Large-scale scattering-augmented optical encryption

Bian, Liheng; Chang, Xuyang; Jiang, Shaowei; Yang, Liming; Zhan, Xinrui; Liu, Shicong; Li, Daoyu; Yan, Rong; Gao, Zhen; Zhang, Jun

Published in:
Nature Communications

Published: 01/01/2024

Document Version:
Final Published version, also known as Publisher's PDF, Publisher's Final version or Version of Record

Published version (DOI):
10.1038/s41467-024-54168-3

Publication details:
Bian, L., Chang, X., Jiang, S., Yang, L., Zhan, X., Liu, S., Li, D., Yan, R., Gao, Z., & Zhang, J. (2024). Large-scale scattering-augmented optical encryption. *Nature Communications*, *15*(1), Article 9807. https://doi.org/10.1038/s41467-024-54168-3

nature communications

Article

https://doi.org/10.1038/s41467-024-54168-3

Large-scale scattering-augmented optical encryption

Received: 2 April 2024

Accepted: 4 November 2024

Published online: 12 November 2024

Check for updates

Liheng Bian[1,2,4] ✉, Xuyang Chang[1,4], Shaowei Jiang[3,4], Liming Yang[3], Xinrui Zhan[1], Shicong Liu[1], Daoyu Li[1], Rong Yan[1], Zhen Gao[1] & Jun Zhang[1] ✉

Data proliferation in the digital age necessitates robust encryption techniques to protect information privacy. Optical encryption leverages the multiple degrees of freedom inherent in light waves to encode information with parallel processing and enhanced security features. However, implementations of large-scale, high-security optical encryption have largely remained theoretical or limited to digital simulations due to hardware constraints, signal-to-noise ratio challenges, and precision fabrication of encoding elements. Here, we present an optical encryption platform utilizing scattering multiplexing ptychography, simultaneously enhancing security and throughput. Unlike optical encoders which rely on computer-generated randomness, our approach leverages the inherent complexity of light scattering as a natural unclonable function. This enables multi-dimensional encoding with superior randomness. Furthermore, the ptychographic configuration expands encryption throughput beyond hardware limitations through spatial multiplexing of different scatterer regions. We propose a hybrid decryption algorithm integrating model- and data-driven strategies, ensuring robust decryption against various sources of measurement noise and communication interference. We achieved optical encryption at a scale of ten-megapixel pixels with 1.23 μm resolution. Communication experiments validate the resilience of our decryption algorithm, yielding high-fidelity results even under extreme transmission conditions characterized by a 20% bit error rate. Our encryption platform offers a holistic solution for large-scale, high-security, and cost-effective cryptography.

Information security and privacy have become critical concerns in the modern age, drawing significant attention from individuals and governments alike. Recent years have seen economic downturns and social unrest triggered by illicit information collection and unauthorized access, underscoring the urgent need for secure encryption techniques[1–4]. In this context, optical encryption has emerged as a promising solution, leveraging the multiple degrees of freedom in lightwaves[5,6], including polarization[7,8], wavelength[9], and wavefront encoding[10,11]. This approach allows for instantaneous and concurrent information processing as light passes through encryption elements, outpacing traditional computer encryption methods that rely on complex algorithms to process each information component individually. The efficiency and enhanced security offered by optical encryption have positioned it as a promising method across various domains, including communication, military applications, and national defense.

[1]State Key Laboratory of CNS/ATM & MIIT Key Laboratory of Complex-field Intelligent Sensing, Beijing Institute of Technology, Beijing, China. [2]Guangdong Province Key Laboratory of Intelligent Detection in Complex Environment of Aerospace, Land and Sea, Beijing Institute of Technology, Zhuhai, China. [3]Department of Biomedical Engineering, University of Connecticut, Storrs, CT, USA. [4]These authors contributed equally: Liheng Bian, Xuyang Chang, Shaowei Jiang. ✉e-mail: bian@bit.edu.cn; zhjun@bit.edu.cn

The field of optical encryption has seen significant advancements over the past few decades. The introduction of double random phase encoding methods in the 1990s[12,13] marked the inception of this field. However, the complexity of optical components involved, such as various lenses, phase masks, and spatial light modulators, along with security vulnerabilities, has impeded broader applications[14]. In contrast, the emergence of metasurfaces has ushered in a new era of optical control, enabling the manipulation of light waves through phase modulation at subwavelength scales[15]. Metasurface-based optical encryption has gained favor due to its compact features, which simplify system configurations[8,11,13,16,17]. The integration of optical encryption with computational imaging techniques has introduced new perspectives in optical information processing[13,18]. Recent developments in optical encryption have explored the integration of deep learning with complex scattering media, offering promising security features[19,20]. However, these approaches also introduce new challenges in system calibration and decryption processes, which result in reduced encryption throughput. Despite the previous advancements, large-scale optical encryption implementations remain largely theoretical. Practical applications are often limited to simple and sparse plaintexts due to challenges in resolution, signal-to-noise ratio (SNR), and precision of encoding elements[21,22]. While digital simulations simplify the implementation of optical encryption, they risk reducing its value to a mere algorithmic process, neglecting the inherent advantages of efficient and rapid parallel processing in optical propagation. Moreover, the security of most optical encryption systems, which rely on artificially generated encoding units, is compromised by their predictability, increasing vulnerability to breaches[2,23]. Consequently, existing optical encryption methodologies face a compromise between encryption throughput, system complexity, and security.

To address these challenges, we present a comprehensive optical encryption technique that integrates a scattering multiplexing ptychographic encryption system, a transmission-efficient compressive sampling strategy, and a hybrid-driven decryption algorithm. Figure 1a illustrates the prototype and workflow of the proposed system. In this process, light transmits through the plaintext and proceeds to a scattering layer, where it undergoes multiplexing via lateral shifts of the layer to encode the wavefront. The detector plane then captures the encoded signal. The scattering layer enhances security in two crucial ways. First, it possesses inherent complexity and randomness governed by its physical nature, making it unclonable and bypassing the insecure predictability of most artificially designed encoders. Second, it simultaneously achieves mixed modulation for both the amplitude and phase of the wavefront, surpassing the unpredictability of conventional single-dimensional modulations (e.g., phase-only spatial light modulators). Our compressive sampling strategy significantly reduces data transmission volume, improving transmission efficiency by approximately an order of magnitude. Furthermore, this approach can be readily combined with various visual algorithms, such as random arrangement and quick response (QR) codes[24], to create a versatile hybrid encryption system.

The decryption process in our optical encryption technique addresses two key challenges: recovering phase information and resolving the underlying problem of compressive sampling. Our decryption algorithm decomposes this complex task into two subproblems, leveraging an alternating projection (AP) solver[25] and a

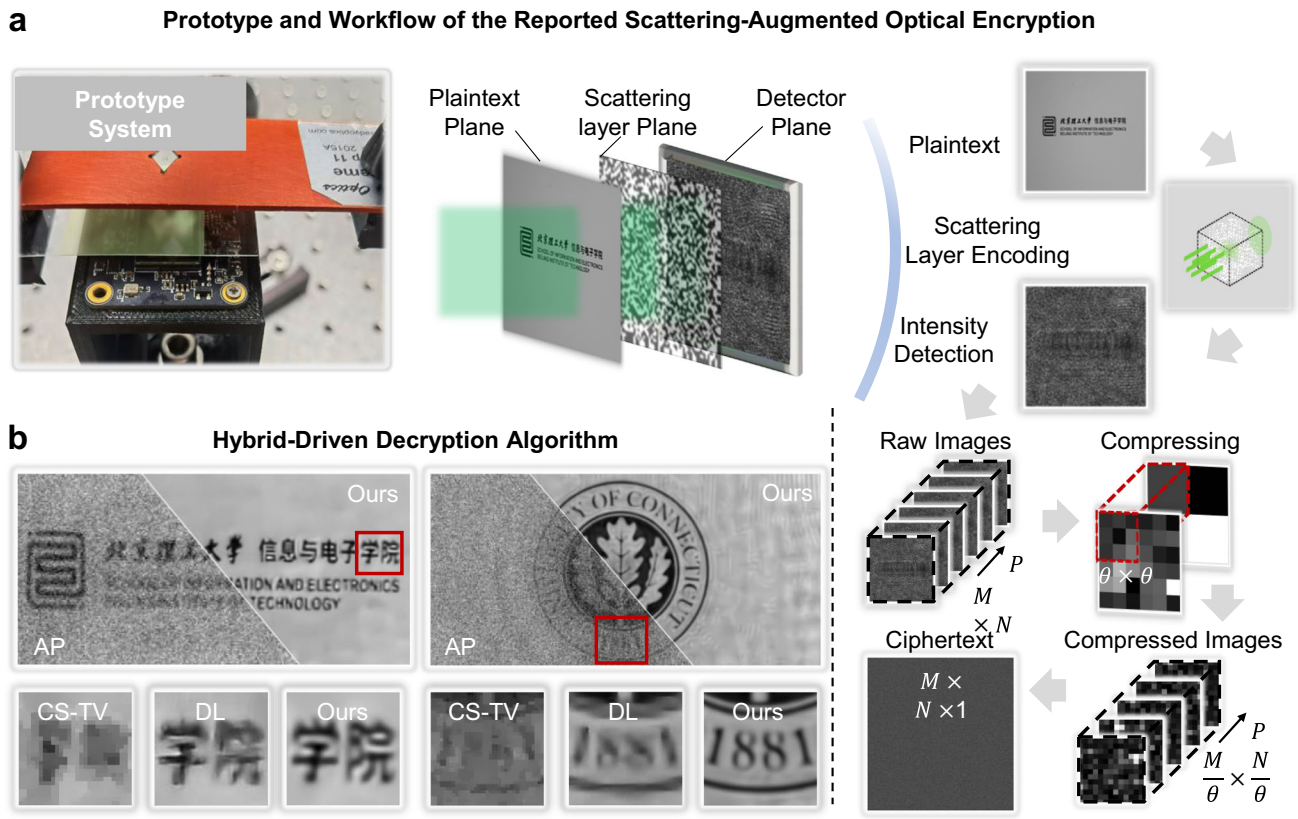

Fig. 1 | Illustration of the reported optical encryption technique. a Prototype and workflow of the reported optical encryption system. **b** Decryption comparison of conventional alternating projection (AP) algorithm, compressive sensing with total variation regularization (CS-TV) algorithm, deep learning (DL) algorithm, and the reported hybrid-driven algorithm (Ours). *M* and *N* represent the number of pixels in the length and width of the Rawdata images, respectively. *P* denotes the number of image frames acquired, and θ represents the compression ratios.

pre-trained denoising neural network[26]. This hybrid approach combines the strengths of conventional optimization methods and deep learning techniques, eliminating the need for an extensive dataset of plaintext-ciphertext pairs. Consequently, our algorithm demonstrates robust resistance to noise and interference during both data acquisition and transmission. Figure 1b illustrates the performance of our decryption algorithm.

To validate the efficacy of our proposed method, we developed a comprehensive prototype capable of optical encryption at an unprecedented scale of ten million pixels, surpassing 4K resolution, with a ~1.23 μm resolution. This achievement exceeds the native capability of the detector (1.67 μm pixel size) without requiring magnification, thereby enhancing cost-effectiveness and facilitating potential miniaturization. Our communication experiments showcase the exceptional robustness of our decryption algorithm, which maintains high-fidelity recovery even under extreme transmission conditions, including bit error rates (BER) as high as 20%. Furthermore, our security assessment reveals that our approach achieves superior randomness and higher ciphertext entropy compared to traditional computer-generated encoding patterns, significantly enhancing the overall security of the encryption system.

Results

Simulations

To validate the effectiveness of our encryption technique, we conducted comprehensive simulations for both single-image and double-image encryption scenarios. We used three natural images as the latent plaintext images, as depicted in Fig. 2a. In our simulations, the illumination wavelength was 532 nm. The propagation distances between the plaintext plane to the scattering layer plane and the scattering layer plane to the ciphertext plane were both 2 cm.

For compressive sampling, we merged 4 × 4 pixels of the intensity-only images at the detector plane. The compression ratio, denoted as θ, is defined as the ratio of the number of pixels in the intensity-only images to that in the compressed image. To ensure that the ciphertexts had the same data volume as the high-resolution plaintexts, we set the number of intensity-only images P to be θ^2. This square relationship also facilitates the implementation of visual encryption algorithms, exemplified here by random arrangement. To assess our decryption algorithm's robustness against noise, we added varying levels of Gaussian noise to the intensity-only images, quantified by the SNR. These measurements were then randomly arranged for visual encryption to generate the final ciphertexts.

Figure 2b displays the final ciphertext, demonstrating the successful concealment of the plaintext without visual information disclosure. Figure 2c, d presents the decryption results for single-image and double-image encryption under different Gaussian noise levels. We compared our decryption method with three established techniques: the alternating projection (AP) phase retrieval algorithm[27], the compressive sensing method with total variation regularization (CS-TV)[28], and the deep learning algorithm (DL)[29]. The neural network structure and training details can be seen in Supplementary Note 1.

Our results demonstrate that the conventional AP method fails to suppress noise effectively, significantly impacting recovery quality. While the CS-TV method outperforms AP in noise reduction and SNR improvement, it struggles with spatial resolution issues caused by compressive sampling. The DL method shows better noise robustness and resolution across various noise levels but lacks sufficient image detail. In contrast, our algorithm effectively recovers high-resolution ciphertext and demonstrates superior noise suppression. It achieves a peak signal-to-noise ratio (PSNR) exceeding 20 dB in single-image encryption, even under severe Gaussian noise conditions (SNR = 2 dB). Additional simulation results and tests for diffraction distance robustness are provided in Supplementary Notes 2 and 3.

Experiments

To validate the effectiveness of our encryption technique, we constructed a comprehensive prototype using a coverslip coated with polystyrene beads (~1 μm) as the scattering layer. We calibrated the scattering layer prior to encryption (details in Methods section and Supplementary Notes 4 and 5). As shown in Fig. 3a, we employed a USAF resolution test chart and a photoetching target (described in Supplementary Note 6) as plaintexts. Figure 3b shows the secret keys used for decryption, including the illumination wavelength, diffraction distance, pixel size of the detector, position shifts, and modulation patterns of the scattering layer, as well as the subsequent visual encryption algorithm. Figure 3c illustrates the complex-domain profile of the scattering layer. Figure 3d showcases the ciphertexts for the amplitude and phase USAF targets, respectively. They demonstrate our technique's ability to encrypt plaintext into chaotic ciphertext successfully. We conducted experiments under various compression ratios (θ) and numbers of intensity-only images (P) to showcase the efficacy of the reported technique. To explore the limit of throughput, we fixed the sizes of raw images and employed them to decrypt high-resolution plaintexts with different resolutions and sizes. We captured varying numbers of intensity-only images at the previously calibrated positions for different compression ratios. It is important to ensure that the selected positions are evenly distributed across the calibration area to reduce the correlation of the captured intensity-only images (for more details, refer to Supplementary Note 7). The visual encryption algorithm used in the experiments was identical to the one used in the simulations.

Figure 3e presents the decryption times for different compression ratios, providing insight into the algorithms' efficiency. Figure 3f, g showcases the decryption results for the amplitude and phase USAF targets, respectively. Columns 1–2 present our algorithm's decryption results, while column 3 compares the performance of DL algorithms. Our findings demonstrate that the CS-TV algorithm fails to recover high-resolution ciphertext, even with complete knowledge of secret keys. Additionally, the performance of the DL algorithm suffers from poor generalization and discrepancies between the simulated training data and the experimental test data. In contrast, our decryption algorithm achieves high-accuracy and high-resolution reconstruction across various plaintext sizes, compression ratios, and numbers of intensity-only images. Notably, with θ = 5, we compressed the data volume to 1/25 and achieved more than ten million pixels (surpassing 4 K resolution) with ~1.23 μm resolution. This surpasses the detector's native capability (1.67 μm pixel size) without the need for magnification configuration, making our approach cost-effective and suitable for miniaturization. Additional results of other comparison algorithms and the photo etching targets are presented in Supplementary Note 6.

To validate the transmission robustness of our encryption technique, we implemented a wireless communication system as shown in Fig. 4a. We utilized the ciphertext with a compression ratio of 4 as the transmission signal. By manipulating transmission distance and environmental interference, we controlled communication quality, quantified by bit error rates (BER). We then employed the received ciphertext and known secret keys to recover the original plaintext.

Figure 4a illustrates the wireless communication system setup. Figure 4b displays the received ciphertexts and corresponding constellation diagrams for different BERs, providing a visual representation of communication quality. Figure 4c presents the decryption results under different BERs. For quantitative comparison, we generated a reference ground truth using a high-accuracy reconstruction result using 1521 intensity-only images. The results demonstrate that the conventional AP method is highly susceptible to measurement noise and transmission interference, with the decryption quality rapidly deteriorating as BER increases. While CS-TV and DL algorithms demonstrate some noise suppression capabilities, they fail to resolve finer details due to resolution limitations. In contrast, our algorithm

https://doi.org/10.1038/s41467-024-54168-3

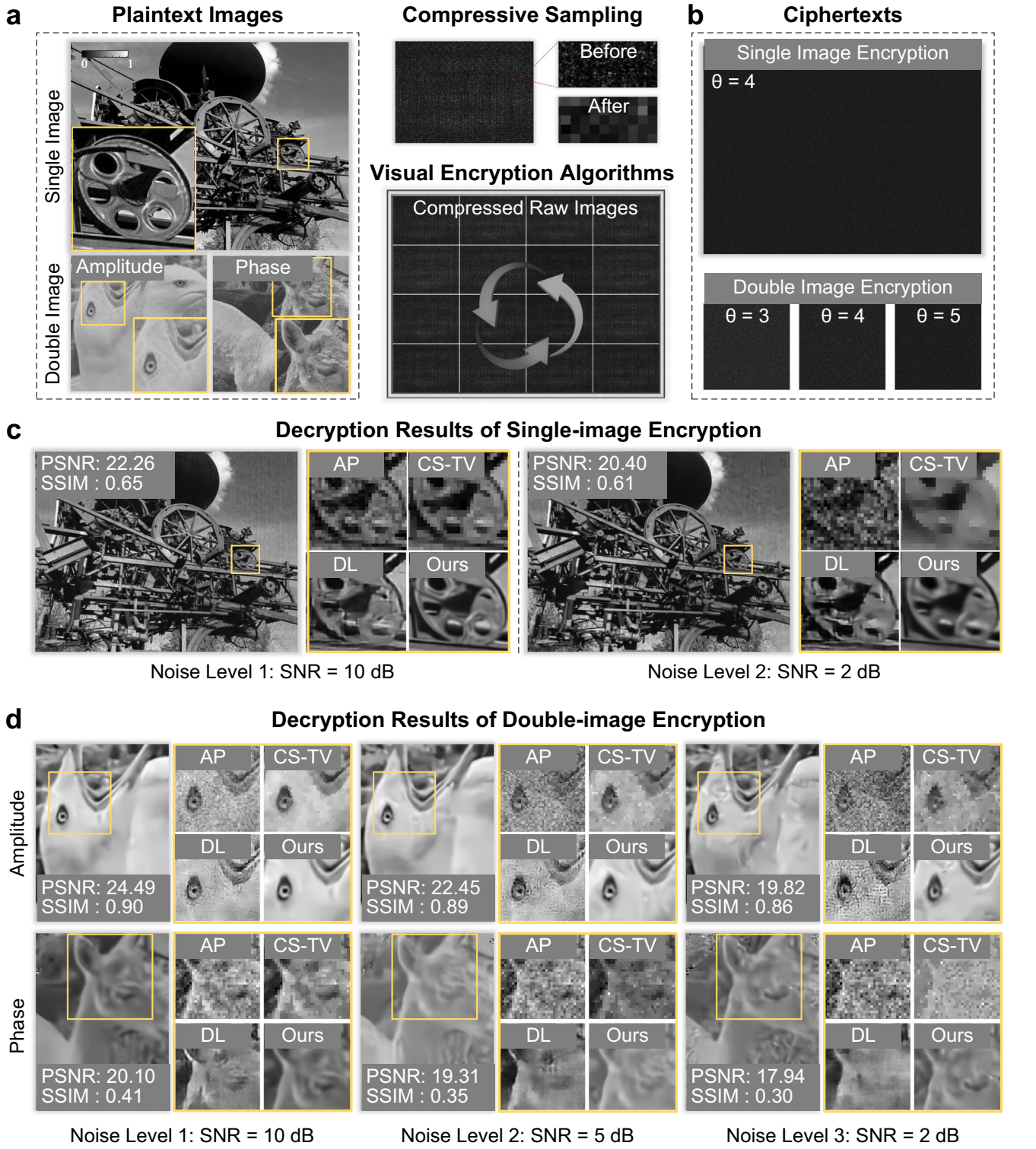

Fig. 2 | Simulation results for single-image and double-image encryption. **a** Original plaintext images. After the optical encryption, the compressed intensity-only images are randomly arranged for visual encryption. **b** Final ciphertexts under different compression ratios θ. **c** Decryption results for the single-image encryption under $\theta = 4$. **d** Decryption results for the double-image encryption under $\theta = 4$. SNR means signal-to-noise ratio.

can successfully retrieve the plaintext even under extreme transmission conditions with a 20% BER, showcasing its superior robustness and efficacy in challenging communication environments.

Security analysis

Encoding patterns are crucial secret keys in optical encryption. We investigated the relationship between the number of correct patterns and decryption quality using a USAF resolution test chart with a compression ratio of 4. Figure 5a presents quantitative results for different numbers of correct patterns, Fig. 5b shows a cross-section of Group 7 under these conditions, and Fig. 5c presents visual results for different numbers of correct patterns. Our findings underscore the significance of modulation patterns in concealing plaintext. Performance metrics (PSNR and SSIM) showed little improvement with

https://doi.org/10.1038/s41467-024-54168-3

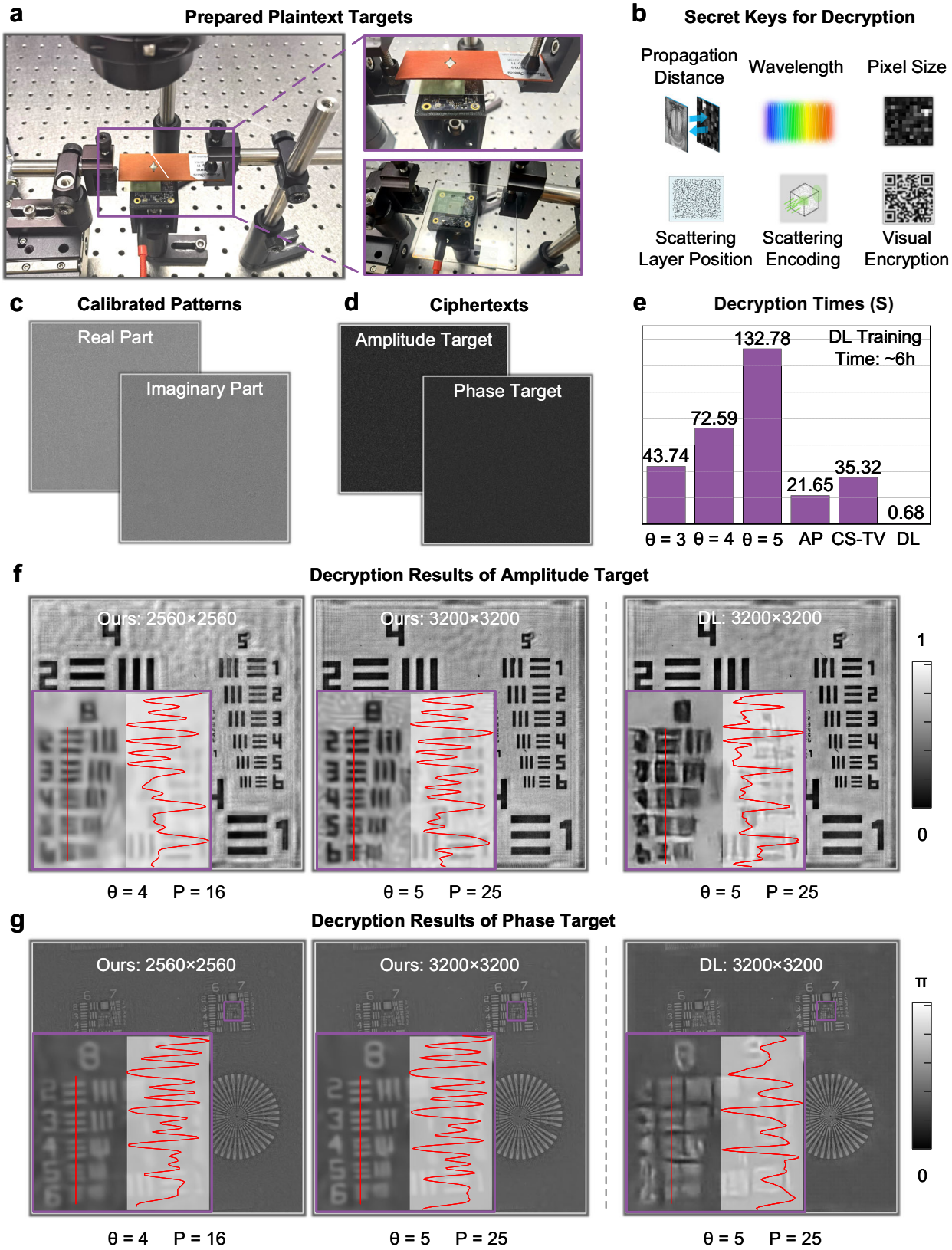

Fig. 3 | Experimental results. a Prepared plaintext targets. **b** Security keys are used for encryption. **c** Real and imaginary components of the calibrated scattering layer. **d** Ciphertexts for the amplitude and phase USAF targets. **e** Decryption times (in seconds) of the decryption algorithms. The first three elements are the running time of the reported algorithms under different compression ratios and recovery sizes. **f**–**g** Decryption results of the amplitude and phase targets under different compression ratios θ and the number of intensity-only images P. Additional results can be found in Supplementary Note 6.

https://doi.org/10.1038/s41467-024-54168-3

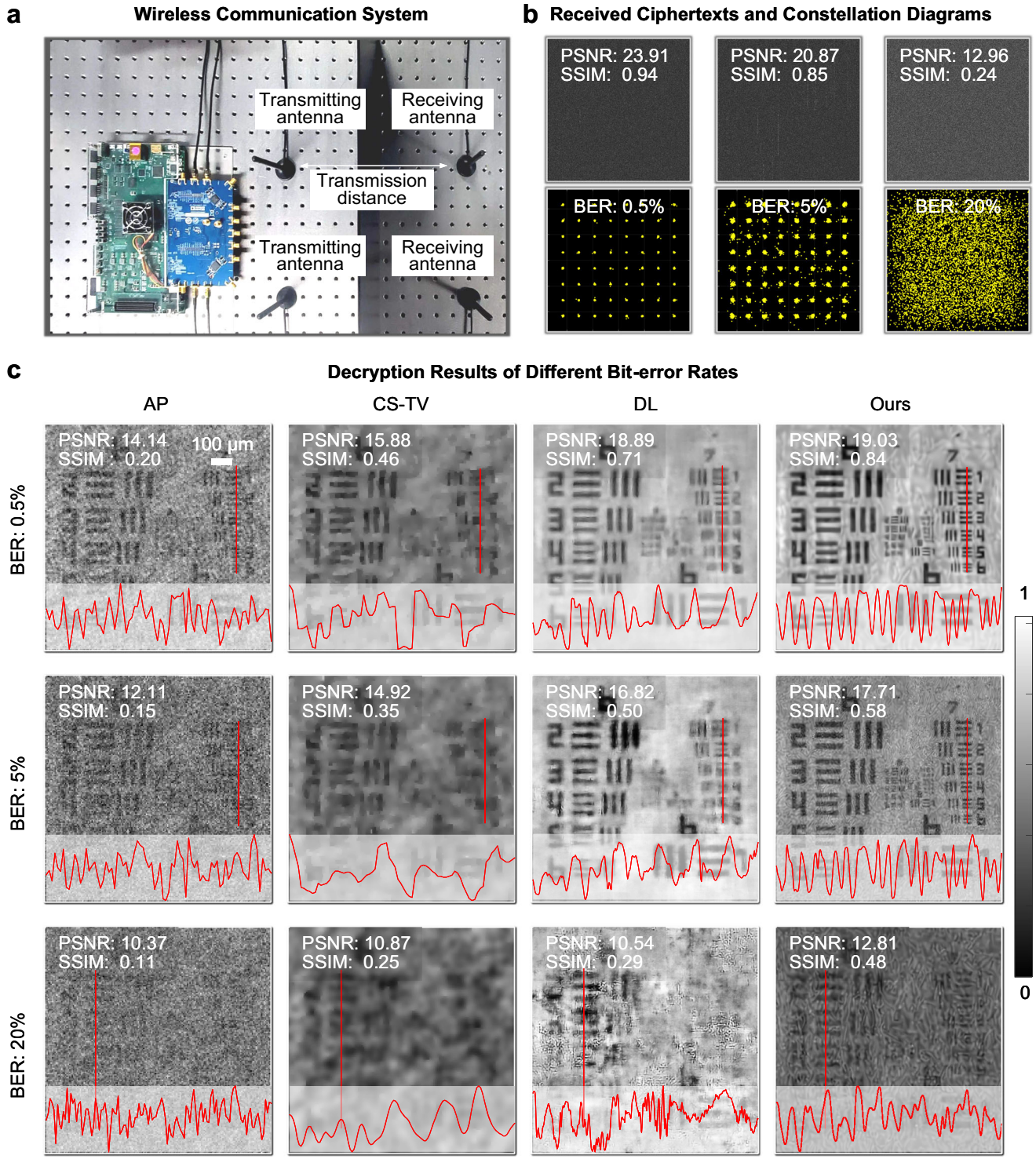

Fig. 4 | Results of wireless transmission using the reported technique. **a** Wireless communication system. **b** Received ciphertexts and constellation diagrams under different bit error rates (BER). Constellation diagrams are used to evaluate the transmission quality. **c** Decryption results under different BERs. Complete results can be found in Supplementary Note 6.

incorrect patterns, only exhibiting a marked increase when all patterns were known. Additional security key test results are available in Supplementary Note 8.

A potential vulnerability in encoding-based optical encryption systems is the inference of image information from coarse outlines if they partially crack the security key[9]. To mitigate this risk, we propose a hybrid encryption strategy that combines multiple security layers. In this approach, the original image is first converted into a QR code, which is then used as input for our optical encryption system. This method offers several advantages: even if an attacker partially cracks the optical encryption, they would still face the challenge of decoding an incomplete QR code, which requires high-quality, complete images to function properly. To demonstrate the effectiveness of this hybrid approach, we conducted simulations using parameters identical to those in Fig. 2's single-image encryption, with a compression sampling ratio of 4. As shown in Fig. 5d, even when the optical encryption is

https://doi.org/10.1038/s41467-024-54168-3

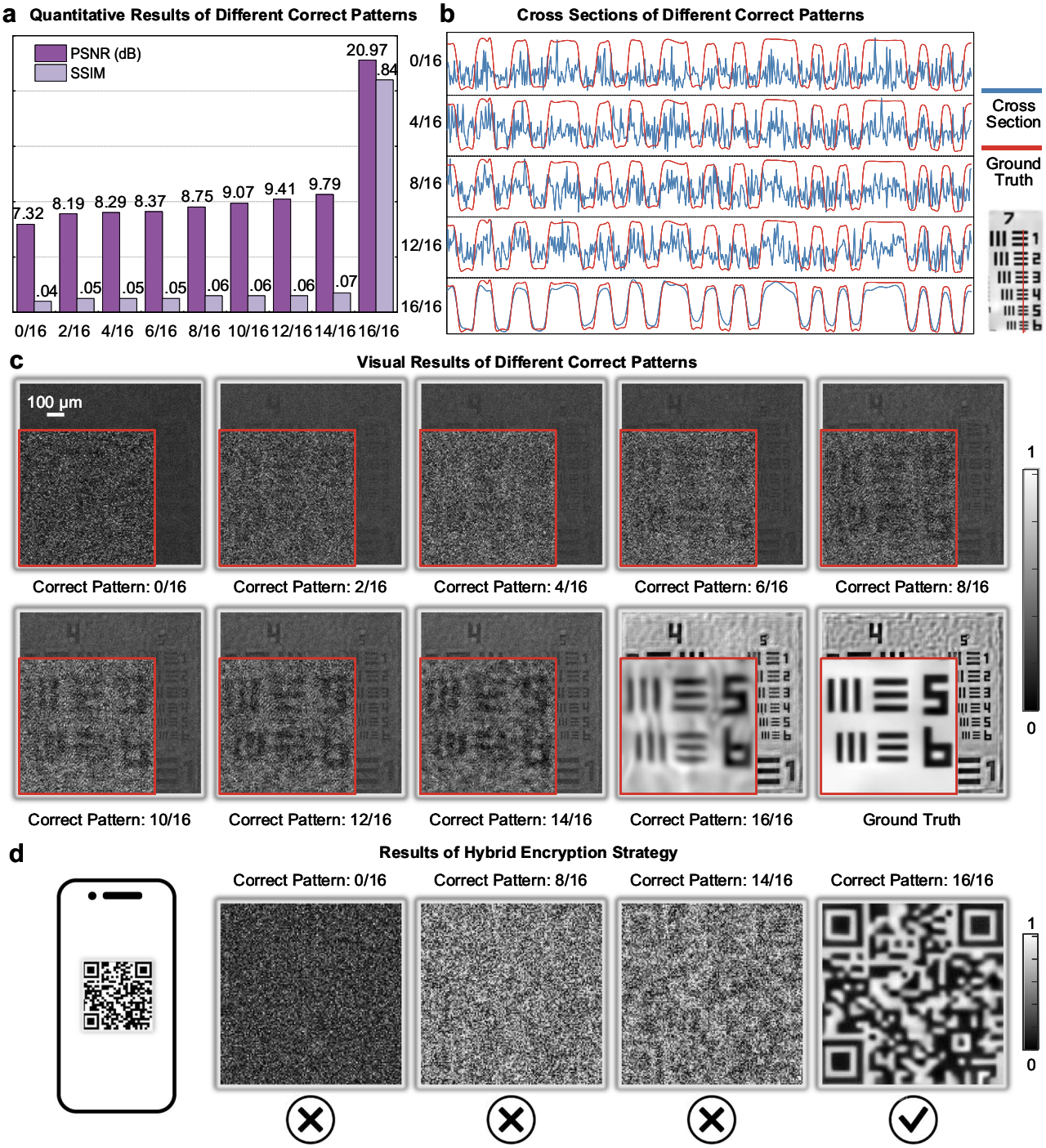

Fig. 5 | Security test using different numbers of correct patterns. a Quantitative results (PSNR & SSIM) under different numbers of correct patterns. **b** Cross-section of Group 7 under different numbers of correct patterns. **c** Visual results under different numbers of correct patterns. **d** Simulation results of a hybrid encryption strategy using QR codes to mitigate the risk of partial security key cracking.

partially compromised, the resulting image is a distorted version of the QR code that cannot be successfully scanned or decoded, thereby preventing meaningful information extraction. This hybrid strategy not only adds an extra layer of security but also offers flexibility to adapt to various security contexts and emerging threats by allowing the use of different forms of digital pre-encryption beyond QR codes.

To validate the advantages and security of using a random scattering layer, we conducted a comprehensive analysis of the randomness of modulation patterns and ciphertext information entropy. It is well-established that random number generation (RNG) algorithms can only produce pseudo-random numbers[2], which potentially introduces vulnerabilities. We employed the randomness test procedures from the National Institute of Standards and Technology (NIST)[30] to compare the randomness of modulation patterns generated by different RNG algorithms (Supplementary Note 9). The comparison algorithms include linear congruence (LC)[31], XORshift (Xor)[32], Mersenne twister (MT)[33], and the calibrated scattering layer we used. We present the test results of 15 projects in Table 1, where we used *P*-values to quantify the evaluation results, with higher *P*-values indicating better randomness. For the remaining four projects, we evaluated the

https://doi.org/10.1038/s41467-024-54168-3

Table 1 | NIST test results. It contains 15 items, and our method outperforms others in eight of them

Methods Projects	LC	XorShift	MT	Ours
Frequency	0.6170	0.8383	0.6862	**0.8461**
Frequency within a block	0.1015	0.4123	0.0712	**0.8245**
Runs	0.6052	0.3001	**0.7816**	0.6825
Longest run of ones in a block	0.7321	**0.8182**	0.1905	0.5499
Binary matrix rank	0.3430	0.0457	0.3963	**0.6488**
Spectral	0.0684	0.0269	**0.2475**	0.0389
Overlapping template matching	0.6447	0.4373	**0.6746**	0.5207
Maurer's universal statistical	0.9271	0.8679	0.7650	**0.9942**
Linear complexity	0.5517	0.2786	0.5803	**0.7659**
Approximate entropy	**0.9861**	0.7717	0.8627	0.8398
Cumulative sums	0.4781	0.4999	**0.5432**	0.5353
Non-overlapping template matching	**148/148**	147/148	144/148	**148/148**
Serial	2/2	2/2	2/2	2/2
Random excursions	6/8	**8/8**	4/8	**8/8**
Random excursions variant	16/18	**18/18**	16/18	**18/18**

Bold font indicates the best methods in each row.

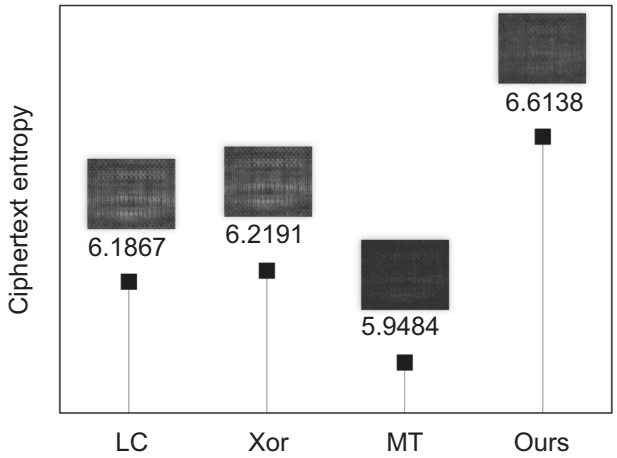

Fig. 6 | Results of ciphertext entropy. The comparison algorithms include linear congruence (LC)[31], XORshift (Xor)[32], Mersenne twister (MT)[33], and the calibrated scattering layer we used (Ours). The images in the figure correspond to ciphertexts generated using different random numbers.

performance using the passing rate. Our strong-randomness modulation of disordered scattering achieved the best performance in eight projects, demonstrating a significant advantage over other algorithms.

To further validate security, we compared the ciphertext entropy of different RNG algorithms (Supplementary Note 10). In information theory, the entropy of a random variable represents the average level of "uncertainty" in the variable's potential outcomes[34]. In image encryption, ciphertext entropy can evaluate statistical correlation and the difficulty of withstanding attacks. Figure 6 illustrates the ciphertext entropy comparison results, showing that our technique generated ciphertext with the largest information entropy, indicating greater unpredictability compared to other methods.

Brute-force attacks represent a persistent threat to cryptographic systems. To assess our system's resilience against such attacks, we conducted a thorough analysis of its theoretical vulnerability, as detailed in Supplementary Note 11. Our calculations reveal that even with the computational power of a supercomputer, exhausting the entire key space would require impractical amounts of time. This robustness stems from the vast keyspace inherent in our encryption method. While we acknowledge that practical attacks might leverage prior knowledge to expedite the cracking process, the sheer magnitude of our key space provides a formidable barrier against brute-force attempts. To contextualize our system's strength, we compared its key space with those of existing optical encryption techniques (also in Supplementary Note 11). Our large-scale encryption methodology yields a significantly larger key space, substantially increasing the complexity and computational demands of potential brute-force attacks. This comparative analysis underscores the enhanced security our approach offers against one of the most fundamental cryptographic threats.

Imaging through scattering media techniques poses potential risks to our encryption system[35–46]. However, these techniques typically rely on specialized hardware configurations, such as time-gated systems[35] or guide-star wavefront shaping[42], and specific physical principles like the optical memory effect[43,44]. These specialized setups and prior information are not applicable to the speckle images captured by our optical encryption platform, thereby limiting their effectiveness as potential attach vectors. While deep learning-assisted imaging through scattering media can bypass some of these limitations, it faces significant challenges in the context of our system. The primary hurdle is the difficulty in obtaining the extensive training pairs required for effective cracking[40]. Additionally, these methods often exhibit poor generalization across different scattering media, further complicating any attempts to compromise our system's security[41]. Recent advances in diffractive deep neural networks (D2NNs) theoretically suggest the possibility of brute-force attacks by exploiting the correlation length of the scattering media[47,48]. However, D2NNs typically operate in the terahertz range, and the fabrication accuracy and associated costs required for visible-light diffractive layers make brute-force attacks economically unfeasible[47]. Furthermore, our system's security is enhanced by its complexity compared to typical D2NN implementations. While D2NNs generally assume a phase-only diffuser, our scattering layer encodes both amplitude and phase information. This dual encoding adds an extra layer of complexity that current D2NN models are not designed to handle effectively. Lastly, D2NNs have primarily been deployed on simple and sparse targets. The complex, information-rich scenes encountered in our large-scale encryption system would likely pose significant challenges for these networks, potentially leading to reduced efficacy or performance degradation[49]. This mismatch between the typical application domain of D2NNs and the characteristics of our encryption system provides an additional buffer against potential attacks.

Discussion

We have presented a large-scale scattering-augmented optical encryption technique based on scattering multiplexing ptychography. By employing a shifting random scattering layer to encode targets, we simultaneously enhance security and encryption throughput, achieving ten million pixels with 1.23 μm resolution. This surpasses the detector's native capability (1.67 μm pixel size) without magnification, offering a cost-effective approach suitable for miniaturization. Our method incorporates a compressive sampling strategy that clusters neighboring scattered pixels, reducing data volume by approximately an order of magnitude. The decryption algorithm, combining conventional optimization with advanced deep learning techniques, demonstrates strong generalization and noise robustness. Wireless communication experiments verify the algorithm's ability to retrieve high-fidelity results even under extreme transmission conditions with a 20% bit error rate. Security analysis confirms that our encryption scheme exhibits superior randomness and higher ciphertext entropy, bolstering its resilience against potential attacks.

The reported encryption technique has the potential for enhancing information security, especially when combined with deep learning[50,51] or metamaterials[52]. Future advancements could focus on

several key areas. First, the selection of scattering materials could be optimized using a data-driven approach[53,54], moving beyond manual selection to discover materials with ideal scattering characteristics. This approach would foster interdisciplinary research between information technology and materials science, leveraging deep learning strategies. Second, while current scattering materials are thin and modeled as 2D planes, the development of advanced 3D encoders in optical authentication systems[55,56] suggests a promising direction for optical encryption. Implementing thick 3D scattering layers could significantly enhance both the complexity and capacity of the security key space[57]. Third, the scattering-augmented encryption technique could be combined with various computational imaging modalities, including single-pixel imaging[58], polarimetric imaging[59], all-optical diffractive networks[47,48,60,61] and coherent imaging[62,63], or nonlinear optical methods[64], potentially leading to novel hybrid systems with enhanced capabilities.

The wide-field and high-resolution capabilities of our system also have broader applications. We have demonstrated its potential in high-throughput quantitative phase microscopy of biological samples, including mouse kidneys and U87MG cells (Fig. S15 and Supplementary Note 13). However, the current long data collection time (~50 s) limits its real-time capability for clinical diagnosis, presenting an area for future improvement. Despite this limitation, we believe that our technique offers valuable new insights into information security, bioscience, and related fields, paving the way for innovative applications and further technological advancements.

Methods

Experiment setup

The experimental prototype in Fig. 3a utilized a fiber-coupled diode (532 nm, 5 mW) as the light source, a coverslip coated with polystyrene beads (~1 μm) as the scattering layer, and a detector with 1.67-μm pixel size (MT9J003 ON Semiconductor). The primary criterion for choosing polystyrene particle size is to guarantee obvious speckle patterns can be captured by the detector to hide plaintexts. In this case, the smaller particle size can realize better encryption throughput and the 2D model assumption. The 1 μm particle size is a suitable tradeoff for the degree of scattering and throughput. The scattering layer was placed at a distance of approximately 0.68 mm from the detector, while the sample was positioned at a distance of approximately 0.71 mm from the scattering layer.

Scattering layer calibration

Throughout the calibration phase, the detector consistently captured diffraction images at a constant frame rate of 30 frames per second. We adjusted the scattering layer across 1521 distinct positions, acquiring corresponding intensity-only measurements. The scattering layer shift step size was ~1–3 μm to balance motion blur and image similarity. The entire process of data collection for calibration took approximately 50 s. The calibration employs an algorithm derived from the extended ptychographic iterative engine (ePIE)[65,66], as detailed in Supplementary Note 4. This algorithm is designed to concurrently reconstruct the profiles of both the sample and the scattering layer using the collected measurements. The resultant images facilitate the recovery of the scattering layer's complex-domain profile, as depicted in Fig. 3b. Our calibration methodology necessitates only a singular setup procedure. Once the calibration is complete, the same scattering layer can be utilized to encrypt additional plaintexts without requiring any further adjustments. This approach significantly accelerates the encryption process and eliminates the need for repetitive calibration tasks.

Wireless transmission system

The wireless communication system was composed of a prototype board, the Xilinx Zynq7000 Series System-on-Chip (SoC) ZC706, and an AD9361-based software radio communication system[67]. The system transmitted at a center frequency of 2.45 GHz with a bandwidth of 10 MHz. It utilized 64 quadrature amplitude modulation (64QAM) and orthogonal frequency division multiplexing (OFDM). The wireless transmission takes ~70 s for a 2560 × 2560 ciphertext.

Forward model of the reported optical encryption system

The encryption technique presented in this study is based on the diffraction modality. Assuming that the plaintext consists of 2D images, we denote the wavefront of the plaintext plane, the scattering layer plane, and the detector plane as $\mathcal{P}(x,y), \mathcal{S}(x,y), \mathcal{D}(x,y)$, respectively. The forward model begins with the illumination of the plaintext by a light source, followed by propagation a distance z_1 to the scattering layer plane. The wavefront propagation is mathematically described using the Rayleigh–Sommerfeld model[68]

$$\mathcal{S}(x,y,z_1) = \mathcal{F}^{-1}\left\{H\left(f_x,f_y,z_1\right)\cdot\mathcal{F}[\mathcal{P}(x,y)]\right\} \tag{1}$$

where F and $\mathcal{F}^{-1}$ represent 2D Fourier transform (FT) and inverse FT, respectively. $H(f_x,f_y,z_1)$ is the transfer function defined by the angular spectrum theory[69]

$$H\left(f_x,f_y,z\right) = \begin{cases} \exp\left[i\frac{2\pi}{\lambda}z\sqrt{1-\lambda^2\left(f_x^2+f_y^2\right)}\right], & f_x^2+f_y^2 \le \frac{1}{\lambda^2} \\ 0 & otherwise, \end{cases} \tag{2}$$

where λ is the illumination wavelength, and (f_x,f_y) represent the frequency coordinates.

We move the scattering layer to different $x-y$ positions, where each position corresponds to a wavefront modulation pattern $\mathcal{M}_l(l=1,2,\ldots)$. The scattering layer is modeled as a 2D plane (Supplementary Note 5). The wavefront that passes the scattering layer can be represented as

$$\mathcal{S}_l(x,y,z_1) = \mathcal{S}(x,y,z_1)\odot\mathcal{M}_l \tag{3}$$

where $\odot$ denotes the Hadamard product. The wavefront further propagates a distance z_2 to the ciphertext plane, namely

$$\mathcal{C}_l(x,y,z_2) = \mathcal{F}^{-1}\left\{H\left(f_x,f_y,z_2\right)\cdot\mathcal{F}\left[\mathcal{S}_l(x,y,z_1)\right]\right\} \tag{4}$$

Due to the low response of optoelectronic components, we are only able to capture the intensity measurements at the detector plane. Furthermore, the discretization of pixel size and the introduced compressive sampling necessitate wavefront detection in the following form

$$I_l = \left(\left|\mathcal{C}_l\right|^2\right)\downarrow_\theta + \omega \tag{5}$$

where I_l is the lth intensity-only image, $\downarrow_\theta$ denotes the compressive sampling process and ω represents the measurement noise.

Finally, these measurements are encoded using visual encryption techniques, such as random arrangement and QR codes. In this study, we randomly arranged these measurements to form a high-resolution image as the final ciphertext.

The reported decryption algorithm

The decryption process is based on an iterative phase retrieval (PR) technique. However, due to the compressive sampling used during the encryption process, spatial resolution is compromised, which can lead to resolution degradation when using conventional AP algorithms. Additionally, measurement noise and transmission interference further deteriorate the signal quality. To address these challenges, a novel decryption algorithm is proposed, which is capable of recovering a high-resolution (HR) plaintext from the compressed images. Initially,

the ciphertext is decoded through an inverse visual encryption process. After that, the reported decryption algorithm models the problem as a generalized optimization problem

$$\hat{\mathcal{P}} = \underset{\mathcal{P}}{\operatorname{argmin}} f(\mathcal{P}) + g(\mathcal{P}) \tag{6}$$

where $f(\mathcal{P})$ is a data-fidelity term, and $g(\mathcal{P})$ is a regularizer that imposes certain prior constraints. The optimization is rewritten using the generalized alternating projection strategy[70,71] as

$$\begin{aligned} (\mathcal{P}^{(t)}, \mathcal{R}^{(t)}) &= \arg\min_{(\mathcal{P},\mathcal{R})} \tfrac{1}{2}||\mathcal{P} - \mathcal{R}||_2^2 + \eta g(\mathcal{P}) \\ s.t. &|A\mathcal{P}|^2 = \boldsymbol{I}, \end{aligned} \tag{7}$$

where A represents the forward model, including propagation, scattering multiplexing, and compressive sampling. R is an introduced auxiliary variable, t is the iteration and η is a parameter to balance two terms. Equation (7) is solved by alternatively updating P and R.

Updating P: fixed $\mathcal{R}^{(t)}$, $\mathcal{P}^{(t+1)}$ is updated via a Euclidean projection of $\mathcal{R}^{(t)}$ the manifold $|A\mathcal{P}|^2 = \boldsymbol{I}$ as

$$\mathcal{P}^{(t+1)} = \mathcal{R}^{(t)} + \eta \cdot PR\left(\boldsymbol{I} - \left|A\mathcal{R}^{(t)}\right|^2\right) \tag{8}$$

where PR is an inserted solver to solve the data-fidelity term. Due to the alternating projection technique maintaining low computational complexity and strong generalization, we derive the PR solver following the AP strategy. The process begins with a random high-resolution initialization at the plaintext plane and then iteratively propagates to the scattering layer plane and the detector plane. At the scattering layer plane, the calibrated matrix M is incorporated into the complex wavefront. At the detector plane, the phase is retained, and the amplitude is replaced with the intensity-only image $\boldsymbol{I}$. The AP-based solver provides the ability to recover the complex wavefront. More details can be found in Fig. S14 in Supplementary Note 12.

Updating $\mathcal{R}$: given $\mathcal{P}^{(t)}$, $\mathcal{R}^{(t+1)}$ is updated by a denoising neural network solver as

$$\mathcal{R}^{(t+1)} = \mathrm{Net}\left(\mathcal{P}^{(t+1)}\right) \tag{9}$$

To ensure effective denoising and superior performance, we utilize a pre-trained denoising neural network FFDNET[26] to update Eq. (9). FFDNET is a convolutional neural network that provides flexible and fast solutions for a range of noise levels, balancing noise reduction with the preservation of fine details. Besides, it contains a noise map parameter which makes the denoising degree controllable for each iteration. The details and pseudocode of the decryption algorithm can be seen in Supplementary Note 12.

Randomness test

The patterns of the scattering layer represent its transmission matrix, which is a complex-value matrix. We primarily evaluate the randomness of the phase component, which is mapped to the range of 0–255 and then converted to an 8-bit binary code. The NIST standards[30], which comprises 15 criteria, are used to assess the randomness of the phase. Additional information regarding the NIST test and ciphertext entropy can be found in Supplementary Notes 9 and 10.

Reporting summary

Further information on research design is available in the Nature Portfolio Reporting Summary linked to this article.

Data availability

The minimum data that supports this study is available at https://github.com/bianlab/Scatterencryption. The complete data is available under restricted access following the funded project requirements. Access can be obtained by request to the corresponding authors.

Code availability

The code of the hybrid-driven decryption algorithm is available at https://github.com/bianlab/Scatterencryption.

References

1. Anderson, R. & Moore, T. The economics of information security. *Science* **314**, 610–613 (2006).
2. Liu, Y. et al. Device-independent quantum random-number generation. *Nature* **562**, 548–551 (2018).
3. Carnicer, A. & Javidi, B. Optical security and authentication using nanoscale and thin-film structures. *Adv. Opt. Photonics* **9**, 218–256 (2017).
4. Volodin, B., Kippelen, B., Meerholz, K., Javidi, B. & Peyghambarian, N. A polymeric optical pattern-recognition system for security verification. *Nature* **383**, 58–60 (1996).
5. Matoba, O. et al. Optical techniques for information security. *Proc. IEEE* **6**, 1128–1148 (2009).
6. Javidi, B. et al. Roadmap on optical security. *J. Opt.* **18**, 083001 (2016).
7. Fang, X., Ren, H. & Gu, M. Orbital angular momentum holography for high-security encryption. *Nat. Photonics* **14**, 102–108 (2020).
8. Zhao, R. et al. Multichannel vectorial holographic display and encryption. *Light-Sci. Appl.* **7**, 1–9 (2018).
9. Chen, W., Javidi, B. & Chen, X. Advances in optical security systems. *Adv. Opt. Photonics* **6**, 120–155 (2014).
10. Ren, H. et al. Complex-amplitude metasurface-based orbital angular momentum holography in momentum space. *Nat. Nanotechnol.* **15**, 948–955 (2020).
11. Qu, G. et al. Reprogrammable meta-hologram for optical encryption. *Nat. Commun.* **11**, 1–5 (2020).
12. Refregier, P. & Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **20**, 767–769 (1995).
13. Zheng, P. et al. Metasurface-based key for computational imaging encryption. *Sci. Adv.* **7**, eabg0363 (2021).
14. Liao, M. et al. Deep-learning-based ciphertext-only attack on optical double random phase encryption. *Opto-Electron. Adv.* **4**, 200016–1 (2021).
15. Dorrah, A. H. & Capasso, F. Tunable structured light with flat optics. *Science* **376**, eabi6860 (2022).
16. Dong, F. et al. Information encoding with optical dielectric metasurface via independent multichannels. *ACS Photonics* **6**, 230–237 (2018).
17. Li, J. et al. Addressable metasurfaces for dynamic holography and optical information encryption. *Sci. Adv.* **4**, eaar6768 (2018).
18. Liu, H.-C. et al. Single-pixel computational ghost imaging with helicity-dependent metasurface hologram. *Sci. Adv.* **3**, e1701477 (2017).
19. Zhou, L., Xiao, Y. & Chen, W. Learning complex scattering media for optical encryption. *Opt. Lett.* **45**, 5279–5282 (2020).
20. Zhao, Q. et al. Speckle-based optical cryptosystem and its application for human face recognition via deep learning. *Adv. Sci.* **9**, 2202407 (2022).
21. Scheuer, J. Optical metasurfaces are coming of age: Short-and long-term opportunities for commercial applications. *ACS Photonics* **7**, 1323–1354 (2020).
22. Kaissner, R. et al. Electrochemically controlled metasurfaces with high-contrast switching at visible frequencies. *Sci. Adv.* **7**, eabd9450 (2021).
23. Douglass, P. M., O'Connor, T. & Javidi, B. Automated sickle cell disease identification in human red blood cells using a lensless single random phase encoding biosensor and convolutional neural networks. *Opt. Express* **30**, 35965–35977 (2022).

24. Markman, A., Javidi, B. & Tehranipoor, M. Photon-counting security tagging and verification using optically encoded QR codes. *IEEE Photonics J.* **6**, 1–9 (2013).
25. Shechtman, Y. et al. Phase retrieval with application to optical imaging: a contemporary overview. *IEEE Signal Proc. Mag.* **32**, 87–109 (2015).
26. Zhang, K., Zuo, W. & Zhang, L. FFDNet: toward a fast and flexible solution for cnn-based image denoising. *IEEE T. Image Process* **27**, 4608–4622 (2018).
27. Fienup, J. R. Phase retrieval algorithms: a comparison. *Appl. Opt.* **21**, 2758–2769 (1982).
28. Candes, E. J., Li, X. & Soltanolkotabi, M. Phase retrieval via Wirtinger flow: theory and algorithms. *IEEE T. Inform. Theory* **61**, 1985–2007 (2015).
29. Rivenson, Y., Zhang, Y., Günaydın, H., Teng, D. & Ozcan, A. Phase recovery and holographic image reconstruction using deep learning in neural networks. *Light-Sci. Appl.* **7**, 17141–17141 (2018).
30. Rukhin, A., Soto, J., Nechvatal, J., Smid, M. & Barker, E. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Tech. Rep., Booz-allen and hamilton inc mclean va (2001).
31. Marsaglia, G. The structure of linear congruential sequences. in *Applications of Number Theory to Numerical Analysis* 249–285 (Elsevier, 1972).
32. Marsaglia, G. Xorshift rngs. *J. Stat. Softw.* **8**, 1–6 (2003).
33. Matsumoto, M. & Nishimura, T. Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator. *ACM Trans. Model. Comput. Simul.* **8**, 3–30 (1998).
34. Shannon, C. E. A mathematical theory of communication. *Bell Syst. Tech. J.* **27**, 379–423 (1948).
35. Kang, S. et al. Imaging deep within a scattering medium using collective accumulation of single-scattered waves. *Nat. Photonics* **9**, 253–258 (2015).
36. Badon, A. et al. Distortion matrix concept for deep optical imaging in scattering media. *Sci. Adv.* **6**, eaay7170 (2020).
37. Kang, S. et al. Tracing multiple scattering trajectories for deep optical imaging in scattering media. *Nat. Commun.* **14**, 6871 (2023).
38. Boniface, A., Dong, J. & Gigan, S. Non-invasive focusing and imaging in scattering media with a fluorescence-based transmission matrix. *Nat. Commun.* **11**, 6154 (2020).
39. Escobet-Montalbán, A. et al. Wide-field multiphoton imaging through scattering media without correction. *Sci. Adv.* **4**, eaau1338 (2018).
40. Sanghvi, Y., Yaswanth, K. & Uday, K. K. Embedding deep learning in inverse scattering problems. *IEEE Trans. Comput. Imaging* **6**, 46–56 (2019).
41. Li, Y., Xue, Y. & Tian, L. Deep speckle correlation: a deep learning approach toward scalable imaging through scattering media. *Optica* **5**, 1181–1190 (2018).
42. Horstmeyer, R., Ruan, H. & Yang, C. Guidestar-assisted wavefront-shaping methods for focusing light into biological tissue. *Nat. Photonics* **9**, 563–571 (2015).
43. Bertolotti, J. et al. Non-invasive imaging through opaque scattering layers. *Nature* **491**, 232–234 (2012).
44. Katz, O. et al. Non-invasive single-shot imaging through scattering layers and around corners via speckle correlations. *Nat. Photonics* **8**, 784–790 (2014).
45. Zhu, L. et al. Large field-of-view non-invasive imaging through scattering layers using fluctuating random illumination. *Nat. Commun.* **13**, 1447 (2022).
46. Popoff, S. M. et al. Controlling light through optical disordered media: transmission matrix approach. *N. J. Phys.* **13**, 123021 (2011).
47. Luo, Y. et al. Computational imaging without a computer: seeing through random diffusers at the speed of light. *eLight* **2**, 4 (2022).
48. Lin, X. et al. All-optical machine learning using diffractive deep neural networks. *Science* **361**, 1004–1008 (2018).
49. Liu, J. et al. Research progress in optical neural networks: theory, applications and developments. *PhotoniX* **2**, 1–39 (2021).
50. Wetzstein, G. et al. Inference in artificial intelligence with deep optics and photonics. *Nature* **588**, 39–47 (2020).
51. Metzler, C. A., Ikoma, H., Peng, Y. & Wetzstein, G. Deep optics for single-shot high-dynamic-range imaging. In *Proc. Conference on Computer Vision and Pattern Recognition (CVPR)*, 1375–1385 (CVPR, 2020).
52. Li, L., Zhao, H., Liu, C., Li, L. & Cui, T. J. Intelligent metasurfaces: control, communication and computing. *eLight* **2**, 1–24 (2022).
53. Hamdia, K. M. et al. A novel deep learning based method for the computational material design of flexoelectric nanostructures with topology optimization. *Finite Elem. Anal. Des.* **165**, 21–30 (2019).
54. Kim, Y. et al. Deep learning framework for material design space exploration using active transfer learning and data augmentation. *NPJ Comput. Mater.* **7**, 1–7 (2021).
55. Markman, A., Carnicer, A. & Javidi, B. Security authentication with a three-dimensional optical phase code using random forest classifier. *J. Opt. Soc. Am. A* **33**, 1160–1165 (2016).
56. Matoba, O. & Javidi, B. Encrypted optical memory system using three-dimensional keys in the Fresnel domain. *Opt. Lett.* **24**, 762–764 (1999).
57. Guo, C. et al. Depth-multiplexed ptychographic microscopy for high-throughput imaging of stacked bio-specimens on a chip. *Biosens. Bioelectron.* **224**, 115049 (2023).
58. Yuan, S., Liu, X., Zhou, X. & Li, Z. Multiple-image encryption scheme with a single-pixel detector. *J. Mod. Opt.* **63**, 1457–1465 (2016).
59. Yang, L. et al. Lensless polarimetric coded ptychography for high-resolution, high-throughput gigapixel birefringence imaging on a chip. *Photon. Res.* **11**, 2242–2255 (2023).
60. Bai, B. et al. To image, or not to image: class-specific diffractive cameras with all-optical erasure of undesired objects. *eLight* **2**, 14 (2022).
61. Bai, B. et al. Data-class-specific all-optical transformations and encryption. *Adv. Mater.* **35**, 2212091 (2023).
62. Liu, Y. et al. Robust far-field imaging by spatial coherence engineering. *Opto-Electron. Adv.* **4**, 210027–1 (2021).
63. Bian, L. et al. *Complex-Domain Enhancing Neural Network for Large-scale Coherent Imaging* (SPIE, 2022).
64. Hou, J. & Situ, G. Image encryption using spatial nonlinear optics. *eLight* **2**, 3 (2022).
65. Maiden, A. M. & Rodenburg, J. M. An improved ptychographical phase retrieval algorithm for diffractive imaging. *Ultramicroscopy* **109**, 1256–1262 (2009).
66. Jiang, S. et al. Resolution-enhanced parallel coded ptychography for high-throughput optical imaging. *ACS Photonics* **8**, 3261–3271 (2021).
67. Shi, T., Guo, W., Yang, L. & Li, A. Remote wideband data acquiring system based on zc706 and ad9361. In *IEEE International Wireless Symposium (IWS)* 1–4 (IEEE, 2015).
68. Shen, F. & Wang, A. Fast-fourier-transform based numerical integration method for the Rayleigh–Sommerfeld diffraction formula. *Appl. Opt.* **45**, 1102–1110 (2006).
69. Steward, E. G. *Fourier Optics: An Introduction* (Courier Corporation, 2004).
70. Liao, X., Li, H. & Carin, L. Generalized alternating projection for weighted-2,1 minimization with applications to model-based compressive sensing. *SIAM J. Imaging Sci.* **7**, 797–823 (2014).
71. Yuan, X. Generalized alternating projection based total variation minimization for compressive sensing. In *IEEE International Conference on Image Processing (ICIP)*, 2539–2543 (IEEE, 2016).

Acknowledgements
This work was supported by the National Natural Science Foundation of China under Grants 62322502 (L.B.), 61827901 (J.Z. and L.B.), and 62088101 (J.Z. and L.B.), the Guangdong Province Key Laboratory of Intelligent Detection in Complex Environment of Aerospace, Land and Sea under Grant 2022KSYS016 (L.B.), and BIT Research and Innovation Promoting Project under Grant 2022YCXZ006 (X.C. and L.B.).

Author contributions
L.B. and X.C. conceived the idea. X.C., S.J., L.Y., X.Z., D.L., and R.Y. conducted the simulations and experiments. S.J. and L.Y. built the prototype and collected data. X.C., S.L., and Z.G. built the wireless communication system. J.Z. and L.B. supervised the project. All the authors contributed to writing and revising the manuscript, and participated in discussions during the project.

Competing interests
L.B., X.C., and J.Z. hold patents on technologies related to the devices developed in this work (China patent numbers ZL 2020 1 0534696.1, ZL 2020 1 1157900.9, ZL 2020 1 1157901.3, and ZL 2021 1 0214825.3) and submitted related patent applications. The remaining authors declare no competing interests.

Additional information
Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41467-024-54168-3.

Correspondence and requests for materials should be addressed to Liheng Bian or Jun Zhang.

Peer review information *Nature Communications* thanks Shumin Xiao and the other, anonymous, reviewer(s) for their contribution to the peer review of this work. A peer review file is available.