PHOTONICS Research

Simultaneously enhancing capacity and security in free-space optical chaotic communication utilizing orbital angular momentum

Yiqun Zhang,[1,2,†] Mingfeng Xu,[2,3,†] Mingbo Pu,[2,3,4] Mengjie Zhou,[5] Jiazheng Ding,[5] Shuangcheng Chen,[5] Kun Qiu,[1] Ning Jiang,[1,6] and Xiangang Luo[2,4,*]

[1] School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
[2] State Key Laboratory of Optical Technologies on Nano-Fabrication and Micro-Engineering, Institute of Optics and Electronics, Chinese Academy of Sciences, Chengdu 610209, China
[3] Research Center on Vector Optical Fields, Institute of Optics and Electronics, Chinese Academy of Sciences, Chengdu 610209, China
[4] School of Optoelectronics, University of Chinese Academy of Sciences, Beijing 100049, China
[5] Tianfu Xinglong Lake Laboratory, Chengdu 610299, China
[6] e-mail: uestc_nj@uestc.edu.cn
[†] These authors contributed equally to this work.
[*] Corresponding author: lxg@ioe.ac.cn

Received 26 May 2023; revised 28 September 2023; accepted 13 October 2023; posted 16 October 2023 (Doc. ID 496535); published 30 November 2023

Optical chaotic signals emitted from an external-cavity feedback or injected laser diode enable small-signal information concealment in a noise-like carrier for secure optical communications. Due to the chaotic bandwidth limitation resulting from intrinsic relaxation oscillation frequency of lasers, multiplexing of optical chaotic signal, such as wavelength division multiplexing in fiber, is a typical candidate for high-capacity secure applications. However, to our best knowledge, the utilization of the spatial dimension of optical chaos for free-space secure communication has not yet been reported. Here, we experimentally demonstrate a free-space all-optical chaotic communication system that simultaneously enhances transmission capacity and security by orbital angular momentum (OAM) multiplexing. Optical chaotic signals with two different OAM modes totally carrying 20 Gbps on–off keying signals are secretly transmitted over a 2 m free-space link, where the channel crosstalk of OAM modes is less than −20 dB, with the mode spacing no less than 3. The receiver can extract valid information only when capturing approximately 92.5% of the OAM beam and correctly demodulating the corresponding mode. Bit error rate below the 7% hard-decision forward error correction threshold of 3.8×10^{-3} can be achieved for the intended recipient. Moreover, a simulated weak turbulence is introduced to comprehensively analyze the influence on the system performance, including channel crosstalk, chaotic synchronization, and transmission performance. Our work may inspire structured light application in optical chaos and pave a new way for developing future high-capacity free-space chaotic secure communication systems.

https://doi.org/10.1364/PRJ.496535

1. INTRODUCTION

In comparison with wireless radio communication, free-space optical (FSO) communications have attracted great interest due to their higher capacity and security [1–3]. In practical scenarios, however, the security of FSO systems is susceptible to atmospheric scattering and beam divergence as the transmission distance increases, making it possible to be intercepted using additional receivers [4,5], especially for those scenarios where the paramount need is to ensure secure transmission of high-data confidentiality, such as underwater communication, star–earth communication, interstellar communication, deep space communication, and similar contexts. Consequently, enhancing the physical-layer security of FSO systems has gained increasing attention in recent years. Optical chaotic signals enable small-signal information concealment in noise-like chaotic carriers. Combined with chaos synchronization, it can enhance the information security of the physical layer to achieve secure optical transmission [6,7]. Although it has been well investigated in fiber optic channels [8–14], the exploration of optical chaotic communication in FSO links is still in its infancy [5,15–20], particularly in terms of experimental investigations, as summarized in Table 1.

Optical chaotic signals emitted from external-cavity feedback or injected laser are impacted by the intrinsic relaxation oscillation of a laser, which limits their bandwidth to only a few

2327-9125/23/122185-09 Journal © 2023 Chinese Laser Press

Table 1. Secure Data Transmission of Chaos-Based FSO Experimental Systems

Transmission Wavelength (nm)	Spatial Mode	Number of Transmission Channels	Transmission Environment	Capacity	Distance	Bit Error Rate	Refs.
690	Gauss	1	Outdoor	60 kbps	5 km	1.92×10^{-2}	[15]
5700	Gauss	1	No turbulence	0.5 Mbps	1 m	6×10^{-2}	[18]
1550	Gauss	1	Simulated $D/r_0 \approx 2.4$	8 Gbps	10 m	2.4×10^{-3}	[20]
1550	Laguerre–Gauss	2	Simulated $D/r_0 \approx 1.2$	20 Gbps	2 m	2.1×10^{-3}	This work

gigahertz, making it challenging to support high-capacity FSO secure communication [21]. Although several schemes for generating broadband chaotic signals have been proposed [22–29], the poor synchronization quality and stability of the high-frequency part of chaotic carriers restrict the enhancement of private communication capacity. Alternatively, multiplexing of optical chaotic signals is a typical candidate for high-speed secure application. In fact, traditional schemes used in fiber optic channels are limited to manipulating the time, frequency, phase, and/or polarization domains of chaotic lasers. However, the utilization of spatial dimension of optical chaotic signals well-suited for FSO links has not yet been reported.

On the other hand, as an intrinsic degree of freedom of light, orbital angular momentum (OAM) has attracted great attention in optical communication and quantum information due to its discrete unbounded orthogonal modes in the spatial dimension [30,31]. Recently, OAM multiplexing has been experimentally demonstrated to enhance capacity in classical and quantum communication [32–34], including in free space [35–38], fiber [39,40], and on-chip [41]. This offers a promising opportunity to establish a high-speed FSO chaotic secure communication system with the spatial optical field manipulation of optical chaos.

Here, we propose a capacity- and security-enhanced FSO chaotic communication scheme by exploring the spatial dimension of chaotic signals. A proof-of-concept transmission experiment that encrypts 20 Gbps on–off keying data with all-optical chaos modulation and spatial OAM multiplexing is successfully demonstrated. The influence of mode spacing between two OAM channels on channel crosstalk is quantitatively analyzed to optimize transmission performance. The security of the proposed systems guaranteed by the inherent profiles of optical chaos and OAM is investigated separately. Valid information can only be obtained at the receiver side when the majority parts of OAM beams are captured and demodulated correctly as well as the same chaotic synchronization hardware parameters implemented on the transmitter side. Additionally, weak atmospheric turbulence with $D/r_0 \approx 1.2$, where D is the aperture of the optical system and r_0 is the Fried parameter, is introduced to systematically investigate the effects of atmospheric turbulence on the OAM mode crosstalk, chaotic synchronization, and transmission performance. Overall, the proposed chaos-based OAM multiplexing FSO system allows for a private transmission with a bit error rate (BER) below the 7% hard-decision forward error correction (HD-FEC) threshold of 3.8×10^{-3}.

2. EXPERIMENTAL SETUP

Figure 1 shows the experimental setup of the proof-of-principle secure chaos-based OAM multiplexing FSO communication system. On Alice's side, a commercial external-cavity semiconductor laser (ECSL) with conventional optical feedback is utilized as a drive laser (DL) source to generate the chaotic optical carrier. The optical feedback loop consists of an 80:20 fiber coupler (FC1), a polarization controller (PC1), a variable optical attenuator (VOA1), and a fiber mirror (M1). After passing through an optical isolator (ISO1), the chaotic optical carrier is modulated by 10 Gbps nonreturn-zero on–off keying (NRZ-OOK) signals from a 65-GS/s arbitrary waveform generator (AWG) through a 10 GHz Mach–Zehnder modulator (MZM) to achieve message encryption. The encryption performance can be characterized by the masking coefficient β, which is defined as the ratio of the peak-to-peak value of the message signal to the peak-to-peak value of the chaotic carrier signal and can be flexibly adjusted by the amplitude range of the AWG. An erbium-doped fiber amplifier (EDFA) and VOA2 are used to precompensate for the power impairment in the OAM

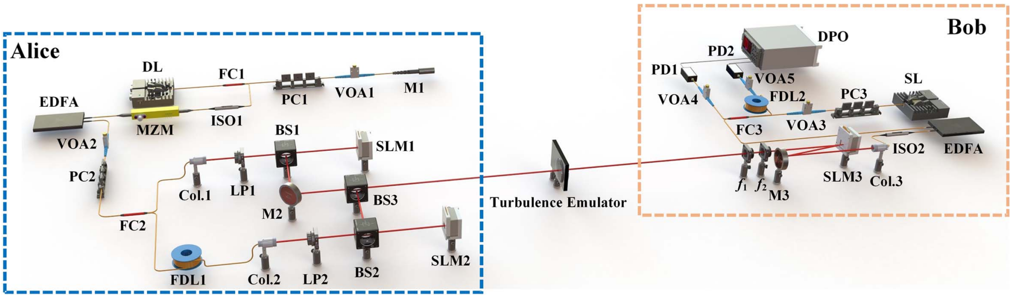

Fig. 1. Experimental setup of the secure chaos-based OAM multiplexing FSO communication system. DL, drive laser; FC, fiber coupler; PC, polarization controller; VOA, variable optical attenuator; M, mirror; ISO, optical isolator; MZM, Mach–Zehnder modulator; EDFA, erbium-doped fiber amplifier; FDL, fiber delay line; Col., collimator; LP, linear polarizer; BS, beam splitter; SLM, spatial light modulator; SL, slave laser; PD, photodetector; DPO, digital phosphor oscilloscope.

modulation and beam combination parts and to control the power incident on the spatial light modulators (SLMs).

The encrypted signal is split into two branches, whose data streams are decorrelated by inserting a 10 m single-mode fiber (SMF) in the lower channel. Each beam is collimated in free space and converted to a different OAM mode of $l = -3$ or $l = +1$ using a computer-generated phase hologram loaded on the SLM, where l denotes the topological charge. The SLM used here is a phase-only reflective phase modulator with a spatial resolution of 12.5 μm. PC2 and a free-space linear polarizer (LP) are used to optimize the polarization of the light incident to SLMs. The two OAM beams are spatially multiplexed using a beam splitter (BS) and coaxially propagated in free space for ~2 m. In laboratory conditions, no distortions are observed during the propagation of multiplexed beams in such an optical link. Therefore, to simulate the effect of turbulence, we introduced external wavefront distortion using a turbulence emulator. The turbulence emulator is a thin phase screen plate mounted on a rotating platform and placed in the middle of the optical path. The equivalent effective Fried coherence length r_0 is about 2.5 mm. Considering that the beam diameter D when passing through the thin phase plate is about 3 mm, the emulated turbulence is classified as weak turbulence, with $D/r_0 \approx 1.2$, which is the turbulence strength corresponding to the subsequent discussion of the effect of atmospheric turbulence on the system performance.

After free-space transmission, a beam down-collimator system comprising two lenses with focal lengths of $f_1 = 50$ mm and $f_2 = -30$ mm is used to reduce the size of the received optical beam for OAM demultiplexing and detection. On Bob's side, to detect the data transmitted on each OAM channel, SLM3 is used to conduct the OAM demultiplexing. The OAM beam is converted to a Gaussian-like beam using an inverse-phase hologram loaded on SLM3, while the other beam remains in an OAM state with a nonzero charge. Only the correctly converted Gaussian beam could be coupled into the SMF for later detection and processing. Moreover, a small signal EDFA is used here to compensate for the free-space link loss. The encrypted signal is then split into two parts using a 2 × 2 fiber coupler (FC3). One part, with its state of polarization adjusted by PC3, is unidirectionally injected into the slave laser (SL) for chaos synchronization, and the synchronized chaotic signal is detected by a photodetector (PD1). The other part passes through a delay line to eliminate the synchronization error and is then detected by PD2. The recovered message is decrypted by subtracting the synchronized chaos signal from the encrypted transmitted signal and then filtered by a lowpass fourth-order Butterworth filter with a cut-off frequency of $0.8R$, where R is the transmission bit rate. In our experiment, the operation wavelengths of DL and SL are set to 1549.68 nm, and their emission powers are set to 0 dBm. The feedback strength of DL is fixed at −10 dB. The bandwidths of both PDs are 20 GHz. A high-speed digital phosphor oscilloscope (DPO) collects the two signals detected by the PDs with a sampling rate of 100 GSa/s and two 59 GHz bandwidth channels. The transmission efficiencies of OAM_{-3} and OAM_{+1} are 5.2% and 3.4%, respectively. The low transmission efficiency obtained in this framework is due to the use of beam splitters to generate OAM modes. While this approach enhances the modulation efficiency of the OAM mode, it inevitably results in a substantial energy loss at the modulation end. In addition, another purpose of such an approach is to conserve the space taken up by the experimental setup, as the method involving small-angle reflection requires the construction of a longer modulation optical path.

3. RESULTS AND DISCUSSION

In this section, we thoroughly investigate and discuss the system's channel crosstalk, security, and transmission performance, along with the impact of atmospheric turbulence on the proposed scheme. It is noteworthy that the results presented in the first two subsections were obtained without considering the influence of atmospheric turbulence.

A. Channel Crosstalk Analysis

Crosstalk among OAM modes during OAM multiplexing may arise due to multiple factors, such as beam axis misalignment with the center of the SLM, aberrations, and atmospheric turbulence, which will cause significant degradation in the performance of communication systems. To clarify, we denote the channel that generates the OAM beam using SLM1 as CH1 and the channel that generates the OAM beam using SLM2 as CH2. In our experiment, channel crosstalk is defined as the ratio of the power received on the desired channel when the other channel is transmitting with the desired channel off (P_{others}) to the power received on the desired channel when only the desired channel is transmitting with the other channel off (P_{self}); that is, $\eta_{\mathrm{Crosstalk}} = 10\log_{10}(P_{\mathrm{others}}/P_{\mathrm{self}})$. We investigate the impact of OAM mode spacing Δl between two channels on power crosstalk and chaotic synchronization crosstalk to determine the channel spacing with optimal mode purity distribution. Theoretically, the mode spacing can be infinite due to the inherent orthogonality characteristic of OAM. However, in practical communication systems, various factors, such as the transceiver aperture, modulation devices, and transmission distance, impose limitations on the largest OAM mode. Here, the mode spacing is determined by fixing the OAM order loaded on SLM2 in CH2 ($l_2 = +1$) and changing the OAM order loaded on SLM1 in CH1 ($l_1 = \{+2, -1, -2, -3\}$), corresponding to the mode spacing $\Delta l = \{1, 2, 3, 4\}$.

Figure 2 illustrates the normalized power crosstalk of the two OAM multiplexed channels. The four power values measured in each mode spacing case are normalized to the maximum value, which is detected when transmitting and receiving OAM l_1. It should be noted that there is a power difference of approximately −4.2 dB between CH2 and CH1. This difference is likely due to the fact that the beam diameter of CH2 is slightly larger than that of CH1, leading to imperfect demodulation at SLM3 compared with CH1; further, the transmission efficiency of CH1 is also better than CH2. Figure 2(a) presents the results measured without the chaos feedback structure (i.e., blocking the 20% parts of the output at FC1). It can be seen that, as the mode spacing increases, the crosstalk continuously decreases, reducing from −14.84 to −31.12 dB for CH1 and from −8.62 to −27.98 dB for CH2. When $\Delta l = 3$, the crosstalk drops below −20 dB, indicating that the impact of

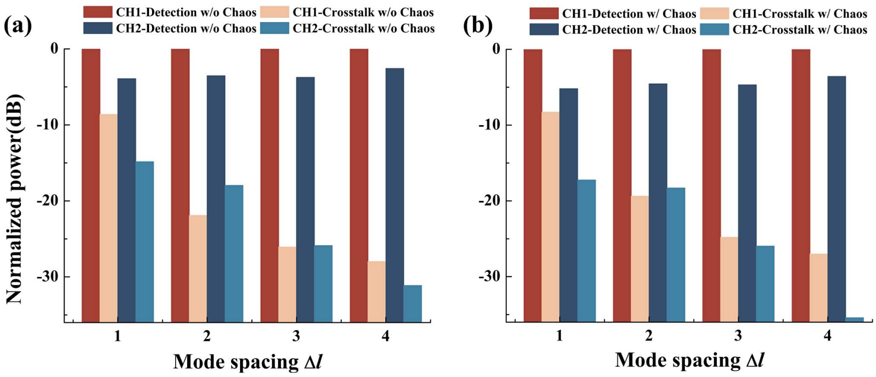

Fig. 2. Measured channel crosstalk for the two OAM modes (a) without chaos feedback loop and (b) with chaos feedback loop. Take mode spacing $\Delta l = 1$ as an example: CH1-Detection means CH1 sends OAM_{+2}, while the inverse phase hologram OAM_{-2} is loaded on SLM3 for direct demodulation when CH2 is blocked. CH1-Crosstalk means the crosstalk from CH2 to CH1, that is, CH2 sends OAM_{+1}, while OAM_{-2} is loaded on SLM3 when CH1 is blocked.

channel crosstalk on the transmission performance is negligible. As shown in Fig. 2(b), the evolutions of the detection power and crosstalk power with mode spacing for both channels are similar to those in Fig. 2(a) after adding the chaos feedback loop structure. This indicates that the presence of chaotic signals exhibiting random intensity fluctuations in the time domain does not alter the spatial energy distribution of the optical field. In other words, chaotic cryptography is compatible with free-space OAM multiplexed communication systems. It is worth noting that there is a notable discrepancy in the CH2 crosstalk arising at $\Delta l = 4$. The absolute values of crosstalk power are 0.05 μW in the absence of chaotic structure and 0.02 μW in its presence. The slight power reduction is intuitively attributed to measurement errors from experimental factors since it is unable to measure the crosstalk power from CH1 to CH2 in both structures simultaneously.

Chaotic synchronization is the core of chaotic confidential communication technique, which usually employs the cross-correlation coefficient (CC) to quantify synchronization quality [10]. A CC value of 0.9 or above is considered to achieve high-quality chaotic synchronization in most chaos-related applications. We then investigate the effect of OAM mode spacing Δl on chaotic synchronization performance, as depicted in Fig. 3(a). Here, synchronization crosstalk is defined as the CC value calculated on the desired channel when the other channel is transmitting with the desired channel off. When $\Delta l = 1$, the CC values for both channels with direct detection are around 0.8, while the crosstalk CC values are even higher than those in direct detection cases, indicating that severe crosstalk between OAM channels will threaten the security of the chaotic confidential communication system. As Δl increases, the synchronization crosstalk gradually decreases, and the CC values for both channels stabilize above 0.9 in the case of direct detection when $\Delta l \geq 3$. Figures 3(b) and 3(c) depict the cross-correlation curves of CH1 and CH2 with CC values of 0.94 and 0.92, respectively, for $\Delta l = 4$. The results show that the chaotic encrypted signals transmitted by both channels achieve high-quality chaotic synchronization with the locally generated chaos at the receiver, guaranteeing the performance of subsequent chaotic decryption.

Subsequently, we investigate the effect of mode spacing on the transmission performance of chaotic OAM multiplexing communication systems, as shown in Fig. 4. The transmission performances of CH1 and CH2 are similar, and, for the sake

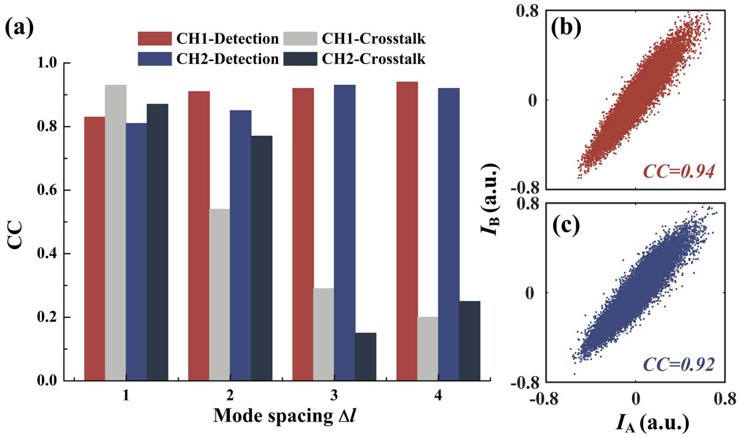

Fig. 3. (a) Measured chaotic synchronization channel crosstalk for the two OAM modes; (b) cross-correlation plot for CH1 when $\Delta l = 4$; (c) cross-correlation plot for CH2 when $\Delta l = 4$.

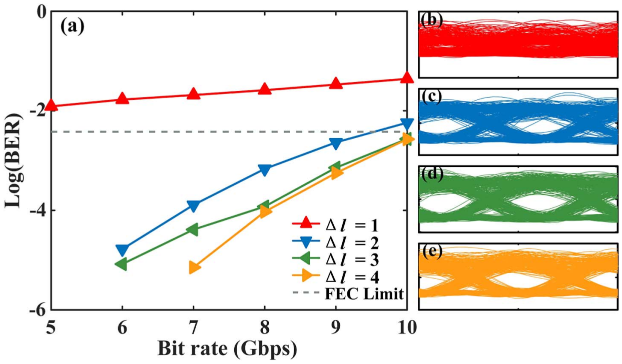

Fig. 4. Performance of the chaos-based OAM multiplexing FSO communication system with different mode spacing. (a) Measured BER curves for different mode spacing for CH2 in the case of direct detection. Take mode spacing $\Delta l = 1$ as an example: direct detection means the BER value when CH1 sends OAM_{+2} and CH2 sends OAM_{+1}, while the inverse phase hologram OAM_{-1} is loaded on SLM3 for CH2 direct demodulation. Eye diagram at $R = 8$ Gbps for (b) $\Delta l = 1$, (c) $\Delta l = 2$, (d) $\Delta l = 3$, and (e) $\Delta l = 4$.

of simplify, we only present the BER curve of CH2. It can be observed that, when $\Delta l = 1$, the BER of the decrypted data exceeds the hard decision forward error correction (HD-FEC) threshold, indicating serious crosstalk between two OAM channels and poor chaotic decryption performance ($\mathrm{CC} \approx 0.79$). At this point, the corresponding eye diagram is closed at $R = 8$ Gbps. As the mode spacing increases, the transmission performance of CH2 gradually improves, and when Δl reaches 3, CH2 can support a maximum communication rate of 10 Gbps. Based on the above analysis of channel crosstalk with mode spacing, we choose $\Delta l = 4$, i.e., SLM1 is loaded with OAM_{-3} and SLM2 is loaded with OAM_{+1} for subsequent experiments.

B. Security and BER Performances

Conventional FSO communication systems are considered to have inherent security properties due to the narrow beam and high directionality of the laser. However, as the laser undergoes scattering and beam divergence during atmospheric transmission, there is a possibility of unauthorized interception of the beam by other receivers. The security of the proposed encrypted FSO communication system is derived from the inherent security properties of chaotic signals and OAM beams.

In this context, the scheme's security is first evaluated from the perspective of chaos. Take CH2 as an example, Figs. 5(a)–5(c) show the temporal waveforms of the NRZ-OOK signal from generation to encryption to decryption process at the transmission rate of 7 Gbps; Figs. 5(d)–5(f) represent the corresponding eye diagrams. The original information signal is directly detected and collected by the DPO. After connecting the chaotic external feedback loop, the small signal is completely concealed in the chaotic carrier by adjusting the signal amplitude output of AWG, as shown in Fig. 5(b). The intensity of the encrypted signal shows noise-like fluctuations, and the communication eye diagram is tightly closed. When the hardware parameters such as the lasers' chip, drive current, and temperature control of DL and SL are well matched, the legitimate receiver can locally generate a synchronized chaotic signal by injection-locking mechanism and chaotic filtering effect. Figure 5(c) shows the decrypted message signal obtained by offline DSP processing with only slight differences compared with Fig. 5(a), which indicates the information can be effectively recovered by the legitimate receiver. Chaos-modulated encryption schemes are vulnerable to a link attacking approach called "direct detection with linear filtering" (DDLF), where the eavesdropper directly detects the encrypted data using a PD and filters the data with a cutoff frequency equaling the transmission rate to recover the original message [7,18]. This phenomenon is caused by the uneven power spectrum of the chaotic optical carrier generated by the conventional optical feedback structure. Specifically, the low-frequency components of the signal have low power, leading to relatively low efficiency in concealing information. Consequently, the original information can potentially be extracted through a DDLF attack [12]. In the following discussion, we assume that the eavesdropper has prior knowledge of the OAM pattern transmitted in the link and couples the correctly demultiplexed beam into SMF for the DDLF attack. Figure 5(g) depicts the BER performance for encrypted messages, legally decrypted messages, and illegally received messages for both channels. Here, 2×10^9 bits are used to calculate the BER values for each case. The BERs of the encrypted messages for both channels

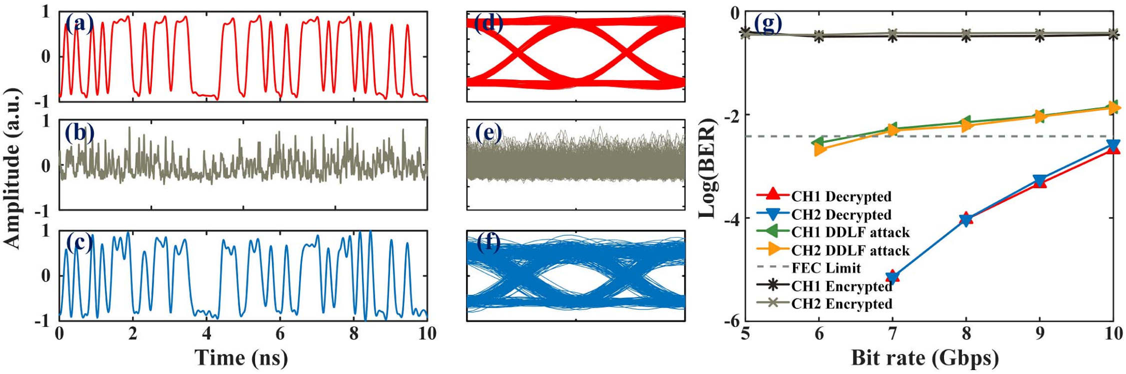

Fig. 5. Experimental temporal waveforms for CH2 of (a) the original NRZ-OOK signal at the output of AWG, (b) the encrypted signal at the output of MZM, and (c) the decrypted signal after offline DSP. Eye diagrams of (d) the original NRZ-OOK signal, (e) the encrypted signal, and (f) the decrypted signal. (g) BER performances for CH1 and CH2 in the case of legal reception, illegal reception, and encryption.

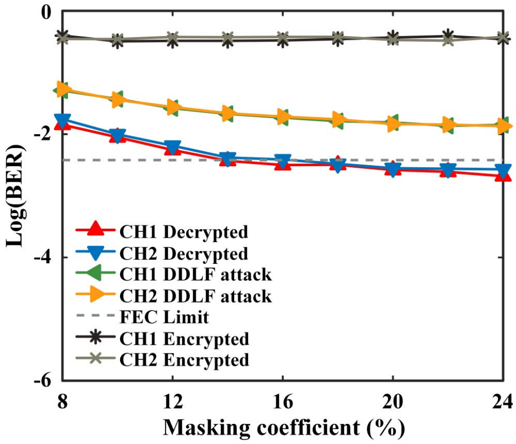

Fig. 6. Measured BER curves for different cases as a function of masking coefficient β.

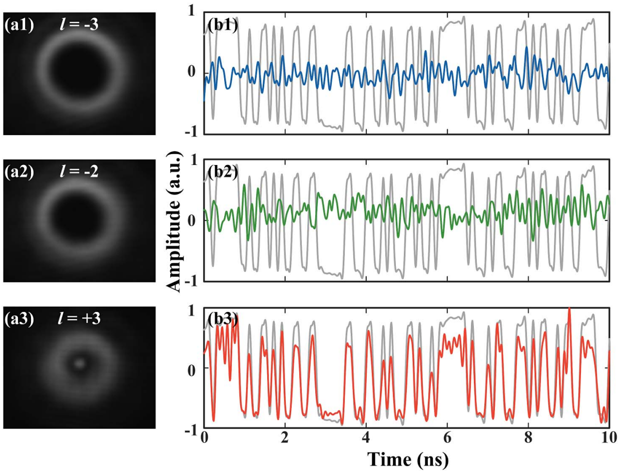

Fig. 7. (a1)–(a3) Intensity profiles of demodulated beams for different loading patterns ($l = -3$, $l = -2$, $l = +3$) when transmitting $l = -3$ and $+1$; (b1)–(b3) temporal waveforms of corresponding original message (gray line) and recovered message (colored line) at $R = 10$ Gbps.

maintain a high level (larger than 0.2), indicating excellent encryption performance. For the legitimate receiver, the BERs of CH1 and CH2 are both below the FEC limit, and the maximum communication rate of each channel reaches 10 Gbps; for the illegal eavesdropper, the BERs are much higher than that of the legal receiver, and the system can no longer support the recovery of the original data when $R \geq 7$ Gbps.

In our chaos-modulated FSO communication system, the masking coefficient β is a crucial parameter for evaluating the encryption efficiency, as the information is superimposed on the carrier by the MZM. The BER curves with β for both channels at $R = 10$ Gbps for encrypted, decrypted, and intercepted messages are shown in Fig. 6. The BERs for decrypted and intercepted messages gradually decrease with the increase of β; when β reaches around 18%, the BER of the legitimate receiver drops below the FEC limit. In contrast, when β is less than 24%, the BERs for encrypted and intercepted messages are always higher than 3.8×10^{-3}. However, when β is further increased, it can be predicted that there is a possibility that the BER of messages obtained by means of DDLF is below the FEC threshold. These results indicate that a low masking coefficient can effectively resist DDLF link eavesdropping but at the cost of sacrificing the transmission and decryption performance. Therefore, a trade-off between the security and transmission performance of the system is necessary, and properly setting the bit rate ($R \geq 7$ Gbps) and the masking coefficient ($18\% \leq \beta \leq 24\%$) in our system enables information to be effectively hidden and recovered in the chaotic optical carrier and resist eavesdropping.

Our proposed scheme using OAM to carry the multiplexing data offers another inherent security enhancement. On the one hand, the beam's OAM mode can be considered a physical key preassigned by the transceivers, albeit with a limited key space. The OAM data can only be collected into the SMF when the receiver uses a phase hologram with the inverse OAM order of the transmitter, making the SMF act as a mode selector. The largest OAM mode supported by both channels in the proposed system is found to be $\text{OAM}_{\pm 10}$, indicating that the size of the key space is 21. To verify the secure property offered by the OAM modes, it is assumed that the receiver has the same chaotic synchronization hardware structure as the transmitter and utilizes different modes for demodulation. Figure 7 shows the intensity profiles of the demodulated optical fields and the corresponding decrypted message waveforms for different phase holograms used by the receiver at $R = 10$ Gbps. As shown in Fig. 7(a3), the OAM beam is transformed into a Gaussian-like beam with a bright spot in the center only when the phase hologram loaded on SLM3 is set to $l = +3$. Figure 7(b3) shows that the data after correct OAM demultiplexing and chaotic decryption are nearly identical to the original information. On the contrary, as shown in Figs. 7(b1) and (b2), where the receiver uses the wrong phase hologram for demultiplexing, the demodulated light field still retains a donut shape, and the decrypted message waveforms appear as noise dithering.

On the other hand, the inherent security property of OAM also stems from the fact that the recovery of OAM data from atmospherically scattered light is complicated due to the time-varying scattering process that randomizes the phase structure of the OAM beams [4]. Despite the seemingly limited size of the key space offered by the OAM mode, an eavesdropper must still intercept the OAM beam should he wish to demodulate the OAM mode through exhaustive approaches. In this scenario, we assume an eavesdropper intercepts part of the OAM lights field by loading a partially blocked phase hologram on SLM3. Figure 8 presents the experimentally measured BER curves of both channels at $R = 10$ Gbps with varying percentages of phase hologram blocking. In the case of full reception, the BERs of the decrypted data for both channels are approximately 2.1×10^{-3}, while the BER detected by DDLF is above the FEC threshold, indicating that the eavesdropper cannot correctly decrypt the tapped optical signal without knowing the hardware parameters of the chaotic system. At this time, the chaotic system guarantees the security of the proposed communication systems. As the percentage of blocking increases, both the BERs by chaotic decryption and DDLF increase;

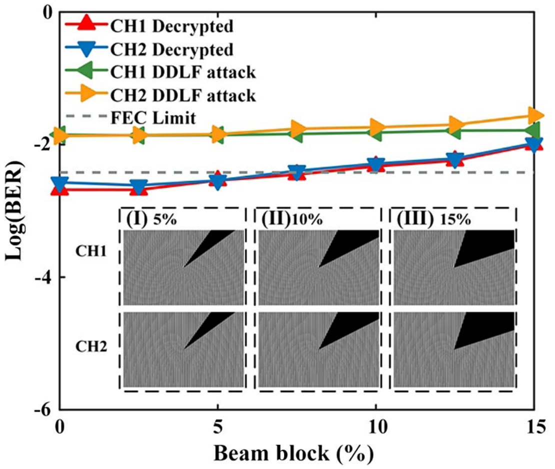

Fig. 8. Measured BER as a function of the percentage of beam block for secure chaos-based OAM multiplexing FSO transmission link. Insets (I) to (III) show the phase holograms partially blocked in SLM3.

when the portion of blocking is higher than 7.5%, the BER by chaotic decryption exceeds the FEC threshold. The above result implies that, even if the eavesdropper knows the precise parameters of the chaotic laser system and steals 92.5% of the optical field, no valid information can be obtained from it. Therefore, the security of the proposed chaos-based OAM multiplexing communication system is further enhanced.

C. Atmospheric Turbulence Analysis

One of the critical challenges in implementing such a transmission system is the impact of atmospheric turbulence on light as it propagates through the free-space channel. The random fluctuations in the refractive index of the atmosphere cause vortex beams to suffer from phase distortion, beam spreading, singularities drift, and other phenomena, all of which lead to crosstalk between neighboring OAM channels and degradation of the information capacity and transmission performance of the FSO communication system. In our system, we introduce weak atmospheric turbulence with $D/r_0 \approx 1.2$ in the transmission link and discuss the influence of turbulence on the optical field, channel crosstalk, chaotic synchronization, and transmission performance. Figures 9(a)–9(c) compare the intensity profiles of two independent OAM beams and the multiplexed beam under different scenarios. It can be observed that the OAM beam experiences beam diverging after a short free-space link transmission. Under the weak atmospheric turbulence, it is evident that the OAM light fields degrade, resulting in nonuniform intensity distribution and the slightly irregular spot shape. The crosstalk matrices for OAM_{-3} and OAM_{+1}, with and without atmospheric turbulence, are presented in Figs. 9(d) and 9(e). The OAM beams suffer from intermodal crosstalk caused by turbulence, leading to degradation of approximately 10 and 22 dB for CH1 and CH2, respectively.

We then analyzed the effect of turbulence on free-space unidirectional injection-locked chaotic synchronization. Figures 10(a) and 10(b) depict the crosstalk matrices of the synchronization CCs for CH1 and CH2 in the absence and presence of turbulence, respectively. In the absence of turbulence, the chaotic carriers achieve high-quality synchronization ($\text{CC} > 0.9$) with the local-end chaotic signals at the desired channels, with less crosstalk between them. However, when weak turbulence is introduced, their channels' synchronization performance deteriorates rapidly ($\text{CC} \approx 0.85$) while increasing synchronization channel crosstalk. Figure 10(c) illustrates the evolution of BER with transmission rate R for both channels with and without turbulence. The transmission performance of both channels is almost identical and supports a maximum transmission rate of 10 Gbps/channel in the case of no turbulence. In the presence of turbulence, the transmission performance of both channels deteriorates, reducing the maximum transmission capacity to 8 Gbps/channel. This degradation is caused by atmospheric turbulence, which affects the transmission quality and reception efficiency of the OAM beams and degrades the synchronization performance of the chaotic system. The difference in performance between the two channels is because BER values of only one channel can be measured at a time, given the device limitations, while the turbulence phase

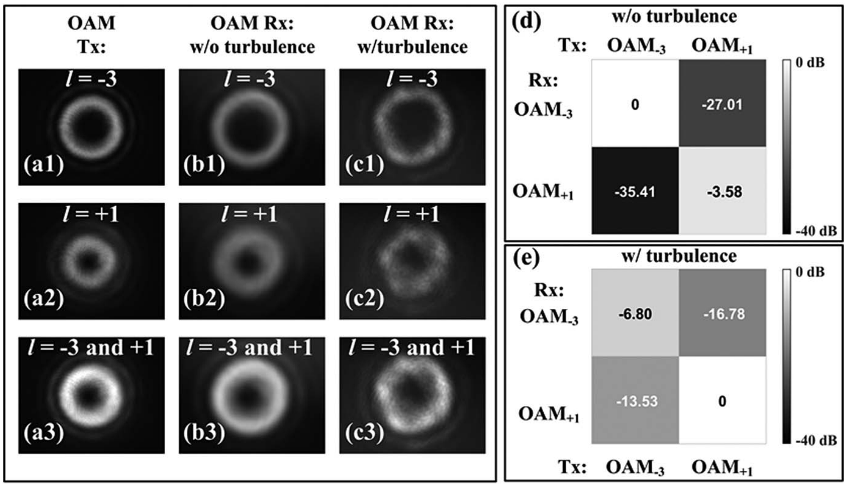

Fig. 9. Intensity profiles of (a1)–(a3) generated OAM beams ($l = -3$, $l = +1$, and superposition of $l = -3$ and $+1$) at Tx (transmitter); (b1)–(b3) received OAM beams ($l = -3$, $l = +1$, and superposition of $l = -3$ and $+1$) at Rx (receiver) without turbulence; (c1)–(c3) received OAM beams ($l = -3$, $l = +1$, and superposition of $l = -3$ and $+1$) at Rx with weak turbulence. Normalized channel crosstalk matrix of OAM multiplexing (d) without turbulence; (e) with turbulence.

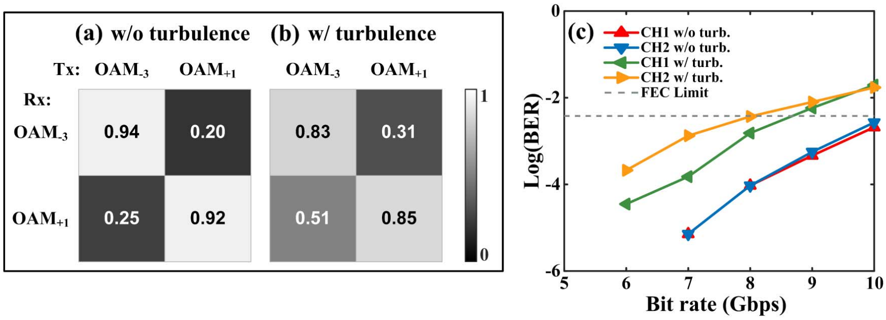

Fig. 10. Measured chaotic synchronization channel crosstalk matrix (a) without turbulence; (b) with turbulence. (c) BER performance for CH1 and CH2 as a function of bit rate R, in the case of no turbulence and with turbulence.

screen is time-varying. From the above results, it can be inferred that the proof-of-principle experimental demonstration of our chaos-based OAM multiplexing FSO system is highly sensitive to atmospheric turbulence. Therefore, corresponding turbulence mitigation techniques should be employed to ensure the purity of the OAM beam and the synchronization performance of the chaotic signal in practical application links.

4. CONCLUSION

In conclusion, a secure FSO communication system is proposed and experimentally demonstrated using all-optical chaos modulation and OAM. We discuss the impact of OAM mode spacing on the channel crosstalk, chaotic synchronization, and transmission performance. Increasing the mode spacing to four results in channel crosstalk below −20 dB and high-quality synchronization with CC > 0.9. We successfully transmit private 10 Gbps/channel OOK signals with BER below 7% HD-FEC in a free-space link of 2 m. The information security of this system is guaranteed by the inherent properties of the chaotic carrier and the OAM beam. On the one hand, even in the scenario where an eavesdropper captures the entire spatial structure of the OAM beam and accurately demodulates it into a Gaussian beam using exhaustive methods or deep learning techniques, the demodulated data remain noise-like properties, and chaotic carrier cannot be synchronized without prior knowledge of the hardware parameters of the chaotic system. Consequently, the information remains undecipherable. On the other hand, even if the eavesdropper knows the hardware parameters of the chaotic system and captures 92.5% of the OAM beams, valid information still cannot be obtained, where these two assumptions are challenging to realize in practical applications. To the best of our knowledge, this is the first experiment to introduce OAM in chaotic communication systems to enhance security and data capacity simultaneously, resulting in the highest transmission rate achieved in chaotic FSO communication to date.

Further, we analyze the effect of atmospheric turbulence on the proposed system's performance. The results demonstrate that turbulence not only degrades the optical field information of the OAM beams but also reduces the synchronization performance of the chaotic system. Therefore, different turbulence mitigation techniques are needed for practical applications, such as using adaptive optics [42,43], MIMO balanced detection [44], vector optical manipulation [45], and other channel compensation algorithms [46]. Moreover, an exciting next step is to realize long-distance chaotic secure communication with a large aperture optical system, such as planar digital optics [47]. This work is a crucial step in applying chaotic cryptography to space communication systems and extends a new approach toward manipulating the spatial dimension of chaotic signals to achieve security and bandwidth enhancement for chaos-based applications.

Funding. National Natural Science Foundation of China (62105338, 62171087); Sichuan Science and Technology Program (2021JDJQ0023, 2021ZYCD001); Fundamental Research Funds for the Central Universities (ZYGX2019J003); Science and Technology Commission of Shanghai Municipality (SKLSFO2020-05).

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. R. Zhang, N. Hu, H. Zhou, K. Zou, X. Su, Y. Zhou, H. Song, K. Pang, H. Song, A. Minoofar, Z. Zhao, C. Liu, K. Manukyan, A. Almaiman, B. Lynn, R. Boyd, M. Tur, and A. Willner, "Turbulence-resilient pilot-assisted self-coherent free-space optical communications using automatic optoelectronic mixing of many modes," Nat. Photonics **15**, 743–750 (2021).
2. Z. Zhu, M. Janasik, A. Fyffe, D. Hay, Y. Zhou, B. Kantor, T. Winder, R. W. Boyd, G. Leuchs, and Z. Shi, "Compensation-free high-dimensional free-space optical communication using turbulence-resilient vector beams," Nat. Commun. **12**, 1666 (2021).
3. W. Shao, Y. Wang, S. Jia, Z. Xie, D. Gao, W. Wang, D. Zhang, P. Liao, B. Little, S. Chu, W. Zhao, W. Zhang, W. Wang, and X. Xie, "Terabit FSO communication based on a soliton microcomb," Photon. Res. **10**, 2802–2808 (2022).
4. G. Gibson, J. Courtial, and M. Padgett, "Free-space information transfer using light beams carrying orbital angular momentum," Opt. Express **12**, 5448–5456 (2004).
5. M. Li, Y. Hong, Y. Song, and X. Zhang, "Effect of controllable parameter synchronization on the ensemble average bit error rate of space-to-ground downlink chaos laser communication system," Opt. Express **26**, 2954–2964 (2018).
6. 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 **438**, 343–346 (2005).

7. A. Zhao, N. Jiang, S. Liu, Y. Zhang, and K. Qiu, "Generation of synchronized wideband complex signals and its application in secure optical communication," Opt. Express **28**, 23363–23373 (2020).
8. L. Wang, X. Chen, X. Mao, L. Jiang, S. Li, Y. Sun, Y. Wang, L. Yan, and A. Wang, "Performance improvement of coherent optical chaos communication using probabilistic shaping," Opt. Lett. **48**, 1008–1011 (2023).
9. L. Jiang, J. Feng, L. Yan, A. Lin, S. Li, H. Yang, Y. Dong, L. Wang, A. Wang, Y. Wang, W. Pan, and B. Luo, "Chaotic optical communications at 56 Gbit/s over 100-km fiber transmission based on a chaos generation model driven by long short-term memory networks," Opt. Lett. **47**, 2382–2385 (2022).
10. A. Zhao, N. Jiang, S. Liu, Y. Zhang, and K. Qiu, "Physical layer encryption for WDM optical communication systems using private chaotic phase scrambling," J. Lightwave Technol. **39**, 2288–2295 (2021).
11. Z. Gao, Q. Wu, L. Liao, B. Su, X. Gao, S. Fu, Z. Li, Y. Wang, and Y. Qin, "Experimental demonstration of synchronous privacy enhanced chaotic temporal phase en/decryption for high speed secure optical communication," Opt. Express **30**, 31209–31219 (2022).
12. N. Jiang, A. Zhao, C. Xue, J. Tang, and K. Qiu, "Physical secure optical communication based on private chaotic spectral phase encryption/decryption," Opt. Lett. **44**, 1536–1539 (2019).
13. L. Wang, Y. Guo, D. Wang, Y. Wang, and A. Wang, "Experiment on 10-Gb/s message transmission using an all-optical chaotic secure communication system," Opt. Commun. **453**, 124350 (2019).
14. J. Ke, L. Yi, Z. Yang, Y. Yang, Q. Zhuge, Y. Chen, and W. Hu, "32 Gb/s chaotic optical communications by deep-learning-based chaos synchronization," Opt. Lett. **44**, 5776–5779 (2019).
15. N. Rulkov, M. Vorontsov, and L. Illing, "Chaotic free-space laser communication over a turbulent channel," Phys. Rev. Lett. **89**, 277905 (2002).
16. V. Annovazzi-Lodi, G. Aromataris, M. Benedetti, and S. Merlo, "Secure chaotic transmission on a free-space optics data link," IEEE J. Quantum Electron. **44**, 1089–1095 (2008).
17. M. Sepantaie, N. Namazi, and A. Sepantaie, "Spectral analysis and implementation of secure chaotic free-space optical communication systems," Opt. Eng. **57**, 106101 (2018).
18. O. Spitz, A. Herdt, J. Wu, G. Maisons, M. Carras, C. Wong, W. Elsäßer, and F. Grillot, "Private communication with quantum cascade laser photonic chaos," Nat. Commun. **12**, 3327 (2021).
19. W. Li, Y. Jiang, W. Fu, S. Wu, and M. Li, "Atmospheric intensity scintillation effect on BER performance of space downlink chaos laser communication system," Opt. Eng. **61**, 066102 (2022).
20. Y. Zhang, M. Xu, M. Pu, Q. Chen, M. Zhou, S. Chen, K. Qiu, N. Jiang, and X. Luo, "Experimental demonstration of an 8-Gbit/s free-space secure optical communication link using all-optical chaos modulation," Opt. Lett. **48**, 1470–1473 (2023).
21. Y. Fu, M. Cheng, X. Jiang, Q. Yu, L. Huang, L. Deng, and D. Liu, "High-speed optical secure communication with an external noise source and an internal time-delayed feedback loop," Photon. Res. **7**, 1306–1313 (2019).
22. T. Malica, G. Bouchez, D. Wolfersberger, and M. Sciamanna, "Spatiotemporal complexity of chaos in a phase-conjugate feedback laser system," Opt. Lett. **45**, 819–822 (2020).
23. D. Chang, Z. Zhong, J. Tang, P. Spencer, and Y. Hong, "Flat broadband chaos generation in a discrete-mode laser subject to optical feedback," Opt. Express **28**, 39076–39083 (2020).
24. N. Jiang, Y. Wang, A. Zhao, S. Liu, Y. Zhang, L. Chen, B. Li, and K. Qiu, "Simultaneous bandwidth-enhanced and time delay signature-suppressed chaos generation in semiconductor laser subject to feedback from parallel coupling ring resonators," Opt. Express **28**, 1999–2009 (2020).
25. M. Xu, F. Zhang, M. Pu, X. Li, X. Ma, Y. Guo, R. Zhang, M. Hong, and X. Luo, "Metasurface spatiotemporal dynamics and asymmetric photonic spin-orbit interactions mediated vector-polarization optical chaos," Phys. Rev. Res. **3**, 013215 (2021).
26. A. Zhao, N. Jiang, J. Peng, S. Liu, Y. Zhang, and K. Qiu, "Parallel generation of low-correlation wideband complex chaotic signals using CW laser and external-cavity laser with self-phase-modulated injection," Opto-Electron. Adv. **5**, 200026 (2022).
27. M. Chai, L. Qiao, X. Wei, S. Li, C. Zhang, Q. Wang, H. Xu, and M. Zhang, "Broadband chaos generation utilizing a wavelength-tunable monolithically integrated chaotic semiconductor laser subject to optical feedback," Opt. Express **30**, 44717–44725 (2022).
28. M. Xu, Q. He, M. Pu, F. Zhang, L. Li, D. Sang, Y. Guo, R. Zhang, X. Li, X. Ma, and X. Luo, "Emerging long-range order from freeform disordered metasurface," Adv. Mater. **34**, 2108709 (2022).
29. Y. Zeng, P. Zhou, Y. Huang, P. Mu, and N. Li, "Wideband and high-dimensional chaos generation using optically pumped spin-VCSELs," Opt. Express **31**, 948–963 (2023).
30. A. Yao and M. Padgett, "Orbital angular momentum: origins, behavior and applications," Adv. Opt. Photon. **3**, 161–204 (2011).
31. M. Padgett, "Orbital angular momentum 25 years on," Opt. Express **25**, 11265–11274 (2017).
32. A. Willner, K. Pang, H. Song, K. Zou, and H. Zhou, "Orbital angular momentum of light for communications," Appl. Phys. Rev. **8**, 041312 (2021).
33. J. Wang, J. Liu, S. Li, Y. Zhao, J. Du, and L. Zhu, "Orbital angular momentum and beyond in free-space optical communications," Nanophotonics **11**, 645–680 (2022).
34. S. Khonina, N. Kazanskiy, M. Butt, and S. Karpeev, "Optical multiplexing techniques and their marriage for on-chip and optical fiber communication: a review," Opto Electron. Adv. **5**, 210127 (2022).
35. J. Wang, J. Yang, I. Fazal, N. Ahmed, Y. Yan, H. Huang, Y. Ren, Y. Yue, S. Dolinar, M. Tur, and A. Willner, "Terabit free-space data transmission employing orbital angular momentum multiplexing," Nat. Photonics **6**, 488–496 (2012).
36. T. Lei, M. Zhang, Y. Li, P. Jia, G. Liu, X. Xu, Z. Li, C. Min, J. Lin, C. Yu, H. Niu, and X. Yuan, "Massive individual orbital angular momentum channels for multiplexing enabled by Dammann gratings," Light Sci. Appl. **4**, e257 (2015).
37. L. Zhu, M. Deng, B. Lu, X. Guo, and A. Wang, "Turbulence-resistant high-capacity free-space optical communications using OAM mode group multiplexing," Opt. Express **31**, 14454–14463 (2023).
38. M. Lavery, C. Peuntinger, K. Gunthner, P. Banzer, D. Elser, R. Boyd, M. Padgett, C. Marquardt, and G. Leuchs, "Free-space propagation of high-dimensional structured optical fields in an urban environment," Sci. Adv. **3**, e1700552 (2017).
39. J. Zhang, J. Liu, L. Shen, L. Zhang, J. Luo, J. Liu, and S. Yu, "Mode-division multiplexed transmission of wavelength-division multiplexing signals over a 100-km single-span orbital angular momentum fiber," Photon. Res. **8**, 1236–1242 (2020).
40. L. Zhu, A. Wang, S. Chen, J. Liu, Q. Mo, C. Du, and J. Wang, "Orbital angular momentum mode groups multiplexing transmission over 2.6-km conventional multi-mode fiber," Opt. Express **25**, 25637–25645 (2017).
41. H. Ren, X. Li, Q. Zhang, and M. Gu, "On-chip noninterference angular momentum multiplexing of broadband light," Science **352**, 805–809 (2016).
42. Y. Ren, G. Xie, H. Huang, N. Ahmed, Y. Yan, L. Li, C. Bao, M. Lavery, M. Tur, M. Neifeld, R. Boyd, J. Shapiro, and A. Willner, "Adaptive-optics-based simultaneous pre- and post-turbulence compensation of multiple orbital-angular-momentum beams in a bidirectional free-space optical link," Optica **1**, 376–382 (2014).
43. Y. Guo, L. Zhong, L. Min, J. Wang, Y. Wu, K. Chen, K. Wei, and C. Rao, "Adaptive optics based on machine learning: a review," Opto-Electron. Adv. **5**, 200082 (2022).
44. L. Li, R. Zhang, P. Liao, Y. Cao, H. Song, Y. Zhao, J. Du, Z. Zhao, C. Liu, K. Pang, H. Song, A. Almaiman, D. Starodubov, B. Lynn, R. Bock, M. Tur, A. Molisch, and A. Willner, "Mitigation for turbulence effects in a 40 Gbit/s orbital-angular-momentum-multiplexed free-space optical link between a ground station and a retro-reflecting UAV using MIMO equalization," Opt. Lett. **44**, 5181–5184 (2019).
45. X. Luo, M. Pu, F. Zhang, M. Xu, Y. Guo, X. Li, and X. Ma, "Vector optical field manipulation via structural functional materials: tutorial," J. Appl. Phys. **131**, 181101 (2022).
46. X. Wang, T. Wu, C. Dong, H. Zhu, Z. Zhu, and S. Zhao, "Integrating deep learning to achieve phase compensation for free-space orbital-angular-momentum-encoded quantum key distribution under atmospheric turbulence," Photon. Res. **9**, B9–B17 (2021).
47. X. Luo, "Multiscale optical field manipulation via planar digital optics," ACS Photon. **10**, 2116–2127 (2023).