CHINESE OPTICS LETTERS

Vol. 19, No. 5 | May 2021

Secure orthogonal time-frequency multiplexing with two-dimensional encryption for optical-wireless communications

Jie Zhong (钟 捷)[1], Ji Zhou (周 骥)[2*], Shecheng Gao (高社成)[2], and Weiping Liu (刘伟平)[2]

[1] School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou 510006, China

[2] Department of Electronic Engineering, College of Information Science and Technology, Jinan University, Guangzhou 510632, China

*Corresponding author: zhouji@jnu.edu.cn

Received October 9, 2020 | Accepted November 8, 2020 | Posted Online February 16, 2021

This paper firstly, to the best of our knowledge, proposed two-dimensional (2D) encryption based on the Arnold transformation for implementing a secure DC-biased optical orthogonal time-frequency multiplexing (DCO-OTFM) in optical-wireless communications (OWCs). The encrypted data is transformed to the particular 2D matrix and decrypted by the only key to get the correct information. Meanwhile, the number of keys in 2D encryption is enormous, which prevents eavesdroppers from exhaustively searching secret keys rapidly to find the right decryption. Numerical results demonstrate that the secure DCO-OTFM based on 2D encryption can effectively prevent signal decryption from the eavesdropper, which has good secure performance for applying in OWC.

Keywords: orthogonal time-frequency multiplexing; two-dimensional encryption; physical layer security; optical-wireless communications.

DOI: 10.3788/COL202119.050603

1. Introduction

As an emerging modulation technique, orthogonal time-frequency-space (OTFS) has been proposed to tackle the dynamics in multipath time-varying wireless channels[1]. Its main idea is to modulate the symbol onto two-dimensional (2D) orthogonal basis functions set in the delay-Doppler domain. Then, traditional modulations, such as orthogonal frequency division multiplexing (OFDM), deal with the signal in the time-frequency domain. This promising scheme, which simplifies detection and channel estimation in the high mobility scenarios, also improves bit error rate (BER) performance in systems through some static multipath channels, such as optical-wireless communications (OWCs). Recently, a series of researches have emerged to discuss performance improvement or new applicable scenarios with OTFS[2–4]. Schemes including novel channel estimation, equalization, and detection methods for OTFS were introduced[5–8]. An efficient method was proposed to reduce the peak-to-average power ratio (PAPR) in the OTFS network[9]. A robust beamforming was designed for the OTFS combined with a non-orthogonal multiple-access (NOMA) system[10]. A joint radar and communication system with OTFS was proposed[11]. Multiple-input multiple-output (MIMO) OTFS systems were investigated for underwater acoustic communication[12]. In our previous work, a 2D Hermitian symmetry was proposed for generating real-valued OTFS signals in OWC systems[13].

Physical layer security techniques have been widely studied for optical OFDM systems. The data can be encrypted by a chaotic scrambling matrix based on a one-dimensional (1D) logistic map for OFDM[14]. 2D encryption was proposed for the OFDM signal to implement time-frequency domain encryption or dynamic secret key encryption[15,16]. The chaotic sequences of the key were used to encrypt time synchronization of the OFDM frame, perform subcarrier masking, and manage the fractional order of the fractional Fourier transform[17]. The encryption based on the Walsh–Hadamard transform not only enhanced the security of the OFDM signals but also reduced their PAPR[18]. The chaotic secret keys were used at discrete chaotic space or with a secure hash algorithm to encrypt the OFDM signals[19,20]. A chaotic method based on orthogonal matrix transform was designed to encrypt the pulse amplitude modulated symbols to generate real-valued OFDM signals[21]. Augmented communication was proposed for the OFDM system to realize both a high spectral efficiency and a security link[22]. The encryption algorithm scrambled both the quadrature amplitude modulation (QAM) constellations and subcarriers for the NOMA-OFDM systems[23]. The birefringent with

Goos–Hanchen shifts was used to control space time holes for information cloaking[24].

In this paper, we exploit the 2D characteristic of orthogonal time-frequency multiplexing (OTFM) signals, which can be directly encrypted by 2D encryption. We produce the real-valued OTFM signal with a 2D Hermitian symmetry, which makes sure the OTFM is suitable for the DC-biased OWC. Then, the 2D signal is encrypted with an Arnold transformation extended from the traditional transform[25]. Finally, a new secure DC-biased optical OTFM (DCO-OTFM) with 2D encryption is proposed. The legitimate user transforms the received signal to the particular 2D matrix and deciphers them with the correct key. The number of secret keys in the 2D encryption is enormous. Therefore, it is almost impossible for the eavesdropper to exhaustively search all keys to find out the right decryption. Simulation results are introduced to verify our design.

Annotations: All through the paper, we use normal letters, lowercase boldface, and uppercase boldface to denote scalar, vector, and matrix, respectively. Conjugate, transpose, and conjugate transpose operations are indicated by the superscripts $(\cdot)^*$, $(\cdot)^T$, and $(\cdot)^H$. The matrix operators $\mathbf{F}_M$ and $\mathbf{F}_M^H$ are set to denote the M-point discrete Fourier transform (DFT) and the inverse DFT (IDFT) operations, respectively.

2. Secure DCO-OTFM System

A DCO-OTFM system over the optical-wireless channel contains a single transmitter and receiver set as Alice and Bob, which is shown in Fig. 1, and the signals can be easily intercepted by the eavesdropper due to the openness of wireless communications. In order to provide good performance in the physical layer security, we propose the secure DCO-OTFM scheme with 2D encryption. An OTFM symbol consisting of MN samples is transmitted by M subcarriers, where T_s is the sampling interval, so each symbol duration is NT_s. In Alice, the real-valued OTFM is generated with inverse symplectic finite Fourier transform (ISFFT), 2D Hermitian symmetry method, and Heisenberg transform. We cipher the OTFM with the 2D encryption based on Arnold transformation. The encrypted OTFM matrices convert to vector signals with the cycle prefix (CP) addition. After DC bias addition and zero clipping, the encrypted DCO-OTFM signals $s_E(t)$ are converted into optical signals and transmitted, in which the optical-wireless channel response $h(\tau)$ is defined in the following expression:

$$h(\tau) = \sum_{p=0}^{P} h_p \delta(\tau - \tau_p), \tag{1}$$

where h_p denotes the channel coefficient, τ_p is the delay associated with the pth propagation path, and the channel contains $P+1$ propagation paths. The optical-wireless channel model should be suitable for multiple common OWC scenarios, in which both the line of sight and non-directed channels are considered. Thus, the ceiling-bounce (CB) model is exploited to study the multipath effect[26]. So, Eq. (1) in the CB model defines the impulse response as

$$h_{\mathrm{cb}}(\tau) = \frac{6a^6}{(\tau + a)^7} u(\tau), \tag{2}$$

where $a = 12\sqrt{11/13}D$, D denotes the root-mean-square (RMS) delay spread caused by multiple reflections, and the unit step function is set as $u(\tau)$. So, we represent the encrypted signal at the receiver as

$$y_E(t) = h_{\mathrm{cb}}(\tau)^* s_E(t) + n(t). \tag{3}$$

In Bob, the encrypted signals are transformed into the particular 2D matrix after frequency channel estimation. Then, the matrix can be deciphered with the only correct key and

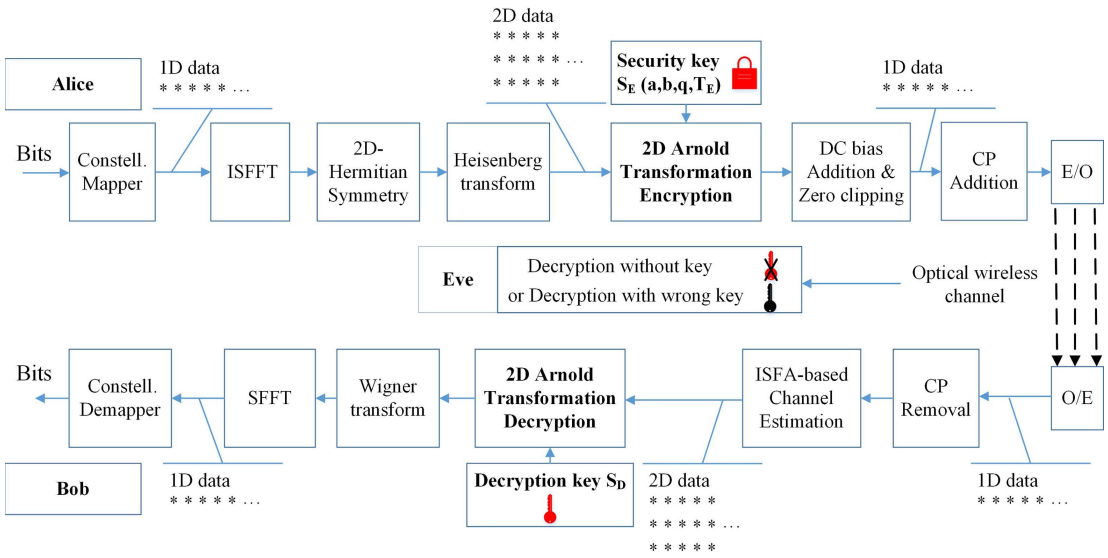

Fig. 1. Block diagram of secure DCO-OTFM system for OWC. E/O, electro/optic; O/E, optic/electro.

demodulated to get the correct information. Meanwhile, the data on the Eve side cannot be converted to the right matrix or decrypted with the right key. The details of our encryption scheme will be introduced in the following paragraphs.

3. 2D Encryption for OTFM

We introduce OTFM modulation in this part. As shown in the Alice part of Fig. 1, the information bits of OTFM are firstly transformed into QAM signals. Then, the signal vector will be reshaped as a 2D matrix before the ISFFT transform. We define each element in the original matrix as $x_o(k,l)$, where $k \in [0,N-1]$ and $l \in [0,M/2-2]$ are integers based on the subcarriers and samples in an OTFM symbol. Thus, the element of the modulated matrix with ISFFT is represented as

$$X_o(n,m) = \frac{2}{N(M-2)} \sum_{k=0}^{N-1} \sum_{l=0}^{M/2-2} x_o(k,l) e^{j2\pi\left(\frac{nk}{N} - \frac{2ml}{M-2}\right)}, \tag{4}$$

where $n \in [0,N-1]$ and $m \in [1,M/2-1]$ are integers. A 2D Hermitian symmetry is proposed for OTFM to guarantee that the time-domain information is real-valued before transmission, which is similar to the Hermitian symmetry for optical OFDM. The $N \times M$ matrix $\mathbf{X}$ is defined as

$$\begin{cases} X(n,0) = X(n,M/2) = 0, & n \in [0,N-1], \\ X(n,m) = X_o(n,m), & n \in [0,N-1], m \in \left[1, \frac{M-2}{2}\right], \\ X(n,m) = X_o^*(n,M-m), & n \in [0,N-1], m \in \left[\frac{M+2}{2}, M-1\right]. \end{cases} \tag{5}$$

The matrix $\mathbf{X}$ is modulated to the OTFM matrix after the Heisenberg transform, which is implemented by the M-point IDFT operation[12] and denoted as

$$\tilde{\mathbf{X}} = \sqrt{M} \mathbf{F}_M^H \mathbf{X}^T. \tag{6}$$

Each element in this time-domain matrix $\tilde{\mathbf{X}}$ is expressed as

$$\begin{aligned} \tilde{x}(m,n) &= \frac{1}{\sqrt{M}} \sum_{m=0}^{M-1} X^T(n,m) e^{j2\pi \frac{ml}{M}} \\ &= \frac{2}{\sqrt{M}} \sum_{m=1}^{M/2-1} [a(m,n), b(m,n)] \begin{bmatrix} \cos\varphi \\ -\sin\varphi \end{bmatrix}, \end{aligned} \tag{7}$$

where $X(n,m) = a(n,m) + jb(n,m)$, $\varphi = 2\pi ml/M$; thus, the $M \times N$ matrix $\tilde{\mathbf{X}}$ is a real-valued matrix. The matrix can be ciphered with 2D encryption presented in the next part.

Conventional Arnold transformation is usually applied for the scrambling transform of the 2D $M \times M$ image matrix. All image pixels keep their gray values and change their coordinates in each Arnold transformation with the regulation in the following equation:

$$\begin{bmatrix} m' \\ n' \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & 1+ab \end{bmatrix} \begin{bmatrix} m \\ n \end{bmatrix} \mathbf{mod}\,(M), \tag{8}$$

where a and b should be positive integers, and $(m,n),(m',n')$ represent the original and new coordinate values, respectively. The periodicity of Arnold transformation was proved existent, which means that the encryption and decryption can be executed in one expression. The periodicity varies with the change of parameters a,b,M; thus, we can set different secret keys with proper security parameters.

The periodicity of Arnold transformation has been proved to exist in 2D encryption for the non-equilateral matrix[27]. The coordinate scrambling expression is shown as

$$\begin{bmatrix} m' \\ n' \end{bmatrix} = \begin{bmatrix} 1 & a \\ bq & 1+abq \end{bmatrix} \begin{bmatrix} m \\ n \end{bmatrix} \mathbf{mod} \begin{bmatrix} M \\ N \end{bmatrix}, \tag{9}$$

where the parameter q is defined as

$$q = \frac{N}{\gcd(M,N)}. \tag{10}$$

The operator $\gcd(A,B)$ presents the greatest common divisor of A and B, and other parameters have the same definition as in Eq. (8). Once we set a,b,M,N, we can get the Arnold transformation periodicity T_{Ar}. After we choose a proper parameter T_E, which defines the number of transformations operated in encryption and is less than T_{Ar}, the secret key $S_E = (a,b,q,T_E)$ is set. With S_E, we encrypt the OTFM matrix $\tilde{\mathbf{X}}$ by operating T_E times in Eq. (9) to get the ciphered 2D signal $\tilde{\mathbf{X}}_E$.

Before we convert the 2D matrix to 1D data, we employ the biasing and clipping procedure to generate unipolar signals. A proper DC bias should be added to the bipolar signal to ensure all elements in $\tilde{\mathbf{X}}_E$ are positive. With parallel to serial (P/S) conversion, each matrix $\tilde{\mathbf{X}}_E$ transforms into the encrypted vector $\tilde{\mathbf{X}}_E$. Then, the symbol vector is added with a CP of length L. The OTFM frame $\mathbf{S}_E$ formed by K vectors turns to the baseband signal $\mathbf{S}_E$ with P/S conversion, which is transmitted after electro-optic conversion. We introduce the process of the decryption scheme in the subsequent section.

4. 2D Decryption for OTFM

On the legal receiver of the OTFM system, $\mathbf{y}_E$ turns into 1D encrypted signals after the DC average component removal and serial to parallel conversion. The lower part of Fig. 1 briefly depicts the channel estimation diagram, where frequency domain equalization with CP removal is employed to eliminate the inter-symbol interference (ISI). The first I symbols in $\mathbf{y}_E$ are set as the training symbols. In consideration of the reduction in the training symbols' overhead, we apply the method of intra-symbol frequency-domain averaging (ISFA) to acquire the reckoned channel response $\hat{H}_{\mathrm{ISFA}}$[28]. With $\mathbf{y}_E$ and $\hat{H}_{\mathrm{ISFA}}$, the time-domain vector $\hat{\mathbf{X}}_E$ is obtained, which is then transformed into 2D matrix $\hat{\mathbf{X}}_E$. The $M \times N$ dimension of $\hat{\mathbf{X}}_E$ should be the

same as that of $\tilde{\mathbf{X}}_E$, which ensures that the data can be decrypted correctly.

In Bob, we set the decryption key $S_D = (a,b,q,T_D)$, where T_D is defined as

$$T_D = T_{\mathrm{Ar}} - T_E, \tag{11}$$

and other parameters stay the same as those in S_E. The key S_D indicates that we execute T_D times scrambling in Eq. (9) for each $\hat{\mathbf{X}}_E$ to get the deciphered matrix $\hat{\mathbf{X}}_D$.

Next, we demodulate $\hat{\mathbf{X}}_D$, and the operation is similar to that in our previous work[13]. We first apply the inverse of the Heisenberg transform and the Wigner transform on $\hat{\mathbf{X}}_D$. Thus, the frequency domain signal is achieved by

$$\tilde{\mathbf{X}} = \frac{1}{\sqrt{M}} \mathbf{F}_M \hat{\mathbf{X}}_D, \tag{12}$$

where $\tilde{\mathbf{X}}$ is the Hermitian symmetry because of the definition in Eq. (5). Then, we use the effective data in $\tilde{\mathbf{X}}$ to form matrix $\tilde{\mathbf{X}}_o$, and the element of $\tilde{\mathbf{X}}_o$ is defined as

$$\tilde{X}_o(u,v) = \tilde{X}^T(n,m), \quad n \in [0,N-1], \quad m \in [1,M/2-1], \tag{13}$$

where $u \in [0,N-1]$ and $v \in [0,M/2-2]$. $\tilde{\mathbf{X}}_o$ turns into the QAM signals with symplectic finite Fourier transform (SFFT), where we obtain the constellation value by

$$\tilde{x}_o(k,l) = \sum_{u=0}^{N-1} \sum_{v=0}^{M/2-2} \tilde{X}_o(u,v) e^{-j2\pi\left(\frac{uk}{N} - \frac{2vl}{M-2}\right)}, \tag{14}$$

where $k \in [0,N-1]$ and $l \in [0,M/2-1]$. The decrypted bits are achieved after constellation demapping.

5. Simulation Setup and Results

In the following part, the simulation setup and the superiority of the 2D secret key are introduced. Then, we display the performance of secure DCO-OTFM with different decryption keys for two QAM modes. One OTFM symbol consists of 4096 samples in all of the simulations. CP is set as $L = 16$ to counteract ISI, which is 1/256 of the length of each symbol period. Each DCO-OTFM frame contains $K = 128$ symbols, where the first $I = 4$ symbols are used for training symbols, and the information payload is transmitted in the remaining 124 symbols.

We analyze the relationship between the periodicity value T_{Ar} of Arnold transformation and parameters M,N at first. According to the principle of Arnold transformation, when M,N are fixed, no matter how we set a,b, the range of T_{Ar} is confirmed. Table 1 shows all values of T_{Ar} when we set $N = 16$, $M = 256$, or $M = 512$, which means both $q = 1$. We find that T_{Ar} has 16 choices when $M = 256$ and 18 choices when $M = 512$. If the eavesdropper intends to find out the right secret key, he first needs to get the correct parameters M,N of the 2D OTFM signals to derive the right T_{Ar}. However, the OTFM signals can be modulated in the arbitrary 2D matrix theoretically and optical signals are transmitted in the 1D mode through the OWC channel. The optional number of the 2D matrix pattern is large in practical modulation. It is difficult for the eavesdropper to find out the correct T_{Ar} by exhaustively searching all possible M,N. Thus, he cannot get the only decryption key of 2D encryption rapidly. So, the 2D encryption enhances the physical layer security of the OTFM.

Table 1. All Possible Periodicity Values T_{Ar} for Different M, with $N = 16$, $q = 1$ and a, b as the Arbitrary Integers.

	Periodicity Value					
$M = 256$	256	192	128	96	64	48
	32	24	16	12	8	
	6	4	3	2	1	
$M = 512$	512	384	256	192	128	96
	64	48	32	24	16	12
	8	6	4	3	2	1

Next, we further discuss the relationship between T_{Ar} and parameters a,b. In Table 2, we set $M = 256$, $N = 16$, and $a = 1$, and demonstrate partial values of T_{Ar} by different b. For example, nine different b can get the periodicity $T_{\mathrm{Ar}} = 192$, which means that even if the eavesdropper gets the right T_{Ar} or M,N, he cannot find the right key at once and decrypt the data correctly. In fact, for each specific T_{Ar}, the number of related a and b couples can be up to the 10^5 level. We sum up the analysis from Tables 1 and 2 and conclude that the size of the key space for S_E depending on different a,b,M,N is at least in the 10^{12} level. It would be tough work for the eavesdropper to find the only right S_E from the tremendous secret key pool in a short time.

Table 2. Values of T_{Ar} Depend on Different b, with $M = 256$, $N = 16$, $q = 1$, and $a = 1$.

b	1	2	3	4	5
T_{Ar}	192	128	192	256	96
b	6	7	8	9	10
T_{Ar}	64	96	256	192	128
b	41	42	43	44	45
T_{Ar}	192	128	192	256	48
b	46	47	48	49	50
T_{Ar}	32	48	256	192	128
b	297	298	299	300	301
T_{Ar}	192	128	192	256	48
b	302	303	304	305	306
T_{Ar}	32	48	256	192	128

We then show the BER performance of secure OTFM schemes. In simulations, each OTFM symbol is transmitted in $N = 16$ sampling time interval durations by $M = 256$ subcarriers. The signals' transmission rate is set to 100 Mbit/s, the DC bias is set to 7 dB, and RMS delay spread is set to 10 ns in the CB channel. Figure 2 illustrates the performance of BER for three decryption modes in different QAM modes. The BER performance of unencrypted DCO-OTFM signals is set as the benchmark, and the required SNR should reach or be lower than threshold of BER 1×10^{-3}.

In Fig. 2(a), we illustrate the performance contrast between Bob and the eavesdropper with 4QAM signals. When the transmission SNR ≥ 32 dB, Bob succeeds in signal decryption and achieves the communication requirement. The performance of a secure DCO-OTFM scheme has a little loss compared with the unencrypted system. An OTFM symbol is transmitted through N time slot, which is different from an OFDM symbol transmitted in one time slot. The elements in one row of the OTFM matrix are processed together in the 2D demodulation. These elements are in the same time slot for unencrypted OTFM. However, each row of the encrypted OTFM matrix contains multi-time slot elements after 2D decryption. The correlations of noise among different time slots are usually weaker than that of one time slot in common sense. This leads to more deviations between each row of the received decrypted data and original data than those of unencrypted data. The loss caused by 2D decryption will further make more errors with the encrypted data in the demodulation, which brings out BER loss after demapping. We do not need to raise any SNR to reach the transmission threshold. On the other hand, the eavesdropper demodulates the signals directly or deciphers them with a wrong decryption key. He cannot get the correct data with any SNR. The constellation coordinates on the right side of the figure also compare the effect of the secret key. In Fig. 2(b), we find that for the 16QAM encrypted signal, the SNR of secure OTFM communication needs to raise about 8 dB to reach the same performance of unencrypted signals, which is the reason for the loss being the same as that for 4QAM signals. The secure DCO-OTFM scheme brings out partial performance loss for high-order modulation signals. Both subfigures demonstrate good secure performance in our proposed system with 2D encryption.

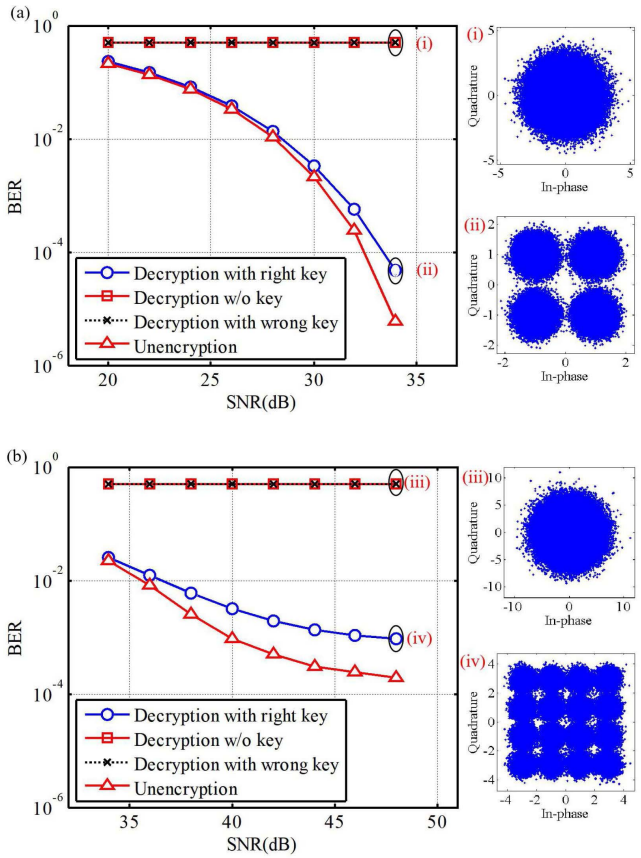

Fig. 2. Performance of BER versus SNR for deciphered signals with different keys through CB channel; w/o, without. (a) BER and decoded constellations for 4QAM signals. (b) BER and decoded constellations for 16QAM signals.

6. Conclusion

In this paper, a secure DCO-OTFM in OWC was firstly implemented with 2D encryption. A 2D Hermitian symmetry is utilized in the modulation to generate the real-valued OTFM matrix, and then the signals were encrypted with a 2D Arnold transformation. In the signal recovery of the legal user, we applied the proper equalization method, transformed the signals to the particular 2D matrices, and deciphered them with the right key. As a result, the data could be demodulated correctly. The number of keys in 2D encryption is enormous, which was analyzed to verify the superiority of 2D encryption. Consequently, it is nearly impossible for the eavesdropper to get the right cipher key. Numerical results showed that our proposed schemes can prevent signal decryption from the eavesdropper. All of the results revealed that our secure DCO-OTFM based on 2D encryption has good secure performance for applying in OWC.

Acknowledgement

This work was supported by the National Key R&D Program of China (No. 2018YFB1802300), the National Natural Science Foundation of China (Nos. 61875076 and 62005102), the Fundamental Research Funds for the Central Universities (No. 21619309), the Leading Talents of Guangdong Province Program (No. 00201502), the Natural Science Foundation of Guangdong Province (No. 2019A1515011059), and the Open Fund of IPOC (BUPT) (No. IPOC2019A001).

Reference

1. R. Hadani, S. Rakib, M. Tsatsanis, A. Monk, A. J. Goldsmith, A. F. Molisch, and R. Calderbank, "Orthogonal time frequency space modulation," in *2017 IEEE Wireless Communications and Networking Conference (WCNC)* (2017), p. 1.

2. A. Farhang, A. RezazadehReyhani, L. E. Doyle, and B. Farhang-Boroujeny, "Low complexity modem structure for OFDM-based orthogonal time frequency space modulation," IEEE Wireless Commun. Lett. **7**, 344 (2018).
3. P. Raviteja, E. Viterbo, and Y. Hong, "OTFS performance on static multipath channels," IEEE Wireless Commun. Lett. **8**, 745 (2019).
4. S. Tiwari and S. S. Das, "Circularly pulse-shaped orthogonal time frequency space modulation," Electron. Lett. **56**, 157 (2020).
5. W. Yuan, Z. Wei, J. Yuan, and D. W. K. Ng, "A simple variational Bayes detector for orthogonal time frequency space (OTFS) modulation," IEEE Trans. Veh. Technol. **69**, 7976 (2020).
6. X. Wu, S. Ma, and X. Yang, "Tensor-based low-complexity channel estimation for mm wave massive MIMO-OTFS systems," J. Commun. Inf. Netw. **5**, 324 (2020).
7. G. D. Surabhi and A. Chockalingam, "Low-complexity linear equalization for OTFS modulation," IEEE Commun. Lett. **24**, 330 (2020).
8. Y. Liu, S. Zhang, F. Gao, J. Ma, and X. Wang, "Uplink-aided high mobility downlink channel estimation over massive MIMO-OTFS system," IEEE J. Sel. Areas Commun. **38**, 1994 (2020).
9. S. Gao and J. Zheng, "Peak-to-average power ratio reduction in pilot-embedded OTFS modulation through iterative clipping and filtering," IEEE Commun. Lett. **24**, 2055 (2020).
10. Z. Ding, "Robust beamforming design for OTFS-NOMA," IEEE OJ-COMS **1**, 33 (2020).
11. L. Gaudio, M. Kobayashi, G. Caire, and G. Colavolpe, "On the effectiveness of OTFS for joint radar parameter estimation and communication," IEEE Trans. Wireless Commun. **19**, 5951 (2020).
12. M. J. Bocus, A. Doufexi, and D. Agrafiotis, "Performance of OFDM-based massive MIMO OTFS systems for underwater acoustic communication," IET Commun. **14**, 588 (2020).
13. J. Zhong, J. Zhou, W. Liu, and J. Qin, "Orthogonal time-frequency multiplexing with 2D Hermitian symmetry for optical-wireless communications," IEEE Photon. J. **12**, 7901110 (2020).
14. L. Zhang, X. Xin, B. Liu, and Y. Wang, "Secure OFDM-PON based on chaos scrambling," IEEE Photon. Technol. Lett. **23**, 998 (2011).
15. L. Zhang, X. Xin, B. Liu, and X. Yin, "Physical secure enhancement in optical OFDMA-PON based on two-dimensional scrambling," Opt. Express **20**, B32 (2012).
16. T. Wu, C. Zhang, H. Wei, and K. Qiu, "PAPR and security in OFDM-PON via optimum block dividing with dynamic key and 2D-LASM," Opt. Express **27**, 27946 (2019).
17. L. Deng, M. Cheng, X. Wang, H. Li, M. Tang, S. Fu, P. Shum, and D. Liu, "Secure OFDM-PON system based on chaos and fractional Fourier transform techniques," J. Lightwave Technol. **32**, 2629 (2014).
18. A. A. E. Hajomer, X. Yang, and W. Hu, "Chaotic Walsh–Hadamard transform for physical layer security in OFDM-PON," IEEE Photon. Technol. Lett. **29**, 527 (2017).
19. B. Liu, L. Zhang, X. Xin, and N. Liu, "Piecewise chaotic permutation method for physical layer security in OFDM-PON," IEEE Photon. Technol. Lett. **28**, 2359 (2016).
20. H. S. Gill, S. S. Gill, and K. S. Bhatia, "A novel chaos-based encryption approach for future-generation passive optical networks using SHA-2," J. Opt. Commun. Netw. **9**, 1184 (2017).
21. Z. Hu and C. Chan, "A real-valued chaotic orthogonal matrix transform-based encryption for OFDM-PON," IEEE Photon. Technol. Lett. **30**, 1455 (2018).
22. M. H. Khadr and H. Elgala, "Augmented communications: spectral efficiency and security enhanced visible light communications by design," Chin. Opt. Lett. **18**, 090601 (2020).
23. Y. Yang, C. Chen, W. Zhang, X. Deng, P. Du, H. Yang, W. Zhong, and L. Chen, "Secure and private NOMA VLC using OFDM with two-level chaotic encryption," Opt. Express **26**, 34031 (2018).
24. H. Khan, M. Haneef, and Bakhtawar, "Space–time cloaks through birefringent Goos–Hänchen shifts," Chin. Opt. Lett. **17**, 032701 (2019).
25. Z. Shang, H. Ren, and J. Zhang, "A block location scrambling algorithm of digital image based on Arnold transformation," in *Proceedings of the 9th International Conference for Young Computer Scientists* (2008), p. 2942.
26. J. B. Carruthers and J. M. Kahn, "Modeling of nondirected wireless infrared channels," IEEE Trans. Commun. **45**, 1260 (1997).
27. L. Shao, Z. Qin, B. Liu, H. Gao, and J. Qin, "2D bi-scale rectangular mapping and its application in image scrambling," J. Comput.-Aided Des. Comput. Graphics **21**, 1025 (2009).
28. X. Liu and F. Buchali, "Intra-symbol frequency-domain averaging based channel estimation for coherent optical OFDM," Opt. Express **16**, 21944 (2008).