2018 IEEE International Conference on Systems, Man, and Cybernetics

A Novel Differential-Chaos-Shift-Keying Secure Communication Scheme

Hang Cai, Zhongyun Hua, Hejiao Huang*
School of Computer Science and Technology, Harbin Institute of Technology, Shenzhen, 518055, China
Email:huazhongyun@hit.edu.cn; *huanghejiao@hit.edu.cn

***Abstract*—To securely communicate information in different networks, this paper introduces a novel secure communication scheme using non-coherent modulation. The transmitter is to generate transmitted signal by modulating the chaotic sequences and information bits, while the receiver can recover the information bits without generating a synchronized duplication of the chaotic sequence. Each frame can transmit two information bits. Thus, it can achieve a high transmission rate. Performance analysis demonstrates that the proposed communication scheme has high performance in resisting Gaussian noise and simulation results shows that it has better bit-error rate performance than a newly developed method in the additive-white-Gaussian-noise channel.**

Keywords*—Chaos communication, differential chaos shift keying (DCSK), non-coherent modulation

I. Introduction

With the fast development of digital technology, more and more data are generated and spread through all kinds of networks. When data are transmitted in the networks, they can be easily captured by different kinds of unauthorized accesses. For these data transmitted in the networks, many of them contain private or secret information. If they are obtained without authorization, serious security accidents may happen. For example, if the military communication of a country is wiretapped by some spies or other hostile counties, state security accident may happen. Thus, it is quite important to protect data when they are transmitted in networks [1], [2].

Chaotic systems have many meaningful properties like initial state sensitivity and aperiodicity. These properties make the behaviors of chaotic systems hard to be predicted. Thus, chaos theory is widely used in all kinds of security applications such as cryptography [3], [4] and secure communication [5]. For the secure communication schemes using chaos, the transmitter first embeds the data into the chaotic signal to form new transmitted signal, and then sends the transmitted signal to the receiver through networks. When receiver receives the signal, it can recover the embedded data [5], [6]. As the chaotic signals are irregular and look like noise, attackers can't obtain any useful information from the signals without knowing the predefined rules [7], [8]. Thus, the signals can be transmitted through all kinds of networks, including public networks.

In the last few decades, many secure communication schemes using chaos have been developed [6], [9]. According to the data recovery mechanisms, the developed secure communication schemes can be divided into two categories: chaos-based coherent modulation scheme [5], [10] and chaos-based non-coherent modulation scheme [5], [6], [9], [11]–[14]. In a chaos-based coherent modulation scheme, the receiver needs a synchronized copy of reference signal to recover the information bits. For example, the chaos shift keying (CSK) introduced in [10]. This kind of modulation is widely used in the chaos-based spread spectrum systems. The main disadvantage of this modulation is its limited security level. As this modulation method has a short linear complexity, the communication schemes using this modulation may be successfully attacked using a linear regression [15]. Besides, in the wireless communication environment, receivers of communication schemes using coherent modulation need to know the accurate information of channel state. This also limit the performance and enhance the implementation complexity. In a chaos-based non-coherent modulation scheme, receiver is able to recover the information bits using the inner correlation of received signal and thus doesn't need to generate a synchronized duplication of the chaotic sequence. For example, the differential chaos shift keying (DCSK) introduced in [11]. When signals are transmitted in all kind of networks, non-linear distortion, attenuation or noise interference may happen. The communication schemes using non-coherent modulation can well deal with this situation, because they recover information data using the inner characteristic of the received signals. Thus, the non-coherent modulation shows better performance than coherent modulation in many application scenarios. Recently, many communication schemes using non-coherent modulation have been developed [11]–[14], [16]. However, some of them also have some weaknesses. For example, some schemes can only transmit one bit in a transmission frame and they generate a frame using a reference signal directly with a copy of the reference signal. Then the transmission rate is low and the security is weak.

To obtain secure communication scheme with better transmission rate and higher security, this paper proposes a new chaos-based secure communication scheme using non-coherent modulation. The scheme consists of two components: the transmitter and the receiver. The transmitter generates the transmission signal using the chaotic sequence and information bits. Each frame of the transmission signal includes two parts with the same length. The first part is a M-length chaotic sequence that acts as reference signal, while the second part is the modulation result of the reference signal with two information bits. When the receiver receives a frame, it can recover the two information bits using the inner correlation, and thus it doesn't need to generate a synchronized duplication of the chaotic sequence. Performance analysis and simulation results show that the proposed chaos-based communication scheme can achieve better performance in bit-error rate.

The rest of this paper is structured as follows. Section II in-

2577-1655/18/$31.00 ©2018 IEEE
DOI 10.1109/SMC.2018.00310

troduces the proposed communication scheme and Section III analyzes its performance. Section IV simulates the scheme and compares it with other scheme and Section V concludes this paper.

II. The Communication Scheme Using Non-Coherent Modulation

This section describes the principle of the proposed communication scheme. It contains two components: the transmitter and the receiver.

A. The Structure of Transmitter

The transmitted signal is obtained from the data and chaotic signal and Fig. 1 shows the format of the transmitted signal in our scheme. One can see that a frame consists of a reference signal and an information-bearing signal. The reference signal is a chaotic sequence with length M, while the information-bearing signal consists of two parts. One part is the multiplication of the first bit with the reference signal X, and the other part is the multiplication of the second bit with the modified reference signal X^*. These two kinds of reference signal are created by the chaotic generator. The structure of the chaotic generator is displayed in Fig. 2. The reference signal X is a M-length original sequence directly generated from the chaotic generator, while the reference signal X^* is obtained by first setting the values in the odd positions of X as opposite numbers, and then swapping the values of adjacent parity positions. The relationship between X and X^* in a frame is represented as

$$\begin{cases} X^*_{2i-1} &= X_{2i} \\ X^*_{2i} &= -X_{2i-1} \end{cases}, \quad i \in \{1, 2, ..., \frac{M}{2}\} \tag{1}$$

It is noticed that the transmitted signal format contains two bits in frame. Thus, the proposed scheme can achieve double transmitting speed, compared with the original DCSK.

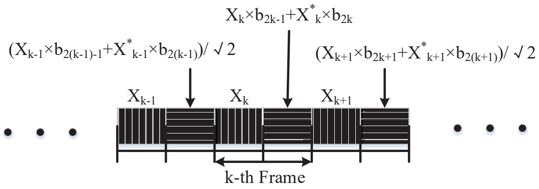
X_k×b_2k-1+X*_k×b_2k
(X_k-1×b_2(k-1)-1+X*_k-1×b_2(k-1))/ √2
(X_k+1×b_2k+1+X*_k+1×b_2(k+1))/ √2
X_k-1
X_k
X_k+1
k-th Frame

Fig. 1: The transmitted signal format in the proposed communication scheme.

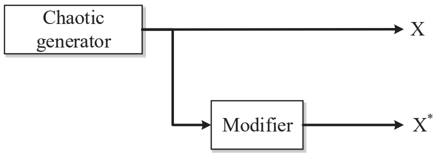

Fig. 2: The modified chaotic generator.

Fig. 3 shows the structure of in the proposed communication scheme. Each frame can embed two bits. The original reference signal X is modulated by the first bit, while the modified reference signal X^* is modulated by the second bit. As a signal frame is of $2M$ and its length is twice of the reference signal, a M time delay is required when generating a signal frame. Suppose that the reference signal $X = \{x_i | i = 1, 2, \cdots, M\}$, and the two transmitted bits are b_0 and b_1, the generation of a transmitted signal frame S can be calculated as

$$S = \begin{cases} x_i, & \text{if } 1 < i \leq M; \\ (b_1 x_{i-M} + b_2 x_{i-M+1})/\sqrt{2}, & \text{if } M < i \leq 2M \cap \\ & \quad i = 2n+1 \ (n \in \mathbb{N}); \\ (b_1 x_{i-M} - b_2 x_{i-M+1})/\sqrt{2}, & \text{if } M < i \leq 2M \cap \\ & \quad i = 2n \ (n \in \mathbb{N}) \end{cases} \tag{2}$$

Using the frame generation rules in Eq. (2), the transmitter can synchronically generate transmitted signal using the chaotic sequences and transmitted information bits.

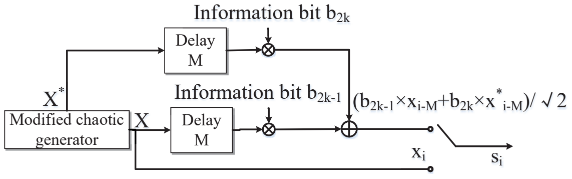

Fig. 3: The structure of transmitter in the proposed communication scheme.

B. The Structure of Receiver

The receiver is to recover the information bits from the received signal. As each frame of the received signal contains two information bits, the receiver needs two synchronous branches to demodulate the received signal. The first bit can be exacted by multiplying the reference signal X with the information-bear signal, while the second bit is demodulated by multiplying the other reference signal X^* with the information-bear signal. As the two branches use the same information-bearing signal, they can share one time synchronization mechanism without introducing extra cost. Thus, when using the timing-synchronization algorithm in this scheme, the receiver can recover the two information bits with fast speed and low complexity. Fig. 4 shows the receiver structure of the proposed scheme. As can be seen that r is the received signal. The signal r' is obtained by modifying from r using the principle of Eq. (1), namely

$$\begin{cases} r'_{2i-1} &= r_{2i} \\ r'_{2i} &= -r_{2i-1} \end{cases}, \quad i \in \{1, 2, ..., \frac{M}{2}\} \tag{3}$$

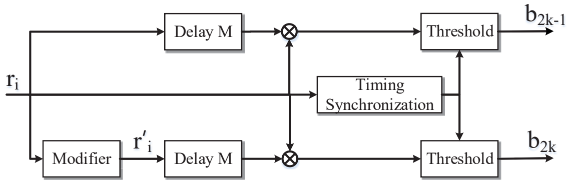

Fig. 4: The structure of receiver in the proposed communication scheme.

To extract the two information bits in a frame, the receiver also needs a M time delay. The two correlator outputs for the two bits in the k-th frame can be calculated as

$$Z_{2k-1} = \sum_{i=2kM+1}^{2kM+M/2} r_i r_{i-M} \tag{4}$$

and

$$Z_{2k} = \sum_{i=2kM+1}^{2kM+M/2} r_i r'_{i-M} \tag{5}$$

Usually, most transmission channels are noise channels. When signals are transmitted in these channels, they will be blurred by different noise. The most common noises are the while Gaussian noise. Suppose the received signal $r = S + \xi$, then the correlator output for the first bit of the k-th frame can be rewritten as

$$\begin{aligned}
Z_{2k-1} = &\sum_{i=2kM-M+1}^{2kM} (s_i + \xi_i)(s_{i-M} + \xi_{i-M}) \\
= &\sum_{i=(k-1)M+1}^{(k-1)M+M/2} (x_{2i} + \xi_{2i})(\frac{b_{2k-1}x_{2i}}{\sqrt{2}} - \frac{b_{2k}x_{2i-1}}{\sqrt{2}} + \xi_{2i+M}) \\
&+ (x_{2i-1} + \xi_{2i-1})(\frac{b_{2k-1}x_{2i-1}}{\sqrt{2}} + \frac{b_{2k}x_{2i}}{\sqrt{2}} + \xi_{2i+M-1}) \\
= &\frac{b_{2k-1}}{\sqrt{2}} \sum_{i=2(k-1)M+1}^{2(k-1)M+M} (x_i^2) + \gamma,
\end{aligned} \tag{6}$$

where

$$\begin{aligned}
\gamma = &\sum_{i=(k-1)M+1}^{(k-1)M+M/2} (\frac{b_{2k}x_{2i-1}x_{2i}}{\sqrt{2}} + x_{2i-1}\xi_{2i+M-1} \\
&+ \frac{b_{2k-1}x_{2i-1}\xi_{2i-1}}{\sqrt{2}} + \frac{b_{2k}x_{2i}\xi_{2i-1}}{\sqrt{2}} + \xi_{2i-1}\xi_{2i+M-1} \\
&- \frac{b_{2k}x_{2i-1}x_{2i}}{\sqrt{2}} + x_{2i}\xi_{2i+M} + \frac{b_{2k-1}x_{2i}\xi_{2i}}{\sqrt{2}} \\
&- \frac{b_{2k}x_{2i-1}\xi_{2i}}{\sqrt{2}} + \xi_{2i}\xi_{2i+M}) \\
= &\sum_{i=2(k-1)M+1}^{2(k-1)M+M} (x_i\xi_{i+M} + \frac{b_{2k}x_i\xi'_i}{\sqrt{2}} + \frac{b_{2k-1}x_i\xi_i}{\sqrt{2}} + \xi_i\xi_{i+M})
\end{aligned} \tag{7}$$

The correlator output for the second bit of the k-th frame can be rewritten as

$$\begin{aligned}
Z_{2k} = &\sum_{i=2kM-M+1}^{2kM} (s_i + \xi_i)(s'_{i-M} + \xi'_{i-M}) \\
= &\sum_{i=(k-1)M+1}^{(k-1)M+M/2} (x_{2i} + \xi_{2i})(\frac{b_{2k-1}x_{2i-1}}{\sqrt{2}} + \frac{b_{2k}x_{2i}}{\sqrt{2}} + \xi_{2i+M-1}) \\
&- (x_{2i-1} + \xi_{2i-1})(\frac{b_{2k-1}x_{2i}}{\sqrt{2}} - \frac{b_{2k}x_{2i-1}}{\sqrt{2}} + \xi_{2i+M}) \\
= &\frac{b_{2k}}{\sqrt{2}} \sum_{i=2(k-1)M+1}^{2(k-1)M+M} (x_i^2) + \eta,
\end{aligned} \tag{8}$$

where

$$\begin{aligned}
\eta = &\sum_{i=(k-1)M+1}^{(k-1)M+M/2} (\frac{b_{2k-1}x_{2i-1}x_{2i}}{\sqrt{2}} + x_{2i}\xi_{2i+M-1} \\
&+ \frac{b_{2k-1}x_{2i-1}\xi_{2i}}{\sqrt{2}} + \frac{b_{2k}x_{2i}\xi_{2i}}{\sqrt{2}} + \xi_{2i}\xi_{2i+M-1} \\
&- \frac{b_{2k-1}x_{2i-1}x_{2i}}{\sqrt{2}} + x_{2i-1}\xi_{2i+M} - \frac{b_{2k-1}x_{2i}\xi_{2i-1}}{\sqrt{2}} \\
&+ \frac{b_{2k}x_{2i-1}\xi_{2i-1}}{\sqrt{2}} - \xi_{2i-1}\xi_{2i+M}) \\
= &\sum_{i=2(k-1)M+1}^{2(k-1)M+M} (x_i\xi'_{i+M} + \frac{b_{2k}x_i\xi_i}{\sqrt{2}} + \frac{b_{2k-1}x_i\xi'_i}{\sqrt{2}} + \xi_i\xi'_{i+M})
\end{aligned} \tag{9}$$

The first items in Eqs. (6) and (8) are useful signal components, in which the contained two bits can be obtained. The remainders in Eqs. (6) and (8), namely γ and η are the zero-mean disturbance components. They contain not only the noise part caused by the transmission channel, but also the deviations caused by the precision truncation of chaotic sequences. Although the remainders in Eqs. (6) and (8) may cause positive or negative effects to the correlator outputs, the useful signal components contain main part of information. Thus, we can still demodualte the two information bits according to the symbols of the correlator outputs, namely

$$b_{2k-1} = \begin{cases} 1, & \text{for} \quad Z_{2k-1} > 0; \\ 0, & \text{for} \quad Z_{2k} < 0. \end{cases} \tag{10}$$

$$b_{2k} = \begin{cases} 1, & \text{for} \quad Z_{2k-1} > 0; \\ 0, & \text{for} \quad Z_{2k} < 0. \end{cases} \tag{11}$$

III. Performance Analysis

As the Tent map has complex chaotic behavior and it can output random chaotic trajectories. We use the symmetric Tent map as the source chaotic map to obtain chaotic signal in our proposed communication scheme. Mathematically, the symmetric Tent map is defined as

$$x_{i+1} = 1 - 2|x_i|, \tag{12}$$

where x_i is the iteration value and $x_i \in (-1, 1)$. Using the analysis method in [17], the output of the receiver can be expressed as

$$S = b_l A + b_l \zeta + \phi, \tag{13}$$

where $A = E[x_i^2]M/\sqrt{2}$ ($E[\cdot]$ demonstrates the mathematical expectation), $\zeta = (\sum_{i=1}^{M} x_i^2) - A$ and ϕ denotes the γ in Eq. (6) or the η in Eq. (8). As every frame in Fig. 1 carries two information bits, we can easily get $A = E_b/\sqrt{2}$, where E_b is the average bit energy of transmitted signal. Besides, the γ and η are the zero-mean disturbance. Then the mean values of Z_{2k-1} and Z_{2k} can be presented as

$$E[Z_{2k-1}] = \frac{b_{2k-1}}{\sqrt{2}} E[\sum_{i=2(k-1)M+1}^{2(k-1)M+M} x_i^2] = \frac{b_{2k-1}}{\sqrt{2}} E_b \tag{14}$$

$$E[Z_{2k}] = \frac{b_{2k}}{\sqrt{2}} E[\sum_{i=2(k-1)M+1}^{2(k-1)M+M} x_i^2] = \frac{b_{2k}}{\sqrt{2}} E_b \tag{15}$$

Here, we use the Gaussian approximation method introduced in [17] to analyze the performance of bit error rate. When signal is transmitted in the additive white Gaussian noise (AWGN) channel, the generated Gaussian noises are independent and their mean value is 0. The noise variance is represented as $N_0/2$. We can easily calculate the variance of ζ as

$$\sigma_\zeta^2 = \frac{9E_b^2}{10M} \tag{16}$$

and the variance of ζ as

$$\sigma_\phi^2 = E_b N_0 + \frac{N_0^2}{4} M \tag{17}$$

Therefore, the variance of Z_a ($a = 2k-1$ or $2k$) can be represented as

$$\sigma_{Z_a}^2 = \frac{9E_b^2}{10M} + E_b N_0 + \frac{N_0^2}{4} M \tag{18}$$

Using the estimation method proposed in [17], the bit error rate of proposed scheme is as follows:

$$\begin{aligned} BER &= 0.5P(Z_a < 0|b_a = 1) + 0.5P(Z_a > 0|b_a = 0) \\ &= \frac{1}{2} erfc(\sqrt{\frac{E_b}{4N_0}(1 + \frac{9}{10M}\frac{E_b}{N_0} + \frac{M}{4}\frac{N_0}{E_b})^{-1}}) \end{aligned} \tag{19}$$

where $erfc(\cdot)$ denotes the complementary error function [18].

IV. Simulation Results

This section simulates the proposed secure communication scheme in the AWGN channel and investigates its performance of bit error rate (BER). Firstly, we analyze the BER formation of the proposed communication scheme against the spreading factor M. Fig. 5 shows the relationship between the BER performance with the spreading factor M under different levels of Gaussian noise. As can be seen, when the spreading factor is set as a small value, the proposed scheme has a big BER value, which means that the receiver mistakenly demodulate many information bits. With the increasement of M, the BER value becomes smaller. However, when M increases to a threshold, the BER value become larger again. This means that there exist a proper spreading factor M that can make the proposed communication scheme achieve the best BER performance. Also, for different levels of Gaussian noise, the best spreading factor M is different. Users have great flexibility to choose different settings of M for different levels of AWGN channel.

To show the superiority of the proposed scheme, we compare its BER performance with a newly developed communication scheme, namely RS-DCSK proposed in [19]. Fig. 6 shows the simulation schemes of the two schemes under different signal-to-noise ratio (SNR). One can see that with the increasement of SNR, both the proposed scheme and RS-DSCK can achieve better BER performance under different settings of the spreading factor M. Besides, under the same settings of the SNR and M, the proposed communication scheme has better BER performance than RS-DCSK. This indicates that the proposed communication scheme has better reliability.

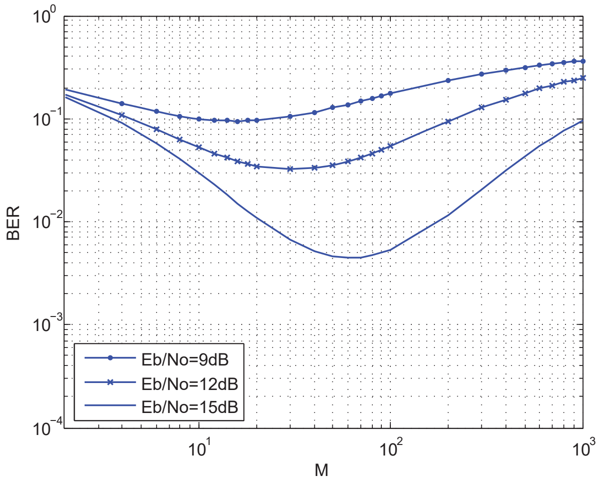

Fig. 5: The BER performance of the proposed communication scheme against the spreading factor M under different levels of Gaussian noise.

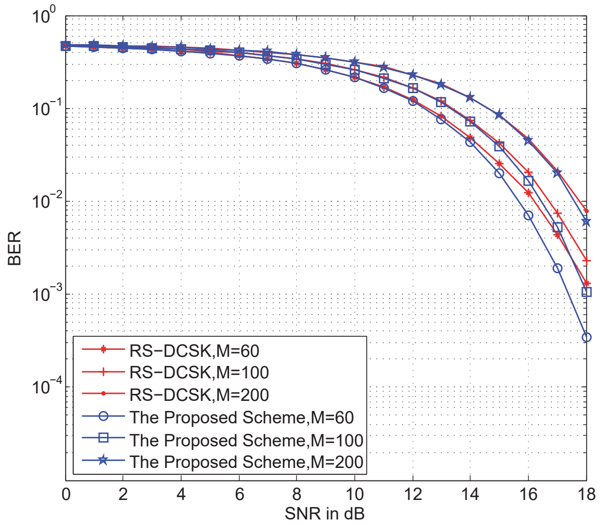

Fig. 6: The BER performance of the proposed scheme and RS-DCSK under different SNR.

V. Conclusion

This paper proposed a novel communication scheme. It follows the classical differential-chaos-shift-keying structure. The communication scheme consists of two parts, namely the transmitter and the receiver. The transmitter is to modulate chaotic sequences with the information bits to get the transmission signal. The chaotic sequences are generated using the symmetric Tent map, which has complex chaotic behavior. As the non-coherent modulation is used, each frame of the transmission signal contains two information bits and thus can achieve a faster transmission speed. The receiver is to recover the information bits using the inner correlations of frame.

Performance analysis was provided to show that the proposed scheme has high performance in AWGN channel. Simulation results show that it has better BER performance than a newly developed communication scheme.

Acknowledgements

This work is financially supported by National Natural Science Foundation of China under Grant No. 61701137, No. 11371004 and No. 61672195, National Science and Technology Major Project under Grant No. 2016YFB0800804 and No. 2017YFB0803002, and Shenzhen Science and Technology Plan under Grant No. J-CYJ20170307150704051, No. JCYJ20170811160212033, No. JCYJ20160318094336513, No. JCYJ20160318094101317 and No. KQCX20150326141251370.

References

[1] Z. Hua and Y. Zhou, "Design of image cipher using block-based scrambling and image filtering," *Information Sciences*, vol. 396, pp. 97–113, 2017.

[2] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Processing*, vol. 144, pp. 134–144, 2018.

[3] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Optics and Lasers in engineering*, vol. 88, pp. 197–213, 2017.

[4] X. Chai, "An image encryption algorithm based on bit level brownian motion and new chaotic systems," *Multimedia Tools and Applications*, vol. 76, no. 1, pp. 1159–1175, 2017.

[5] G. Kaddoum, "Wireless chaos-based communication systems: A comprehensive survey," *IEEE Access*, vol. 4, pp. 2621–2648, 2016.

[6] G. Cai, L. Wang, L. Kong, and G. Kaddoum, "SNR estimation for FM-DCSK system over multipath rayleigh fading channels," in *2016 IEEE 83rd Vehicular Technology Conference (VTC Spring)*, 2016, pp. 1–5.

[7] Z. Hua, B. Zhou, and Y. Zhou, "Sine-transform-based chaotic system with FPGA implementation," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 3, pp. 2557–2566, 2018.

[8] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D logistic-sine-coupling map for image encryption," *Signal Processing*, vol. 149, pp. 148–161, 2018.

[9] J. Bao, W. Xu, L. Wang, and T. Huang, "Performance analysis and subcarriers power allocation for MC-QCSK," in *2015 International Conference on Wireless Communications and Signal Processing (WCSP),*, 2015, pp. 1–5.

[10] H. Dedieu, M. P. Kennedy, and M. Hasler, "Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 40, no. 10, pp. 634–642, 1993.

[11] G. Kolumban, B. Vizvári, W. Schwarz, and A. Abel, "Differential chaos shift keying: A robust coding for chaos communication," in *Proc. NDES*, vol. 96, 1996, pp. 87–92.

[12] H. Yang and G.-P. Jiang, "High-efficiency differential-chaos-shift-keying scheme for chaos-based noncoherent communication," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 59, no. 5, pp. 312–316, 2012.

[13] ——, "Reference-modulated dcsk: a novel chaotic communication scheme," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 60, no. 4, pp. 232–236, 2013.

[14] G. Kaddoum, E. Soujeri, C. Arcila, and K. Eshteiwi, "I-dcsk: An improved noncoherent communication system architecture," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 62, no. 9, pp. 901–905, 2015.

[15] G. Burel and C. Bouder, "Blind estimation of the pseudo-random sequence of a direct sequence spread spectrum signal," in *21st Century Military Communications Conference Proceedings*, vol. 2, 2000, pp. 967–970.

[16] C. Tse and F. Lau, "Chaos-based digital communication systems," *Operating Principles, Analysis Methods and Performance Evaluation*, 2003.

[17] M. Sushchik, L. S. Tsimring, and A. R. Volkovskii, "Performance analysis of correlation-based communication schemes utilizing chaos," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 47, no. 12, pp. 1684–1691, 2000.

[18] B. Sklar, *Digital communications*. Prentice Hall Upper Saddle River, 2001, vol. 2.

[19] H. Yang, G. Jiang, L. Xia, and X. Tu, "Reference-shifted dcsk modulation scheme for secure communication," in *2017 International Conference on Computing, Networking and Communications (ICNC)*, 2017, pp. 1073–1076.