2]. However, when the cloud sharing is convenient for people to share vast quantities of information, we are also faced with the risk of information being leaked, tampered and forged [3]–[5]. To protect the privacy of data holder, it is very necessary and urgent to encrypt the information before sharing to the cloud server [6], especially the image information that is one of the most popular multimedia. Therefore image encryption technology has attracted great attentions. A variety of encryption techniques such as data encryption standard (DES),

Blowfish, and Rivest-Shamir-Adleman (RSA) can be used to realize image encryption. Nevertheless, the image has intrinsic features of bulk data capacity and high correlation among pixels, thus these traditional encryption algorithms are inappropriate for practical image encryption.

Owing to the chaos-based algorithms having revealed some exceptionally good properties in related aspects concerning complexity, speed, security and computing power, the chaos-based algorithms have provided a novel way to deal with the intractable problem of secure and fast image encryption [12]. Chaos has many characteristics, such as initial condition sensitivity, topologically mixing, and periodic orbits density [7]. Hence, the chaotic signal has natural concealment and unpredictability. In virtue of the excellent characteristics, chaos has been applied in almost every industry or trade: physical random bit generation [8], liquid level sensor [9], optical network security [10], intelligent image protection [11], and especially in image encryption field [12]–[14], [17]–[23]. A fast and secure symmetric image encryption scheme employed the 3D chaotic cat map to shuffle the positions of image pixels [12]. Two-dimensional logistic chaotic map with complicated basin structures and attractors was used for image encryption [13]. An enhanced chaotic tent map was utilized in a novel color image encryption scheme that revealed high security [14]. Various optical image encryption and hiding techniques contributed splendid research triumphs as providing high-speed parallel processing capacity and multiple dimensions hiding ability of image data, such as fractional Fourier transform, Fresnel transform, joint transform correlator, and off-axis holography system [15], [16].Integrating the advantages of both optical transform and chaos system, a double optical image encryption scheme was proposed [17]. Compared to numerical simulations, hardware implementation for chaos-based secure image encryption is difficult to realize, thus some scholars attempted to implement myriad image encryption schemes on hardware platform to address this challenge, such as on advanced reduced instruction set computer machine (ARM) [18], [19], and on field-programmable gate array (FPGA) [20], [21]. Nevertheless, the aforementioned image encryption schemes are all implemented on the traditional chaotic systems, which are restricted by low speed, fast attenuation, and high implementation cost [23].

To dispose the problems of traditional chaos mentioned above, optical chaos was introduced into image encryption [22], which has larger bandwidth, slower attenuation, faster speed, higher complexity, and higher security [24], [25]. Therefore, optical chaos has a commendable application prospect in the field of image encryption. We adopted vertical-cavity surface emitting lasers (VCSELs) to constitute a fast and secure symmetric image encryption-then-transmission scheme [22]. Afterwards, a novel image encryption algorithm based on a cascade-coupled semiconductor ring lasers system was completed [23].However, the above schemes focused on theoretical research, there are almost no schemes on image encryption based on optical chaos in experiment. The direct cause behind this is that compared to numerical simulation, it is formidable to achieve hardware implementation for such a color image encryption and transmission system based on optical chaos. Consequently, we have noted that no experimental works combined with the advantages of optical chaos and hardware implementation are reported.

In this paper, to the best of our knowledge, we first experimentally implement a novel color image encryption and transmission system based on all-hardware platform. In view of the fact that (a) ARM-embedded platform has faster speed and lower power consumption, and that (b) the VCSEL subject to positive optoelectronic feedback (POEF) is more flexible and reliable compared with optical injection and optical feedback, we design and implement a novel color image encryption and transmission system combining the advantages of ARM-embedded platform and the VCSEL subject to POEF. Compared with the complex cascade laser system structure in the [22], [23], a VCSEL under POEF structure in this paper is more convenient, effective and cost-saving in the actual hardware implementation environment. Our system is mainly composed of three parts: the laser module, the hardware board module, and the cloud service module. Among them, the hardware board module is made up of analog to digital conversion (ADC) board and ARM-embedded board. In the experiment, we adjust the parameters of VCSEL to obtain the optical chaotic output required by the encryption key. The core chip reads the data of optical chaos through the ADC module. In the image encryption scheme, the improved gravity model is used to confuse the positions of the original image, and then the double sine map and “XOR plus mod” operation are wielded to diffuse the values of scrambled image, which has better image encryption effect compared to [22]. After that, the encrypted image is secretly shared to cloud services and can be decrypted by our

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JPHOT.2020.3020077, IEEE Photonics Journal

hardware. Both experimental and simulation results with security analysis are demonstrated. Therefore, this paper contributes a novel practicable method for the protection of industrial information, and provides a prototype machine for reference in the design of industrial and commercial information security products.

The rest of this paper is organized as follows. In Section 2, the experiment setup is introduced in detail. In Section 3, the experiment methods are introduced and studied. In Section 4, the experiment results are exhibited and evaluated. Finally, concluding remarks are summarized in Section 5.

2. Experiment Setup

The schematic diagram of our experimental setup is expatiated in Fig. 1. A 1550-nm VCSEL subject to POEF is used in this experiment with a threshold current of 2.1 mA. The VCSEL is driven by an ultra-low-noise and high-accuracy current source (ILX-Lightwave LDC-3724B). Throughout the process of the experiment, the laser temperature is steady at 22.5 °C. In order to make the output of the laser chaotic, the feedback strength is fixed at 0.21, the delay feedback is fixed at 2.5 ns, and the bias current is fixed at 5.4 mA. The output of laser is split into two parts after passing through an optical isolator (OI, isolation $>$ 55 dB) and a beam splitter (BS). One part is transformed into an electronic signal and then fed back to the laser to form a delayed positive feedback loop comprised of a variable attenuator (VA), a photoelectronic detector (PD, Agilent 83440B), and an electronic amplifier (EA, Agilent 83006A). Meanwhile, the other part is transmitted to the ADC module via a PD (New Focus 1544-B). Here, we adopt AD9226 chip and its corresponding peripheral circuit to form the ADC module, which can convey the collected optical chaotic data to the image encryption and decryption module. Our hardware experiment platform of Samsung Exynos4412 is shown in Fig. 2. We debug programs in the exploitation environment of Ubuntu 12.04.2 with VMware 10.0.1.

As we can see from Fig. 1, user1 operates the computer1 and transfers the original image into the image encryption and decryption module (IEDM) via USB drive1. The original image can be shuffled and diffused by applying improved gravity model and double sine map in the IEDM after entering a 16-byte encryption key by user1. After that, user1 can copy the encrypted image from IEDM to computer1 using USB drive1. In this circumstance, user1 can upload the encrypted image to the cloud server for sharing. For the sake of acquiring clear image, user2 can download the encrypted image from the cloud server to computer2. Only after obtaining the authorization of user1, user2 can obtain the correct 16-byte key

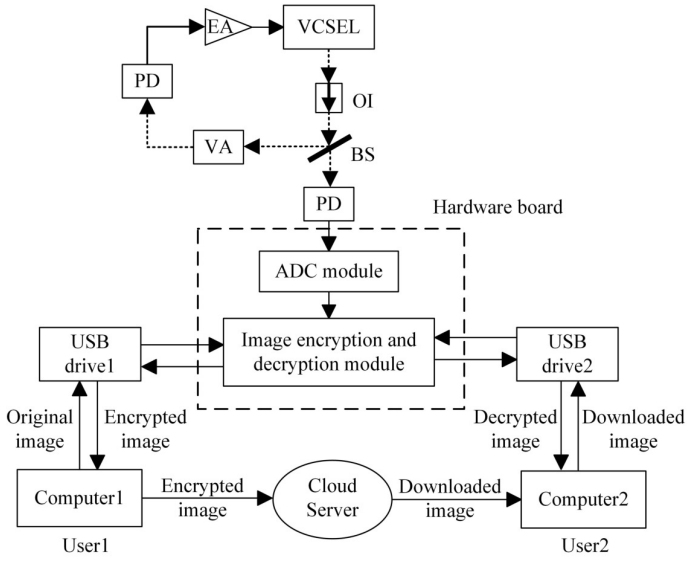

Fig. 1. The schematic diagram of experimental setup. VCSEL: vertical-cavity surface-emitting laser; OI: optical isolator; BS: beam splitter; VA: variable attenuator; PD: photoelectric detector; EA: electronic amplifier; ADC: analog to digital conversion; USB: universal serial bus.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JPHOT.2020.3020077, IEEE Photonics Journal

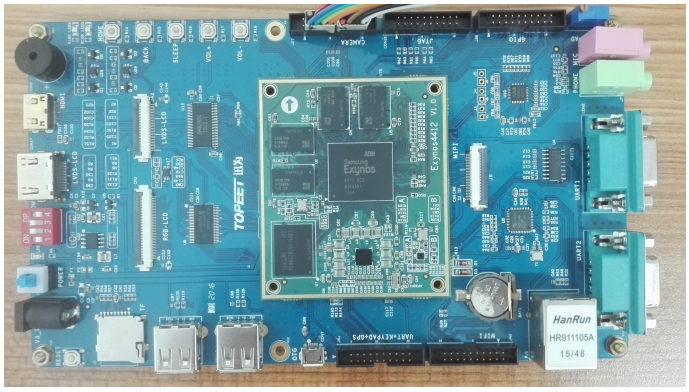

Fig. 2. The hardware experimental platform of Samsung Exynos 4412.

used for decryption. Here, the downloaded image is transferred from computer2 to IEDM via USB drive2. The IEDM decrypts the downloaded image with the correct key, and then user2 can deliver the decrypted image to computer2 by USB drive2. Afterwards, user2 obtains a clear decrypted image containing all the information of user1's original image. Therefore, a novel color image encryption and transmission system using optical chaos based on ARM-embedded platform is realized. The important thing to note here is that the IEDM can store the 16-byte optical chaos key needed in the encryption process at the preset address. This 16-byte optical chaos key is collected at the moment when the image is encrypted. In other words, the key will be different when the image is encrypted at different times. The IEDM can store substantial keys, and different encrypted images at different times correspond to their respective keys, which are called different encryption modes. The user can encrypt successfully with the key of the corresponding address, otherwise, the encrypted image will be decrypted incorrectly. And if the 16-byte optical chaotic key in the IEDM is deleted, the encrypted image can not be decrypted properly as well. Table I lists the 16-byte keys and their addresses of different encryption modes.

TABLE I
OPTICAL CHAOS KEYS AND THEIR ADDRESSES OF DIFFERENT ENCRYPTION MODES.

Address	Optical Chaos Key															
00000000	00	29	2A	5E	FD	2F	2A	FF	52	2D	00	99	2D	37	7F	59
00000010	00	6E	7A	6B	2B	2B	2B	2F	2D	FE	16	69	5F	2E	2B	2D
00000020	34	2D	2C	2A	2E	2B	B2	00	6E	67	2C	00	6A	2C	6A	2B
00000030	2C	30	2D	95	6A	42	FB	80	55	00	2A	00	BA	2C	2C	D5
00000040	00	AF	00	3D	5A	6E	2B	2C	86	A6	65	2D	2A	56	99	39

3. Theoretical Model

In this section, the rate equation model for the laser system and the encryption methods used in the application will be described in detail. We design the mechanism of secret key generation. The color image is separated into its three components RGB (Red, Green, Blue), and we make use of the improved gravity model to scramble the pixel positions of the three components R, G, B. Besides, we exploit the double sine map and the "XOR plus mod" to diffuse the pixel values of the three scrambled components. In the end, the methods in the theoretical model are implemented on ARM-embedded platform.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JPHOT.2020.3020077, IEEE Photonics Journal

3.1. Rate Equation Model for VCSEL with POEF

Under such a proposed scheme, our rate equation model is based on the spin-flip model (SFM) [26]. The rate equations for VCSEL with POEF can be expressed as [27]:

$$\frac{dE_{x,y}}{dt} = k(1+i\alpha)[(N-1)E_{x,y} \pm inE_{y,x}] \mp (\gamma_a + i\gamma_p)E_{x,y} + F_{x,y} \tag{1}$$

$$\frac{dN}{dt} = -\gamma_e N(1+P) + \gamma_e \mu[1+\eta\frac{P(t-\tau)}{P_0}] - i\gamma_e n(E_y E_x^* - E_x E_y^*)] \tag{2}$$

$$\frac{dn}{dt} = -\gamma_s n - \gamma_e nP - i\gamma_e N(E_y E_x^* - E_x E_y^*)] \tag{3}$$

where the subscripts x and y stand for x linear polarized mode and y linear polarized mode, respectively. E is the slowly varied complex amplitude of the field, N is the total carrier inversion between the conduction and valence bands, and n accounts for the difference between carrier inversions for the spin-up and spin-down radiation channels, k is the cavity delay rate, α is the line-width enhancement factor, γ_e is the decay rate of total carrier population, γ_s is the spin relaxation rate, γ_a is the linear anisotropy of dichroism, and γ_p is the linear birefringence rate, respectively. η is the feedback index corresponding to the strength of feedback, τ is the optical feedback delay time, μ is the normalized injection current, $P = |E_x|^2 + |E_y|^2$ is the normalized output power. Ultimately, the effect of spontaneous emission noise ($F_{x,y}$) is included by introducing a zero mean complex Gaussian noise source. $F_{x,y}$ can be defined by following equations [28]:

$$F_x = \sqrt{\beta_{sp}/2}(\sqrt{N+n}\xi_1 + \sqrt{N-n}\xi_2) \tag{4a}$$

$$F_y = -i\sqrt{\beta_{sp}/2}(\sqrt{N+n}\xi_1 - \sqrt{N-n}\xi_2) \tag{4b}$$

where β_{sp} is the spontaneous emission rate, and $\xi_{1,2}$ are complex Gaussian white noises with zero mean.

The rate equations (1)-(4) can be numerically solved by fourth-order Runge-Kutta algorithm. During the calculation, the used parameters of VCSEL are given as follows: k = 300 ns^{-1}, α = 3, γ_e = 1 ns^{-1}, γ_p = 192.1 ns^{-1}, γ_a = 1 ns^{-1}, γ_s = 1000 ns^{-1}, τ = 2.5 ns, η = 0.21, μ = 2.5, β_{sp} = 10^{-6} ns^{-1}.

3.2. Secret Key Definition

A secure cryptographic system is often extremely sensitive to the secret key, thus the cipher-text ought to possess a close correlation with the key. For this purpose, an ideally key generation mechanism is devoted in our encryption system. In the key mechanism, the secret key (represented as K_E) is built by two portions. One is optical chaotic sequence generated from VCSEL. We randomly pick out sixteen 8-bit long binary sequences (represented as K_O). Simultaneously, the other is a string of sixteen characters input by the user. This sixteen characters can also be indicated as sixteen 8-bit long binary sequences (represented as K_U). Hence there must be a transform from K_O and K_U to K_E in the mechanism, with the purpose of protecting the key from opponent's attacks. The key generation mechanism can be described as follows:

At first we mix the K_O and K_U via the XOR operation, which can be defined as:

$$K_E = K_O \oplus K_U \tag{5}$$

Furthermore, the cryptographic control parameters (x_0, y_0, z_0, C_1, C_2, G, r_1, r_2) can be obtained by means of the key K_E. Among them, x_0, y_0, z_0, C_1, C_2, G dominate the permutation process, and r_1, r_2 control the diffusion process. The cryptographic control parameters of the color image encryption system can be

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JPHOT.2020.3020077, IEEE Photonics Journal

gained by the following formulas:

$$\begin{cases} x_0 = round(((K_E(1)+K_E(2))/K)\times(L-1))+1 \\ y_0 = round(((K_E(3)+K_E(4))/K)\times(L-1))+1 \\ z_0 = round(((K_E(5)+K_E(6))/K)\times(L-1))+1 \\ C_1 = round(((K_E(7)+K_E(8))/K)\times(L-1))+1 \\ C_2 = round(((K_E(9)+K_E(10))/K)\times(L-1))+1 \\ G = (((K_E(11)+K_E(12))/K)+7)\times 10^{12} \\ r_1 = ((K_E(13)+K_E(14))/K)\times 0.2+0.5 \\ r_2 = ((K_E(15)+K_E(16))/K)\times 0.4+1.4 \end{cases} \tag{6}$$

where $K_E(i)$ is the ith 8-bit long binary sequence in K_E; $K = M \times L - 1$, M and L represent the width and height of the image, respectively. Here, x_0, y_0, z_0, C_1, C_2 are all the integers from 1 to 256; G, r_1 and r_2 are accurate to the eighth decimal place. The definition of parameter range will be specified in detail later.

3.3. Permutation Process

One of the most valid methods to encrypt image is to scramble the image. The original image is scrambled and transformed into a cluttered and illegible image. Inspired by the law of gravity, a novel method of image scrambling is applied to the field of image encryption [29]. Hypothesizing the image is located on the plane $z = 0$ in three-dimensional space, each pixel of image has its own mass, and the position (i, j, 0) of each particle has a function with its mass. In addition, suppose a particle P is located at (x_0, y_0, z_0) outside the plane of image, and its mass also has a relationship with the position of image particle. Thus, there is a gravitation between every particle of image and particle P. The improved gravity model can be expressed as follows:

$$F_{ij} = G\frac{m_0(i,j)m_{ij}}{(x_0-i)^2+(y_0-j)^2+z_0^2} \tag{7a}$$

$$m_0(i,j) = 3\times((i^3+2j^2+C_1)\ mod\ 256) \tag{7b}$$

$$m_{ij} = 4i^2+j^2+C_2 \tag{7c}$$

where G is gravity coefficient, $m_0(i,\ j)$ is the mass of particle P, (x_0, y_0, z_0) is the location of particle P, m_{ij} is the mass of pixel, (i, j) is the location of pixel, C_1 and C_2 are the constants, *mod* returns the remainder after division. To guarantee that the denominator in Eq. 7(a) is not zero, the location z_0 cannot be equal to zero. Meanwhile, in order to conform the gravity model theory and make the scrambling process work preferable, we set the parameters x_0, y_0, z_0, C_1, and C_2 be the arbitrary integers between 1 and 256, the parameter G be the arbitrary value between 7×10^{12} and 8×10^{12}, which is accurate to the eighth decimal place.

The calculated gravitational values are sorted in ascending order. Then we assign the index of the sorted vector to the original vector, where the index changes the location of pixels. This permutation process is iterated five times to receive the ultimate scrambled result. So far, the permutation process has been completed. However, the scrambled image has a frail resistance for the statistical attack, thus a diffusion process that can surmount this flaw is extraordinarily indispensable.

3.4. Diffusion Process

Diffusion algorithm can promote image pixels to interact with each other. If one pixel changes, then it will change another pixel until most of the pixels have been changed, causing avalanche effect that makes the encrypted image to be utterly dissimilarity. In our diffusion process, the pixel value is changed by double sine map and "XOR plus mod" operation.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JPHOT.2020.3020077, IEEE Photonics Journal

The double sine map is a cascade chaotic system that consists of two identical sine map [30], [31], which can be expressed as following formula:

$$x_{n+1} = r_2 \sin(\pi r_1 \sin(\pi x_n)) \tag{8}$$

where r_1 and r_2 are two parameters. In diffusion encryption, the output of the double sine map demanded to be chaotic.

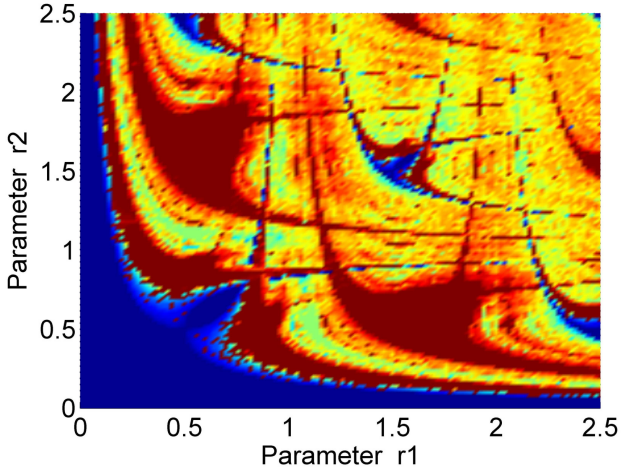

Fig. 3. The mapping of the dynamic behavior of double sine map in the parameter space of (r_1, r_2).

Fig. 3 shows the mapping of the dynamic behavior of double sine map in the parameter space of r_1 and r_2. From the Fig. 3, the crimson domains represent chaotic behaviors of the double sine map. There are a great deal of regions in chaotic behavior, and we select $r_1 \in [0.5, 0.7]$ and $r_2 \in [1.4, 1.8]$ for stronger key space and better resistance to brute force attack.

An appropriate chaotic value is acquired from the above double sine map, then the value is digitized by amplifying with a proper scaling and sampling, determined as follows:

$$\Psi(n) = D \times x(n) \tag{9}$$

where D is the magnification, which is determined to be 150. Then we can obtain the encrypted image by the XOR-plus-mod method, defined as following formula:

$$E(n) = \Psi(n) \oplus \{[I(n) + \Psi(n)] \ mod \ T\} \oplus E(n-1) \tag{10}$$

where *E(n)* is the value of the current XOR-ed, *E(n-1)* is the preciously output cipher-pixel, *I(n)* is the currently operated pixel, T is the color level.

3.5. Encryption and Decryption Process

The entire image encryption process is completed by the following eight steps:

Step 1: Separate the color image in trichromatic RGB value. Execute the following 2-7 steps for each RGB component.

Step 2: The optical chaos key (K_O) is exclusive or operated with the user key (K_U) to obtain the encryption key (K_E).

Step 3: Take advantage of K_E to calculate control parameters in the permutation and diffusion processes.

Step 4: Parameters x_0, y_0, z_0, C_1, C_2, and G are substituted into Eq. 7(a-c) to calculate gravity values.

Step 5: These gravity values are sorted in ascending order and the corresponding indexes are recorded. Then the ranked indexes are used to change the locations of pixels so as to complete a permutation process. Iterate this process five times, and obtain the scrambled image.

Step 6: Exploit the parameters r_1 and r_2 for the chaotic data of the double sine map described in Eq. 8.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JPHOT.2020.3020077, IEEE Photonics Journal

Step 7: Properly amplify the chaotic data of Eq. 8, and then the scrambled image and the magnified chaotic data are utilized to do the calculation of Eq. 10. The diffusion image in which the pixel values are changed is obtained. Iterate the Step 4-7 two times to get the final encrypted image.

Step 8: Merge three scrambled and diffused RGB components, the final encrypted image is obtained.

The decryption process is resemblant to the encryption process elaborated above, thus the decryption process is the inverse encryption process.

4. Results And Discussion

This section exhibits the dynamic characteristics of the laser, as well as the results of image encryption/decryption and cloud security sharing. The experimental results and numerical simulation results are furnished simultaneously with comparative discussions.

4.1. Dynamic Behavior of VCSEL

To guarantee the high security of the encryption algorithm, the laser must has chaotic behaviors. Fig. 4 shows the dynamic characteristics of the laser worked, where Fig. 4(a) and Fig. 4(b) are the red and blue figures in first and second row, revealing the experiment and simulation results, respectively, which embody time series, power spectra, and phase portraits. As can be descried from the time series, there are random intensity pulses, resemble to the intensity fluctuation of noise. The power spectra are broad peak continuous spectrum. Furthermore, rambling dots are randomly distributed over a wide range in the phase portraits. Judging by the typical chaotic features of Fig. 4, the chaotic behaviors of VCSEL are actualized in both experiment and simulation.

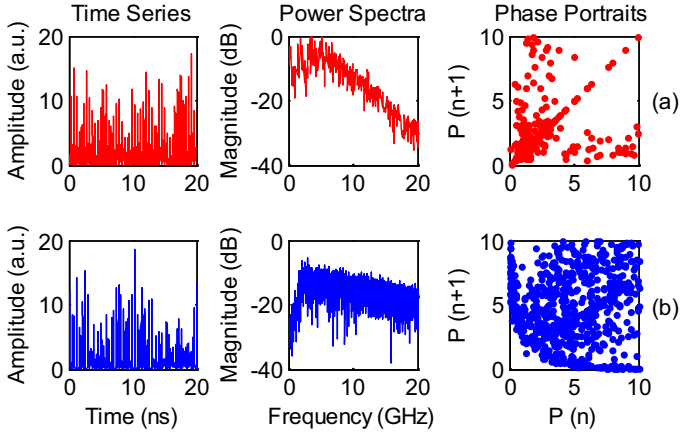

Fig. 4. The dynamic behavior of VCSEL on time series, power spectra and phase portraits. (a) Experiment results; (b) Numerical simulation results.

4.2. Image Encryption/Decryption Results and Security Sharing in Cloud Services

The encryption of original image is conducted on a 256×256 colored Baboon. Users can expediently upload their encrypted files to the cloud server and share the extract code to a designated person. The encrypted files can be checked anytime and anywhere by the designated person, which not merely realizes the data sharing, but also ensures the privacy efficaciously. In our work, the images encrypted by experiment and numerical simulation are not only shared securely in the cloud services but also correctly decrypted.

Fig. 5 shows the experiment and simulation results of image encryption/decryption and security sharing in cloud services. As we can see from Fig. 5(b), the encrypted and uploaded image is completely unrecognizable, and the original image cannot be conjectured from the visual sense. Thus, the raw data are under a high-level security protection. Fig. 5(c) represents the encrypted image downloaded from cloud services. We can estimate whether there is any error in the process of cloud security sharing by making difference between uploaded image and downloaded image. It can be seen from Fig. 5(d), an entire black

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JPHOT.2020.3020077, IEEE Photonics Journal

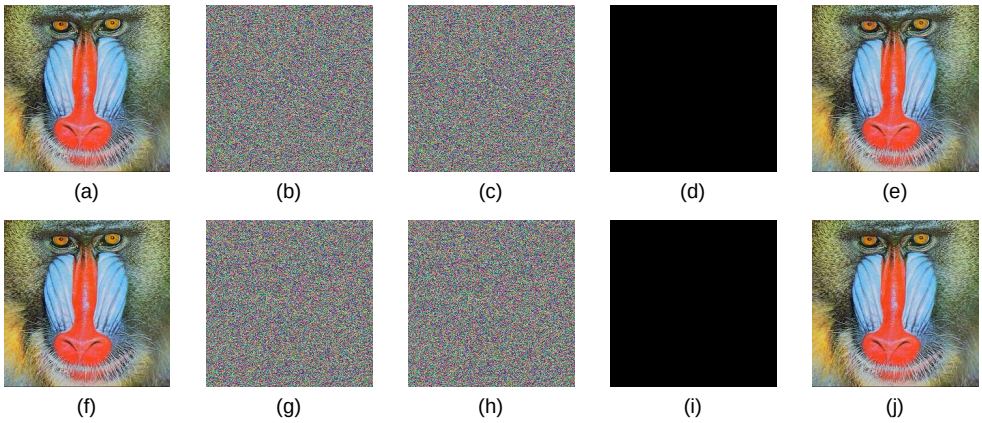

Fig. 5. The experiment and simulation results of image encryption/decryption and security sharing in cloud services. (a)-(e) Original image, encrypted and uploaded image, downloaded image, difference image, and decrypted image in experiment; (f)-(j) Original image, encrypted and uploaded image, downloaded image, difference image, and decrypted image in numerical simulation.

image signifies that the value of each pixel in difference image is 0. The result of Fig. 5(d) testifies that the encrypted image can be transmitted almost without error in cloud services. Fig. 5(e) catches the decrypted image that is nearly identical to original image. Meantime, the numerical simulation results are demonstrated in Figs. 5(f)-(j). Through the results of ten times encryptions and decryptions, we find that there are 0.1268% and 0.1202% differences between decrypted image and original image in the experiment and simulation, respectively. Accordingly, our system can commendably accomplish the operation of image encryption/decryption and security sharing in cloud services in both experiment and simulation.

5. Security Analysis

High security is the quintessence of image encryption system. A good image encryption system should possess the competence to resist any different types of attacks. For attesting security property, we have carried out diversified attack tests and security analysis in experiment and numerical simulation.

5.1. Key Space Analysis

To provide an encryption algorithm with high security, the key space should be large enough to make exhaustive attacks infeasible. In our proposed image encryption algorithm, the secret key K_E is comprised of sixteen 8-bit long binary sequences, with key space size $2^{8\times16}=2^{128}\approx3.4028\times10^{38}$, which is more than 2^{100}. Compared with the key space size 3.9402×10^{185} and 12×10^{98} in [34], [35], the key space of our algorithm is relatively small due to the limited memory of hardware, but there is still the possibility of improvement in the future. Moreover, opponents may also make exhaustive attacks directly by speculating cryptographic control parameters. For the permutation process, the parameters x_0, y_0, z_0, C_1 and C_2 are all the arbitrary integers from 1 to 256, hence the key space $KS_{x_0}=KS_{y_0}=KS_{z_0}=KS_{C_1}=KS_{C_2}=2^8$. And the parameter G is the arbitrary value between 7×10^{12} and 8×10^{12}, which is accurate to the eighth decimal place, thus the key space $KS_G=10^8$. Similarly, for the diffusion processes, the map parameters $r_1\in[0.5, 0.7]$ and $r_2\in[1.4, 1.8]$ with a step of 10^{-8}, so the key space $KS_{r_1}=2\times10^7$ and $KS_{r_2}=4\times10^7$. After that, the total key space $KS=KS_{x_0}KS_{y_0}KS_{z_0}KS_{C_1}KS_{C_2}KS_GKS_{r_1}KS_{r_2}\approx8.79\times10^{34}$. Accordingly our proposed image encryption algorithm has a large enough key space to resist the exhaustive attack.

5.2. Statistical Analysis

On some occasions, the opponent has a certain probability to reconstruct the image according to the distribution of statistical characteristics. Hence, an ideal cryptosystem must be robust against statistical attacks. In this paper, we validate the proposed encryption system can resist statistical attacks via the histogram and the correlation of two adjacent pixels.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JPHOT.2020.3020077, IEEE Photonics Journal

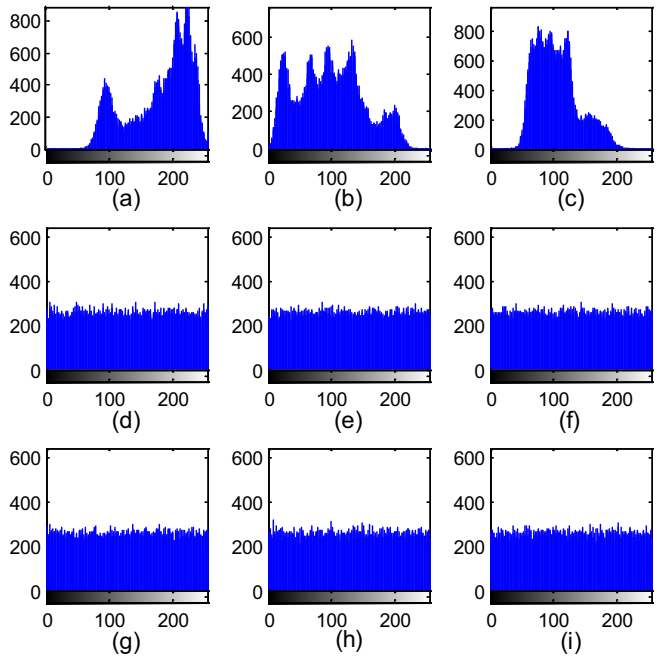

Fig. 6. Histograms of the original and encrypted images of Lena. (a)-(c) Original R, G, B images; (d)-(f) Encrypted R, G, B images in experiment; (g)-(i) Encrypted R, G, B images in simulation.

The histogram of an image is a momentous characteristic in image analysis, which reveals the distribution information of pixel values. Figs. 6(a)-(c) display the histograms of RGB colors for the original image. It is known from these figures that the histograms of the original image take on palpable characteristic peaks, which can provide the attackers some information of the original image. Figs. 6(d)-(f) present the histograms of the encrypted image in experiment, which are exceedingly uniformed and remarkably different from the original images. Figs. 6(g)-(i) represent the results of numerical simulation and show the resemblant outcomes to Figs. 6(d)-(f).

Furthermore, to test the correlation of adjacent pixels on vertical, horizontal, and diagonal directions, we randomly choose 10000 pairs of adjacent pixels from the images in both experiment and numerical simulation. The formula for calculating the correlation coefficients of pixels was illustrated in [12], [33].

The elaborated results of correlation coefficients for three orientations with R, G, B components of the original image and their corresponding ciphered images are listed in Table II.

TABLE II
CORRELATION COEFFICIENTS OF ADJACENT PIXELS FOR THE HORIZONTAL, VERTICAL AND DIAGONAL ORIENTATIONS IN ORIGINAL, EXPERIMENTAL AND SIMULATIVE ENCRYPTED IMAGES.

Correlation	Original plaintext image			Experimental ciphertext image			Simulated ciphertext image		
coefficients	R	G	B	R	G	B	R	G	B
Horizontal	0.7757	0.6810	0.8122	0.0288	0.0218	0.0336	0.0143	0.0004	0.0740
Vertical	0.8383	0.7579	0.8518	0.0018	0.0096	0.0084	0.0094	0.0035	0.0072
Diagonal	0.7779	0.6737	0.8002	0.0083	0.0062	0.0012	0.0029	0.0088	0.0077

Table II clearly presents that the correlation coefficients of the original image are close to 1. By contrast, the absolute values of all encrypted image correlation coefficients are nearly 0, intimating the adjacent pixels in the encrypted image virtually have no correlation.

Consequently, the histogram distributions of the encrypted images and the correlation of adjacent pixels

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JPHOT.2020.3020077, IEEE Photonics Journal

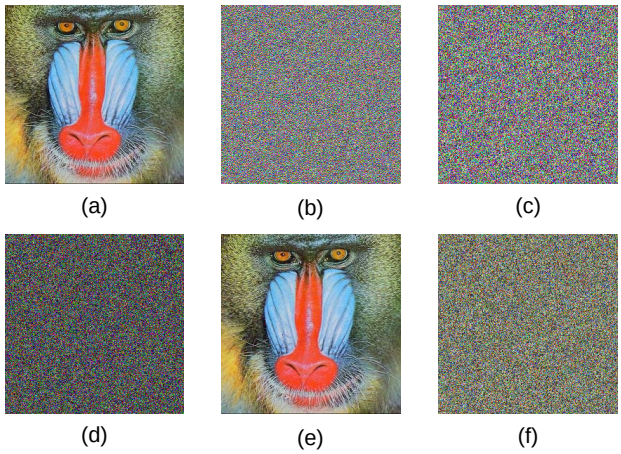

Fig. 7. Key sensitivity test in experiment. (a) Original image; (b) Encrypted image with Key1=98765432109876ab; (c) Encrypted image with Key2=98765432109876ac; (d) Difference between Fig. 7(b) and Fig. 7(c); (e) Decrypted image with Key1=98765432109876ab; (f) Decrypted image with Key3=88765432109876ab.

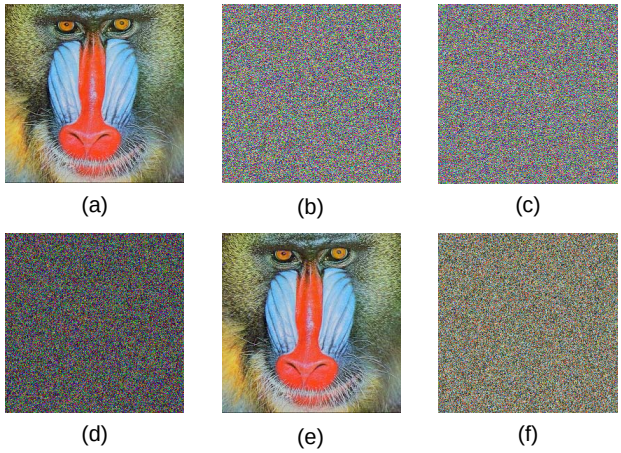

Fig. 8. Key sensitivity test in numerical simulation. (a) Original image; (b) Encrypted image with Key1=98765432109876ab; (c) Encrypted image with Key2=98765432109876ac; (d) Difference between Fig. 8(b) and Fig. 8(c); (e) Decrypted image with Key1=98765432109876ab; (f) Decrypted image with Key3=88765432109876ab.

are taken into account comprehensively, and our proposed system can resist statistical attacks very well.

5.3. Key Sensitivity Analysis

A splendid encryption system will be extremely sensitive to the secret key. The significance of key sensitivity is that even if the secret key has a tiny change, it will cause the encrypted image to be completely different. For the proposed encryption system, the evaluation of secret key sensitivity is made.

Fig. 7 displays the test of key sensitivity, where Fig. 7(a) is the original image. The Key1 “9876543210987 6ab” is utilized to encrypt the original image, and the encryption result is shown in Fig. 7(b). In the test, the sixteen bit key is changed by one bit, and the Key2 “98765432109876ac” is obtained. Fig. 7(c) shows the result of encrypted image with Key2. Afterwards the difference between Fig. 7(b) and Fig. 7(c) is revealed in Fig. 7(d). The difference of the image encrypted by Key1 and Key2 is 99.6424%, which justifies a high key sensitivity. In addition, the encrypted image of Fig. 7(b) is decrypted by the Key1 and Key3

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JPHOT.2020.3020077, IEEE Photonics Journal

"88765432109876ab", which have only a change of one bit as well. As seen from the Fig. 7(e), the image decrypted by Key1 is almost identical to the original image. Nevertheless the Fig. 7(f) decrypted by Key3 is hardly discernible. In the meantime the test of key sensitivity in numerical simulation is presented in Fig. 8. By comparison, it is found that the simulation results are consistent with the experimental results. The above tests adequately illustrate that the proposed encryption system is extremely sensitive to the key.

5.4. Information Entropy Analysis

As a measure of the complexity of a system, information entropy represents the uncertainty of random variables and is the average amount of information after eliminating redundancy, which is proposed by C. E. Shannon inspiring from thermodynamics and can be calculated by the following formula [33]:

$$H(x) = -\sum_{i=0}^{2^n-1} P(x_i)\ log_2 P(x_i) \tag{11}$$

where x is the information source, and $P(x_i)$ is the probability of symbol x_i. For an image, there will be 2^8 states of information source with same probability. Hence we can calculate ideal information entropy $H(x) = 8$, which can be treated as truly random. Table III depicts our information entropy results and the comparison results for the same original plaintext image Baboon.

TABLE III
THE RESULTS OF INFORMATION ENTROPY.

Information entropy H(x)	Encrypted image
Experimental results	7.9903
Simulative results	7.9900
Ref. [14]	7.9997
Ref. [32]	7.9993
Ref. [33]	7.9993

As indicated in Table III, the information entropy values of encrypted images in experiment and simulation are very close to the theoretical ultimate 8. Contrast with the results in Refs. [14], [32], [33], our entropy values are slightly lower but exceedingly approach to ideal value 8. Therefore, our proposed encryption system can fortuitously divulge the information with low feasibility and almost negligible.

5.5. Differential Attack Analysis

Ordinarily, an antagonist can modify only one pixel of the original image to observe the change of encryption results. Through contrasting the difference, the antagonist can clarify an amount of valuable information from two encrypted images and original image. A good encryption system should guarantee that two encrypted images are different, even if there is only one difference of a pixel between them. To examine the performance of one pixel change on a encrypted image by the proposed scheme, the number of pixels change rate (NPCR) and the unified average changing intensity (UACI) are two quantitative indicators applied commonly. The NPCR and UACI between two encrypted image E_1 and E_2 can be depicted by the following formulas [33]:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times L} \times 100\% \tag{12}$$

$$D(i,j) = \begin{cases} 0, & E_1(i,j) = E_2(i,j) \\ 1, & E_1(i,j) \neq E_2(i,j) \end{cases} \tag{13}$$

$$UACI = \frac{1}{M \times L} \sum_{i,j} \frac{|E_1(i,j) - E_2(i,j)|}{255} \times 100\% \tag{14}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JPHOT.2020.3020077, IEEE Photonics Journal

where M and L represent the width and height of the image, respectively. Table IV lists the calculated results of NPCR and UACI in experiment and numerical simulation. The data of each component for tested image show that the means of NPCR and UACI are over 99% and 33%. Compared with Ref. [22], this paper can resist differential attack better owing to larger NPCR and UACI, and nearer to ideal values than Refs. [21], [23], [34], [35]. Therefore our system has a good capacity to endure the differential attack.

TABLE IV
THE RESULTS OF NPCR AND UACI.

Calculated value		NPCR(%)	UACI(%)
Experimental encrypted image	R	99.62	33.44
	G	99.60	33.49
	B	99.61	33.46
Simulative encrypted image	R	99.60	33.46
	G	99.62	33.43
	B	99.61	33.42
Ref. [21]	R	99.61	33.46
	G	99.60	33.43
	B	99.64	33.48
Ref. [22]		96.27	24.09
Ref. [23]		99.65	33.32
Ref. [34]		99.60	33.48
Ref. [35]		99.63	33.47

5.6. Robustness Analysis

Encrypted image is inevitably contaminated by various noises when it is transmitted in real communication channels. Meanwhile, the encrypted image in the receiving terminal may be fragmentary due to packet loss, malicious attacks and other problems when it is transmitted over the Internet or in the cloud, resulting in data loss. An image encryption system should be robust enough to resist noise attacks and data loss attacks. The performance of the robustness analysis can be validated by peak signal to noise ratio (PSNR) and mean square error (MSE), which are computed as following formulas:

$$PSNR = 10 \times \log_{10}(\frac{255^2}{MSE}) \tag{15}$$

$$MSE = \frac{1}{M \times L} \sum_{i=1}^{M-1} \sum_{j=1}^{L-1} (I_D(i,j) - I(i,j)) \tag{16}$$

where M and L are the size of image, $I_D(i,j)$ is the pixels of decrypted image, and $I(i,j)$ is the pixels of original image. The smaller value of MSE and higher value of PSNR signify better robustness performance.

Fig. 9 demonstrates the results of noise attack test in experiment, where the encrypted images are contaminated by Gaussian noise with zero mean value and different variances. Fig. 9(a)-(c) are the encrypted images with variance changes from 0.0001 to 0.0005, and Fig. 9(d)-(f) are their corresponding decrypted images, which can be roughly distinguished visually.

For acquainting the performance of noise attack recovery more concretely, the correlation coefficients, MSE, and PSNR are studied in Table V. Both in experiment and simulation, the PSNRs are more than 30, the decrypted images have high correlation coefficients. Contrast our results with Ref. [32], the lower MSE, higher PSNR and correlation coefficients are obtained, which means our decrypted images are closer to original images. Hence, our encryption algorithm has a robustness property on resisting noise attack.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JPHOT.2020.3020077, IEEE Photonics Journal

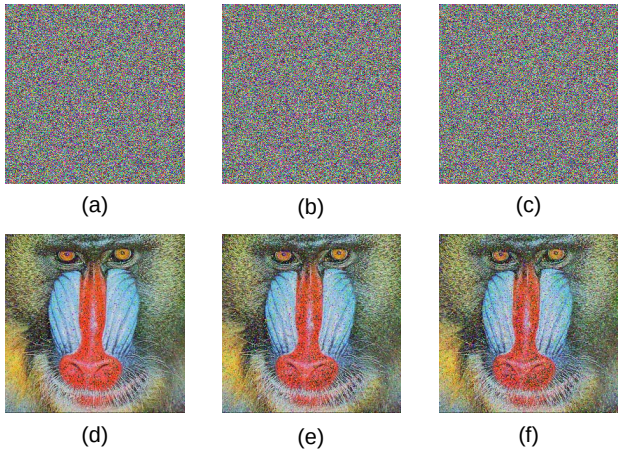

Fig. 9. Noise attack test in experiment. (a) Encrypted image with Gaussian noise (Mean=0, Variance=0.0001); (b) Encrypted image (Mean=0, Variance=0.0003); (c) Encrypted image (Mean=0, Variance=0.0005); (d)-(f) Decrypted image of (a)-(c).

TABLE V
THE RESULTS OF NOISE ATTACK TEST.

Noise attack	Variance	MSE	PSNR	Correlation
Experimental results	0.0001	32.2246	33.0489	0.7868
	0.0003	47.4294	31.3703	0.7465
	0.0005	57.3107	30.5484	0.6556
Simulative results	0.0001	31.4787	33.1506	0.7800
	0.0003	48.8577	31.2415	0.7073
	0.0005	56.6178	30.6013	0.6410
Ref. [32]	0.0001	48.1323	31.3064	0.6271
	0.0003	66.4563	29.9054	0.5392
	0.0005	74.8654	29.3880	0.4910

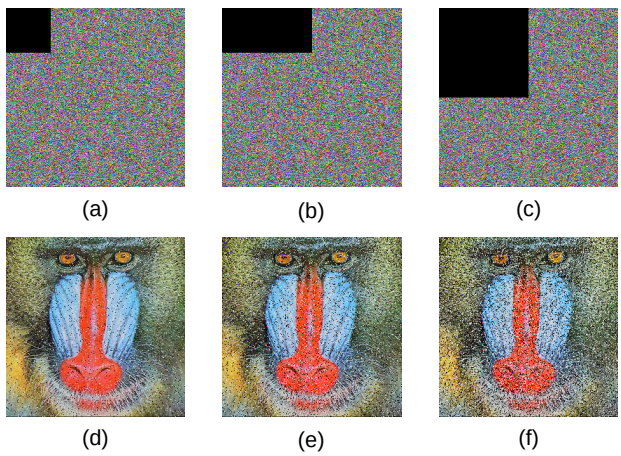

Fig. 10. Data loss attack test in experiment. (a) Encrypted image with 64×64 $(1/16)$ data loss; (b) Encrypted image with 64×128 $(1/8)$ data loss; (c) Encrypted image with 128×128 $(1/4)$ data loss; (d)-(f) Decrypted image of (a)-(c).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JPHOT.2020.3020077, IEEE Photonics Journal

TABLE VI
THE RESULTS OF NOISE ATTACK TEST.

Data loss attack	Loss pixels	MSE	PSNR	Correlation
Experimental results	64×64 $(1/16)$	8.4737	38.8501	0.6910
	64×128 $(1/8)$	16.6073	35.9278	0.6905
	128×128 $(1/4)$	31.3479	33.1687	0.6878
Simulative results	64×64 $(1/16)$	8.1962	38.9947	0.6911
	64×128 $(1/8)$	15.8545	36.1293	0.6899
	128×128 $(1/4)$	31.5531	33.1404	0.6896
Ref. [32]	64×64 $(1/16)$	8.0500	39.1800	0.6900
	64×128 $(1/8)$	15.7900	36.1600	0.6200
	128×128 $(1/4)$	30.9500	33.2900	0.3500

Fig. 10 reveals the results of data loss attack test in experiment. Fig. 10(a)-(c) are the encrypted images with pixels loss of 64×64 $(1/16)$, 64×128 $(1/8)$, and 128×128 $(1/4)$, and Fig. 10(d)-(f) are their corresponding decrypted images, which can be roughly identified.

To grasp more details of decrypted image, the correlation coefficients, the MSE, and the PSNR are listed in Table VI. Both in experiment and simulation, the PSNRs are more than 33, and the decrypted images have high correlation coefficients. Compare to Ref. [32], the higher correlation coefficients are gained, which means our encryption algorithm has a robustness property on resisting data loss attack. Therefore, the implemented system has good robustness to noise attack and data loss attack.

6. Conclusion

In this paper, we experimentally implement a novel color image encryption and transmission system based on optical chaos and realize it on ARM-embedded platform. In our system, the optical chaotic signals are reached from the VCSEL and converted to the digitized data by ADC module. We investigate the dynamic behaviors of VCSEL and chaotic output is observed with appropriate parameters in the experiment. The secret key that plays a decisive effect in the encryption process is randomly selected from digital optical chaotic data. In the ARM-embedded platform, the original image is confused and diffused by using the improved gravity model and the double sine map. After that the encrypted image is securely shared on cloud services. The downloaded image from the cloud services can be fully decrypted by our hardware board. Moreover, we analyze the security of the encryption system. The experiment results show that the implemented system has a large key space to resist exhaustive attacks, uniformed histograms and low correlation coefficients of adjacent pixels to make statistical attacks invalid, high sensitivity to the key and plain image, high information entropy to resist entropy attack, and high values of NPCR and UACI to resist differential attack, which demonstrate high security and good encryption effect. Remarkably, the key space is limited by the memory of hardware system to some extent, and needs to be improved in future work. Meanwhile, the numerical simulation of the proposed system is also investigated in our work. By contrast, the simulation results are in good agreement with the experimental results. Therefore, our implemented system has a potential prospect in the field of industrial and commercial information encryption.

References

[1] G. Q. Hu, D. Xiao, T. Xiang, S. Bai, and Y. S. Zhang, "Compressive sensing based privacy preserving outsourcing of image storage and identity authentication service in cloud," *Inf. Sci.*, vol. 387, pp. 132-145, May 2017.
[2] G. Brunette, and R. Mogull, "Security guidance for critical areas of focus in cloud computing v2. 1," *Cloud Security Alliance*, pp. 1-76, 2009.
[3] X. K. Shu, J. Zhang, D. F. Yao, and W. C. Feng, "Fast detection of transformed data leaks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 3, pp. 528-542, Mar. 2016.

[4] C. P. Yan, C. M. Pun, and X. C. Yuan, "Quaternion-Based image hashing for adaptive tampering localization," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 12, pp. 2664-2677, Dec. 2016.

[5] A. Sharma, and S. Sundaram, "On the exploration of information from the DTW cost matrix for online signature verification," *IEEE Trans. Cybern.*, vol. 48, no. 2, pp. 611-624, Feb. 2018.

[6] Z. Yan, W. X. Ding, X. X. Yu, H. Q. Zhu, and R. H. Deng, "Deduplication on encrypted big data in cloud," *IEEE Trans. Big Data*, vol. 2, no. 2, pp. 138-150, Jun. 2016.

[7] R. L. Devaney, *An Introduction to Chaotic Dynamical Systems*, 2nd ed. Boulder, Colorado: Westview Press, 2003.

[8] S. Y. Xiang, B. Wang, Y. Wang, and Y. Hao, "2.24-Tb/s Physical Random Bit Generation With Minimal Post-Processing Based on Chaotic Semiconductor Lasers Network," *J. Lightwave Technol.*, vol. 37, no. 16, pp. 3987-3993, Aug. 2019.

[9] D. Wang, Z. P. Xue, B. Q. Jin, Y. Wang, Y. Zhang, and M. J. Zhang, "Chaotic Correlation Optical Fiber Liquid Level Sensor," *J. Lightwave Technol.*, vol. 37, no. 3, pp. 1023-1028, Feb. 2019.

[10] C. F. Zhang, W. Zhang, C. Chen, X. J. He, and K. Qiu, "Physical-Enhanced Secure Strategy for OFDMA-PON Using Chaos and Deoxyribonucleic Acid Encoding," *J. Lightwave Technol.*, vol. 36, no. 9, pp. 1706-1712, May 2018.

[11] B. Hu, Z. H. Guan, N. X. Xiong, and H. C. Chao, "Intelligent impulsive synchronization of nonlinear interconnected neural networks for image protection," *IEEE Trans. Ind. Inform.*, vol. 14, no. 8, pp. 3775-3787, Aug. 2018.

[12] G. R. Chen, Y. B. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons and Fractals*, vol. 21, no. 3, pp. 749-761, Jul. 2004.

[13] M. Preishuber, T. Hütter, S. Katzenbeisser, and A. Uhl, "Depreciating motivation and empirical security analysis of chaos-based image and video encryption," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2137-2150, Sept. 2018.

[14] C. X. Zhu, and K. H. Sun, "Cryptanalyzing and improving a novel color image encryption algorithm using RT-Enhanced chaotic tent maps," *IEEE Access*, vol. 6, pp. 18759-18770, Mar. 2018.

[15] S. Liu, C. L. Guo, and J. T. Sheridan, "A review of optical image encryption techniques," *Opt. Laser Technol.*, vol. 57, pp. 327-342, Apr. 2014.

[16] S. M. Jiao, C. Y. Zhou, Y. S. Shi, W. B. Zou, and X. Li, "Review on optical image hiding and watermarking techniques," *Opt. Laser Technol.*, vol. 109, pp. 370-380, Jan. 2019.

[17] Y. S. Zhang and D. Xiao, "Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform," *Opt. Lasers Eng.*, vol. 51, no. 4, pp. 472-480, Apr. 2013.

[18] H. Z. Zheng, S. M. Yu, and J. H. Lü, "Design and ARM platform-based realization of digital color image encryption and decryption via single state variable feedback control," *Int. J. Bifurcation Chaos*, vol. 24, no. 4, p. 1450049, Apr. 2014.

[19] Z. S. Lin, S. M. Yu, J. H. Lü, and G. R. Chen, "Design and ARM-Embedded implementation of a chaotic map-based real-time secure video communication system," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 25, no. 7, pp. 1203-1216, Jul. 2015.

[20] Q. X. Wang, S. M. Yu, C. Q. Li, J. H. Lü, X. L. Fang, and J. M. Bahi, "Theoretical design and FPGA-Based implementation of higher-dimensional digital chaotic systems," *IEEE Trans. Circuits Syst. I*, vol. 63, no. 3, pp. 401-412, Mar. 2016.

[21] S. K. Chen, S. M. Yu, J. H. Lü, G. R. Chen, and J. B. He, "Design and FPGA-Based realization of a chaotic secure video communication system," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 9, pp. 2359-2371, Sept. 2018.

[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. Lightwave Technol.*, vol. 34, no. 22, pp. 5101-5109, Nov. 2016.

[23] J. F. Li, S. Y. Xiang, H. N. Wang, J. K. Gong, A. J. Wen, "A novel image encryption algorithm based on synchronized random bit generated in cascade-coupled chaotic semiconductor ring lasers," *Opt. Lasers Eng.*, vol. 102, pp. 170-180, Mar. 2018.

[24] A. Argyris, D. Syvridis, L. Larger, L. Annovazzi, P. Colet, I. Fisher, J. Garcia, C. R. Mirasso, and K. A. Shore, "Chaos-based communications at high bit rates using commercial fibre-optic links," *Nature*, vol. 438, no. 17, pp. 343-346, Nov. 2005.

[25] V. Annovazzi, 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.

[26] J. M. Regalado, F. Prati, M. S. 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.

[27] Y. Y. Xie, H. J. Che, W. L. Zhao, Y. X. Huang, W. H. Xu, X. Li, and J. C. Li, "Dynamics of 1550-nm VCSELs with positive optoelectronic feedback: theory and experiments,"*IEEE Photonics J.*, vol. 6, no. 6, p. 1502508, Dec. 2014.

[28] L. Wang, Z. M. Wu, J. G. Wu, 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. 2014.

[29] X. Y. Wang, N. Wei, and D. D. Zhang, "A novel image encryption algorithm based on chaotic system and improved Gravity Model," *Opt. Commun.*, vol. 338, pp. 209-217, Mar. 2015.

[30] Y. C. Zhou, Z. Y. Hua, C. M. Pun, and C. L. P. Chen, "Cascade chaotic system with applications," *IEEE Trans. Cybern.*, vol. 45, no. 9, pp. 2001-2012, Sept. 2015.

[31] Z. Y. Hua, B. H. Zhou, and Y. C. Zhou, "Sine-Transform-Based chaotic system with FPGA implementation," *IEEE Trans. Ind. Electron.*, vol. 65, no. 3, pp. 2557-2566, Mar. 2018.

[32] X. L. Chai, Z. H. Gan, and M. H. Zhang, "A fast chaos-based image encryption scheme with a novel plain image-related swapping block permutation and block diffusion," *Multimed. Tools Appl.*, vol. 76, no. 14, pp. 15561-15585, Jul. 2017.

[33] Z. H. Gan, X. L. Chai, D. J. Han, and Y. R. Chen, "A chaotic image encryption algorithm based on 3-D bit-plane permutation," *Neural Comput. Appl.*, vol. 31, no. 11, pp. 7111-7130, May 2019.

[34] X. L. Chai, X. L. Fu, Z. H. Gan, Y. Lu, and Y. R. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Process.*, vol. 155, pp. 44-62, Feb. 2019.

[35] X. L. Chai, X. Y. Zheng, Z. H. Gan, and Y. R. Chen, "Exploiting plaintext-related mechanism for secure color image encryption," *Neural Comput. Appl.*, vol. 32, no. 12, pp. 8065-8088, Jun. 2020.