IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 7, 2019, accepted October 21, 2019, date of publication October 25, 2019, date of current version November 7, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2949704

An Image Encryption Scheme Based on Hybrid Electro-Optic Chaotic Sources and Compressive Sensing

WEIDONG SHAO[1], MENGFAN CHENG[2], CHENKUN LUO[2], LEI DENG[2], MINMING ZHANG[2], SONGNIAN FU[2], MING TANG[2], (Senior Member, IEEE), AND DEMING LIU[2]

[1]School of Cyber Science and Engineering, Huazhong University of Science and Technology, Wuhan 430074, China
[2]School of Optical and Electronic Information, Huazhong University of Science and Technology, Wuhan 430074, China

Corresponding author: Mengfan Cheng (chengmf@mail.hust.edu.cn)

This work was supported in part by the National Key Research and Development Program of China under Grant 2018YFB1801304, in part by the State Key Laboratory of Advanced Optical Communication Systems and Networks (LOCT) under Grant 2019GZKF7, in part by the National Natural Science Foundation of China (NSFC) under Grant 61675083, and in part by the Key Project of Research and Development Program of Hubei Province under Grant 2017AAA046.

ABSTRACT In this paper, a novel image encryption scheme based on analog-digital hybrid electro-optic chaotic sources and compressive sensing is proposed. Distinguished from other existing chaos-based encryption schemes, analog-digital hybrid electro-optic chaotic sources are utilized, in which the synchronization of chaotic systems can be achieved by transmitting binary digital bits. The robustness of the encryption scheme can be significantly improved and the theoretical transmission distance will be much longer because of digital chaos synchronization. Moreover, owing to the compression of compressive sensing and the sensitivity to initial values of chaotic sources, the proposed scheme can greatly reduce the amount of data and strengthen safety. Exhaustive simulations and analysis demonstrate that the proposed scheme is of good peculiarities such as high efficiency, good robustness and security.

INDEX TERMS Chaotic communication, compressed sensing, encryption, image processing.

I. INTRODUCTION

With the emergence of the fifth generation (5G) mobile networks, all sectors of society will unleash the potential of digitalization and upgrade further. The security of information, a considerable part of which is in graphical form, is involved in lots of fields, such as national security, individual privacy and economic activities. Thus, image encryption has been extensively studied. Recently, many image encryption schemes based on chaotic systems have been proposed [1]–[4]. Since chaotic systems are suitable for cryptography for its sensitivity to system initial parameters and unpredictability of system states.

On the other hand, the processing of images with high precision and large size is a matter of increasing concern [5], which is often omitted in design and security analysis of image encryption schemes. Therefore, the image compression is particularly important for efficient transmission. Compressive sensing (CS), first proposed in [6], is a novel sensing modality at a sub-Nyquist rate, which samples the sparse or compressible signals in original domain or in some transform domain [7]. It can be considered as a representation, with the randomness through the projection and reduction in dimensions, of a signal. Due to the fact that CS can be applied in cryptography and compression simultaneously, many novel solutions of encryption have been proposed [8], [9]. Lately, image encryption schemes based on chaotic CS have become a research focus. In [10], a combination of CS and the Logistic chaotic sequence was carried out. Zhou et al. proposed an efficient image compression–encryption scheme based on 2D compressive sensing and Chen's hyper-chaotic system [11]. A solution for simultaneous image encryption and compression based on CS and three-dimensional (3-D) Cat map was proposed in [12]. The above methods are proved to have the similar performance to the schemes based on CS with common

The associate editor coordinating the review of this manuscript and approving it for publication was Ahmet M. Elbir.

random matrix. Note that digital chaos systems are utilized in these schemes, and the dynamical degradation phenomenon cannot be ignored when this type of chaotic system is realized with finite precisions in digital computing devices [13]. The short period cycles make the solutions based on digital chaos questionable and unreliable [14], [15]. In order to avoid the possible security level decline resulting from the weakness of digital chaos, the researchers have turned sight to analog chaotic systems. A method combining CS with optical chaos is proposed in [16] and it is demonstrated that the optical chaos can lead to good and robust reconstruction of original signals. Theoretically, optical chaos exhibits some exceptional advantages such as wide bandwidth, high dynamical complexity [17]–[19]. Hence, optical chaos can be applied in mass data processing and provide a relatively high security level and high encryption speed. Xie et al. proposed an image encryption-then-transmission system based on optical chaos [20]. In [21], an image encryption system based on a double optical chaotic system was proposed. Li et al. proposed an encryption algorithm based on cascade-coupled semiconductor ring lasers system [22]. Owing to the good properties of optical chaos, these schemes are proved to be efficient and secure. Nevertheless, optical chaos systems practically adopt analog signals to achieve synchronization, which requires strictly identical parameters of systems at the transceiver ends. Meanwhile, the broadband analog optical signals transmitted in fiber links can be affected by the distortion arising from fiber attenuation, chromatic dispersion, fiber nonlinearities, phase noise, polarization effect. Thus, the robustness of the chaos-based image encryption scheme is critical to practical applications and more works are need to focus on it.

In this paper, we propose a novel image encryption-transmission scheme based on analog-digital hybrid electro-optic chaotic sources and compressive sensing. Based on our previous work [23], an electro-optic chaos source is proposed, which integrates the advantages of analog chaotic system and digital chaos. The analog part can generate broadband signals with high dynamical complexity and the digital part establishes the robust long-distance synchronization between two parties for its inherent resistance to the interference of noise [24]. Owing to the hybrid structure, the chaos source shows its potential to be applied in radar and random bit sequences generation [25], [26]. We apply the electro-optic chaos source, combined with CS, to construct a robust and efficient image encryption scheme. The sensing matrix of CS is constructed from the chaotic sequence generated from the analog-digital chaotic sources. Simulations and analysis demonstrate the validity, security and robustness of the proposed encryption-transmission scheme.

II. SYSTEM MODEL AND METHODS

A. ANALOG-DIGITAL HYBRID CHAOS

The proposed analog-digital hybrid chaotic source is shown in Fig. 1. The chaos system is an evolution of the conventional Ikeda system [27]. The transmission from phase modulation to intensity modulation (PM-to-IM) is implemented by a dispersion manipulation device (DMD), which can refer to a fiber Bragg grating (FBG), or a segment of dispersion compensation fiber. The efficiency of the transmission varies with the frequency of the signal and thus a nonlinear filtering effect is induced. The digital part extracts new bits to accomplish the feedback loop and the analog-digital hybrid chaotic system is eventually accomplished.

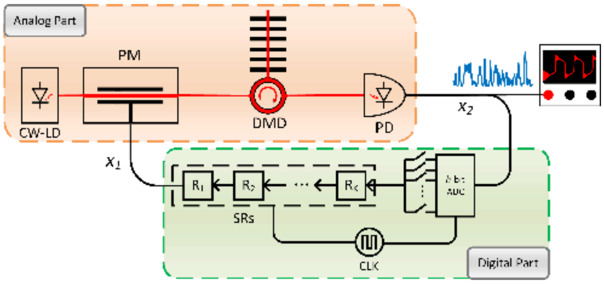


FIGURE 1. The diagram of the chaotic source. CW-LD, continuous-wave laser diode; PM, phase modulator; DMD, dispersion manipulation device; PD, photodiode; ADC, analog-digital converter; SRs, shift registers; CLK, clock frequency.

The mathematical expression of the phase modulation is

$$E\,(t) = \sqrt{P_0}\exp\left[j\,(\omega_0 t + \varphi_0)\right]\exp[jmx_1(n)], \tag{1}$$

where $E(t)$ represents the electric field of the output light signal. ω_0, φ_0 and $x_1(n)$ are the angular frequency, initial phase of the input light and the modulating digital signal, respectively. n is a natural number. $m = (V_S/V_\pi)\pi$ denotes the modulation index, where V_S is the amplitude of input signal and V_π is the half-wave voltage of the PM. The transfer function of DMD in frequency domain can be expressed as

$$H\,(\omega) = \exp[j(d/2)(\omega - \omega_0^2)], \tag{2}$$

where d is the cumulative dispersion value. The reflected optical field can be expressed as $E_1\,(t) = E(t) \otimes h(t)$, where "$\otimes$" denotes convolution and $h\,(t)$ is the time-domain expression of $H\,(\omega)$. The optical signal is transformed to the electrical signal by a photodiode (PD), which can be represented as $x_2\,(t) = E_1 \cdot E_1^*$, where E_1^* is the complex conjugate of E_1. The h-bit analog-digital converter (ADC) converts the analog electrical signal to a digital one. Then, one bit of the parallel digital signal is extracted and sent to a series of shift registers (SR) as the feedback bit. Under the control of the clock frequency (CLK), the continuous laser emitted from the laser diode is phase modulated, and a closed feedback loop is thus formed. The proceeding can be expressed as

$$x_1\,(n+K) = f(g(x_2(t-\tau)\cdot\delta(t-nT+kT))), \tag{3}$$

$$g\,(x) = \begin{cases} round\,\left(x \cdot 2^h\right), & x < 1 - \dfrac{1}{2^{h+1}} \\ 2^h - 1, & x > 1 - \dfrac{1}{2^{h+1}}, \end{cases} \tag{4}$$

$$f\,(x) = \left(x \cdot 2^{1-B}\right)\mathrm{mod}\;2. \tag{5}$$

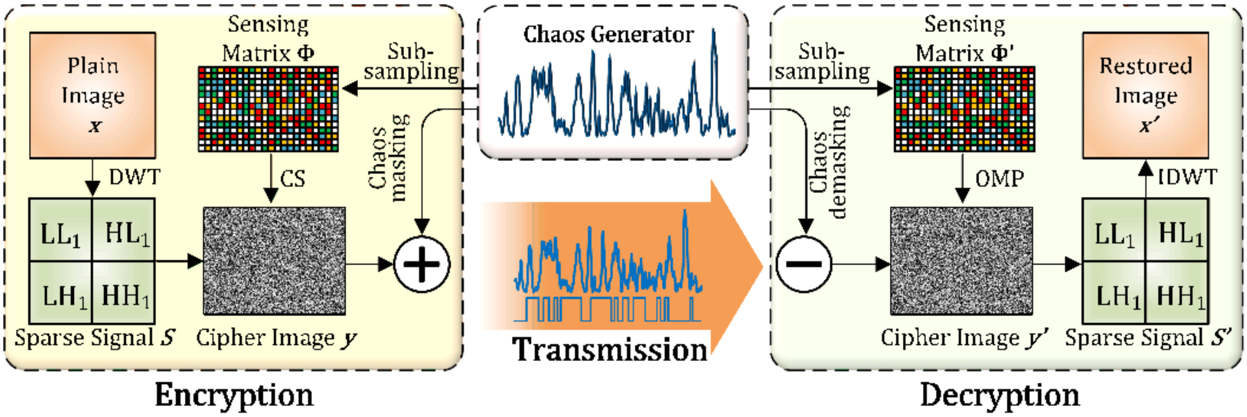


FIGURE 2. Block diagram of how CS works in encryption-transmission scheme.

Here, T is the clock period and $\tau = K \cdot T$ is the time delay of the SRs with the length K. Function $g(x)$ and $f(x)$ represent the process of quantification and bit extraction. $round(x)$ returns the nearest integrant of the value x and B determines which bit of ADC to be the feedback bit. When $B = 1$, the least significant bit of the h-bit digital signals is extracted and sent to SRs as the feedback signal.

According to our previous work [23], with properly selected system parameters, broadband optical chaotic signals can be acquired and the good performance regarding robustness, dynamical properties and complexity can be guaranteed. The analog-digital hybrid structure could overcome the dynamical degradation in pure digital systems in some degree. According to [28], dynamical chaos may survive and be indistinguishable from that of the original chaotic system if randomness is associated with discretization. Therefore, the randomness introduced by the analog circuit can compensate for the short period cycles. Meanwhile, the digital part in our scheme makes it easy to process the signals and transmit for a long haul in communication networks. The complement to each other makes the system a good candidate in practical applications.

B. COMPRESSIVE SENSING

CS combines the sampling and compression steps into one action. For a signal $\boldsymbol{x} \in \boldsymbol{R}^N$, it can be represented as a linear combination of columns of $\boldsymbol{\Psi} \in \boldsymbol{R}^{N\times N}$ or the basis vectors as

$$\boldsymbol{x} = \sum_{i=1}^{N} \psi_i s_i = \boldsymbol{\Psi}^{\boldsymbol{T}} \boldsymbol{S}, \tag{6}$$

where $\boldsymbol{S} \in \boldsymbol{R}^N$ denotes the sparse coefficient vectors. The compression is realized by the sensing matrix $\boldsymbol{\Phi} \in \boldsymbol{R}^{M\times N}(M \ll N)$. The measurements $\boldsymbol{y}$ with length M can be obtained in the linear measurement process, which can be represented as

$$\boldsymbol{y} = \boldsymbol{\Phi x}. \tag{7}$$

The measurements $\boldsymbol{y}$ can be expressed as

$$\boldsymbol{y} = \boldsymbol{\Phi x} = \boldsymbol{\Phi \Psi^T S} = \boldsymbol{\Theta S}, \tag{8}$$

where $\boldsymbol{\Theta} = \boldsymbol{\Phi\Psi^T}$ is the measurement matrix with the size of $M \times N$. The recovery of the original signal $\boldsymbol{x}$ from the measurements $\boldsymbol{y}$ can be posed as a convex optimization problem and it can be solved by utilizing linear programming solvers. Here, we use the Orthogonal Matching Pursuit (OMP) algorithm which is a step-by-step iterative method and can lower the computational complexity [29], [30]. To perfectly recover the original signal from the measurements $\boldsymbol{y}$, the matrix $\boldsymbol{\Theta}$ must obey Restricted Isometry Property (RIP) [31].

Definition 1: A matrix $\boldsymbol{\Phi} \in \boldsymbol{R}^{M\times N}$ satisfies the Restricted Isometry Property of order k when there exists a constant $\delta \in [0, 1]$ and it has $(1-\delta)\,\|\boldsymbol{s}\|_2^2 \le \|\boldsymbol{\Phi s}\|_2^2 \le (1+\delta)\,\|\boldsymbol{s}\|_2^2$ for a k-sparse $\boldsymbol{s}$.

Bandeira et al. have proved that testing whether a matrix satisfies RIP is NP-hard [32]. Another simpler condition which guarantees stable solution is the incoherence between the matrix $\boldsymbol{\Phi}$ and basis $\boldsymbol{\Psi}$. It is proved that any chaos system that can yield an approximately independent and identical distribution sequence will generate chaotic sensing matrix satisfying the RIP [33].

The block diagram describing how CS works in our image processing scheme is shown in Fig. 2. Here, we take an $N \times N$ 256-grey-scale picture as the input message. To make full use of CS, which performs better when processing sparse signals, we utilize the two-dimensional Discrete Wavelet Transform (DWT) to decompose the plain image. In Fig. 2, LL_1, HL_1, LH_1 and HH_1 are the coefficient matrices in the wavelet transform domain. They indicate the high and low frequency components in the horizontal and vertical direction of the image. The sparse representation of the plain image can be measured by the matrix $\boldsymbol{\Phi}$, the design of which directly influences the performance of signal reconstruction. Let $\varepsilon(D, e_*)$ be the sequence sub-sampled and quantized from the chaotic sequence e_i with the interval factor D and the first sampled value e_*. In order to strengthen the robustness of the scheme, the dual thresholds quantization is utilized as a post-processing technique [34], [35]. Each element of $\boldsymbol{\Phi}$, denoted by ϕ, is a decimal number converted from every eight adjacent binary bits of $\varepsilon(d, e_0)$. To adapt the size of image, the sequence constituting the matrix $\boldsymbol{\Phi}$ with length NM is acquired. Then, we can construct the sensing matrix $\boldsymbol{\Phi}$ column by column with the sequence $\{\phi\}_{n=0}^{NM-1}$, that is

$$\boldsymbol{\Phi} = \frac{1}{\sqrt{M}\sigma}\begin{pmatrix} \phi_{11} & \cdots & \phi_{1N} \\ \vdots & \ddots & \vdots \\ \phi_{M1} & \cdots & \phi_{MN} \end{pmatrix}, \tag{9}$$

where σ is the standard deviation of $\{\phi_{ij}\}$, and $1 \leq i \leq M, 1 \leq j \leq N$. The scaler $1/(\sqrt{M}\sigma)$ is used for normalization. Owing to the sampling distance d, the entries of ϕ_{ij} are approximately independent and satisfy identical distribution, i.e. a.i.i.d. In [10], Yu has proved that the a.i.i.d sensing matrix, constructed following (9), satisfies RIP for constant $\delta > 0$ with overwhelming probability, providing that $k \leq O(M/log(N/k))$. To further enhance the security performance in the transmission channel, chaos masking (CMS) technique [36] is utilized, details of which will be elaborated in the next subsection.

In the receiver, after chaos de-masking, the sparse representation of plain image can be reconstructed by OMP algorithm with the uniform sensing matrix $\boldsymbol{\Phi}'$ generated with the same rules. The primary steps of OMP algorithm are stated in Table 1. In the iteration of OMP, the residual is always orthogonal to the selected column of $\boldsymbol{\Phi}$ and it will not be selected in the subsequent loop, which can expedite the convergent speed of iteration.

TABLE 1. **The primary steps of omp algorithm.**

Input:	The measurement vector $\boldsymbol{y}$ The normalized sensing matrix $\boldsymbol{\Phi}$
Initialize the residual $\boldsymbol{r_0} = \boldsymbol{y}$ and the set of selected variables $\boldsymbol{\Phi}(c_0) = \emptyset$; Loop: • Find the variables $\boldsymbol{\Phi}_{t_i}$ solving the maximization problem $max_t\lvert\boldsymbol{\Phi}'_t r_{i-1}\rvert$; • Add the $\boldsymbol{\Phi}_{t_i}$ to the set of selected variables and add c_i to the set of indexes of selected ones; • Let $\boldsymbol{P_i} = \boldsymbol{\Phi}(c_i)\big(\boldsymbol{\Phi}(c_i)'\boldsymbol{\Phi}(c_i)\big)^{-1}\boldsymbol{\Phi}(c_i)'$ denote the projection onto the linear space spanned by the elements of $\boldsymbol{\Phi}(c_i)$; • Update the residual $\boldsymbol{r_i} = (\boldsymbol{I} - \boldsymbol{P}_i)\boldsymbol{y}$; The loop breaks when the residual is smaller than the threshold δ. The estimate $\boldsymbol{S}'$ has nonzero indices at the components listed in $\{c_i\}$.	
Output:	The reconstructed signal $\boldsymbol{S}'$

After the reconstruction, we can then get the restored image with Inverse Discrete Wavelet Transform (IDWT). The data transmitted in the main channel is compressed by CS with the compression ratio $r = M/N$, which will decrease the energy consumption of data transmission and improve the efficiency of the communication network.

C. IMAGE ENCRYPTION SCHEME

Based on analog-digital hybrid electro-optic chaotic sources and compressive sensing, we proposed an image encryption-transmission scheme, and its schematic diagram is shown in Fig. 3. The compressed image data of Alice is further masked by the analog chaotic carrier and then transmitted to Bob. Another logical channel is used to transmit the digital signal and the restored image can be achieved at Bob with the synchronized chaotic signal and OMP algorithm.

Owing to the digital synchronization strategy, robust transmission between Alice and Bob will be established. Synchronized analog chaotic signals can be generated by deploying components of identical parameters at both ends. After sampling and quantifying the analog electrical signal x_2 with ADC, Alice can get binary bits and transmit them to SRs in the local loop. Then, the digital signal x_1 will be amplified and modulated on a light wave with a PM to complete the feedback loop. The feedback bits b generated at Alice are also transmitted to Bob by a digital transmitter (Tx) over digital optical communication network in the meantime. Bob receives the feedback bits b' by a digital receiver (Rx) and regenerates the digital signal x'_1. Theoretically, with corresponding components and matched delay-time, Bob can achieve the same chaotic signals $-x'_2$ as Alice, where "$-$" represents the opposite direction.

In the end of Alice, the plain image is transformed into the encrypted one by CS with the complex and unpredictable chaotic sequences generated from the analog-digital hybrid chaos system. The sensing matrix $\boldsymbol{\Phi}$ is designed with the chaotic sequences following (9). Then, the encrypted image is transformed into binary on-off keying (OOK) format optical messages with smaller amplitude and mixed with chaotic carrier signals according to some proportions to ensure that no information related to the plain image is leaked. Let $m_0 + x_2$ be the transmission signal in Alice and the encrypted image m_0 can be achieved by subtracting x'_2 from $m_0 + x_2$, which is performed by adding the currents coming from the ordinary and sign-inverting photodiode (i.e., PD and IPD, respectively). Then, following the reconstruction method of CS mentioned in the previous subsection, we will obtain the decrypted image.

High quality chaos synchronization between the output analog chaotic signal x_2 and its counterpart x'_2 lays the groundwork for effective encryption and transmission of images. From the perspective of chaotic CS, the consistency between matrix $\boldsymbol{\Phi}$ and $\boldsymbol{\Phi}'$ is significantly dependent on the synchronization quality between x_2 and x'_2. In order to ensure the robustness, dual thresholds quantization is used. When x_2 and x'_2 are quantified into binary bits by Alice and Bob respectively, the values larger than the high threshold are coded as "1" and the ones smaller than the low threshold are coded as "0". Those values between the two thresholds are discarded. The thresholds are given as $Thr_H = mean\,(e) + \xi \cdot \sigma_e$, where $mean\,(e)$, σ_e and ξ are the average value and standard deviation of e_i and the factor controlling the dual thresholds gap, respectively. During the commissioning stage, the dual thresholds gap is determined by adjusting the parameter t. Considering the bits discarded in the quantization, the sensing matrix can remain unchanged for a period

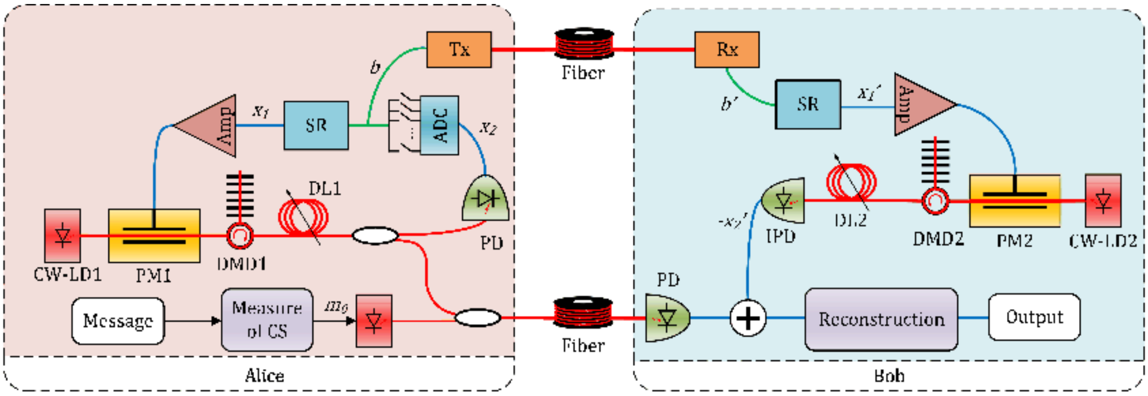


FIGURE 3. The schematic diagram of the image processing scheme.

of time to make up for the potential loss of efficiency. From the transmission point of view, correct chaos de-masking also relies on well synchronized chaotic signals. In this stage, the quality of synchronization is mainly influenced by the parameter mismatch of components, which is the primary problem we probed into.

III. NUMERICAL SIMULATIONS

A. THE CHAOTIC SIGNAL

To investigate the feasibility of the proposed scheme, a series of simulation are carried out with MATLAB R2015b and VPItransmissionMaker 9.0 software. Key parameters are listed by Table 2.

TABLE 2. Key parameters of the simulation system.

Description	Value
Feedback bits generation rate	10G bit/s
Emission frequency of LDs	193.1 THz
Average power of LDs P_0	1 mW
Initial phase of LDs φ_0	0 deg
Modulation index of PM m	π
Cumulative dispersion value d	3000 ps/nm
Number of registers of SR K	30
Dual thresholds determinative factor ξ	0.1

Figs. 4(a) and (b) display the time series and autocorrelation function (ACF) of the chaotic signal captured by PD. The noise-like intensity fluctuations in the time series demonstrate the typical features of chaos. In the curve of ACF, the steep peak and the quick decay indicate the good property of randomness and non-repetition of the chaotic signal. The typical Lyapunov exponent of the chaotic signal is the positive value 0.0739, which means the system has been in the state of chaos.

B. ENCRYPTION RESULT

A 256 × 256 pixels 256-scale gray picture is chosen as the test image, as shown in Fig. 5(a). The parameters constructing the chaotic sensing matrix are set as $D = 5$, $M = 192$, $e_* = e_{150}$. In Fig. 5(b) and (c), it is observed that the cipher image is converted into mess totally and leaks no useful information related to corresponding plain image and the scheme can reconstruct the initial image successfully after transmission through 40km standard single mode fiber (SSMF). Note that the size of the cipher image is smaller compared with the size of the original image and the recovered image, since the compression and encryption are implemented simultaneously in CS.

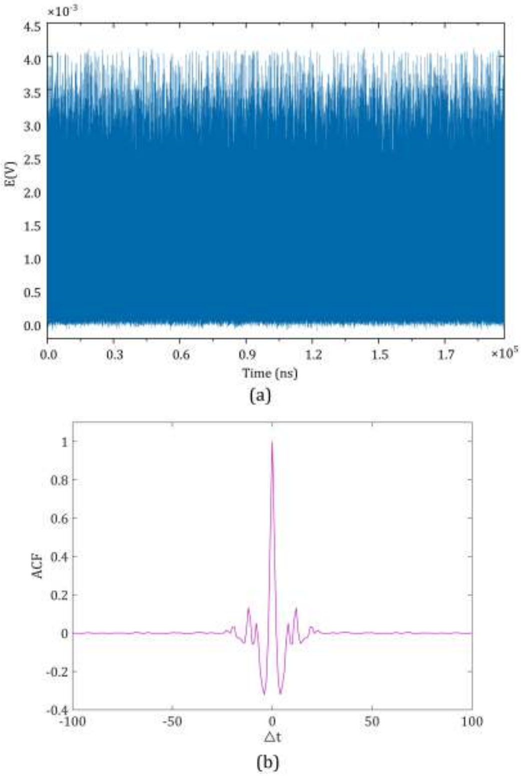


FIGURE 4. (a) the time series of the output chaotic laser (b) the autocorrelation function (ACF) of the chaotic signal.

In order to quantify the performance of image recovery, peak signal to noise ratio (PSNR) is introduced. In the field

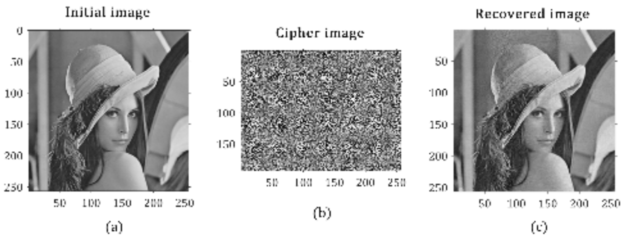


FIGURE 5. Simulation results of the image encryption system. (a) The initial image; (b) The cipher image; (c) The recovered image.

of image processing, PSNR can be defined as

$$PSNR = 20log_{10}(MAX_f/\sqrt{MSE}), \qquad (10)$$

where MAX_f means the maximum value existing in the image, such as 255 here, and MSE is mean squared error. MSE can be expressed as

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f\,(i,j) - g(i \cdot j)\|^2, \qquad (11)$$

where m, n, f and g are the numbers of rows and columns of pixels of the image, the matrix data of initial image and the matrix data of the recovered image, respectively.

Empirically, PSNR of 30 dB can guarantee good recovery, and when it decays to 20 dB, the recovery effect becomes generally acceptable. The reconstruction will fail when PSNR falls to 10 dB, even though picture messages are more robust and less vulnerable to disturbances than text messages. In this case, PSNR of the image recovery is 31.7743 dB, which means good performance of image reconstruction.

IV. DISCUSSION AND COMPARISON

A. SECURITY ANALYSES

1) HISTOGRAM ANALYSIS

An image histogram, the basic attribute of digital image, is the pictorial description of the distribution of pixel intensities. The histogram of a plain image is distinctive to others for its unique pattern, which enable attackers to deduce the information of the image by statistical analysis of the histogram. As can be seen in Fig. 6, the histogram of the cipher image is uniformly distributed and the redundancy of the plain image is well hidden, which means no relevance can be found between plain images and cipher images.

2) CORRELATION ANALYSIS

The correlation between adjacent pixels is the intrinsic property of a meaningful image. By an effective image encryption, the correlation between adjacent pixels will be sufficiently low. We randomly select 4000 pixels as the sample and calculate the correlation γ_{xy} in horizontal, vertical and diagonal directions. Taking x, y and N as the gray-level values of the selected adjacent pixels and the number of samples respectively, we can get the mean $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$, variation $D(x)\frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$ and covariance $cov(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))$. The definition of correlation coefficients can be presented as $\gamma_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$. The correlation coefficients of plain image and cipher image in three dimensions are listed in Table 3 and the adjacent pixel dots are plotted in Fig. 7. (a), (b) and (c) represent correlation plots of the plain image in horizontal, vertical and diagonal directions severally, and (d), (e) and (f) are correlation plots of the cipher image. We can notice that, the pixels in the plain image are relatively gathered on the diagonal, regardless of the dimension, and the correlation coefficients of the plain image approach 1, which indicates the strong correlation between adjacent pixels. With the effective image encryption, the pixel dots are scattered over the entire plane and the correlation coefficients are all close to 0, which indicate a good correlation performance. Hence, the image data can be protected against from statistical attacks and the security can be guaranteed by the proposed scheme.

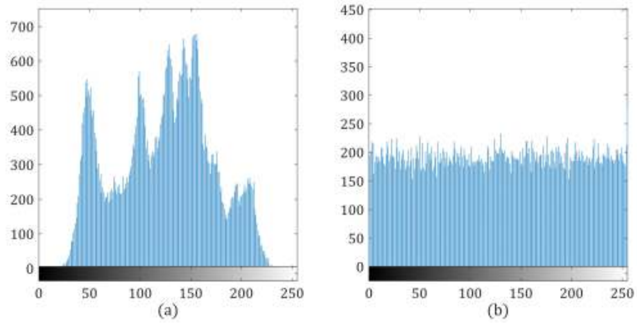


FIGURE 6. Histogram of (a) the plain image and (b) the cipher image.

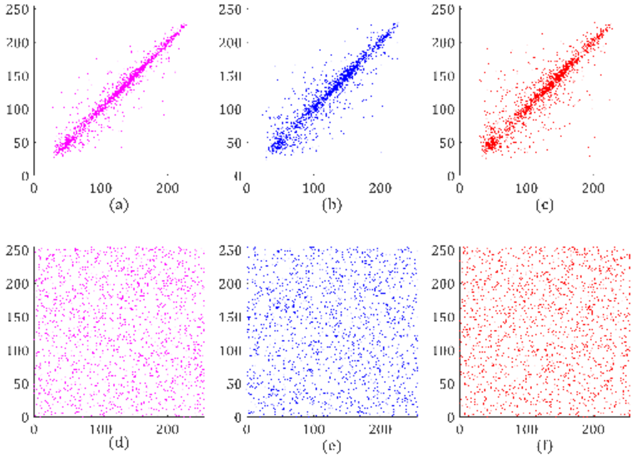


FIGURE 7. Pixel correlation analysis: the adjacent pixel dots in horizontal, vertical and diagonal directions.

TABLE 3. Correlation coefficients of adjacent pixels.

Image	Horizontal	Vertical	Diagonal
Plain image	0.96655	0.93627	0.90381
Cipher image	-0.026365	0.036622	-0.016428

3) INFORMATION ENTROPY

Information entropy refers to the disorder or uncertainty of an information source [39]. If we have a set of possibilities with probabilities $\{P_{S_i}\}$, the entropy $H(s)$ of a message source s is

$$H(s) = -\sum_{i=0}^{2^N-1} P(s_i)\, log_2 P(s_i)\,. \qquad (12)$$

Theoretically, the entropy of a random source consisting of 2^N symbols is N. For a 256-grey-scale image, the entropy should be 8. The entropy of the plain Lena image is 7.4532 dB, and the entropy of the cipher image is up to 7.9845 dB. The performance is good enough to resist brute force attack, considering the smaller size of the cipher text after encryption and compression.

B. ROBUSTNESS ANALYSIS

The robustness of the system is mainly dependent on the synchronization quality between chaotic signals x_2 and x_2'. Due to the fact that digital signals are easy to process, recover and reshape with the highly developed digital communication technologies in long haul transmissions, the digital x_1' is assumed to be received error free. Therefore, the synchronization quality is determined by parameter mismatch of the analog devices between two parties.

The parameters of modules in the analog feedback loop are considered: cumulative dispersion of FBG d, modulation index of PM m and the difference of time-delay Δt. We depict the mismatch ratios of d and m as $r_1 = (d - d_*)/d_*$ and $r_2 = (m - m_*)/m_*$, where d_* and m_* are the reference values in Alice.

Firstly, we investigate the impact of parameter mismatch on the bit error rate (BER) of the analog transmission channel. As shown in Fig. 8 (a), (b) and (c), the cipher image m_0 can be received error free when $r_1 \in (-0.33\%, 0.33\%)$, $r_2 \in (-11.11\%, 11.11\%)$ and $\Delta t \in (-10\,ps, 10\,ps)$. With the rise in mismatch degrees, BER increases dramatically. These phenomena indicate that the transmission process is robust to a certain degree of parameter mismatch, yet sensitive enough for an unauthorized eavesdropper. The cipher data is hard to acquire correctly without knowing the parameters.

After the cipher image is received by Bob, the decryption process at the digital domain is also influenced by the parameter mismatch. Since the consistency of sensing matrixes are determined by the synchronization degree. We use PSNR as the indicator of the performance of image decryption. As shown in Fig. 8 (d), in the range of $[-1.5, 1.5]$ of r_1, a PSNR lager than 30 dB can be guaranteed, which means the good performance of recovery. When r_1 is out of range, PSNR will decrease rapidly, indicating a failed decryption. In Fig. 8 (e), the good recovery of image can be maintained in the range of [-0.05, 0.05] for r_2. The quality of decryption will decline greatly when r_2 is beyond the tolerance. By contrast, Δt in the range of [-12ps, 12ps] can maintain the PSNR over 30 dB, shown in Fig. 8 (f). The sensitivity to time-delay mismatch is result of the great variation of chaotic signals when time-delay changes. The above results demonstrate that the scheme is robust for the parameters, which gives tolerance for mismatch in practical application, and the security is also guaranteed.

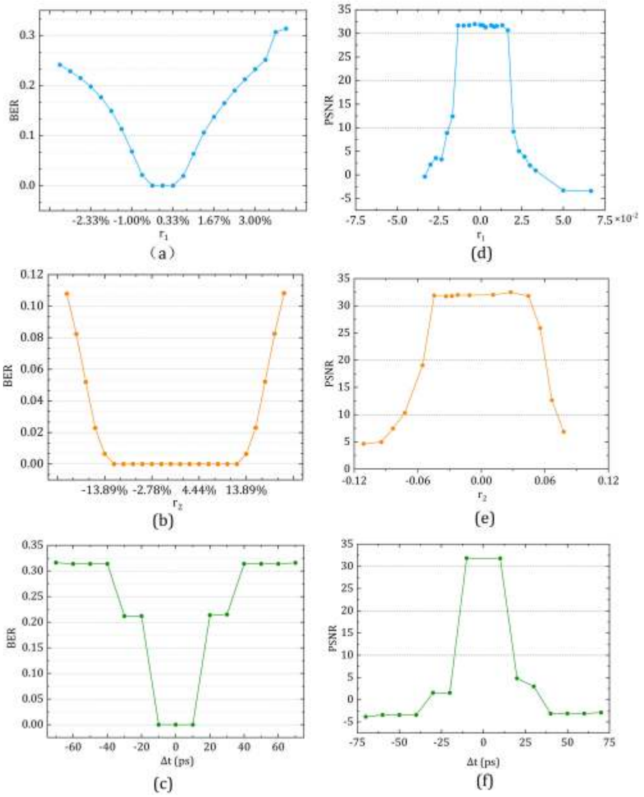


FIGURE 8. The impact of parameter mismatch on BER and PSNR.

According to the analyses above, the overall performance of the image reconstruction is influenced simultaneously by the analog transmission-demasking stage and the digital decryption in CS stage. Practically, the performance of transmission can be improved further by forward error correction (FEC) coding techniques. And, by increasing the dual-quantization gap determining factor ξ, the tolerance for parameter mismatch will be broadened, making it easier to synchronize. However, more bits will be abandoned in quantization with the increase of ξ. There is a trade-off between the performance of the image decryption and the redundancy and efficiency of system.

C. COMPARISON AND INDUCTION

We compared our scheme with some recent image encryption schemes based on CS and chaos in [11], [37], [38] in PSNR, correlation coefficients and information entropy. The comparison results are shown in Table 4, Table 5 and Table 6, respectively.

As shown in Table 4, our scheme can get a PSNR near the average level. We can conclude that our scheme has the similar performance in image recovery compared with the other schemes. From the comparison results shown in Table 5 and Table 6, it can be found that our scheme has slightly

TABLE 4. PSNR under different encryption schemes.

Schemes	r	PSNR (dB)
Our scheme	0.75	**31.7743**
Ref [11]		29.2184
Ref [37]		32.9831
Ref [38]		33.25

TABLE 5. Comparison in correlation coefficients.

Scheme	Horizontal	Vertical	Diagonal
Plain image	0.96655	0.93627	0.90381
Our scheme	**-0.026365**	**0.036622**	**-0.016428**
Ref [11]	−0.0015	0.0041	0.0069
Ref [37]	0.0001082	−0.0011035	−0.0014243
Ref [38]	0.0033	0.0027	0.0014

TABLE 6. Comparison in information entropy.

Scheme	Information entropy
Plain image	7.4532
Our scheme	**7.9845**
Ref [11]	7.9935
Ref [37]	7.9968
Ref [38]	7.9975

larger correlation coefficients and a little smaller information entropy than the others. This fact could be attributed to the absence of pixel position perturbing strategy in our scheme.

It is worth noting that the schemes we compared above are based on digital chaotic maps. As indicated in [15], the orbit of a digital chaos system will enter a cycle after a transient process, some short cycles could also exist under low calculation precision. The degradation of the dynamics hides potential security threats in these digital systems. This limitation may be remedied in some degree by some enhancement methods, like increasing the arithmetic precision or cascading among multiple digital chaotic maps. However, this will also increase the computational complexity.

To overcome the weakness of digital chaos, optical analog chaos-based image encryption and transmission systems are proposed [20], [21]. Broadband and highly complex optical chaotic signal can meet the demands of security and high-speed transmission at a same time. Nevertheless, the synchronization between transceivers in [20], [21] is established by injecting a chaotic signal from a master laser into two slave laser systems. The synchronization signal is in analog form and needs to travel over a long distance. The analog signal will inevitably be distorted by various optical impairments and is hard to accurately recover after a long-distance transmission, which will degrade the synchronization.

Compared with these analog chaos-based schemes, our method is proposed based on an analog-digital chaotic source which can take the digital signals as the synchronization signal. It is more robust against the distraction. Error free transmission is not very hard to guarantee by using existing digital communication technologies. As a result, the synchronization performance will be improved under long-haul transmission scenario. The digital part of our chaotic system is formed by a series of shift registers, which is simple to implement with low computing load. The randomness introduced by the optical analog components makes the overall system reveal the non-periodic and complex chaotic characteristic.

From the digital encryption point of view, considering the limited generation rate of the sensing matrix, we use the same sensing matrix for a period of time to implement real-time encryption. The sensing matrix may be obtained under known plaintext attack (KPA) or chosen plaintext attack (CPA). However, the proposed image protection method relies on the coordination of different layers, namely the CS encryption algorithm at digital field and chaos mask transmission at analog field. From the analog transmission point of view, the encrypted and compressed images are converted to binary bits, and then masked by non-periodic optical chaotic signal with the bandwidth over several GHz to establish a real time secure transmission. In the overall system, the keys are the analog parameters including the time-delay, dispersion, etc., and these parameters are hard to obtain even under KPA/CPA. As a result, high-speed robust transmission and high security level are simultaneously ensured by the analog-digital chaos source.

V. CONCLUSION

We proposed a novel image encryption-transmission scheme based on hybrid electro-optic chaotic sources and CS. The analog-digital chaos source is used to construct the sensing matrix of CS and chaos masking is also utilized to enhance the security of the system. The digital synchronization signals can improve the robustness of the scheme and suitable for long-haul transmission. It is proved that the proposed scheme can encrypt image well and has a good robustness for the parameter mismatch. Meanwhile, the proposed scheme implements encryption and compression at the same time, which makes it a promising candidate for image encryption and high-speed transmission. Our future work will focus on two main points. First, we will improve the structural design of the analog-digital chaotic source. In order to enlarge the analog parameter space and increase the complexity of the chaotic signal, more extension and evolution will be carried out based on the existing digital part and analog part. Then, we will turn to realize the whole system in experiments based on the numerical simulations. Different solutions with practical significance will be proposed according to the different requirements of security and transmission under various scenarios.

REFERENCES

[1] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image Vis. Comput.*, vol. 24, no. 9, pp. 926–934, 2006, doi: 10.1016/j.imavis.2006.02.021.

[2] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos," *Phys. Lett. A*, vol. 372, no. 4, pp. 394–400, 2008, doi: 10.1016/j.physleta.2007.07.040.

[3] Y. Wang, Z. Zhang, G. Wang, and D. Liu, "A pseudorandom number generator based on a 4D piecewise logistic map with coupled parameters," *Int. J. Bifurcation Chaos*, vol. 29, no. 9, 2019, Art. no. 1950124, doi: 10.1142/s0218127419501244.

[4] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Process.*, vol. 92, no. 4, pp. 1101–1108, Apr. 2012, doi: 10.1016/j.sigpro.2011.10.023.

[5] C. Li, Y. Zhang, and E. Y. Xie, "When an attacker meets a cipher-image in 2018: A year in review," *J. Inf. Secur. Appl.*, vol. 48, Oct. 2019, Art. no. 102361, doi: 10.1016/j.jisa.2019.102361.

[6] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006, doi: 10.1109/tit.2006.871582.

[7] M. Rani, S. Dhok, and R. Deshmukh, "A systematic review of compressive sensing: Concepts, implementations and applications," *IEEE Access*, vol. 6, pp. 4875–4894, 2018.

[8] L. Y. Zhang, K.-W. Wong, Y. Zhang, and J. Zhou, "Bi-level protected compressive sampling," *IEEE Trans. Multimedia*, vol. 18, no. 9, pp. 1720–1732, Sep. 2016, doi: 10.1109/tmm.2016.2581593.

[9] J. Wang, L. Y. Zhang, J. Chen, G. Hua, Y. Zhang, and Y. Xiang, "Compressed sensing based selective encryption with data hiding capability," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/tii.2019.2924083.

[10] Y. Lei, J. P. Barbot, G. Zheng, and H. Sun, "Compressive sensing with chaotic sequence," *IEEE Signal Process. Lett.*, vol. 17, no. 8, pp. 731–734, Aug. 2010, doi: 10.1109/Lsp.2010.2052243.

[11] N. R. Zhou, S. M. Pan, S. Cheng, and Z. H. Zhou, "Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing," *Opt. Laser Technol.*, vol. 82, pp. 121–133, Aug. 2016, doi: 10.1016/j.optlastec.2016.02.018.

[12] J. Chen, Y. Zhang, L. Qi, C. Fu, and L. Xu, "Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression," *Opt. Laser Technol.*, vol. 99, pp. 238–248, Feb. 2018, doi: 10.1016/j.optlastec.2017.09.008.

[13] S. Li, M. Cheng, L. Deng, S. Fu, M. Zhang, M. Tang, P. Shum, and D. Liu, "Secure strategy for OFDM-PON using digital chaos algorithm with fixed-point implementation," *J. Lightw. Technol.*, vol. 36, no. 20, pp. 4826–4833, Oct. 15, 2018, doi: 10.1109/jlt.2018.2865222.

[14] C. Li, D. Lin, J. Lü, and F. Hao, "Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography," *IEEE MultiMedia*, vol. 25, no. 4, pp. 46–56, Oct./Dec. 2018, doi: 10.1109/mmul.2018.2873472.

[15] C. Li, D. Lin, B. Feng, J. Lü, and F. Hao, "Cryptanalysis of a chaotic image encryption algorithm based on information entropy," *IEEE Access*, vol. 6, pp. 75834–75842, 2018, doi: 10.1109/access.2018.2883690.

[16] D. Rontani, D. Choi, C.-Y. Chang, A. Locquet, and D. S. Citrin, "Compressive sensing with optical chaos," *Sci. Rep.*, vol. 6, Dec. 2016, Art. no. 35206, doi: 10.1038/srep35206.

[17] F. Rogister, A. Locquet, D. Pieroux, M. Sciamanna, O. Deparis, P. Mégret, and M. Blondel, "Secure communication scheme using chaotic laser diodes subject to incoherent optical feedback and incoherent optical injection," *Opt. Lett.*, vol. 26, no. 19, pp. 1486–1488, 2001.

[18] K. Hirano, T. Yamazaki, S. Morikatsu, H. Okumura, H. Aida, A. Uchida, S. Yoshimori, K. Yoshimura, T. Harayama, and P. Davis, "Fast random bit generation with bandwidth-enhanced chaos in semiconductor lasers," *Opt. Express*, vol. 18, no. 6, pp. 5512–5524, Mar. 2010.

[19] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. García-Ojalvo, C. R. Mirasso, L. Pesquera, and K. A. Shore, "Chaos-based communications at high bit rates using commercial fibre-optic links," *Nature*, vol. 438, no. 7066, p. 343, Nov. 2005.

[20] Y. Xie, J. Li, Z. Kong, Y. Zhang, X. Liao, and Y. Liu,, "Exploiting optics chaos for image encryption-then-transmission," *J. Lightw. Technol.*, vol. 34, no. 22, pp. 5101–5109, Nov. 15, 2016, doi: 10.1109/jlt.2016.2606121.

[21] X.-Q. Fu, B.-C. Liu, Y.-Y. Xie, W. Li, and Y. Liu, "Image encryption-then-transmission using DNA encryption algorithm and the double chaos," *IEEE Photon. J.*, vol. 10, no. 3, Jun. 2018, Art. no. 3900515, doi: 10.1109/jphot.2018.2827165.

[22] J. Li, S. Xiang, H. Wang, J. Gong, and A. 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, doi: 10.1016/j.optlaseng.2017.11.001.

[23] M. Cheng, C. Luo, X. Jiang, L. Deng, M. Zhang, C. Ke, S. Fu, M. Tang, P. Shum, and D. Liu, "An electrooptic chaotic system based on a hybrid feedback loop," *J. Lightw. Technol.*, vol. 36, no. 19, pp. 4259–4266, Oct. 1, 2018, doi: 10.1109/jlt.2018.2814080.

[24] C. Luo, M. Cheng, X. Jiang, L. Deng, M. Zhang, C. Ke, S. Fu, M. Tang, D. Liu, and P. Shum, "Broadband optical chaos generation by constructing a simple hybrid feedback loop," presented at the Int. Top. Meeting Microw. Photon. (MWP), Oct. 2017.

[25] M. Cheng, X. Jiang, C. Luo, Y. Fu, F. Luo, L. Deng, and D. Liu, "Bistatic radar scheme based on the digital-analog hybrid chaos system," *Opt. Express*, vol. 26, no. 17, pp. 22491–22505, Aug. 2018, doi: 10.1364/OE.26.022491.

[26] Z. Zhao, M. Cheng, C. Luo, L. Deng, M. Zhang, S. Fu, M. Tang, P. Shum, and D. Liu, "Synchronized random bit sequences generation based on analog-digital hybrid electro-optic chaotic sources," *J. Lightw. Technol.*, vol. 36, no. 20, pp. 4995–5002, Oct. 15, 2018, doi: 10.1109/jlt.2018.2868498.

[27] K. Ikeda, "Multiple-valued stationary state and its instability of the transmitted light by a ring cavity system," *Opt. Commun.*, vol. 30, no. 2, pp. 257–261, 1979, doi: 10.1016/0030-4018(79)90090-7.

[28] M. Falcioni, A. Vulpiani, G. Mantica, and S. Pigolotti, "Coarse-grained probabilistic automata mimicking chaotic systems," *Phys. Rev. Lett.*, vol. 91, no. 4, Jul. 2003, Art. no. 044101, doi: 10.1103/PhysRevLett.91.044101.

[29] H. Liu, A. Kadir, and X. Sun, "Chaos-based fast colour image encryption scheme with true random number keys from environmental noise," *IET Image Process.*, vol. 11, no. 5, pp. 324–332, 2017, doi: 10.1049/iet-ipr.2016.0040.

[30] Y. C. Pati, R. Rezaiifar, and P. S. Krishnaprasad, "Orthogonal matching pursuit: Recursive function approximation with applications to wavelet decomposition," in *Proc. 27th Asilomar Conf. Signals, Syst. Comput.*, Nov. 1993, pp. 40–44.

[31] V. Cambareri, M. Mangia, F. Pareschi, R. Rovatti, and G. Setti, "Low-complexity multiclass encryption by compressed sensing," *IEEE Trans. Signal Process.*, vol. 63, no. 9, pp. 2183–2195, May 2015.

[32] A. S. Bandeira, E. Dobriban, D. G. Mixon, and W. F. Sawin, "Certifying the restricted isometry property is hard," *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 3448–3450, Jun. 2013.

[33] H. Gan, Z. Li, J. Li, X. Wang, and Z. Cheng, "Compressive sensing using chaotic sequence based on Chebyshev map," *Nonlinear Dyn.*, vol. 78, no. 4, pp. 2429–2438, 2014, doi: 10.1007/s11071-014-1600-1.

[34] C. Xue, N. Jiang, K. Qiu, and Y. Lv, "Key distribution based on synchronization in bandwidth-enhanced random bit generators with dynamic post-processing," *Opt. Express*, vol. 23, no. 11, pp. 14510–14519, May 2015, doi: 10.1364/OE.23.014510.

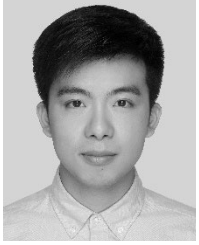
[35] X.-Z. Li, S.-S. Li, and S.-C. Chan, "Correlated random bit generation using chaotic semiconductor lasers under unidirectional optical injection," *IEEE Photon. J.*, vol. 9, no. 5, Oct. 2017, Art. no. 1505411.

[36] 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, doi: 10.1364/ol.24.001200.

[37] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, "An image encryption algorithm based on chaotic system and compressive sensing," *Signal Process.*, vol. 148, pp. 124–144, Jul. 2018, doi:10.1016/j.sigpro.2018.02.007.

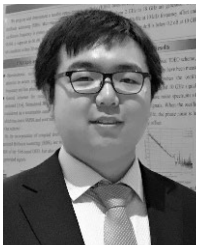
[38] N. Zhou, A. Zhang, J. Wu, D. Pei, and Y. Yang, "Novel hybrid image compression–encryption algorithm based on compressive sensing," *Optik*, vol. 125, no. 18, pp. 5075–5080, 2014, doi: 10.1016/j.ijleo.2014.06.054.

[39] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.



WEIDONG SHAO received the B.S. degree in optoelectronics information science and engineer from Soochow University, Suzhou, China, in 2018. He is currently pursuing the Doctor's degree in cyberspace security with the Huazhong University of Science and Technology. His research interests include secure communications and chaotic encryption.

MENGFAN CHENG received the B.S. degree in information engineering and the M.S. and Ph.D. degrees in computer science from the Huazhong University of Science and Technology, Wuhan, China, in 2005, 2007, and 2012, respectively. He is currently a Lecturer with the Huazhong University of Science and Technology. His research interests include secure communications, chaotic encryption, and chaotic synchronization.



CHENKUN LUO received the B.Eng. degree in optical engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2017, where he is currently pursuing the master's degree in optoelectronic information engineering. His research interests include the design, realization, and application of electro-optical chaos sources.

LEI DENG received the B.S., M.S., and Ph.D. degrees in optoelectronics and information engineering from the Huazhong University of Science and Technology (HUST), Wuhan, China, in 2006, 2008, and 2012, respectively. He was with the Technical University of Denmark as a Guest Ph.D. Student, from 2010 to 2012. He is currently a Professor with the School of Optical and Electronic Information, HUST. His research interests include fiber-optic communications, advanced modulation formats and OFDM in radio-over-fiber (RoF) systems, and next generation passive optical network systems.

MINMING ZHANG is currently a Professor with the Huazhong University of Science and Technology, Wuhan, China. His research interests include optical access networks and optical communication devices.

SONGNIAN FU received the B.Sc. and M.Sc. degrees from Xiamen University, Xiamen, China, in 1998 and 2001, respectively, and the Ph.D. degree from Beijing Jiaotong University, Beijing, China, in 2004. From 2005 to 2010, he was a Research Fellow with the Network Technology Research Center, Nanyang Technological University, Singapore. In 2011, he joined the Wuhan National Laboratory for Optoelectronics, School of Optical and Electronic Information, Huazhong University of Science and Technology, Wuhan, China, as a Professor. His current research interests include all-optical signal processing and fiber laser.

MING TANG (S'01–M'05–SM'11) received the B.Eng. degree from the Huazhong University of Science and Technology (HUST), Wuhan, China, in 2001, and the Ph.D. degree from Nanyang Technological University, Singapore, in 2005. His postdoctoral research from the Network Technology Research Centre was focused on the optical fiber amplifiers, high-power fiber lasers, nonlinear fiber optics, and all-optical signal processing. In February 2009, he was with Tera-photonics group led by Prof. Hiromasa Ito in RIKEN, Sendai, Japan, as a Research Scientist conducting research on terahertz-wave generation, detection, and application using nonlinear optical technologies. Since March 2011, he has been a Professor with the Wuhan National Laboratory for Optoelectronics, School of Optical and Electronic Information, HUST, Wuhan, China. He has published more than 80 technical articles in internationally recognized journals and conferences. His current research interests are concerned with optical fiber based linear and nonlinear effects for communication and sensing applications. Dr. Tang has been a Member of the IEEE Photonics Society, since 2001, and he also is a Member of OSA.

DEMING LIU was born in Hubei, China, in January 1957. He received the Graduate degree from the Chengdu Institute of Telecommunication (now University of Electronic Science and Technology of China), Chengdu, China, in 1984. He is currently a Professor with the Huazhong University of Science and Technology, Wuhan, China. His research interests include optical access networks, optical communication devices, and fiber-optic sensors.