nature communications

Article

https://doi.org/10.1038/s41467-025-65111-5

Ultrahigh-speed optical encryption enabled by spatiotemporal noise chaffing

Received: 11 April 2025

Accepted: 8 October 2025

Published online: 19 November 2025

Check for updates

Jianyang Shi[1,2,3,4,8], Chaoxu Chen[1,2,3,4,8], Haoyu Zhang[1,2,3], Penghao Luo[1], Yuan Wei[1,2,3], Fang Dong[1,4], Ziwei Li[1,2,3,5], Chao Shen[1,2,3,5], Haiwen Cai[4], Junwen Zhang[1,2,3,5] ✉, Xinyuan Fang[6,7] ✉, Nan Chi[1,2,3] ✉ & Min Gu[6,7] ✉

Optical encryption provides strong physical-layer security but is limited by the slow response of spatial light modulators. We propose and experimentally demonstrate a spatiotemporal noise chaffing system inspired by the "chaffing and winnowing" principle for ultrahigh-speed temporal encryption. By exploiting the symmetric spatial properties and orthogonality of conjugated orbital angular momentum (OAM) states, high-speed temporal signals ("wheat") and spatial noise ("chaff") are simultaneously encoded. This mechanism suppresses information leakage by degrading the temporal signal-to-noise ratio while enabling authorized recovery. Furthermore, a variable-weight multimodal OAM (VW-multimodal OAM) scheme combined with a multimodal generation neural network (MGNN) exponentially expands the key space beyond 10^{10}. Experimentally, a record secure transmission rate of 1.25 Tbps per mode is achieved in an eight-channel wavelength-division-multiplexed coherent link. The product of rate and key space surpasses existing methods by five orders of magnitude, establishing a new photonic-security paradigm for future ultrafast and secure communication networks.

Optical encryption provides a robust mechanism for securing information by leveraging the intrinsic physical properties of light[1], such as interference[2], diffraction[3], and polarization[4]. This approach has been widely applied across diverse fields, including sensitive information protection[5], biometric authentication[6], satellite-based quantum communications[7], and anti-counterfeiting labeling[8]. Compared to conventional electronic encryption techniques—such as digital cryptography[9]—optical encryption offers substantial advantages[1,10,11], notably parallel encoding capability, high-speed processing, and immunity to electromagnetic interference, thus providing a highly reliable physical-layer solution for information security.

However, most current optical encryption methods primarily rely on spatial information encoding through modulation and detection devices, including spatial light modulators (SLMs)[12], digital micromirror devices (DMDs)[13], and charge-coupled device (CCD) cameras. These spatial modulation devices inherently suffer from limited switching speeds and low refresh rates, resulting in relatively low information-flow density and restricted transmission rates. Such limitations significantly hinder the adoption of traditional optical encryption methods in high-speed information transmission scenarios.

To achieve ultrahigh-speed information transmission, recent advances in temporal signal transmission—such as coherent detection[14,15], multi-dimensional multiplexing[16,17], and high-order modulation formats[18]—have been widely explored in communication systems. These techniques provide opportunities to dramatically

[1]College of Future Information Technology, Fudan University, Shanghai, China. [2]Shanghai Engineering Research Center of Low-Earth-Orbit Satellite Communication and Applications, Shanghai, China. [3]Shanghai Collaborative Innovation Center of Low-Earth-Orbit Satellite Communication Technology, Shanghai, China. [4]Zhang Jiang Laboratory, Shanghai, China. [5]Peng Cheng Laboratory, Shenzhen, China. [6]School of Artificial Intelligence Science and Technology, University of Shanghai for Science and Technology, Shanghai, China. [7]Institute of Photonic Chips, University of Shanghai for Science and Technology, Shanghai, China. [8]These authors contributed equally: Jianyang Shi, Chaoxu Chen. ✉e-mail: junwenzhang@fudan.edu.cn; xinyuan.fang@usst.edu.cn; nanchi@fudan.edu.cn; gumin@usst.edu.cn

increase the information density of optical encryption, e.g., by extending it from purely spatial to integrated spatiotemporal domains. Nevertheless, directly encrypting temporal signals remains fundamentally challenging because conventional spatial optical encryption schemes fail to adequately prevent unauthorized temporal signal interception. As illustrated in a classic orbital angular momentum (OAM) encryption scheme (Fig. 1a), while spatial encoding stores and encrypts information using spatial modulation patterns, high temporal signal-to-noise (SNR) modulated signals can be directly retrieved by analyzing their light intensity versus time at high spatial SNR locations. Therefore, the core challenge in achieving high-speed optical encryption is to develop an encryption scheme capable of preventing unauthorized interception by eavesdroppers (Eve) in free-space temporal signal transmission, while still allowing legitimate receivers (Bob) to decrypt the transmitted signal without interference.

Inspired by the concept of "chaffing and winnowing"[19] in communication security—where genuine data ("wheat") is obscured by introducing indistinguishable noise ("chaff"), allowing only authorized recipients to extract the true information—we propose and experimentally demonstrate a novel spatiotemporal noise chaffing system, capable of ultrahigh-speed optical encryption at transmission rates exceeding the terabit-per-second (Tbps) scale. Specifically, as shown in Fig. 1b, our approach leverage the symmetric spatial characteristics of conjugate orbital angular momentum (OAM) modes[20] by encoding the temporal information signal and noise separately onto two conjugated OAM states and transmitting them co-axially through free space. Due to their perfect spatial coherence, the signal and noise become indistinguishable to unauthorized interceptors—yielding high spatial SNR but severely degraded temporal SNR for Eve, since temporal signal recovery requires integrating spatial fields at each instant; the conjugate-superposed spatial noise substantially degrades the integrated temporal SNR. Conversely, Bob can recover the signal through mode winnowing at the designated spatial location by applying an inverse OAM mode key, capitalizing on the orthogonality of OAM states. Crucially, we further to enhance encryption security through the introduction of a variable-weight multimodal OAM (VW-multimodal OAM) scheme (Fig. 1c) combined with a multimodal generation neural network (MGNN), substantially expanding the encryption key space. In this scheme, accurate signal recovery by the legitimate receiver requires simultaneous matching of both modal composition and weighting coefficients, effectively mitigating the risk of brute-force attacks.

Through high-speed temporal information transmission experiments, we validate the efficacy and robustness of our proposed method, achieving an unprecedented single-mode data transmission rate of 1.25 Tbps in an 8-channel wavelength-division multiplexing (WDM) coherent system with an encryption key space exceeding 10^{10} supported by a high-accuracy MGNN that produces holograms with a mean square error as low as 10^{-9}. This record-breaking performance, quantified by the product of transmission rate and key space, surpasses current state-of-the-art optical encryption methods by five orders of magnitude, establishing a new benchmark for ultrafast photonic security technologies (Fig. 1d; see Supplementary Note 1 for comparative details). The proposed technique provides transformative potential for future applications in next-generation high-security optical communications networks, including 6 G and low Earth orbit satellite systems.

Results

Principle of spatiotemporal noise chaffing with CVW-multimodal OAM encryption system

To enable optical encryption for high-speed temporal signals, we introduce a conjugated variable-weight multimodal OAM (CVW-multimodal OAM) encryption system. For illustration and visualization, we propose a vector circle based on the system's space bandwidth product (SBP)[21], where the positions of the vectors are determined by the spatial radii of the different OAM states (see Supplementary Notes 2 and 3). As illustrated in Fig. 2a, a conventional optical encryption system encodes the temporal signal $S(t)$ onto an OAM mode $U_l(r,\varphi,z)$, generating the transmitted electric field $E(r,\varphi,z,t)$:

$$E(r,\varphi,z,t) = U_l(r,\varphi,z)S(t). \tag{1}$$

In this conventional scheme, although the legitimate receiver (Bob) can successfully decrypt the transmitted signal using the inverse OAM mode, an eavesdropper (Eve) without the decryption key can still intercept sufficient temporal information—manifested as high-amplitude signals and clear constellation diagrams—by analyzing the ring-like regions with high spatial SNR. In contrast, if a conjugated OAM state $U_{-l}(r,\varphi,z)$ carrying noise $N(t)$ is chaffed co-axially (Fig. 2b), the electric field becomes symmetrically distributed in the vector space, yielding perfect spatial coherence:

$$E(r,\varphi,z,t) = S(t)U_l(r,\varphi,z) + N(t)U_{-l}(r,\varphi,z). \tag{2}$$

In this configuration, the combined intensity exhibits a petal-like pattern due to interference. Consequently, random detection by Eve in high-spatial-SNR regions results in a chaffed signal with degraded temporal SNR and a scattered constellation diagram (see Supplementary Note 6). The detected photocurrent for Eve is given by:

$$\begin{aligned} I_{Eve} &\propto \iint \left|S\cdot U_l + N\cdot U_{-l}\right|^2 r dr d\varphi \\ &= \left(S^2+N^2\right)\iint |U_l|^2 r dr d\varphi + 2Re\left(SN^*\right)\iint \left|U_l^2\right| r dr d\varphi. \end{aligned} \tag{3}$$

Consequently, the chaffed conjugated modes cause Eve's received temporal signal to be heavily degraded, with a diffused constellation diagram that effectively prevents unauthorized information recovery. Conversely, the legitimate receiver (Bob), who possesses the correct decryption key, can winnow the signal precisely at the center of the spatial field. The photocurrent for Bob is:

$$\begin{aligned} I_{Bob} &\propto \iint \left|S\cdot U_0 + N\cdot U_{-2l}\right|^2 r dr d\varphi \\ &= |S|^2 \iint |U_0|^2 r dr d\varphi + \left[|N|^2 + 2Re\left(SN^*\right)\right]\iint |U_{-2l}|^2 r dr d\varphi. \end{aligned} \tag{4}$$

Here, the temporal signal $S(t)$ is concentrated in the fundamental Gaussian mode U_0 at the spatial field center, enabling Bob to reconstruct the pure temporal information, while the noise and mixed components disperse into higher-order modes.

However, encryption based on a monomodal OAM state is inherently vulnerable due to its discrete vector space, making it susceptible to brute-force attacks. Moreover, the petal-like interference intensity pattern of monomodal OAM is strongly correlated with its topological charge, potentially leaking information and posing additional security risks (see Supplementary Note 3). To overcome these limitations, we extend the concept to encode $S(t)$ and $N(t)$ onto pairs of conjugated variable-weight multimodal OAM (CVW-multimodal OAM) states rather than monomodal states (Fig. 2c, d). Although the basic encryption and decryption mechanisms remain similar, this approach significantly increases security by expanding the key space. Accurate decryption now requires simultaneous matching of both modal composition and weight coefficients—a requirement that greatly reduces the probability of successful brute-force attacks. Detailed expanded analysis and derivations are provided in Supplementary Note 5. Any incorrect key results in spatial mismatches, dispersing energy away from the central mode and producing a chaotic constellation. This inherent complexity in the key space thus

https://doi.org/10.1038/s41467-025-65111-5

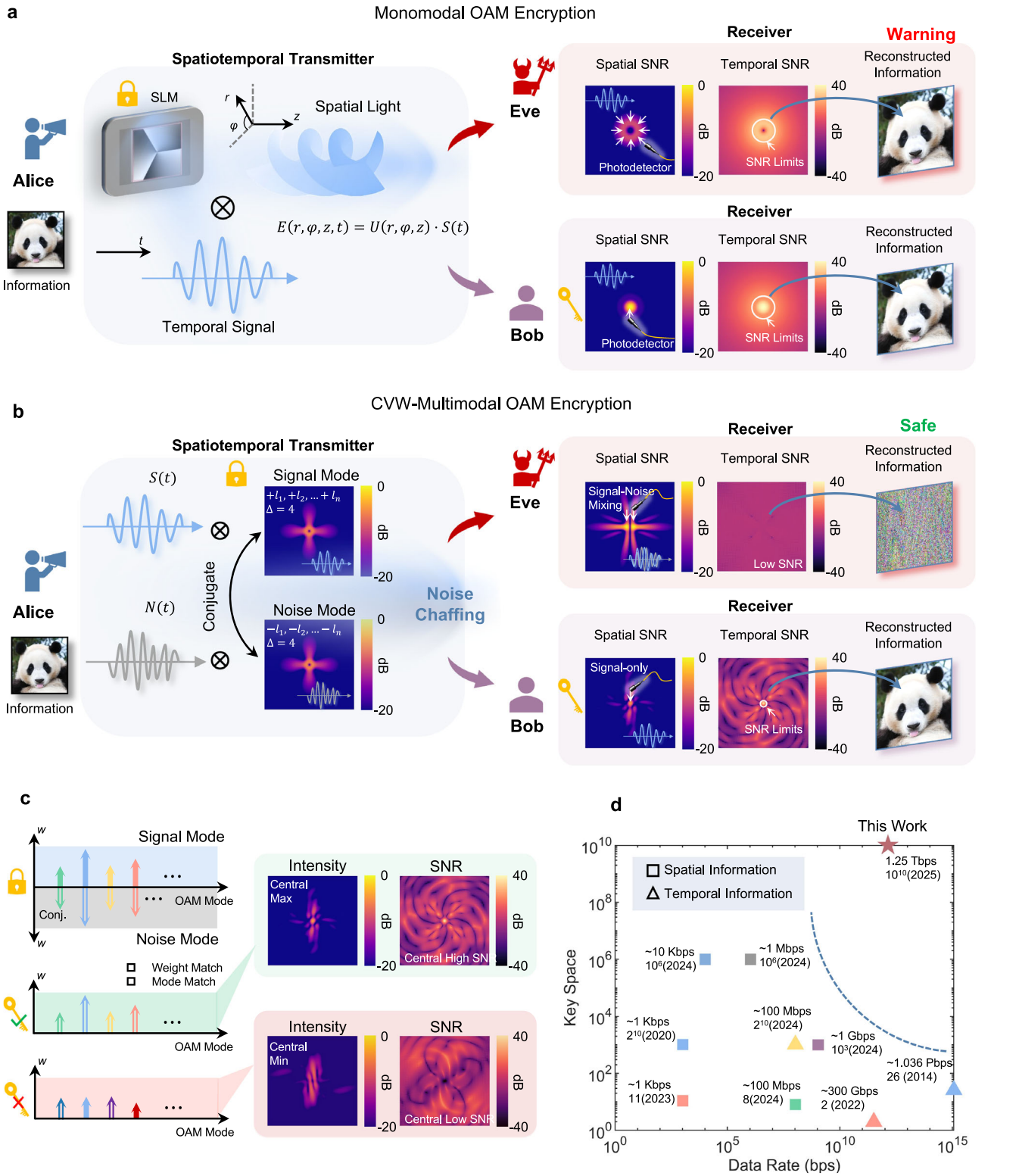

Fig. 1 | Schematic diagram of concept and performance of the spatiotemporal noise chaffing scheme. a Monomodal OAM encryption for temporal information transmission: the temporal signal leaks from the circularly distributed intensity pattern, allowing both the eavesdropper (Eve) and the legitimate receiver (Bob) to retrieve the signal. **b** CVW-multimodal OAM encryption for temporal information transmission: the noise-chaffed signal generated by conjugated mode combinations prevents direct signal detection, while Bob can winnow the information using the correct key. **c** CVW-multimodal OAM encryption requires precise weight and mode matching for decryption, enhancing security and expanding the key space. **d** Conventional high-speed optical information transmission faces a trade-off between transmission rate and physical-layer security, whereas the proposed method achieves a balance, reaching a 1.25 Tbps data rate with a 1010-dimensional key space for encryption.

https://doi.org/10.1038/s41467-025-65111-5

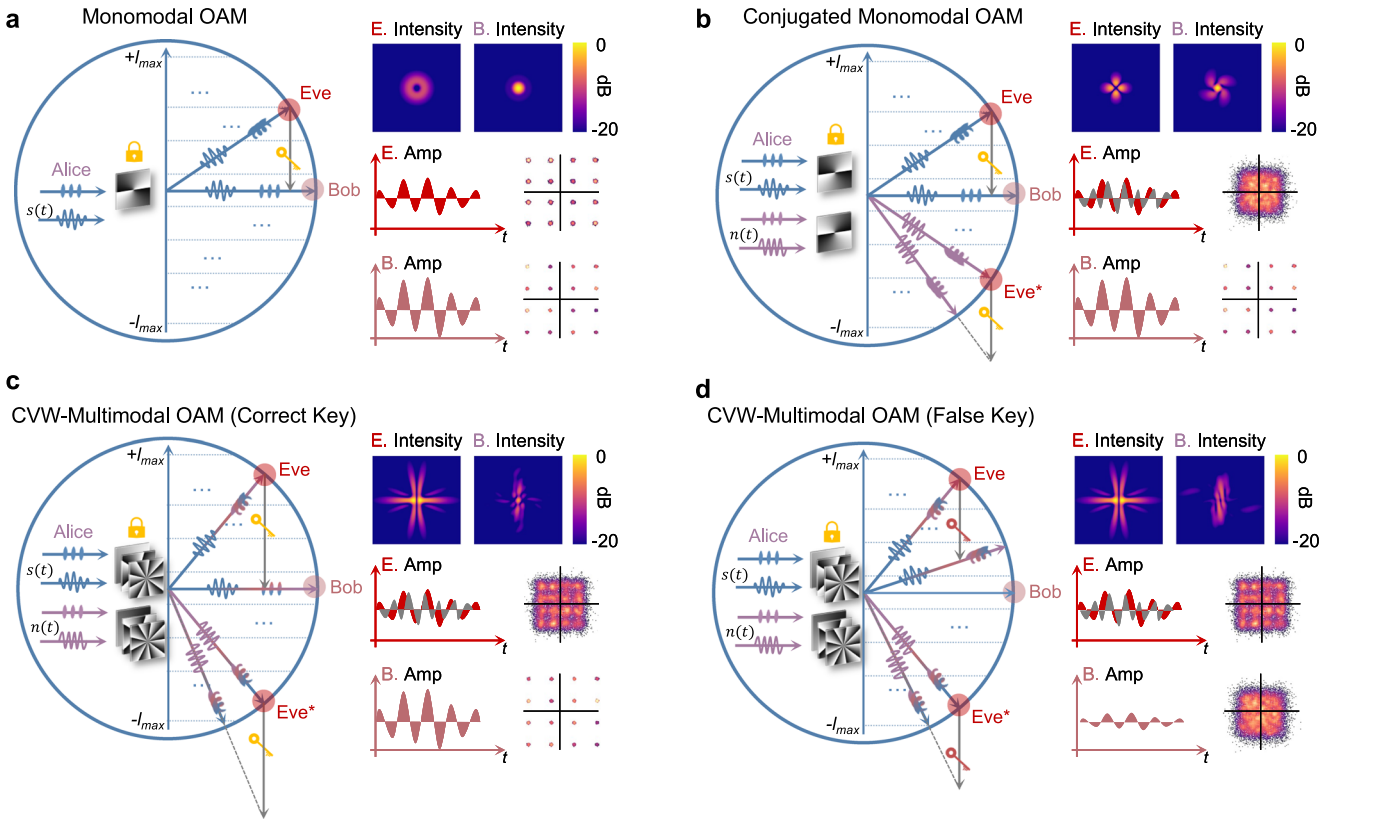

Fig. 2 | Mechanism of noise chaffing CVW-multimodal OAM encryption system. a Encryption and decryption in vector space using monomodal OAM. **b** Encryption and decryption using conjugated monomodal OAM. **c** CVW-multimodal OAM with correct decryption. **d** CVW-multimodal OAM with false decryption.

substantially reduces the risk of brute-force attacks and interception, effectively safeguarding the transmitted temporal data.

Ultra-large OAM key space designed by artificial neural network

The key space of the proposed VW-multimodal OAM system is determined by three parameters: the maximum supported OAM order L, the number of OAM states selected for encryption M, and the weight partition precision δ. The constructed key space K is given by (detailed analyses are provided in Supplementary Note 8):

$$K = 2 \cdot \binom{L}{M} \cdot \binom{\frac{1}{\delta} + M - 1}{M - 1}. \tag{5}$$

Figure 3a illustrates the entire process of key space generation. The resultant VW-multimodal OAM field is expressed as:

$$U(r, \varphi, z) = \sum_{m}^{M} c_m A_m(r, \varphi, z) \exp(i l_m \varphi) \tag{6}$$

where c_m are the weight coefficients assigned to each of the M selected OAM modes, and $A_m(r, \varphi, z)$ denotes the amplitude distribution, which may include both radial and longitudinal field variations. This construction demonstrates an exponentially increasing key space with increasing L and finer δ values. Notably, the parameter M exhibits a non-monotonic behavior—there exists an optimal M that maximizes K, beyond which K decreases as M approaches L.

While Eq. (5) predicts the theoretical key space, practical security evaluation requires assessment of the isolation of mode-weight combinations. Isolation is quantified via the mean crosstalk value (CV), calculated over 1000 randomly generated combinations under various (L, M, δ) configurations. As shown in Fig. 3c, the trends of CV and SNR values for incorrect keys (see calculation methods in Supplementary Note 10) indicate that increasing the number of OAM states and pursuing more precise weight partitioning tend to elevate both CV and SNR. This, in turn, may compromise encryption integrity by reducing the distinguishability between correct and incorrect keys. Based on our analysis of the average CV and SNR values for both correct and incorrect keys, as well as the statistical distribution of tested samples (see Supplementary Fig. 12), we selected the parameters $\delta = 0.1$, $M = 10$, and $L = 20$ in this work. These values represent a carefully optimized trade-off between communication performance and security robustness.

To overcome the limitations of conventional approaches—where multiple power-tunable laser sources coupled with SLMs are required for VW-multimodal OAM generation, and direct superposition introduces significant interference errors (Supplementary Note 9)—we propose a compact single-hologram solution leveraging a Multimodal Generation Neural Network (MGNN), as illustrated in Fig. 3d. The MGNN intelligently optimizes the weight coefficients for the selected OAM modes from the system's supported range (spanning $\pm L$ orders). It compensates for inherent mode interference and intensity non-uniformity through high-dimensional parameter fitting. The output hologram can support VW-multimodal OAM launch with a single beam, eliminating the need for multiple power-tunable sources. Simulation and experimental intensity profiles are provided in Fig. 3e. Compared with conventional pattern search methods[22] (given in Supplementary Note 12) for hologram generation, the MGNN significantly reduces the mean square error (MSE)—dropping by four orders of magnitude from 3.25×10^{-5} to 1.76×10^{-9} as shown in Fig. 3f. This dramatic reduction in error results in higher isolation between closely spaced mode-weight combinations, thereby supporting the large key space of the CVW-multimodal OAM encryption system (see Supplementary Fig. 13). The experimentally obtained mode spectra are illustrated in Supplementary Fig. 16 to validate the performance of both PS and MGNN approaches.

https://doi.org/10.1038/s41467-025-65111-5

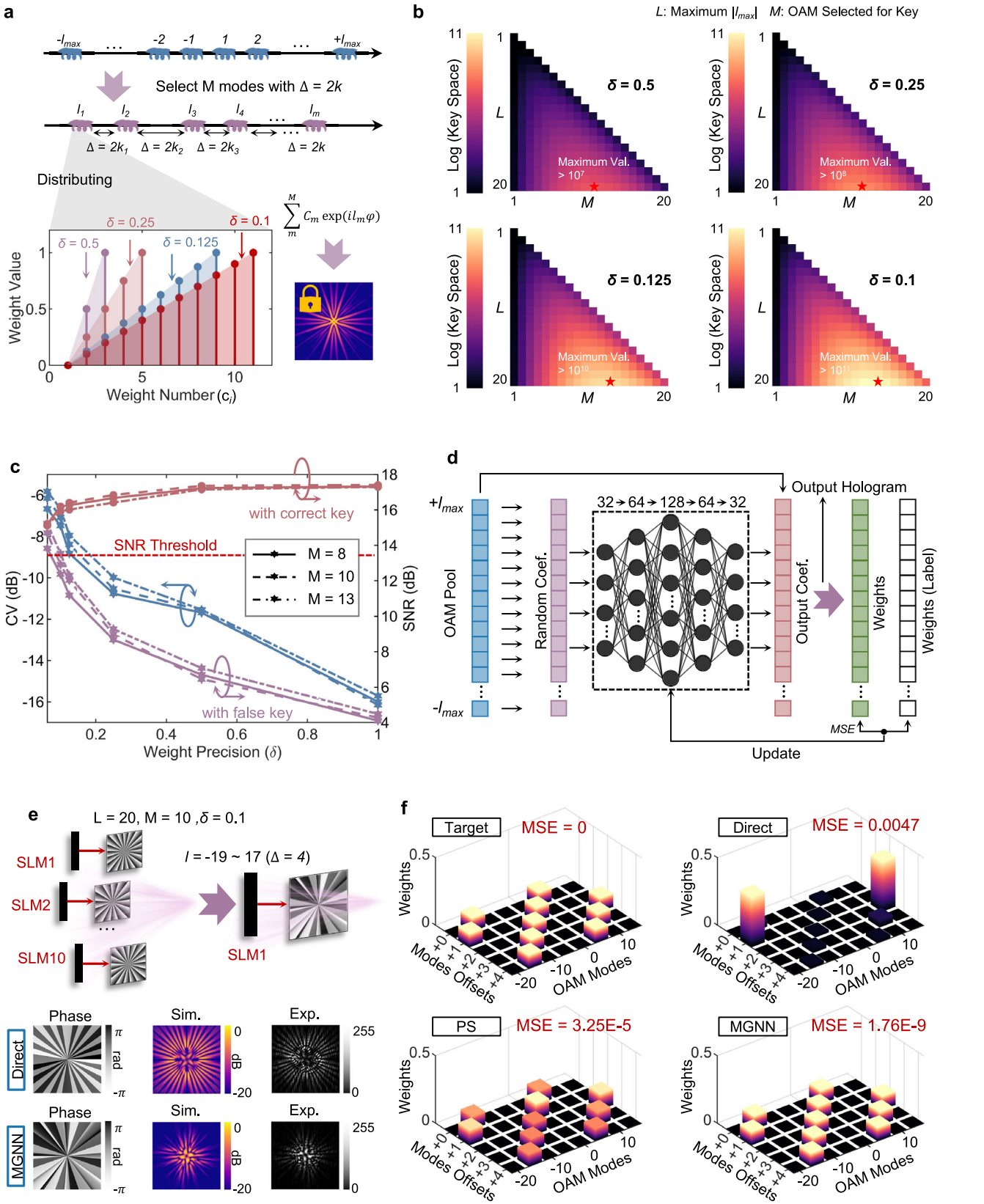

Fig. 3 | Exponentially expanded key space and design of high-precision holograms. a Parameters defining the key space of CVW-multimodal OAM: the largest order of OAM modes supported by system (L), the number of modes selected for CVW-multimodal OAM (M), and the weight precision (δ). **b** Key space size for different weight precisions ($\delta = 0.5, \delta = 0.25, \delta = 0.125$, and $\delta = 0.1$, respectively). **c** Mean crosstalk value and SNR from 1000 random samplings, showing the effect of increasing δ for different M with a fixed $L = 20$. **d** Schematic of a multimodal OAM generation neural network for single hologram broadcasting of CVW-multimodal OAM. **e** Concept of single hologram generation for CVW-multimodal OAM and comparison of simulation and experimental results for direct mode overlap and MGNN. **f** Error comparison between different methods (direct overlapping, pattern search optimization, and MGNN) for CVW-multimodal OAM hologram generation.

https://doi.org/10.1038/s41467-025-65111-5

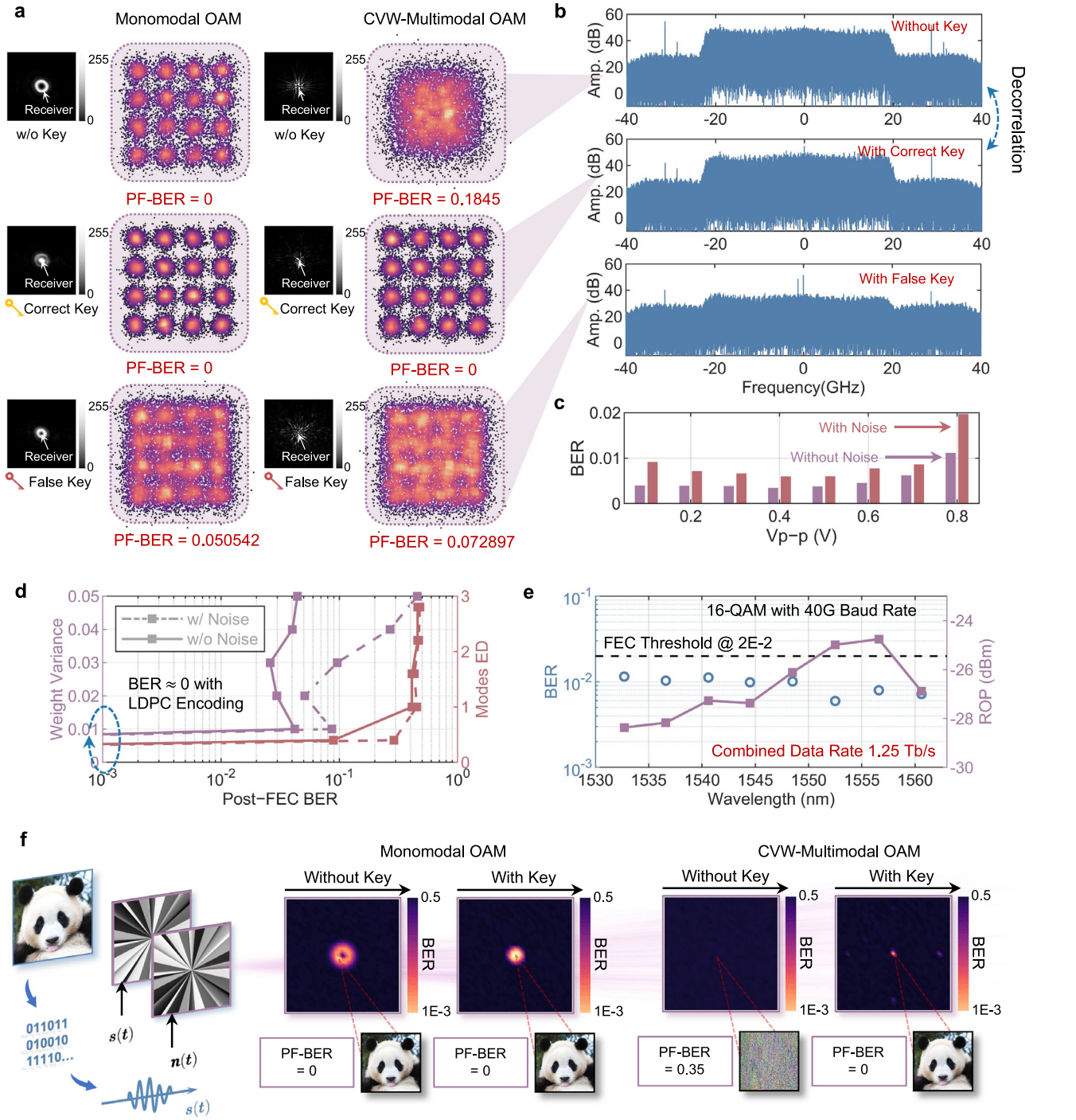

Fig. 4 | Terabit-scale optical encryption for ultrahigh-speed information transmission. a Comparison of constellations for Monomodal OAM and CVW-multimodal OAM encryption under three different scenarios: without key, with correct key, and with false key. **b** Spectrum comparison for three different scenarios in CVW-multimodal OAM, demonstrating the decorrelation of pure and mixed signals. **c** Bar chart of Bit Error Rate (BER) under different signal waveform peak-to-peak voltages for VW-multimodal OAM and CVW-multimodal OAM, illustrating the minimal impact of noise-path introduction. **d** Experiment showing the isolation between different CVW-multimodal OAM combinations using PF-BER, revealing that increased weight variance and enlarged mode ED result in higher BER and false information reconstruction. **e** 8-wavelength multiplexing experiment, presenting ROP and BER for 40 GBaud 16-QAM signals, achieving a combined data rate of 1.25 Tb/s. **f** BER spatial distribution for Monomodal OAM and CVW-multimodal OAM, demonstrating that Monomodal OAM can successfully reconstruct information without decryption, whereas CVW-multimodal OAM effectively hides the information.

Terabit-scale optical encryption for ultrahigh-speed information transmission

Based on the CVW-multimodal OAM encryption system, our approach enables ultrahigh-speed secure information transmission. The experimental validation was performed on an 8-wavelength multiplexed coherent system using a 40 Gbaud 16-QAM temporal signal (See Method Section and Supplementary Note 13). As shown in Fig. 4a, the post-FEC bit error rate (BER) was measured under three conditions —without a decryption key, with the correct key, and with a false key— using both monomodal OAM and CVW-multimodal OAM encryption systems. Under the monomodal OAM encryption scheme, temporal information is significantly leaked, as evidenced by Eve's ability to

intercept the signal through the ring-like spatial intensity distribution. In contrast, the CVW-multimodal OAM system mitigates this vulnerability by superimposing signal and noise, thereby degrading the temporal signal for unauthorized receivers. Eve's detection yields a chaotic constellation with high BER, while Bob, using the correct decryption key, reconstructs the pure temporal information. Figure 4b displays the spectral analysis for three scenarios within the CVW-multimodal OAM encryption system. The similar spectral amplitudes in the cases "with key" and "without key" indicate that the differences in BER are primarily due to the mixing of signal and noise, confirming the effective decorrelation of temporal information (as further explained in Supplementary Note 7). Moreover, Fig. 4c compares the BER for CVW-multimodal OAM encryption and VW-multimodal OAM encryption with and without noise addition. Although the introduction of noise slightly degrades signal quality, the BER remains below the 20% HD-FEC threshold (2×10^{-2}), indicating minimal adverse impact on overall information transmission. Isolation validation experiments further demonstrate that the PF-BER increases by over two orders of magnitude with increasing weight variance and mode Euclidean distance (ED), thereby confirming the robustness and high security of the encryption system (more experimental results are given in Supplementary Fig. 14). By multiplexing all 8 wavelength channels in the C-band (Supplementary Fig. 15), as illustrated in Fig. 4e, the BER for each channel remains below the HD-FEC threshold, achieving a combined data rate of 1.25 Tb/s. The BER distribution visualized in Fig. 4f clearly shows the significant performance difference between the monomodal and CVW-multimodal encryption systems, supporting the efficacy of our approach in securing high-speed optical transmission.

Discussion

In this study, we propose and experimentally demonstrate a novel spatiotemporal optical encryption method inspired by the "chaffing and winnowing" paradigm, achieving a record-breaking secure optical transmission rate of 1.25 Tbps with an unprecedented encryption key space exceeding 10^{10}. This breakthrough effectively overcomes the longstanding limitations of low information density inherent in conventional optical encryption methods by seamlessly integrating temporal encoding and spatial encryption. Central to our approach is the exploitation of the symmetric characteristics of conjugated OAM states, which provides a robust physical mechanism for achieving perfect spatial coherence between the temporal signal and noise to support adding effective chaff. Concurrently, the orthogonality of conjugated OAM states facilitates the spatial separation necessary for precise signal winnowing, enabling reliable information reconstruction by the legitimate receiver. In essence, our method embodies the chaffing and winnowing concept in optical encryption. Moreover, we introduce the concept of VW-multimodal OAM to further enhance system security against brute-force attacks. The accompanying MGNN significantly improves the isolation of mode-weight combinations, thereby supporting an expanded key space. Importantly, because our encryption method operates at the physical layer, it is complementary to electronic encryption techniques, such as digital cryptography. The integration of both approaches can create multilayered protection schemes that further strengthen overall information security.

While the encryption key space is fundamentally determined by the system's SBP, which is closely related to the NA, the use of high-resolution SLM can significantly enhance performance. However, diffraction during free-space transmission imposes limitations on the SBP and thus constrains the overall encryption capacity and communication efficiency (see Supplementary Note 14). Incorporating 4-f relay systems or optical imaging components to mitigate diffraction effects can help maintain spatial coherence and improve system scalability.

Notably, even higher-order modulation formats and advanced multiplexing techniques, e.g., OAM multiplexing, remain available for future implementation, suggesting substantial room for further improvement in transmission speed and capacity. Looking forward, the proposed encryption technique holds significant potential for further miniaturization and integration through advanced photonic platforms, such as metasurfaces[23–25] and on-chip optical systems[26,27]. Such advancements could greatly enhance practical applications, paving the way for revolutionary breakthroughs in secure, ultrahigh-speed optical networks. Ultimately, this method presents a compelling paradigm shift in photonic information security, poised to ensure robust data protection and scalable network solutions in the era of 6G[28] and beyond.

Methods

Experimental setup

We experimentally demonstrated the CVW-multimodal OAM encryption within an 8-wavelength coherent system, as illustrated in Supplementary Fig. 11. The experimental setup consists of two main components: temporal signal transmission and reception, and spatial light modulation.

Temporal signal transmission and reception. For the temporal signal processing, we employed tunable multi-wavelength external cavity lasers (ECLs) (Keysight N7714A) to generate eight-channel laser sources. One laser was set to 1.552 μm, while the remaining wavelengths ranged from 1.561 μm to 1.533 μm, which were combined using a multi-channel optical coupler. The 1.552 μm laser carried a 40 Gbaud 16-QAM temporal signal, while the other wavelengths were separately modulated with the same format to validate wavelength-division multiplexing (WDM) performance. The temporal signals were generated and launched via an arbitrary waveform generator (AWG) (Keysight M8194A, 120 GSa/s). These signals were output through two individual AWG channels for single-polarization in-phase and quadrature (IQ) modulation and coupled with the lasers using Mach-Zehnder modulators (MZMs) (Sumicem T.MXH 1.5–20PD-ADC-LV). Both signal paths were amplified by erbium-doped fiber amplifiers (EDFAs) (Amonics AEDFA–23-B-FA) and combined using a wavelength-selective switch (WSS) (Finisar Waveshaper 4000S). The signals were further amplified by another EDFA (OVLINK EYDFA-C-HP-BA-30-PM-B) before being split into two paths: (1) Signal Path: Directly transmitted into the CVW-multimodal OAM encryption system for spatial optical encryption; (2) Noise Path: Routed through a 1-m delay line to decorrelate from the signal before entering the encryption system, which has been validated in Supplementary Note 7. After passing through the spatial modulation system, the received light was amplified by an EDFA (OVLINK EDFA-C-BA-GF-26-PM-B), and the individual wavelengths were filtered using optical bandpass filters (OBPFs) (EXFO XTM-50-SCL-U). A variable optical attenuator (VOA) (OVLINK SVOA–1000) was used for power control. A variable local oscillator (LO) was employed to maintain zero-difference detection across different wavelengths, and an integrated coherent receiver (ICR) performed electrical-to-optical (E/O) conversion. The resulting electrical signal was sampled by an oscilloscope (OSC) (Keysight UXR0134A, 256 GSa/s) for subsequent digital signal processing (DSP). For both Tx and Rx, DSP has been written in Supplementary Note 13.

Spatial light modulation. In the spatial modulation stage, the temporal signal and noise entered the system through two separate collimators from different ports. Each path passed through a polarizer to align polarization before reaching spatial light modulators (SLM1 and SLM2) (UPOlabs HDSLM80R), which were preloaded with a conjugated CVW-multimodal OAM phase pair. The optical path lengths were precisely matched to ensure signal-noise overlap. The modulation process was performed as follows: (1) Beam Splitters (BS1 and BS2) (50:50) directed the signal and noise beams toward SLM1 and SLM2, respectively; (2) The modulated beams were then combined at BS3, generating the CVW-multimodal OAM state, carrying the signal-noise

mixed temporal information; (3) The combined optical field was experienced 0.4 m free space transmission and then directed to SLM3 (UPOlabs HDSLM80T) for decryption and passed through a lens (f = 150 mm) to perform Fraunhofer far-field transformation. (4) Finally, Beam Splitter BS4 (90:10) separated the optical wave into two paths:

- Path 1: Coupled into a single-mode fiber (SMF) for further temporal signal processing.
- Path 2: Captured by a CCD camera to record the spatial field distribution.

The coupled signal from Path 1 was then forwarded for the second stage of temporal processing, completing the full encryption-decryption cycle.

OAM spectrum calculation

For an arbitrary complex amplitude field $U(r,\varphi,z)$, it can be decomposed into a set of orthogonal OAM basis functions. Given a total of M OAM modes (defined by SBP of system, see Supplementary Note 2), the expansion coefficient $a_m(r,\varphi,z)$ corresponding to the m-th OAM mode is given by:

$$a_m(r,\varphi,z) = \frac{1}{\sqrt{2\pi}} \int_0^{2\pi} U(r,\varphi,z) \exp(-il_m\varphi) d\varphi \tag{7}$$

Here, $a_m(r,\varphi,z)$ represents the coefficient of the m-th OAM mode, obtained by projecting the electric field $U(r,\varphi,z)$ onto the corresponding OAM basis. The energy of the m-th order harmonic factor can then be calculated as:

$$I_m = \int_0^{\infty} |a_m(r,\varphi,z)|^2 r dr \tag{8}$$

The normalized energy spectrum function can be obtained as:

$$p_m = \frac{p_m}{\sum_m^M I_m} \tag{9}$$

In this expression, p_m represents the fractional energy contribution of the m-th OAM mode relative to the total energy distributed over the considered set of modes $[l_1, l_2, \ldots, l_m], m \in M$.

Data availability

The main source data generated in this study have been deposited in the Figshare database under accession code https://doi.org/10.6084/m9.figshare.30291835.

References

1. Liu, S., Guo, C. & Sheridan, J. T. A review of optical image encryption techniques. *Opt. Laser Technol.* **57**, 327–342 (2014).
2. Zhang, Y. & Wang, B. Optical image encryption based on interference. *Opt. Lett.* **33**, 2443–2445 (2008).
3. Chen, W., Chen, X. & Sheppard, C. J. Optical image encryption based on diffractive imaging. *Opt. Lett.* **35**, 3817–3819 (2010).
4. Li, X., Lan, T.-H., Tien, C.-H. & Gu, M. Three-dimensional orientation-unlimited polarization encryption by a single optically configured vectorial beam. *Nat. Commun.* **3**, 998 (2012).
5. Matoba, O., Nomura, T., Perez-Cabre, E., Millan, M. S. & Javidi, B. Optical techniques for information security. *Proc. IEEE* **97**, 1128–1148 (2009).
6. Yan, A., Wei, Y. & Zhang, J. Security enhancement of optical encryption based on biometric array keys. *Opt. Commun.* **419**, 134–140 (2018).
7. Fisher, K. A. et al. Quantum computing on encrypted data. *Nat. Commun.* **5**, 3074 (2014).
8. Zhang, F. et al. Multimodal, convertible, and chiral optical films for anti-counterfeiting labels. *Adv. Funct. Mater.* **32**, 2204487 (2022).
9. Marton, K., Suciu, A. & Ignat, I. Randomness in digital cryptography: a survey. *Rom. J. Inf. Sci. Technol.* **13**, 219–240 (2010).
10. Qu, G. et al. Reprogrammable meta-hologram for optical encryption. *Nat. Commun.* **11**, 5484 (2020).
11. Alfalou, A. & Brosseau, C. Optical image compression and encryption methods. *Adv. Opt. Photonics* **1**, 589–636 (2009).
12. Fang, X., Ren, H. & Gu, M. Orbital angular momentum holography for high-security encryption. *Nat. Photonics* **14**, 102–108 (2020).
13. Shi, Z. et al. Super-resolution orbital angular momentum holography. *Nat. Commun.* **14**, 1869 (2023).
14. Geng, Y. et al. Coherent optical communications using coherence-cloned Kerr soliton microcombs. *Nat. Commun.* **13**, 1070 (2022).
15. Zhang, R. et al. Turbulence-resilient pilot-assisted self-coherent free-space optical communications using automatic optoelectronic mixing of many modes. *Nat. Photonics* **15**, 743–750 (2021).
16. Zou, K. et al. High-capacity free-space optical communications using wavelength-and mode-division-multiplexing in the mid-infrared region. *Nat. Commun.* **13**, 7662 (2022).
17. Yan, Y. et al. High-capacity millimetre-wave communications with orbital angular momentum multiplexing. *Nat. Commun.* **5**, 4876 (2014).
18. Zhang, C. et al. Clone-comb-enabled high-capacity digital-analogue fronthaul with high-order modulation formats. *Nat. Photonics* **17**, 1000–1008 (2023).
19. Rivest, R. L. et al. Chaffing and winnowing: confidentiality without encryption. *CryptoBytes* **4**, 12–17 (1998).
20. Shen, Y. et al. Optical vortices 30 years on: OAM manipulation from topological charge to multiple singularities. *Light Sci. Appl.* **8**, 90 (2019).
21. Zhao, N., Li, X., Li, G. & Kahn, J. M. Capacity limits of spatially multiplexed free-space communication. *Nat. photonics* **9**, 822–826 (2015).
22. Zhu, L. & Wang, J. Simultaneous generation of multiple orbital angular momentum (OAM) modes using a single phase-only element. *Opt. Express* **23**, 26221–26233 (2015).
23. Ren, H. et al. Metasurface orbital angular momentum holography. *Nat. Commun.* **10**, 2986 (2019).
24. Xiong, B. et al. Breaking the limitation of polarization multiplexing in optical metasurfaces with engineered noise. *Science* **379**, 294–299 (2023).
25. Wang, H. L., Ma, H. F. & Cui, T. J. A polarization-modulated information metasurface for encryption wireless communications. *Adv. Sci.* **9**, 2204333 (2022).
26. Ohashi, K. et al. On-chip optical interconnect. *Proc. IEEE* **97**, 1186–1198 (2009).
27. Bi, L. et al. On-chip optical isolation in monolithically integrated non-reciprocal optical resonators. *Nat. Photonics* **5**, 758–762 (2011).
28. 6G-Flagship. *Key Drivers and Research Challenges for 6G Ubiquitous Wireless Intelligence* (6G-Flagship, 2019).

Acknowledgements

We acknowledge the funding support from the National Key Research and Development Program of China (2022YFB2802803), the Natural Science Foundation of China Project (Nos. 61925104, 62422509, 62031011, 62201157), Shanghai Municipal Science and Technology Major Project, and Shanghai Frontiers Science Center Program (2021–2025 No. 20). This research is supported by Zhangjiang Laboratory.

Author contributions

Conceptualization: J.S., C.C. and X.F. Methodology: J.S. and C.C. Material: C.S., Z.L., H.Z. Y.W. and J.Z. Experiment: C.C., P.L., H.Z. and F.D.

Supervision: N.C., M.G., J.Z. and H.C. Writing—original draft: J.S. and C.C. Writing—review and editing: J.S., C.C. and X.F.

Competing interests
The authors declare no competing interests.

Additional information
Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41467-025-65111-5.

Correspondence and requests for materials should be addressed to Junwen Zhang, Xinyuan Fang, Nan Chi or Min Gu.

Peer review information *Nature Communications* thanks the anonymous reviewers for their contribution to the peer review of this work. A peer review file is available.