Optics Letters

Secure turbulence-resistant coherent free-space optical communications via chaotic region-optimized probabilistic constellation shaping

Tingwei Wu,[1,2,3] Wei Zeng,[1,2] Yejun Liu,[1,2,*] Song Song,[1,2] Lun Zhao,[1,2] Chen Chen,[4] Chongfu Zhang,[5] and Lei Guo[1,2]

[1]School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications,Chongqing, China
[2]Institute of Intelligent Communication and Network Security, Chongqing University of Posts and Telecommunications, Chongqing, China
[3]Postdoctoral Research Workstation of Chongqing Key Laboratory of Cyberspace and Information Security, School of Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing, China
[4]Chongqing University, Chongqing, China
[5]School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu, China
*Corresponding author: yjliu@cqupt.edu.cn

Received 15 November 2022; revised 17 December 2022; accepted 29 December 2022; posted 3 January 2023; published 24 January 2023

We propose a chaotic region-optimized probabilistic constellation shaping (CRPCS) scheme to enhance the security and the resistance to turbulence for free-space optical (FSO) communications. For this approach, a four-dimensional hyperchaotic system generates a pseudorandom sequence to rotate and encrypt the constellation. Constellation distribution of short pseudorandom sequences behaves as the law of a non-uniform character. Grouping long pseudorandom sequences and counting the characteristics of constellation distribution can realize probabilistic constellation shaping with low and fixed redundant information. We demonstrate a 56 Gbyte/s coherent FSO communication system based on log-normal and Gamma–Gamma turbulence models with a key space of 10^{75}. The results show that the optical receiver sensitivity is improved by 0.3–1.1 dB, and the transmission distance is also improved by 3.2%–7.0% in different shaping cases.

https://doi.org/10.1364/OL.480981

Free-space optical (FSO) communications have the characteristics of high bandwidth, free spectrum resources, low cost, flexible deployment, high security, and anti-electromagnetic interference [1–3]. They have incalculable application value in the civilian and military fields. Although the FSO system has many advantages, its communication performance can be affected by unpredictable atmospheric conditions, such as atmospheric absorption, scattering, or turbulence. Among these, atmospheric turbulence is a major factor, which may lead to severe degradation of link performance. Improving the communication performance of FSO links in turbulent atmospheres is currently a major challenge.

The chaotic system has a high initial value sensitivity, and its unique properties give it better security performance than traditional encryption methods [4], so it has been widely used in cryptography. Some studies have shown that the FSO system is not absolutely secure [5–7], and it may still encounter illegal intrusions. Eavesdropping in the context of the FSO system may occur when a wiretapper is hidden at the top of the same building as the main receiver [8]. Therefore, applying chaotic encryption to the FSO system can effectively alleviate the security problem of links.

Probabilistic constellation shaping is an optimization technique of coded modulation that improves communication performance by changing the probability distribution of the constellation. The common probabilistic constellation shaping scheme is constant composition distribution matching (CCDM) [9], but this shaping scheme has high algorithm complexity, high redundancy, and relatively insufficient feasibility. Therefore, seeking a probabilistic constellation shaping scheme with low algorithm complexity and low redundancy is necessary. It is feasible to apply the constellation probabilistic constellation shaping to the FSO system to reduce the influence of atmospheric turbulence and improve the performance of links.

In this Letter, we propose a chaotic region-optimized probabilistic constellation shaping (CRPCS) scheme to enhance the security and improve the communication performance of the FSO system shown in Fig. 1. At the transmitter, the encoder uses a four-dimensional hyperchaotic equation to perform rotational encryption on a bit sequence, then changes the constellation probability distribution of the bit sequence based on a sequence grouping and region permutation method, and embeds the generated permutation information at the end of each sequence. In this shaping technique, the algorithm complexity is a fixed value, which does not change with the increase of the signal shaping degree, and is only $O(2n)$. Next, the encrypted shaping sequence is modulated to generate an electrical quadrature amplitude modulation (QAM) signal and modulated on an optical carrier by a Mach–Zehnder modulator (MZM) for transmission. At the receiver, the atmospheric fading signal is received using coherent detection. The digital signal processor (DSP) performs equalization, frequency offset estimation, and phase recovery. The decision device restores the DSP-processed signal into a bit

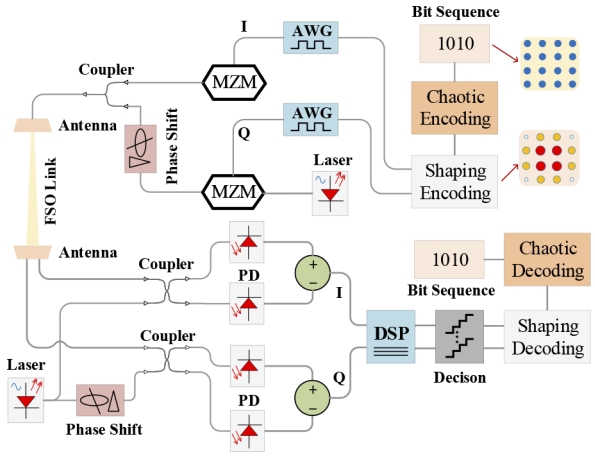

Fig. 1. Coherent FSO system model based on chaotic encryption and probabilistic constellation shaping.

sequence. Finally, the decoder extracts the permutation information in the bit sequence to de-probabilistic constellation shaping and uses the available key to restore the original information.

A four-dimensional hyperchaotic system is used for encryption of our proposed system [10], and can be expressed as

$$\begin{cases} \dot{x} = a(y - x) + w, \\ \dot{y} = cx - y - xz, \\ \dot{z} = xy - bz, \\ \dot{w} = -yz - rw, \end{cases} \tag{1}$$

where $a = 10$, $b = 8/3$, $c = 28$, r<13.667, and $\{x\}$, $\{y\}$, and $\{z\}$ are chaotic sequence variables. When $r = -1$, the four Lyapunov exponents are $\lambda_1 = 0.3381$, $\lambda_2 = 0.1586$, $\lambda_3 = 0$, and $\lambda_4 = -15.1752$, where two positive Lyapunov exponents indicate that the system produces hyperchaotic motion. The chaotic sequence can be calculated as

$$\mathrm{CS} = \mathrm{floor}\left[\mathrm{mod}\left((x + y + z + w) \times 10^{14}, P\right)\right], \tag{2}$$

where floor(·) represents rounding down, mod(·) represents the modulo operation, and P represents the number of rotation phases. Further, the generated chaotic sequence is used as the input of the phase rotation to complete the encryption process. Rotate the constellation points by 0°, 90°, 180°, or 270° to realize four-phase discrete constellation rotation encryption. The formula for the rotation angle θ of each constellation point is

$$\theta = 2\pi \times \frac{\mathrm{CS}_i}{P}, \qquad p \in \{0, 1, \ldots, P-1\}. \tag{3}$$

A QAM symbol is expressed as $Q = m + ni$, so the rotation operation can be expressed as

$$Q' = \begin{pmatrix} m & n \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} 1 \\ i \end{pmatrix}. \tag{4}$$

Since the receiver has a shared chaotic key, it can generate the same chaotic sequence as the transmitter to recover the signal by symmetric decryption.

Constellation distribution of short pseudorandom sequences behaves as the law of a non-uniform character. Grouping long pseudorandom sequences and counting the characteristics of constellation distribution can realize probabilistic constellation shaping [11]. The specific steps are as follows:

Step 1: Group the QAM sequence with length $L = M \times N$, where M is the number of groups, and N is the number of symbols in each group, as shown in Fig. 2(b)(i).

Step 2: Divide the jth ($j = 1, 2, \ldots, M$) group of the QAM sequence into a number of regions, according to the manner shown in Fig. 2(a), and count the number of constellation points in each region.

Step 3: According to the number of constellation points in each region, permutate the constellation points in the four regions of each quadrant, and record the permutation information, as shown in Figs. 2(b)(ii) to 2(vi).

Step 4: Embed the permutation information (PS) behind the QAM sequence, as shown in Fig. 2(b)(vii).

Step 5: Repeat the operation M times.

It is worth mentioning that there will be 24 kinds of quantitative relationship when permutating, and that different quantitative relationships may have the same permutation method. After verification, there are 13 different permutation methods in the actual operation, listed in Table 1, where S represents the number of regional constellation points, and ↔ represents the permutation operation.

The time complexity of this algorithm is only $O(2n)$ because the sequence needs to be traversed once each for statistical operation and probabilistic constellation shaping. At the same time, the redundant information in our algorithm is low, and it is a

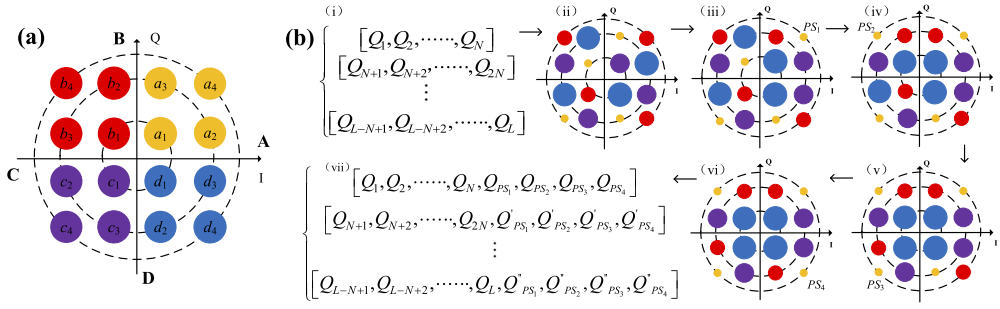

Fig. 2. Principle of region-optimized probabilistic constellation shaping.

Table 1. Region Permutation Methods

Size Relationship	Method
$S_1>S_2>S_3>S_4$, $S_1>S_3>S_2>S_4$	None
$S_1>S_2>S_4>S_3$, $S_1>S_4>S_2>S_3$	$a_4 \leftrightarrow a_3$
$S_1>S_3>S_4>S_2$, $S_1>S_4>S_3>S_2$	$a_4 \leftrightarrow a_2$
$S_2>S_1>S_3>S_4$, $S_2>S_3>S_1>S_4$	$a_2 \leftrightarrow a_1$
$S_2>S_1>S_4>S_3$, $S_2>S_4>S_1>S_3$	$a_4 \leftrightarrow a_3$, $a_2 \leftrightarrow a_1$
$S_3>S_1>S_2>S_4$, $S_3>S_2>S_1>S_4$	$a_3 \leftrightarrow a_1$
$S_4>S_1>S_2>S_3$, $S_4>S_2>S_1>S_3$	$a_4 \leftrightarrow a_3$, $a_3 \leftrightarrow a_1$
$S_3>S_1>S_4>S_2$, $S_3>S_4>S_1>S_2$	$a_4 \leftrightarrow a_2$, $a_3 \leftrightarrow a_1$
$S_4>S_1>S_3>S_2$	$a_4 \leftrightarrow a_1$, $a_4 \leftrightarrow a_2$
$S_4>S_3>S_1>S_2$	$a_4 \leftrightarrow a_2$, $a_2 \leftrightarrow a_1$
$S_2>S_3>S_4>S_1$, $S_2>S_4>S_3>S_1$	$a_2 \leftrightarrow a_1$, $a_4 \leftrightarrow a_2$
$S_3>S_2>S_4>S_1$, $S_3>S_4>S_2>S_1$	$a_3 \leftrightarrow a_1$, $a_4 \leftrightarrow a_3$
$S_4>S_2>S_3>S_1$, $S_4>S_3>S_2>S_1$	$a_4 \leftrightarrow a_1$

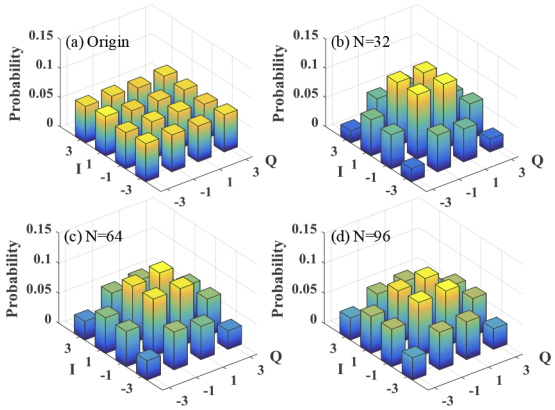

Fig. 3. 16-QAM constellation probability distribution in different shaping cases.

fixed value, which will not increase with the increase of the shaping degree. In particular, the algorithm has no requirement for calculation accuracy and is more feasible at the hardware level.

In this scheme, we can control the shaping case by adjusting the size of N. Figure 3 shows that the smaller N is, the more concentrated the constellation points are in the middle, and the higher the shaping degree is. When N is larger, the distribution of constellation points tends to be flat, and the shaping degree decreases.

The formula for calculating the code rate is

$$R = \frac{k}{k + (n-k)}, \tag{5}$$

where n represents the total bit length, k represents the number of useful bits, and $(n-k)$ represents the redundant bit length.

The formula for calculating the average power of the symbol sequence is

$$\bar{P} = \frac{1}{L}\sum_{i=1}^{L}\sqrt{\mathrm{Re}^2(Q_i) + \mathrm{Im}^2(Q_i)}, \tag{6}$$

where L represents the symbol sequence length, Re(·) represents the real part of the QAM symbol, and Im(·) represents the imaginary part of the QAM symbol.

Table 2. Variation in Code Rate, Average Power, and Average Euclidean Distance

Shaping Case	R	$\overline{P}$	$\overline{\rho}$
Origin	1.000	10.00	2.000
$N = 16$	0.800	8.21	2.434
$N = 32$	0.889	8.50	2.352
$N = 48$	0.924	8.70	2.300
$N = 64$	0.941	8.85	2.262
$N = 80$	0.952	8.96	2.234
$N = 96$	0.975	9.04	2.212

After probabilistic constellation shaping, the average Euclidean distance is calculated as

$$\bar{\rho} = \frac{\bar{P}_{\mathrm{ori}}}{\bar{P}_{\mathrm{ps}}}\bar{\rho}_{\mathrm{ori}}, \tag{7}$$

where $\overline{P}_{\mathrm{ori}}$ represents the average power of the original sequence, $\overline{P}_{\mathrm{ps}}$ represents the Euclidean distance of the original sequence, and $\overline{\rho}_{\mathrm{ori}}$ represents the average power of the sequence after probabilistic constellation shaping.

Table 2 lists the variation in code rate, average power, and average Euclidean distance in different N conditions. The proportion of redundant information will increase when N decreases, so the code rate gradually decreases. However, owing to the increase in the shaping case, the average power decreases, and the average Euclidean distance increases. In practical applications, we can choose the appropriate shaping case according to the variation of the channel.

FSO system performance will be affected by unpredictable atmospheric conditions, and turbulence is a major factor. Therefore, it is significant to test the communication performance in turbulent conditions. We use the log-normal model to simulate weak turbulence, and its probability distribution function is

$$P(F) = \frac{1}{\sqrt{2\pi\sigma_f^2}}\frac{1}{I}\exp\left\{-\frac{(F - E[F])^2}{2\sigma_f^2}\right\}, \qquad I \geq 0, \tag{8}$$

where $E[F]$ represents the expectation of F, σ_f^2 represents the log-amplitude variance, and I represents normalized received irradiance. We use the Gamma–Gamma model to simulate moderate to strong turbulence, and its probability distribution function [12] is

$$P(I) = \frac{2(\alpha\beta)^{(\alpha+\beta)/2}}{\Gamma(\alpha)\Gamma(\beta)} I^{(\alpha+\beta/2)-1} K_{\alpha-\beta}(2\sqrt{\alpha\beta I}), \qquad I>0, \tag{9}$$

where α and β, respectively, represent the effective numbers of large- and small-scale eddies of the scattering process, $K_{\alpha-\beta}(\cdot)$

Table 3. System Parameter Settings

Parameter	Value
Wavelength	1550 nm
Beam divergence	2 mrad
Transmitter aperture diameter	5 cm
Receiver aperture diameter	20 cm
Attenuation	5–15 dB/km
Transmission power	−0.3–16.9 dBm
Scintillation model	Log-normal, Gamma–Gamma
Refractive index structure constant	10^{-16}–10^{-14} $m^{-2/3}$

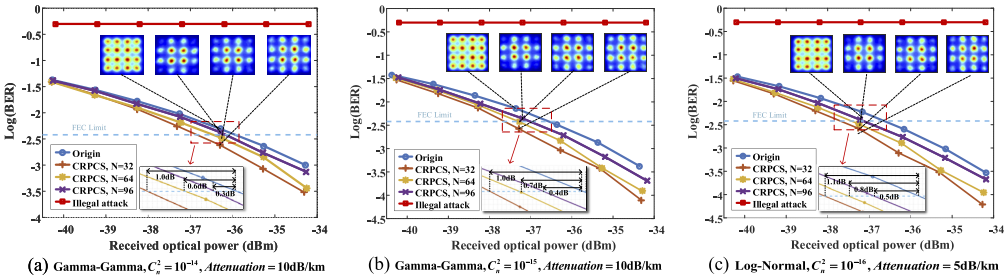

Fig. 4. BER diagram of proposed system in different turbulent conditions and shaping cases: (a) Gamma–Gamma, $C_n^2 = 10^{-14}$, attenuation = 10 dB/km; (b) Gamma–Gamma, $C_n^2 = 10^{-15}$, attenuation = 10 dB/km; (c) log-normal, $C_n^2 = 10^{-16}$, attenuation = 5 dB/km;.

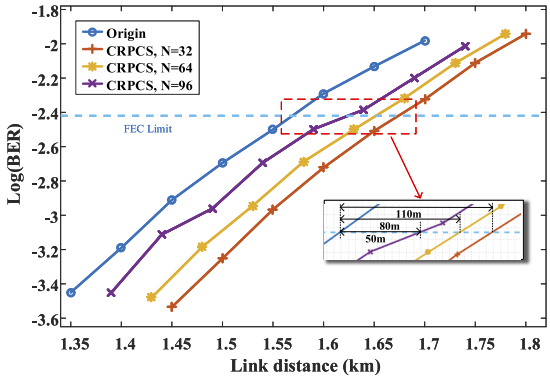

Fig. 5. Transmission distance performance in different shaping cases.

is the modified Bessel function of the 2nd kind of order n, and $\Gamma(\cdot)$ represents the Gamma function.

Table 3 lists the system parameter settings, and Fig. 4 shows the bit error rate (BER) diagram in different turbulent conditions and shaping cases, where C_n^2 represents the atmospheric refractive index structure constant that reflects the intensity of atmospheric turbulence. In terms of security, owing to the lack of the correct chaotic key, illegal attacks cannot obtain any information from the encrypted signal, and the BER is always maintained at 0.5. In addition, we obtain a key space of 10^{75} (five control parameters) through the hyperchaotic equation to resist exhaustive attacks. This shows that the CRPCS scheme guarantees the security of the communication system. In terms of communication performance, the optical receiver sensitivity is improved by 0.3–1.0 dB in moderately strong turbulence, improved by 0.4–1.0 dB in moderate turbulence, and improved by 0.5–1.1 dB in weak turbulence. It can be seen that the CRPCS scheme has a significant performance improvement in different turbulence intensities, especially in weak turbulence. In addition, the shaping case positively correlates with communication performance. Therefore, we can choose a smaller N to resist atmospheric turbulence to some extent when the channel conditions are poor.

Further, we test the transmission distance performance between the CRPCS scheme and the traditional scheme in non-turbulent conditions. As can be seen from Fig. 5, the transmission distance of the CRPCS scheme is improved by 3.2–7.0%. And the higher the shaping degree is, the farther the signal can be transmitted, so we can choose the appropriate shaping degree according to channel changes to meet the needs of transmission distance. These results show that the scheme provides the possibility for the long-distance transmission of the FSO system.

In this Letter, we reveal the new application prospects of chaotic encryption and probabilistic constellation shaping technique in the FSO system. The proposed scheme not only enhances the security but also improves the communication performance with low and fixed redundant information. The results show that the optical receiver sensitivity is improved by 0.3–1.1 dB, and the transmission distance is also improved by 3.2%–7.0% in different shaping cases.

Funding. Chongqing Municipal Education Commission (CXQT21019, KJQN202100616, KJQN202200610); Natural Science Foundation of Chongqing (CSTB2022NSCQMSX0542); National Natural Science Foundation of China (62025105, U21B2005).

Disclosures. The authors declare no conflicts of interest.

Data availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

REFERENCES

1. H. Kaushal and G. Kaddoum, IEEE Commun. Surv. Tutorials **19**, 57 (2017).
2. S. Khankalantary, M. T. Dabiri, and H. Safi, Opt. Commun. **463**, 125309 (2020).
3. S. Song, Y. Liu, J. Wu, T. Wu, L. Zhao, and L. Guo, J. Lightwave Technol. **40**, 7048 (2022).
4. T. Wu, C. Zhang, H. Wei, and K. Qiu, Opt. Express **27**, 27946 (2019).
5. R. Boluda-Ruiz, A. García-Zambrana, B. Castillo-Vázquez, and K. Qaraqe, Opt. Express **27**, 34211 (2019).
6. P. V. Trinh, A. Carrasco-Casado, A. T. Pham, and M. Toyoshima, IEEE Trans. Commun. **68**, 7810 (2020).
7. Y. Ai, A. Mathur, G. D. Verma, L. Kong, and M. Cheffena, IEEE Photonics J. **12**, 1 (2020).
8. M. Eghbal and J. Abouei, J. Opt. Commun. Netw. **6**, 684 (2014).
9. P. Schulte and G. Böcherer, IEEE Trans. Inf. Theory **62**, 430 (2016).
10. K. H. Sun, S. B. He, C. X. Zhu, and Y. He, Acta. Electronica Sinica. **41**, 1765 (2013).
11. Z. Zhang, Y. Luo, C. Zhang, X. Liang, M. Cui, and K. Qiu, J. Lightwave Technol. **40**, 14 (2022).
12. L. C. Andrews, R. L. Phillips, and C. Y. Hopen, *Laser Beam Scintillation with Applications* (SPIE Press, 2001).