Image Encryption-Then-Transmission Using DNA Encryption Algorithm and The Double Chaos

Xing-Quan. Fu,[1] Bo-Cheng. Liu,[1] Yi-Yuan. Xie,[1,2,3] Wei. Li,[1] and Yong. Liu[3]

[1]*School of Electronic and Information Engineering, Southwest University, Chongqing 400715, China*
[2]*Chongqing Key Laboratory of Nonlinear Circuits and Intelligent Information Processing, Chongqing 400715, China*
[3]*School of Optoelectronic Information, University of Electronic Science and Technology of Chengdu, Sichuan 611731, China*

Manuscript submitted? This work was supported in part by the 863 program of China under Grant 2015AA016304, by the National Natural Science Foundation of China under Grant No. 61421002, by the National Natural Science Foundation of Chongqing City under Grant Nos. cstc2016jcyjA2002, by the Postdoctoral Science Foundation of China under Grant Nos. 2016M590875, and by the Fundamental Research Funds for the Central Universities under Grants XDJK2014A017 and XDJK2016A011. Corresponding author: Y. Y. Xie (e-mail: yyxie@swu.edu.cn).

Abstract: According to the DNA encryption algorithm and the double-chaotic system which contains the optical chaos and the coupled map lattice (CML) chaotic system, a novel image encryption-then-transmission system is proposed. In the system, with identical chaotic injection from a master laser with two optical feedbacks, two slave lasers (SL1 and SL2) can output similar chaotic signals served as chaotic carrier to transmit image and used to generate the core part of the encryption scheme. A 128-bit key is selected to generate the original value of the double-chaotic system, which decides the DNA complementary rule, hence, the key is hypersensitive in encryption and decryption process. The security analysis demonstrates the effectiveness of the proposed encryption system. The simulation results verify that the cryptosystem is enough to against the traditional attacks such as statistical attack, differential attack, brute force attack and entropy attack. Moreover, the encrypted image can be the optical message and transmitted in 10 km single mode fiber (SMF) channel from SL1 to SL2. In order to ensure the security, we use the chaos masking (CMS) technique to modulate and demodulate the optical message. Through numerical simulations of the cross-correlation function (CF), the chaos synchronization between SL1 and SL2 is desired. The Q-factor is 9.559 and the bit error rate (BER) is 5.771×10^{-22}.

Index Terms: Image encryption-then-transmission system, double-chaotic system, optical chaos, DNA encryption, semiconductor laser (SL).

1. Introduction

Image encryption based on chaos becomes an universally concernment increasingly. In virtue of the complexity, ergodicity and sensitiveness, chaotic systems are suitable for the cryptography. Since Matthews first put forward the chaos into cryptology in 1989 [1], a lot of chaotic systems are applied to image encryption at present [2]–[18], such as the Chen chaotic system, Lorentz chaotic system, hyper-chaotic system, fractional-order chaotic system and multiple chaotic S-boxes. However, owing to the low bandwidth and high electrical channels attenuation, the traditional electric chaos has great restrictions.

Compared to the electrical chaos, optical chaos can overcome these disadvantages with very large bandwidth, low attenuation, high security, more chaotic and faster [19], [20]. Therefore, optical chaos has a great application prospect in the field of image encryption. A fast and secure symmetric image encryption-then-transmission system using semiconductor lasers is proposed [21]. A master laser (ML) and two slave lasers (SL1 and SL2) are used for generating chaotic signals served as chaotic carrier to transmit image with small BER and high Q-factor. Meantime, the chaotic signals are sampled and discretized to produce

the core part of the encryption scheme. This proposed scheme is effective and highly secure. Recently, a novel image encryption algorithm based on synchronization of physical random bit generated in a cascade-coupled semiconductor ring lasers (CCSRL) system is proposed [22]. The proposed algorithm demonstrates a good encryption performance and is a promising candidate for secure image communication application. However, we notice that there are few reports on image encryption using double chaotic system and DNA encryption algorithm based on optical chaos.

In this paper, by introducing the double chaotic system and DNA encryption algorithm, we propose a novel image encryption-then-transmission system based on optical chaos. The period of a low-dimensional chaotic map is not large, to overcome the weakness, the double-chaotic system is introduced. The distinctive double-chaotic system contains CML chaotic system [11] and optical chaos, which is different from the previous methods of using multiple chaotic systems [23]–[25]. The CML chaotic system and optical chaos are not applied in the processes of the image encryption or decryption, but obtaining a higher-dimensional chaotic system through using the the CML chaotic system to shuffle the position of optical chaotic sequence. Meanwhile, DNA encryption algorithm is also exploited in our work to enhance the security [26]–[29]. The advantage is that the DNA algorithm can store a large amount one-time pad, so it can effectively resist the chosen-plaintext attack. In addition, it has the advantage of ultra low energy consumption [30]. Furthermore, we analyze the security of the image encryption system. The tests (key space, key sensitivity, histogram, information entropy and so on) prove that the proposed system is fabulous and can resist a variety of attacks.

The rest of the paper is organized as follows. The system scheme, methods and algorithm are described in Section 2. The numerical simulation and analysis are drawn in Section 3. Security analysis are presented in Section 4. Finally, the conclusion is given in Section 5.

2. System model and methods

The structure diagrams of our transmission system, encryption system and decryption system are illustrated in Fig. 1. Fig. 1 (a) shows that the output of ML is divided into two parts through a beam splitter (BS), which are feedback to ML to ameliorate the complexity of its dynamics via two mirror (M1 and M2). Then chaotic output of ML is through an optical isolator (OI) and a neutral density filter (NDF), OI can make the output unidirectional and NDF can change rate of the injection. The optical beam becomes two parts through a BS. They are transported by two fibers (F) and injected into SL1 and SL2. Because of the symmetry of our system, the parameters of SLs are same. The sender encrypt the original image by using SL1 and encryption algorithm. The encrypted image transforms the optical message and can be transmitted in 10 km single mode fiber (SMF) channel. The chaos masking (CMS) technique [31] is adopted in order to improve the security during transmission. The receiver can get the decode message through the chaos demodulation technique. Final, the decrypted image can be obtained by using SL2 and decrypted algorithm. As depicted Fig. 1 (b), a 128-bit key is used to generate the initial value of the CML chaotic system. Then, starting to iterate the CML chaotic system to get the chaotic sequence. The encryption process is based on DNA encryption, permutation process and diffusion process, all of these steps need the optical chaotic sequence of SL1, which is shuffled by the CML chaotic system. The operations (decryption steps) in the Fig. 1 (c) is the reverse of the operations (encryption steps) in the Fig. 1 (b).

2.1. The Rate Equations of Distributed Feedback (DFB) Lasers

The rate equations of ML are expressed as:

$$\begin{aligned}\frac{dE_1}{dt} =& \frac{1}{2}[G_n(N_1 - N_0) - \frac{1}{\tau_p}]E_1 \\ &+ \frac{\eta_1}{\tau_{in}}E_1(t-\tau_1)cos(\Delta(t)) \\ &+ \frac{\eta_2}{\tau_{in}}E_1(t-\tau_2)cos(\Delta(t))\end{aligned} \tag{1}$$

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.2018.2827165, IEEE Photonics Journal

$$\frac{d\phi_1}{dt} = \frac{1}{2}\alpha[G_n(N_1 - N_0) - \frac{1}{\tau_p}] - \frac{\eta_1}{\tau_{in}}\frac{E_1(t-\tau_1)}{E_1}sin(\Delta(t)) - \frac{\eta_2}{\tau_{in}}\frac{E_1(t-\tau_2)}{E_1}sin(\Delta(t)) \tag{2}$$

$$\frac{dN_1}{dt} = \frac{J}{ed} - \frac{N_1}{\tau_s} - G_n(N_1 - N_0)|E_1|^2 \tag{3}$$

The rate equations of SLs are expressed as:

$$\frac{dE_{2,3}}{dt} = \frac{1}{2}[G_n(N_{2,3} - N_0) - \frac{1}{\tau_p}]E_{2,3} + \frac{k_{inj1,2}}{\tau_{in}}E_1(t-\tau_{3,4})cos(\Delta(t)) \tag{4}$$

$$\frac{d\phi_{2,3}}{dt} = \frac{1}{2}\alpha[G_n(N_{2,3} - N_0) - \frac{1}{\tau_p}] - \frac{k_{inj1,2}}{\tau_{in}}\frac{E_1(t-\tau_{3,4})}{E_{2,3}}sin(\Delta(t)) \tag{5}$$

$$\frac{dN_{2,3}}{dt} = \frac{J}{ed} - \frac{N_{2,3}}{\tau_s} - G_n(N_{2,3} - N_0)|E_{2,3}|^2 \tag{6}$$

where E_1 is the ML amplitude of optical field, $E_{2,3}$ is the SLs amplitude of optical field $P = |E|^2$ is the density of photons. ϕ_1 is the phase of ML. $\phi_{2,3}$ is the phase of SLs. N_1 is the ML density of carrier. $N_{2,3}$ is the SLs density of carrier. $G_n = v_g\alpha g/\alpha N$ is the differential gain coefficient (v_g is the group velocity of light and g is the semiconductor medium gain). N_0 is the carrier number at transparency. τ_p is the photon lifetimes. η_1 is the optical feedback intensity of M1. η_2 is the optical feedback intensity of M2. $k_{inj_{1,2}}$ is the SLs variable injection coefficient. $\tau_{in} = 2L/C$ is the propagation delay times in the lasers (L is the cavity length and c is the speed of light). $\tau_{1,2}$ the optical feedback delay time of ML. $\tau_{3,4}$ is the optical feedback delay time of the SLs. $\Delta(t) = \phi(t) - \Delta\omega t$ is phase difference ($\Delta\omega$ is the detuning angular frequency between the lasers). J is the density of bias current. e is the electronic charge. d is thickness of the activation layer. τ_p is the carrier lifetime.

2.2. The Double-chaotic System

Coupled Map Lattice: One CML system is described by:

$$x_1(i+1) = (1-B) \times f(x_1(i)) + B \times f(x_2(i)) \tag{7}$$

$$x_2(i+1) = B \times f(x_1(i)) + (1-B) \times f(x_2(i)) \tag{8}$$

where i =1,2,3,...,n is the lattice state index, $B \in (0,1)$ is a constant. In this paper, B is chosen as 0.75. $f(x)$ is a chaotic map, the logistic map is chosen, it is given by: $f(x) = A \times x(1-x)$, A is a parameters and selected as 4. x_1 and x_2 are generated by XOR operation of sixteen 8-bit binary sequences $(a_1, a_2, a_3, ...a_{16})$. They are obtained by the following formulas:

$$\begin{aligned} b_1 &= a_1 \oplus a_{13} & b_2 &= a_2 \oplus a_{13} \\ b_3 &= a_1 \oplus a_{13} & b_4 &= a_4 \oplus a_{14} \\ b_5 &= a_5 \oplus a_{14} & b_6 &= a_6 \oplus a_{14} \\ b_7 &= a_7 \oplus a_{15} & b_8 &= a_8 \oplus a_{15} \\ b_9 &= a_9 \oplus a_{15} & b_{10} &= a_{10} \oplus a_{16} \\ b_{11} &= a_{11} \oplus a_{16} & b_{12} &= a_{12} \oplus a_{16} \end{aligned} \tag{9}$$

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.2018.2827165, IEEE Photonics Journal

$$
\begin{aligned}
c_1 &= b_1 \times 100 + b_2 \times 10 + b_3 \\
c_2 &= b_4 \times 100 + b_5 \times 10 + b_6 \\
c_3 &= b_7 \times 100 + b_8 \times 10 + b_9 \\
c_4 &= b_{10} \times 100 + b_{11} \times 10 + b_{12} \\
c_5 &= b_{12} \times 100 + b_{11} \times 10 + b_{10} \\
c_6 &= b_9 \times 100 + b_8 \times 10 + b_7 \\
c_7 &= b_6 \times 100 + b_5 \times 10 + b_4 \\
c_8 &= b_3 \times 100 + b_2 \times 10 + b_1
\end{aligned} \tag{10}
$$

$$
\begin{aligned}
x_1 &= ((c_1 \oplus c_2 \oplus c_3 \oplus c_4)\, mod\, 256) + 0.1/256 \\
x_2 &= ((c_5 \oplus c_6 \oplus c_7 \oplus c_8)\, mod\, 256) + 0.1/256
\end{aligned} \tag{11}
$$

where $\oplus$ is the XOR operation, $b_1, b_2, ..., b_{12}$ and $c_1, c_2, ..., c_8$ are the intermediate variable. We iterate the CML for 200 times to get rid of the transient effect. Then, a large chaotic sequence can be obtained by CML chaotic system.

Optical chaos: The output of ML separates into two parts through OI, NDF and BS, which are sent to SL1 and SL2, then SL1 and SL2 can output the similar chaotic signal synchronously. On the hand, we use the chaotic signal to modulate the optical message in the transmission, on the other hand, the chaotic signal can transform the digital signal to be the chaotic sequence. The equations of lasers have been given in Section 2.1.

The double-chaotic system: As listed by TABLE I, column A stands for the chaotic sequence of the CML chaotic system; column B stands for the chaotic sequence of the optical chaos; column C stands for the chaotic sequence of the CML chaotic system after shuffling; column D stands for the chaotic sequence of the optical chaos after shuffling. The A column elements correspond to the B column elements from left to right. A column elements are rearranged in ascending order to get the column C. Because of the correspondence between column A and column B, the position of the B column elements are changed to get the column D. We use the D column elements (shuffled chaotic sequence of optical chaos) in the encryption/decryption process.

TABLE I
THE CHAOTIC SEQUENCE OF CML AND OPTICAL CHAOS

A	B	C	D
0.0639	1.6280×10^5	0.0639	1.6280×10^5
0.2349	1.5055×10^5	0.2349	1.5055×10^5
0.7284	1.3827×10^5	0.2569	1.7484×10^5
0.7915	1.2614×10^5	0.3687	1.9752×10^5
0.6603	1.1430×10^5	0.6603	1.1430×10^5
0.8973	1.0290×10^5	0.7284	1.3827×10^5
0.3687	1.9752×10^5	0.7638	1.5698×10^5
0.9310	1.8648×10^5	0.7915	1.2614×10^5
0.2569	1.7484×10^5	0.8973	1.0290×10^5
0.7638	1.5698×10^5	0.9310	1.8648×10^5

2.3. DNA Encryption

The digital image is transformed into a plane of DNA. There are two steps that convert digital images into a plane of DNA and the detail is described as follows:

Step 1: the digital image becomes the bit-plane [32]. It is according to the following operation:

$$G(x,y) = b(7) \times 2^7 + b(6) \times 2^6 + ... + b(0) \times 2^0 \tag{12}$$

where $G(x,y)$ is the value of the pixel at position (x,y) in the image. $b(i)$ is a binary number, only two possible values (0 and 1) for it. Thus the value can be represented by a 8-bit binary. For instance, the value of a pixel is 117, it can be represented by 01110101. From this, digital images can be converted into bit-plane.

Step 2: the bit-plane becomes the DNA-plane. It defines that 0 and 1 are complementary in the binary. Naturally, 00 and 11 are complementary, 10 and 01 are complementary. We use an alphabetic coding for the 2-bit binary. In this paper, we define that 00 is "A", 01 is "G", 10 is "C", 11 is "T", thus, "A" and "T" are complementary, "C" and "G" are complementary. It's liking adenine (A) and thymine (T) are complementary, cytosine (C) and guanine (G) are complementary in biological DNA. There are 24 kinds of alphabetic coding. However, we can only use 8 kinds of alphabetic coding which are satisfying the Watson-Crick complement rule [28] as illustrated by Table II. For example, 01110101 can be represented by "GTGG". Final, the DNA-plane can be obtained.

TABLE II
DNA CODING RULES

Rule	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
C	01	10	00	11	00	11	01	10
G	10	01	11	00	11	00	10	01

There are just 6 kinds of DNA complementary rules [28], as listed in TABLE III. Because they should satisfy two equations:

$$x \neq B(x) \neq B(B(x)) \neq B(B(B(x))) \tag{13}$$

$$x = B(B(B(B(x)))) \tag{14}$$

Where $B(x)$ is the pairing of the x.

TABLE III
DNA COMPLEMENTARY RULES

Rule1	AT	TC	CG	GA
Rule2	AT	TG	GC	CA
Rule3	AC	CT	TG	GA
Rule4	AC	CG	GT	TA
Rule5	AG	GT	TC	CA
Rule6	AG	GC	CT	TA

2.4. The Masking Process.

In order to improve the resistance about the chosen-plaintext attack, we use a masking process that the parts of image are XOR-operated. Through this operation, the sensitivity of the encrypted image to the original pixels is improved and a little change in the original image can cause a significant difference in the encrypted image.

Selecting the left-most column, making XOR-operate of the left-most column and the ith column (i=1,2,3,...n) in turn (the number of the column about the part is n). We can get a horizontal-XOR column,

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.2018.2827165, IEEE Photonics Journal

then, copying the horizontal-XOR column n times. The horizontal-XOR part ($n \times n$) is obtained [32]. It's marked as Se_iH $(1 \le i \le 4)$.

Selecting the last row, making XOR-operate of the last row and the ith row (i=1,2,3,...n) in turn (the number of the row about the part is n). We can get a horizontal-XOR row. After this, copying the horizontal-XOR row n times. The vertical-XOR part($n \times n$) is obtained [32]. It's marked as Se_iV $(1 \le i \le 4)$.

The steps to get the XOR-image as follow:

Step 1: Dividing the original image into four parts equally (Se1, Se2, Se3 and Se4), they are marked as Se_1^{old}, Se_2^{old}, Se_3^{old} and Se_4^{old}. It is shown as Fig. 2. If the number of rows (columns) are odd, copying the last row (right-most column) to make sure that the rows (columns) are even.

Step 2: Getting the new Se1, new Se2, new Se3 and new Se4, they are marked as Se_1^{new1}, Se_2^{new1}, Se_3^{new1} and Se_4^{new1}. The equations are as follow:

$$\begin{aligned} Se_2^{new1} &= Se_1^{old}H \oplus Se_1^{old}V \oplus Se_2^{old} \\ Se_1^{new1} &= Se_2^{new1}H \oplus Se_2^{new1}V \oplus Se_1^{old} \\ Se_3^{new1} &= Se_2^{new1}H \oplus Se_2^{new1}V \oplus Se_3^{old} \\ Se_4^{new1} &= Se_3^{new1}H \oplus Se_3^{new1}V \oplus Se_4^{old} \end{aligned} \tag{15}$$

Step 3: Getting the new Se1, new Se2, new Se3 and new Se4 again, they are marked as Se_1^{new2}, Se_2^{new2}, Se_3^{new2} and Se_4^{new2}. The equations are as follow:

$$\begin{aligned} Se_2^{new2} &= Se_3^{new1}H \oplus Se_3^{new1}V \oplus Se_2^{new1} \\ Se_3^{new2} &= Se_4^{new1}H \oplus Se_4^{new1}V \oplus Se_3^{new1} \\ Se_4^{new2} &= Se_1^{new1}H \oplus Se_1^{new1}V \oplus Se_4^{new1} \\ Se_1^{new2} &= Se_4^{new2}H \oplus Se_4^{new2}V \oplus Se_1^{new1} \end{aligned} \tag{16}$$

where $\oplus$ is the XOR operation.

Step 4: Finally, combining the Se_1^{new2}, Se_2^{new2}, Se_3^{new2} and Se_4^{new2} into a new image.

2.5. Encryption and Decryption Algorithms

The details of encryption algorithm are described as follows:

Step 1: Selecting the sixteen 8-bit key ($a_1, a_2, a_3, ...a_{16}$) and generating the initial value of the CML.

Step 2: Obtaining a lot of sequence by iterating the CML chaotic system to shuffle the sequence of optical chaos. Details are shown in Section 2.2. In this paper, we need a sequence of $36 \times M \times N$ numbers.

Step 3: The digital image is transformed into a plane of DNA. Firstly, we separate three components (Red, Green and Blue) from the digital image. We make the R, G and B components become the bit-plane, the details are shown in Section 2.3. We select the first and the second bit of every pixel to make the first DNA-plane, the third and the fourth bit to make the second DNA-plane, the fifth and sixth bit to make the third DNA-plane and the seventh and eighth bit to make the fourth DNA-plane. In order to improve the key sensitivity and the resistance of the brute-force attack, we use b_i and b_{i+1} $(1 \le i \le 11)$ in the formula (3) to decide that one of the 8 kinds of alphabetic coding in Table II.

$$w_i = (b_i \oplus b_{i+1}) \, mod \, 8 + 1 \tag{17}$$

where w_i is the one of the alphabetic coding. From this, the R, G and B components become twelve DNA-planes.

Step 4: Generating the twelve new DNA-planes by the 6 kinds of the DNA complementary rules. We select the sequence $x_1, x_2, x_3, ..., x_{12 \times M \times N}$ from the optical chaotic sequence. The equation for describing the selection of DNA pairing rules as follows:

$$z_i = (floor(100 \times x_i)) \, mod \, 6 + 1 \tag{18}$$

where x_i represents the optical chaotic sequence. $floor(x)$ is the largest integer that don't more than the x. z_i represents the six different DNA complementary rules in Table III. So we can get twelve new DNA-planes.

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.2018.2827165, IEEE Photonics Journal

Step 5: A big DNA-plane can be obtained by connecting the four DNA-planes in turn. We can get three big DNA-planes from the twelve new DNA-planes.

Step 6: Permutation process. In the same way in Section 2.2, $x_{12\times M\times N+1}, x_{12\times M\times N+2}, ..., x_{24\times M\times N}$ is selected to shuffle the position of the new big DNA-planes in ascending order.

Step 7: Diffusion process. The diffusion process of DNA encryption is different from the conventional diffusion process, due to the DNA-plane is composed of letters. We define 16 new equations, they are shown as followed:

$$\begin{array}{llll} A\bigotimes A=A & A\bigotimes G=G & A\bigotimes C=C & A\bigotimes T=T \\ G\bigotimes A=A & G\bigotimes G=C & G\bigotimes T=C & G\bigotimes C=T \\ C\bigotimes A=C & C\bigotimes G=T & C\bigotimes C=A & C\bigotimes T=G \\ T\bigotimes A=T & T\bigotimes G=A & T\bigotimes C=C & T\bigotimes T=C \end{array} \tag{19}$$

As the matter of fact, there are 4^{12} kinds of equations about it. We just select one of them to encrypt image. It is the same as the step 3, we selected the sequence $x_{24\times M\times N+1}, x_{24\times M\times N+2}, ..., x_{36\times M\times N}$ to generate the $12\times M\times N$ positive integers, which can be expressed as $h_1, h_2, ..., h_{12\times M\times N}$. The equations of the diffusion are detailed below:

$$C(1) = B_{h1}(P(4\times M\times N))\bigotimes P(1) \tag{20}$$

$$C(i) = B_{hi}(C(i-1))\bigotimes P(i) \tag{21}$$

$P(1)$ is the first element of the big DNA-plane, $P(4\times M\times N)$ is the last element of the big DNA-plane. $P(i)$ is the i-th element of the big DNA-plane. $C(1)$ is the first output element of cipher DNA-plane. $C(i)$ is the i-th element of cipher DNA-plane. B_{hi} is the one of 6 kinds of the pairing rules in Table III.

Step 8: The DNA-plane transforms to the digital image. The order is the reversed with the step 2.

Step 9: Display or store the cipher-image.

The decryption process is the reverse operation of the encryption.

3. NUMERICAL SIMULATION AND ANALYSIS

3.1. The Chaotic Lasers

The fourth-order Runge-Kutta algorithm is selected to numerically solve the equation (1) to (6). The internal parameters of lasers are given in the Table IV [35], [36]. In addition, $e = 1.6\times 10^{-19}\,C$, $d = 0.2\,\mu m$,

TABLE IV
PARAMETERS OF ML AND SLS

Parameter	ML	SL1 and SL2
α	3	3
G_n	8.4×10^{-13}	8.4×10^{-13}
τ_{in}	8 ps	8 ps
τ_p	1.93 ps	1.93 ps
τ_s	2.04 ns	2.04 ns
N_0	1.40×10^{24}	1.40×10^{24}
J	5.07×10^{7}	5.07×10^{7}

$\eta_1 = 0.03$, $\eta_2 = 0.04$, $k_{inj_1} = k_{inj_2} = 0.05$, $\tau_1 = \tau_2 = 3\,ns$ and $\tau_3 = \tau_4 = 4.5\,ns$. The dynamic characteristics (times series, power spectra and phase portraits) of ML, SL1 and SL2 are shown in Fig. 3. From the simulation results, the arbitrary intensity pulses of the time series is similar to the intensity fluctuation noise, the power spectra is parallel to the noise background and the dots are randomly distributed in the phase portraits. All the features are the typical features of chaos. The chaotic output of SL1 and SL2 can

be used as the carrier to modulate the message in the communication process. Beyond that, the optical chaotic output can also be exploited to encrypt/decrypt the original /encrypted image.

3.2. Chaos Synchronization

As shown in Fig. 3, the variation properties between SL1 and SL2 are similar, which represents the perfect chaos synchronization. To verity the chaos synchronization between SL1 and SL2 more accurately, the expression of the normalized cross correlation coefficient as follows [35]:

$$C_{a,b}(\Delta t) = \frac{\langle [P_a(t) - \langle P_a(t)\rangle][P_b(t+\Delta t) - \langle P_b(t)\rangle]\rangle}{\sqrt{\langle |P_a(t) - \langle P_a(t)\rangle|^2\rangle \langle |P_b(t+\Delta t) - \langle P_b(t)\rangle|^2\rangle}} \tag{22}$$

where $\langle\ \rangle$ denotes temporal average, the a and b represent SL1 and SL2, $P = |E|^2$ presents the output intensity of laser and Δt is the time shift. $|C|$ is value range of the normalized cross correlation coefficient, which is between 0 and 1. Apparently, the value is more closer to 1, the chaos synchronization is better. Ideally, the value is equal to 1 at $\Delta t = 0\ ns$. From the Fig. 4, the value is infinite approaching to 1 at $\Delta t = 0\ ns$. The simulation result proves the perfect chaos synchronization.

3.3. Transmission Process

The Fig. 5 depicts the transmission of propagating 10 km in the single mode fiber (SMF) channel and the parameters of transmission are given in TABLE V. Furthermore, the modulation depth is 2% and the transmission rate is 10 $Gbit/s$. Fig. 5 displays that the optical message and decoded message are similar and the eye diagram is wide-open and clear, which reflects the transmission is executable and safe and the encoded optical message can be deciphered after transmitted 10 km. Furthermore, the Q-factor [38] and the bit error rate (BER) can inspection the quality of transmission. The Q-factor is evaluated as:

$$Q = \frac{P_1 - P_2}{\sigma_1 - \sigma_2} \tag{23}$$

P is the mean power and σ is the corresponding standard deviations. The result is that Q-factor is 9.559 and the BER is 5.771×10^{-22}, which proves the outstanding quality of the 10 km SFM transmission.

TABLE V
PARAMETERS OF 10 KM SMF

Parameter	Value
Attenuation coefficient	0.2 dB/km
Dispersion coefficient	17 ps/nm/km
Dispersion slope	0.075 ps/nm^2/km
Nonlinear Kerr factor	1.31 $km^{-1}W^{-1}$
Differential group delay	0.2 ps/km

4. SECURITY ANALYSIS

4.1. Key Space

The key space is the measure of whether the cryptosystem is good. In this paper, The key space of the proposed cryptosystem is equal to $2^{128} \approx 3.403 \times 10^{38}$. The space is large enough to resist brute-force attack.

4.2. The Key Sensitivity

A perfect cryptosystem is hypersensitive to the key. A slight change of the key will cause significant difference about the image. So two tests are carried out about the key with one bit difference from 123456890123456 to 1234567890123457. They are shown as Fig. 6 and Fig. 7.

Test 1: Setting the 1234567890123456 and 1234567890123457 to encryption the image separately.The difference between the two encrypted image is 99.31%.

Test 2: Setting the 1234567890123456 to encrypt the image and setting the 1234567890123457 to decrypt the image. The difference between the two decrypted image is 99.3%.

Result: They have proved that the key is hypersensitive in the encryption and decryption process.

4.3. Histogram and Correlation Analysis

The histograms of the original R component, G component and B component are shown in Fig. 8 (a)-(c). As we can see from Fig . 8 (a)-(c) , the gray-scale distribution is very nonuniform. The characteristic peaks are clear and the most of image information can be obtained effortlessly. Fig. 8 (e)-(f) display the histograms of the encrypted R component, G component and B component. It can be seen that the histograms are uniform enough. It proves the excellent property of resisting the statistical attack and the cipher-only attack [39] in our encryption algorithm.

The correlation of the pixels represents the randomness of the gray level. The correlation of the encrypted image and original image are shown in the TABLE VI. The correlations of the original R component, the original G component and the original B component are high and close to 1. In contrast, the correlations of the encrypted R component, the encrypted G component and the encrypted B component are low and close to 0, which indicates that encrypted pixels are distributed randomly.

TABLE VI
CORRELATION COEFFICIENT BETWEEN ORIGINAL AND ENCRYPTED IMAGES

Correlation	Original image			Encrypted image		
	R	G	B	R	G	B
Horizontal	0.9812	0.9709	0.9555	-0.0475	-0.0016	-0.0118
Vertical	0.9474	0.9655	0.9474	0.0196	0.0012	0.0196
Diagonal	0.9652	0.9534	0.9339	0.0135	0.0105	0.0364

4.4. Information Entropy

The information entropy is the significant feature of randomness [40]. The entropy $H(s)$ of a source s can be calculated by the following formula:

$$H(s) = -\sum_{i=0}^{2^N-1} P(s_i)\, log_2\left(P(s_i)\right) \tag{24}$$

where $P(s_i)$ represents the probability of s_i. In this paper, the gray level of the image is 0 from 255 and $2^N - 1 = 255$. Ideally, the probability of s_i is equal and $H(s) = 8$. If the information entropy is closer to 8, the randomness is better. The entropy of the plain-image is 7.4767 and the entropy of the encrypted image is 7.9998, which proves that cryptosystem is secure against entropy attack.

4.5. Differential Analysis

The attacker can get the useful information by changing some pixels of the image. The resistance of encrypted image to differential attacks is usually measured by two indicators: the number of pixels change rate (NPCR) and unified average changing intensity (UACI). In a good cryptosystem, the NPCR should be more closer to 100% and the UACI should be more than 30%. And the NPCR and UACI are given by the following equations:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \tag{25}$$

$$UACI = \frac{\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255}}{W \times H} \times 100\% \tag{26}$$

$C_1(i,j)$ and $C_2(i,j)$ are the gray value of two image, if $C_1(i,j)$ is equal to $C_2(i,j)$, $D(i,j)=1$; else $D(i,j)=0$. The TABLE VII shows that the NPCR and UACI are more than 99% and 33%. The results in TABLE VII indicate that a slight change in original image will result significant difference in encrypted image and the algorithm is effective to resist the differential analysis.

TABLE VII
NPCR AND UACI OF A COLOR IMAGE

Component	NPCR	UACI
R	99.62%	33.46%
G	99.43%	33.21%
B	99.24%	33.83%

5. Conclusion

Due to the complex dynamics of lasers, the lasers can output chaotic signal, which can be adopted in image encryption and transmission. In order to improve the property of the optical chaos, we introduce the CML chaotic system to shuffle the optical chaotic sequence. In addition, the Q-factor is 9.599, BER is 5.771×10^{-22} in the 10 km SMF transmission and the eye diagram is wide-open, which proves that the quality of transmission is commendable. The result of security analysis show the encryption algorithm is effective, such as the key space is large, the key is hypersensitive, histograms are mean distributed after encrypting, and correlation between the adjacent pixel is infinitesimal. Furthermore, the NPCR is closer to 100%, the UACI is more than 30% and entropy is approximately equal to 8. The decrypted image is the same as the original image, which proves the cryptosystem is executable. Therefore, the proposed system is safe and effective, we hope it can be helpful for later researches.

Acknowledgments

This work was supported in part by the 863 program of China under Grant 2015AA016304, by the National Natural Science Foundation of China under Grant No.61421002, by the National Natural Science Foundation of Chongqing City under Grant Nos.cstc2016jcyjA2002, by the Postdoctoral Science Foundation of China under Grant Nos.2016M590875, and by the Fundamental Research Funds for the Central Universities under Grants XDJK2014A017 and XDJK2016A011. The authors wish to thank the anonymous reviewers for their valuable suggestions.

References

[1] R. Matthews, "On the derivation of a chaotic encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29-42, Jan. 1989.
[2] C. X. Zhu, "A new image encryption algorithm based on general Chen's chaotic system," *Journal of Central South University (Science and Technology)*, vol. 37, no. 6, pp. 1142-1148, Dec. 2006.
[3] F. Özkaynak, and A. B. Özer, "A method for designing strong S-Boxes based on chaotic Lorenz system," *Physics Letters A*, vol. 374, no. 36, pp. 3733-3738, Jul. 2010.
[4] J. Zhao, S. Wang, and Y. Chang, "A novel image encryption scheme based on an improper fractional-order chaotic system," *Nonlinear Dynamics*, vol. 80, no. 4, pp. 1721-1729, Jun. 2015.
[5] X. J. Tong, M. Zhang, and Z. Wang, "A joint color image encryption and compression scheme based on hyper-chaotic system," *Nonlinear Dynamics*, vol. 84, no. 4, pp. 2333-2356, Feb. 2016.
[6] L. Zhang, X. Liao, and X. Wang, "An image encryption approach based on chaotic maps," *Chaos, Solitons & Fractals*, vol. 24, no. 3, pp. 759-765, May. 2005.
[7] J. C. Yen, and J. I. Guo, "Efficient hierarchical chaotic image encryption algorithm and its VLSI realisation," *IEEE Proceedings-vision, image and signal processing*, vol. 147, no. 2, pp. 167-175, May. 2000.
[8] Z. H. Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," *Physics Letters A*, vol. 346, no. 1, pp. 153-157, Oct. 2005.
[9] F. Sun, S. Liu, and Z. Li, "A novel image encryption scheme based on spatial chaos map," *Chaos, Solitons & Fractals*, vol. 38, no. 3, pp. 631-640, Nov. 2008.
[10] X. Y. Wang, L. Yang, and R. Liu, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dynamics*, vol. 62, no. 3, pp. 615-621, Nov. 2010.

[11] X. Wu, Y. Li, and J. Kurths, "A new color image encryption scheme using CML and a fractional-order chaotic system," *PloS one*, vol. 10, no. 3, p. e0119660, Mar. 2015.
[12] B. Wang, Y. Xie, and C. Zhou, "Evaluating the permutation and diffusion operations used in image encryption based on chaotic maps," *Optik-International Journal for Light and Electron Optics*, vol. 127, no. 7, pp. 3541-3545, Apr. 2016.
[13] S. M. Seyedzadeh, and S. Mirzakuchaki "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map," *Signal processing*, vol. 92, no. 5, pp. 1202-1215, May. 2012.
[14] X. Y. Wang, L. Yang, and R. Liu, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dynamics*, vol. 62, no. 3, pp. 615-621, Nov. 2010.
[15] G. Ye, K. W. Wong "An image encryption scheme based on time-delay and hyperchaotic system," *Nonlinear Dynamics*, vol. 71, no. 1-2, pp. 259-267, Jan. 2013.
[16] H. Liu, and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps,"*Computers & Mathematics with Applications*, vol. 59, no. 10, pp. 3320-3327, May. 2010.
[17] M. Khan, "A novel image encryption scheme based on multiple chaotic S-boxes,"*Nonlinear Dynamics*, vol. 82, no. 1, pp. 527-533, May. 2015.
[18] M. Khan, and T. Shah "A construction of novel chaos base nonlinear component of block cipher ,"*Nonlinear Dynamics*, vol. 76, no. 1, pp. 377-382, Apr. 2014.
[19] N. Li, B. Kim, and V. N. Chizhevsky, "Fast random bit generation with a single chaotic laser subjected to optical feedback," *SPIE Photonics Europe*, pp. 913427-913427
[20] I. Reidler, Y. Aviad, and M. Rosenbluh, "Ultrahigh-speed random number generation based on a chaotic semiconductor laser," *Physical review letters*, vol. 103, no. 2, pp. 024102, Jul. 2009.
[21] 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," *Journal of Lightwave Technology*, vol. 34, no. 22, pp. 5101-5109, Nov. 2016.
[22] J. F. Li, S. Y. Xiang, H. N. Wang, J. K. Gong, and A.J. Wen, "A novel image encryption algorithm based on synchronized random bit generated in cascade-coupled chaotic semiconductor ring lasers," *Optics and Lasers in Engineering*, vol. 102, pp. 170-180, Mar. 2018.
[23] T. Wang, H. Zhang, Z. H. Li, and Q. H. Zhang, "The images encryption algorithm based on the multi-chaotic systems," *IEEE International Conference on Multimedia Information Networking and Security* , 2009.
[24] L. Hong, and C. Li, "A novel color image encryption approach based on multi-chaotic system," *IEEE 2nd International Conference on Anti-counterfeiting, Security and Identification*, 2008.
[25] Y. C. Zhou, B. Long, and C. P. Chen, "Image encryption using a new parametric switching chaotic system," *Signal processing*, vol. 93, no. 11, pp. 3039-3052, Nov. 2013.
[26] Q. Zhang, L. Guo, and X. Wei, "Image encryption using DNA addition combining with chaotic maps," *Mathematical and Computer Modelling*, vol. 52, no. 11, pp. 2028-2035, Dec. 2010.
[27] X. Wei, L. Guo, and Q. Zhang, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system," *Journal of Systems and Software*, vol. 85, no. 2, pp. 290-299, Feb. 2012.
[28] H. Liu, and X. Wang, "Image encryption using DNA complementary rule and chaotic maps," *Applied Soft Computing*, vol. 12, no. 5, pp. 1457-1466, May. 2012.
[29] Q. Zhang, Q. Wang, and X. Wei, "A novel image encryption scheme based on DNA coding and multi-chaotic maps," *Advanced Science Letters*, vol. 3, no. 4, pp. 447-451, Dec. 2010.
[30] X. Y. Wang, Y. Q. Zhang, and X. M. Bao "A novel chaotic image encryption scheme using DNA sequence operations," *Optics and Lasers in Engineering*, vol. 73, pp. 53-61, Oct. 2015.
[31] 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.
[32] C. Fu, B. Lin, and Y. Miao, "A novel chaos-based bit-level permutation scheme for digital image encryption," *Optics communications*, vol. 284, no. 23, pp. 5415-5423, Nov. 2011.
[33] X. Chai, Z. Gan, and Y. Lu, "A novel image encryption algorithm based on the chaotic system and DNA computing," *International Journal of Modern Physics C*, vol. 28, no. 5, p. 1750069, May. 2017.
[34] S. M. Seyedzadeh, and S. Mirzakuchaki, "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map," *Signal processing*, vol. 92, no. 5, pp. 1202-1215, May. 2012.
[35] A. Valle, M. Sciamanna, and K. Panajotov, "Irregular pulsating polarization dynamics in gain-switched vertical-cavity surface-emitting lasers," *IEEE J. Quantum Electron.*, vol. 44, no. 2, pp. 136-143, Feb. 2008.
[36] M. C. Soriano, F. R. Oliveras, P. Colet, and C. R. Mirasso, "Synchronization properties of coupled semiconductor lasers subject to filtered optical feedback," *Phys. Rev. E*, vol. 78, no. 4, p. 046218, Oct. 2008.
[37] M. Peil, L. Larger, and I. Fischer, "Versatile and robust chaos synchronization phenomena imposed by delayed shared feedback coupling," *Phy. Rev. E*, vol. 76, no. 4, pp. 045201.1-045201.4, Oct. 2007.
[38] I. Shake, H. Takara, and K. Uchiyama, "Quality monitoring of optical signals influenced by chromatic dispersion in a transmission fiber using averaged Q-factor evaluation," *IEEE Photonics Technology Letters*, vol. 13, no. 4, pp. 385-387, Apr. 2001.
[39] X. Wang, and H. Zhang, "A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems," *Nonlinear Dynamics*, vol. 83, no. 1-2, pp. 333-346, Jan. 2016.
[40] S. Behnia, A. Akhshani, and H. Mahmodi, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos Solitons & Fractals*, vol. 35, no. 2, pp. 408-419, May. 2006.

Graphic Abstract

Fig. 1. The structure diagram of our proposed system. (a) Transmission system, (b) Encryption system, (c) Decryption system.

Fig. 2. The four sections of the image.

Fig. 3. Numerically simulated time series, power spectra, and phase portraits of lasers in chaotic state: (a) ML, (b) SL1, (c) SL2.

Fig. 4. Cross correlation coefficients between SL1 and SL2.

Fig. 5. The results of transmission on optical communication. (a) Optical message, (b) Decoded message, (c) Eye diagram of decoded message.

Fig. 6. Encryption key sensitivity analysis: (a) Original image, (b) Encrypted image: key=1234567890123456, (c) Encrypted image: key=1234567890123457.

Fig. 7. Decryption key sensitivity analysis: (a) Encrypted image: key=123456789 0123456, (b) Decrypted image: key=1234567890123456, (c) Decrypted image: key=1234567890123457.

Fig. 8. Histograms of the original/encrypted image. (a) The histogram of R component about original image, (b) The histogram of G component about original image, (c) The histogram of B component about original image, (d) The histogram of R component about encrypted image, (e) The histogram of G component about encrypted image, (f) The histogram of B component about encrypted image.

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.2018.2827165, IEEE Photonics Journal

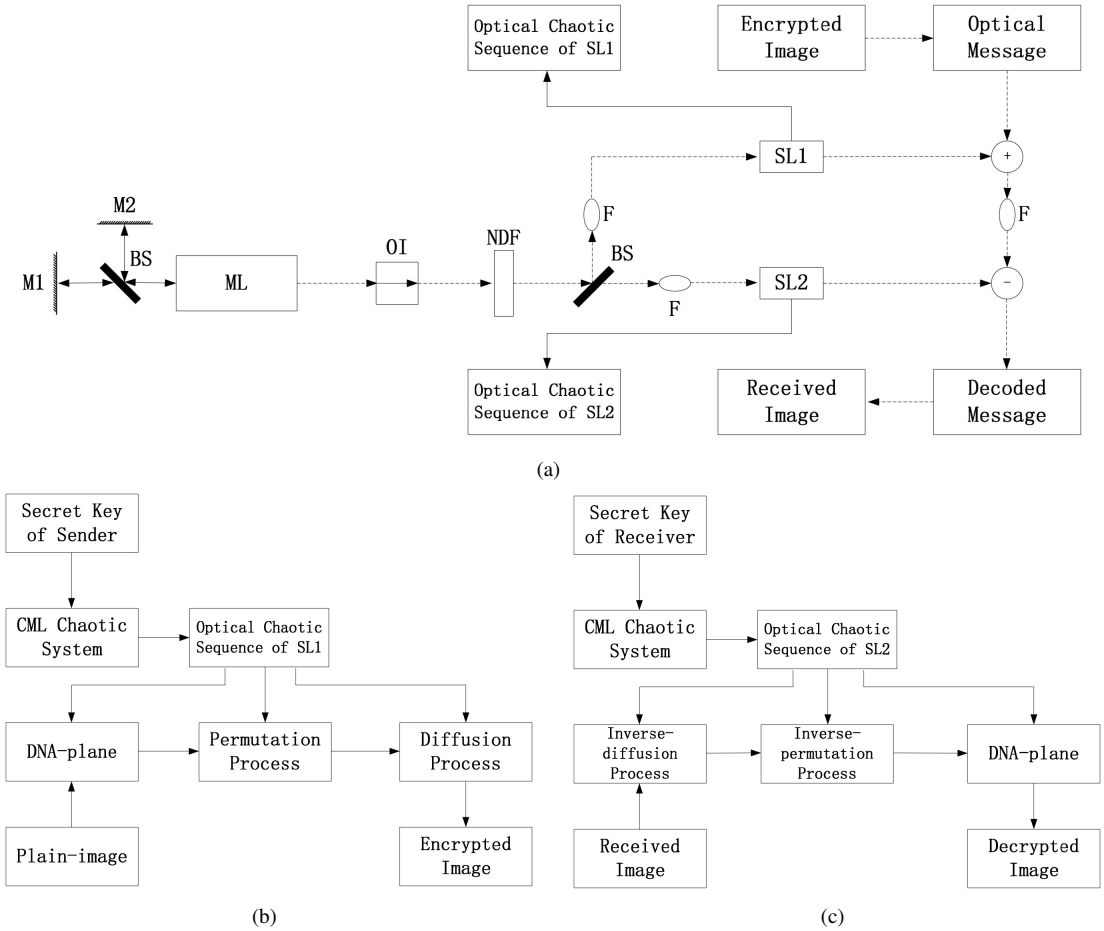


Fig. 1.

Fig. 2.

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.2018.2827165, IEEE Photonics Journal

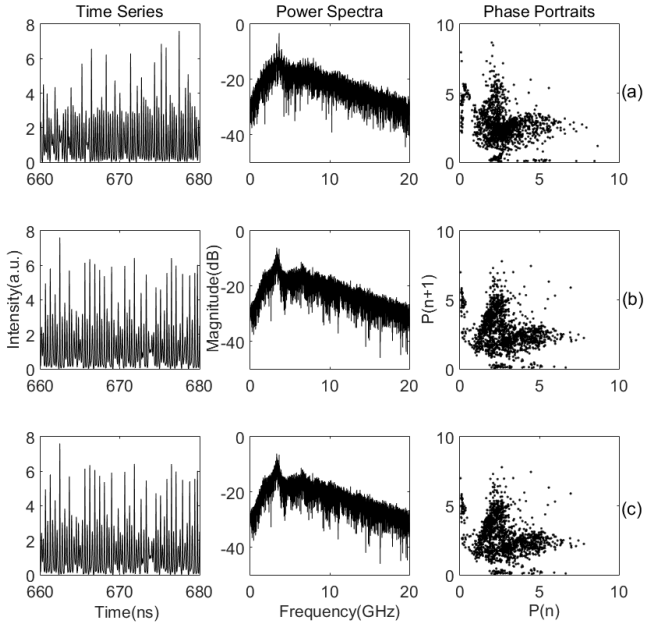


Fig. 3.

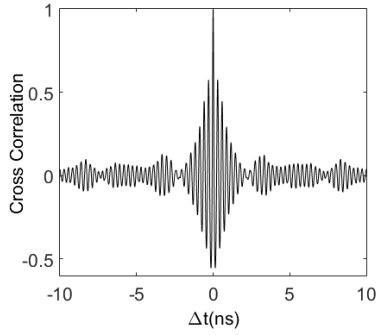


Fig. 4.

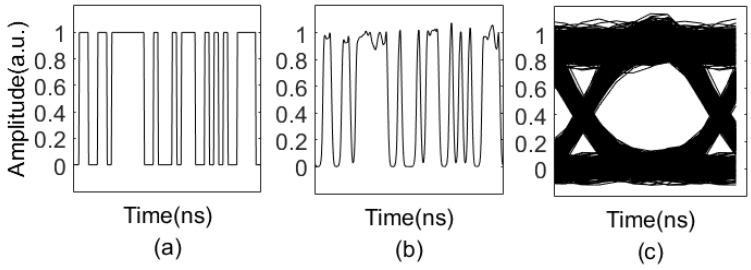
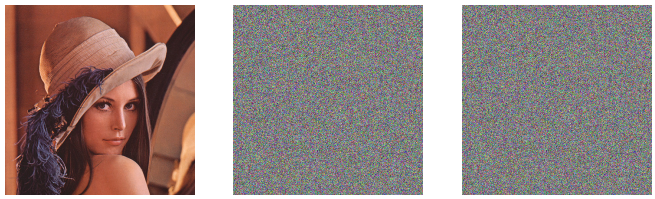


Fig. 5.

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.2018.2827165, IEEE Photonics Journal



(a) (b) (c)

Fig. 6.

(a) (b) (c)

Fig. 7.

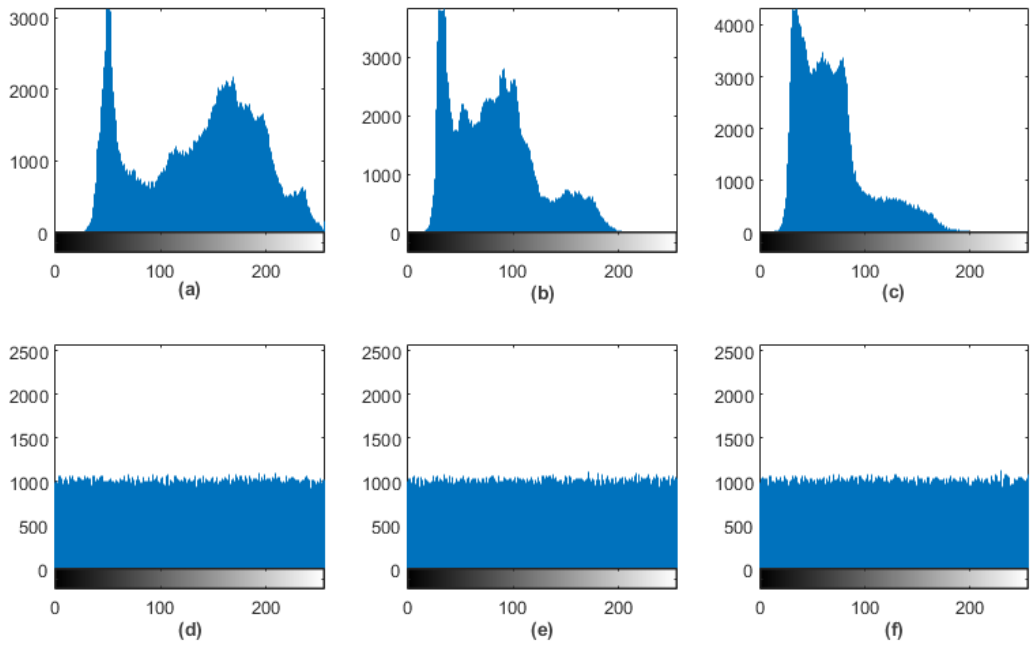


Fig. 8.