OET | Opto-Electronic Technology

Multiple degrees-of-freedom optical encryption via pixel-resolved vectorial holography

Jianzhong Peng, Haoxian Zhou, Mengzhe Shen, Dapeng Wang*, Yu Chen, Renlong Zhang, Fangrui Lin, Xiaoyu Weng* and Junle Qu*

https://doi.org/10.29026/oet.2026.260018



Opto-Electronic Technology

CN 51-1811/O4 ISSN (Print) 2097-6003 ISSN (Online) 2097-8006

Multiple degrees-of-freedom optical encryption via pixel-resolved vectorial holography

Jianzhong Peng, Haoxian Zhou, Mengzhe Shen, Dapeng Wang*, Yu Chen, Renlong Zhang, Fangrui Lin, Xiaoyu Weng* and Junle Qu*

Citation: Peng JZ, Zhou HX, Shen MZ et al. Multiple degrees-of-freedom optical encryption via pixel-resolved vectorial holography. *Opto-Electron Technol* **2**, 260018 (2026).

https://doi.org/10.29026/oet.2026.260018

Received: 21 May 2026; Accepted: 13 July 2026; Published online: 22 September 2026

Related articles

Reconfigurable origami chiral response for holographic imaging and information encryption

Zhibiao Zhu, Yongfeng Li, Jiafu Wang, et al

Opto-Electronic Science 2025, **4**(4): 240026 doi: 10.29026/oes.2025.240026

Dynamic interactive bitwise meta-holography with ultra-high computational and display frame rates

Yuncheng Liu, Ke Xu, Xuhao Fan, et al

Opto-Electronic Advances 2024, **7**(1): 230108 doi: 10.29026/oea.2024.230108

Femtosecond laser maskless direct writing of dual-band crosstalk-free information for all-in-one high-security encryption metasurface

Hanmian Jiang, Zhuguo Li, Dongshi Zhang

Opto-Electronic Advances 2026, **9**(4): 250303 doi: 10.29026/oea.2026.250303

Partially coherent optical chip enables physical-layer public-key encryption

Bo Wu, Wenkai Zhang, Hailong Zhou, et al

Opto-Electronic Advances 2025, **8**(11): 250098 doi: 10.29026/oea.2025.250098

More related articles in Opto-Electronic Journals Group website

Opto-Electronic Journals Group

https://www.oejournal.org

OE_Journal

@OptoElectronAdv

OET | Opto-Electronic Technology

Article

September 2026, Vol. 2, No. 3

Open Access

Multiple degrees-of-freedom optical encryption via pixel-resolved vectorial holography

Jianzhong Peng[1], Haoxian Zhou[1], Mengzhe Shen[2], Dapeng Wang[2]*, Yu Chen[1], Renlong Zhang[1], Fangrui Lin[1], Xiaoyu Weng[1]* and Junle Qu[1]*

Abstract: Optical encryption is pivotal to modern information security, however, conventional techniques mainly rely on the conjugated Fourier-transform relation between recording phase and retrieval information, making them vulnerable to iterative decryption attack. Although the synergy of multiple degrees of freedom (DoFs), such as optical metasurface platforms, offers a potential solution, the pixel-scale localized encrypting specific to confidential information (e.g., letters or patterns) remains elusive. To address this issue, we propose the vectorial optical pen to sketch optical foci for achieving pixel-resolved vectorial holograms. Moreover, the ciphertexts are simultaneously encoded by multiple DoFs, inherently resisting unauthorized access. Specifically, we convert the holographic plaintext (i.e., letters) to the ASCII codes for perfectly-matching the orthogonal polarization modes, yielding ultralow crosstalk and high security. The proposed dynamic and versatile system offers a practical route to high-capacity and high-confidentiality optical cryptography in the big-data era.

Keywords: optical encryption; vectorial holography; optical pen

DOI: 10.29026/oet.2026.260018 | CSTR: 32419.14.oet.2026.260018

Citation: Peng JZ, Zhou HX, Shen MZ et al. Multiple degrees-of-freedom optical encryption via pixel-resolved vectorial holography. *Opto-Electron Technol* **2**, 260018 (2026).

1 Introduction

Information security plays a vital role in modern technological development, whereas contemporary cutting-edge techniques face an ongoing demand for high-fidelity and confidential communication. Optical encryption has garnered significant attention due to its inherent advantages of high-speed parallel processing, multiplexing capacity, and low energy consumption[1–8]. Compared with electron-based information carriers, light possesses more DoFs such as wavelength/frequency, polarization, phase and orbital angular momentum (OAM)[9]. The ability to modulate these DoFs, either individually or in a multiplexed manner, paves the way for developing secure and efficient cryptographic system[10,11].

As the first demonstration of optical encryption, double random phase encoding (DRPE) was initially proposed[2,12,13] and subsequent variant alternatives, e.g., phase-truncated transform[14,15], diffraction-based encryption[16,17], and interference-based encryption[18], have made incredible progress. Nevertheless, the new era of big data raises a fundamental requirement for high-capacity information storage and communication[19]. In this context, optical encryption technologies have evolved to utilize the multi-dimensional physical properties of light for information encoding and encryption. Among various implementations, spatial light modulators (SLMs) establish an indispensable paradigm for actively unlocking these multi-dimensional physical properties at the macroscopic level[20]. Driven by computer-generated holograms, SLM-based systems dynamically shape the optical wavefront to construct structured light fields with desired complex amplitude[21,22]. Through this programmable flexibility, cryptographic information can be concurrently multiplexed into orthogonal DoFs[23–30]. However, the modulation precision of SLM is fundamentally restricted by the diffraction limit. In contrast, optical metasurfaces composed of

Received: 21 May 2026

Accepted: 13 July 2026

Published online: 22 September 2026

[1]State Key Laboratory of Radio Frequency Heterogeneous Integration & Key Laboratory of Optoelectronic Devices and Systems, College of Physics and Optoelectronic Engineering, Shenzhen University, Shenzhen 518060, China; [2]State Key Laboratory of Genome and Multi-omics Technologies, BGI Research, Shenzhen 518083, China.

*Correspondence: DP Wang, E-mail: wangdapeng@genomics.cn; XY Weng, E-mail: xiaoyu@szu.edu.cn; JL Qu, E-mail: jlqu@szu.edu.cn

high-density subwavelength antennas have emerged as promising candidates because of the capacity of encoding multi-DoFs within a chip-scale device[31,32]. In general, the encryption principle of metasurfaces depends on the wavefront modulation, where the building blocks respond to the polarization or amplitude components of light vectors[33]. Consequently, the cryptographic patterns can be encoded via the wavelength[34–36], polarization[37–46], space division, and high-order OAM modes[47,48]. To further improve the decryption fidelity, hybrid mode encoding strategies have progressively evolved from dual-combinations (e.g., wavelength and polarization[49–58], OAM and polarization[59], OAM and wavelength[60]) to the simultaneous manipulation of three or more DoFs[61,62]. Furthermore, to overcome the inherent limitation that static metasurfaces remain structurally inflexible once fabricated, researchers have developed dynamic metasurfaces by incorporating space-time reconfigurable metamaterials[63–69], stimuli-responsive liquid crystals[70,71], and advanced neural network designs[72–74]. Triggered by external stimuli such as thermal or electrical fields, these active platforms can dynamically reconfigure their nanostructures, thereby achieving dynamic and real-time information encryption[75].

However, current optical encryption methods are often plagued by the crosstalk because routine encoding mechanism, i.e., symmetric-key utilization for both the encryption of plaintext and the decryption of ciphertext, are susceptible to the ciphertext attack[14,15,76]. The vulnerability stems from the conjugated relationship between the encrypted information (message or pattern) and the codebook through iterative Fourier transforms. Such weaknesses would be mitigated if the encrypting can be pixel-by-pixel resolved in real space and modulated by the vectorization of information. Unfortunately, pixel-resolved vectorial holography remains elusive. To address this issue, our previous efforts specific to the optical pen (OP) have demonstrated of arbitrary optical foci at the image plane[77–79]. To further advance towards a vectorial optical pen (VOP), we herein synergize the spatial location, polarization, and OAM modes into discrete vectorial foci. Constructed by these discrete foci, the vectorial patterns are exquisitely encoded with multiple DoFs at the pixel level, the system exhibits strong resistance to unauthorized access and intrinsic crosstalk.

In this work, we initially leverage the VOP to construct a dynamicaland secure optical encryption system based on the SLM platform. Unlike cascaded multi-step encoding schemes[14], we encrypt plaintext (e.g., letters) by converting their ASCII codes into holographic patterns encoded by specific OAM and two orthogonal polarization modes. The holographic phase serves as the ciphertext, which is highly sensitive to the parameters of the incident vector beam. The low-crosstalk analyses confirm that decryption definitely fails without the correct incident OAM order and polarization states, validating the system's security and robustness. Our approach effectively surmounts the complexity of traditional optical encryption systems by means of dynamic pixel-resolved modulation, simultaneously enhancing security, information capacity, and flexibility.

2 Results and discussion

2.1 Principle of pixel-resolved optical cryptography

Figure 1 presents a schematic of multiple DoFs optical encryption based on pixel-resolved vectorial holography. The optical encryption system is composed of a multiple DoFs encryption (Fig. 1(a)) and a mode decryption module (Fig. 1(b)). In the multiple DoFs encryption system, the VOP serves as the core component for encoding multi-DoFs by integrating OAM, spatial location, and polarization. This functionality is realized by combining an OP[77] with a vortex polarizer (VP). The holographic phase of the OP governs the encoding of scalar DoFs—specifically, OAM and spatial location—while the VP transforms a linearly polarized beam into a m-order vector vortex beam (VVB), thereby enabling polarization state encoding. In the mode decryption system, the objective lens performs a Fourier transform, thereby retrieving the encrypted multi-dimensional optical information within its focal region.

According to the physical concept of the OP, the imaging plane can be regarded as a drawing canvas, where each optical focus generated by the OP functions as an individual brushstroke. Therefore, one can not only create arbitrary light patterns, but also encode multiple DoFs, including OAM, spatial location, and polarization, for each focus within the light patterns, thereby enabling pixel-resolved optical cryptography. Taking the mode decryption in Fig. 1(c) as an example, the concealed information such as the letter “Z” is encypted by converting it to the ASCII code “90” in which the digits “9” and “0” can be selectively encoded in two orthogonal polarization states. In this encryption system, the holographic phase of the OP loaded onto the SLM serves as the ciphertext, which is highly sensitive to the parameters of the incident light beam, as shown in Fig. S1. If an inappropriate input beam is applied, the retrieved intensity distribution will be altered, causing the encoded optical pattern to become distorted or unrecognizable, thereby ensuring the security of the optical encryption. To validate the pixel-level dynamic modulation capability of VOP and its suitability for optical encryption, we conducted two demonstration experiments using this system.

2.2 Scheme for encoding multiple DoFs

In the first demonstration, as shown in Fig. 2, through the modulation of the VOP, we successfully generated a light pattern "S" with distinct polarization states and a light pattern "L" carrying specific OAM within localized regions on the focal plane of the objective lens. The light pattern “S” consists of 41 optical foci, each corresponding to $|\boldsymbol{RVVB}_{0,\beta}\rangle$, with a distinct linear polarization direction, enabling

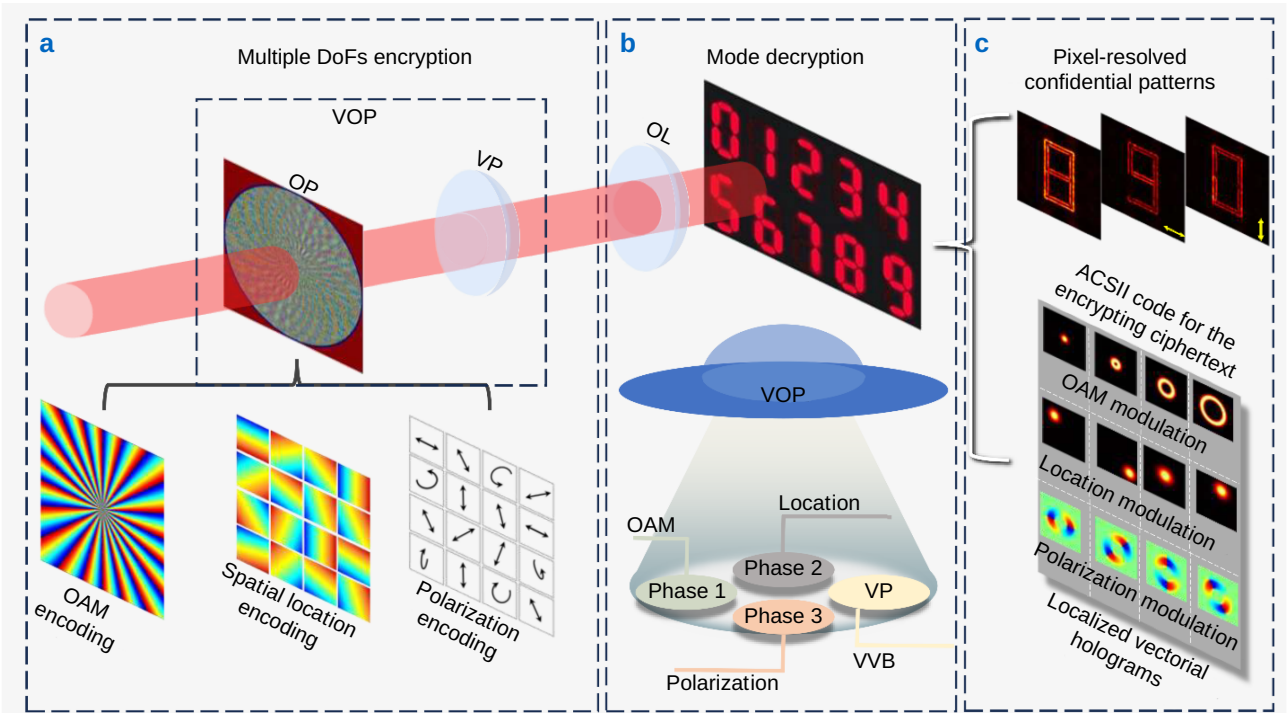

Fig. 1 | Conceptual principle of pixel-resolved optical cryptography. (a) Multiple DoFs encoding process. For a targeted pattern, the VOP is used to encode the multiple DoFs including OAM, spatial location, and polarization modes of the light beam. The VOP is composed of an OP holographic phase loaded onto the SLM together with a VP. The OP holographic phase serve as the ciphertext for the encryption system, while the incident beam generated by the VP serves as the key. (b) Mode decryption. The light beam modulated by the VOP undergoes a Fourier transform via an objective lens, is focused through the objective, decoding into optical focus of corresponding modes on the imaging plane. These focus can be dynamically combined to form arbitrary light patterns. (c) Holographic retrive of pixel-resolved confidential patterns. Plaintext information is concealed within the light pattern through specific encoding. Successful decryption requires simultaneously satisfying the light beam parameters imposed by the VP key, thereby ensuring a high level of security.

gradual intensity variation when observed through a polarizer in any orientation. (Where $|\boldsymbol{RVVB}_{\sigma,\beta}\rangle = \left[\begin{array}{cc}\cos(\sigma\varphi+\beta) & \sin(\sigma\varphi+\beta)\end{array}\right]^{\mathrm{t}}$ denotes a linearly polarized mode with a topological charge of σ and a polarization direction of β, here $\sigma = 0$.) The light pattern "L" is composed of 17 optical foci, each corresponding to $|\boldsymbol{RVVB}_{-1,0}\rangle$, and the OAM carried by these foci produces a hollow structure in the pattern. The results indicate that the variation of OAM order leads to distinct polarization responses in their light patterns. Therefore, changing the OAM inevitably alters the pattern's morphology. This confirms the VOP's outstanding pixel-level dynamic modulation capability, which can be leveraged for flexible optical encryption with low cost and complexity. Videos S1 and S2 show the dynamic hologram variation in real-time by means of the polarization state modulation for the light pattern "S" and the light pattern "L" respectively. The specific OP holographic phase parameters used to generate patterns "S" and "L" are provided in Supplementary Note 6. Additional simulation and experimental results of light patterns are provided in Figs. S9–S14.

2.3 Encryption of plaintext information using ASCII code

In the second demonstration, we designed an encryption process and conducted corresponding simulations and experimental validations. Firstly, based on the correspondence between each uppercase letter and its ASCII code (as shown in Table 1), each letter is converted into a unique two-digit number, thereby digitizing the plaintext. Secondly, the generated focal spots are engineered to form a specific light pattern. This pattern, when projected under specific orthogonal polarization states, reveals the tens and units digits of the ASCII-encoded number, respectively. Finally, a second layer of encryption is added using OAM ensures that incorrect order incident light cannot retrieve the information. As shown in Fig. 3(a), the loaded holographic phase serves as the ciphertext of this system, while the incident light with the correct order and specific polarization state acts as the key. Decryption is successful only when the key matches the ciphertext. More details of this encryption mechanism can be found in Supplementary Section 2.

As shown in Fig. 3, we employed this optical encryption system to encrypt the uppercase letters "S", "Z", and "U",

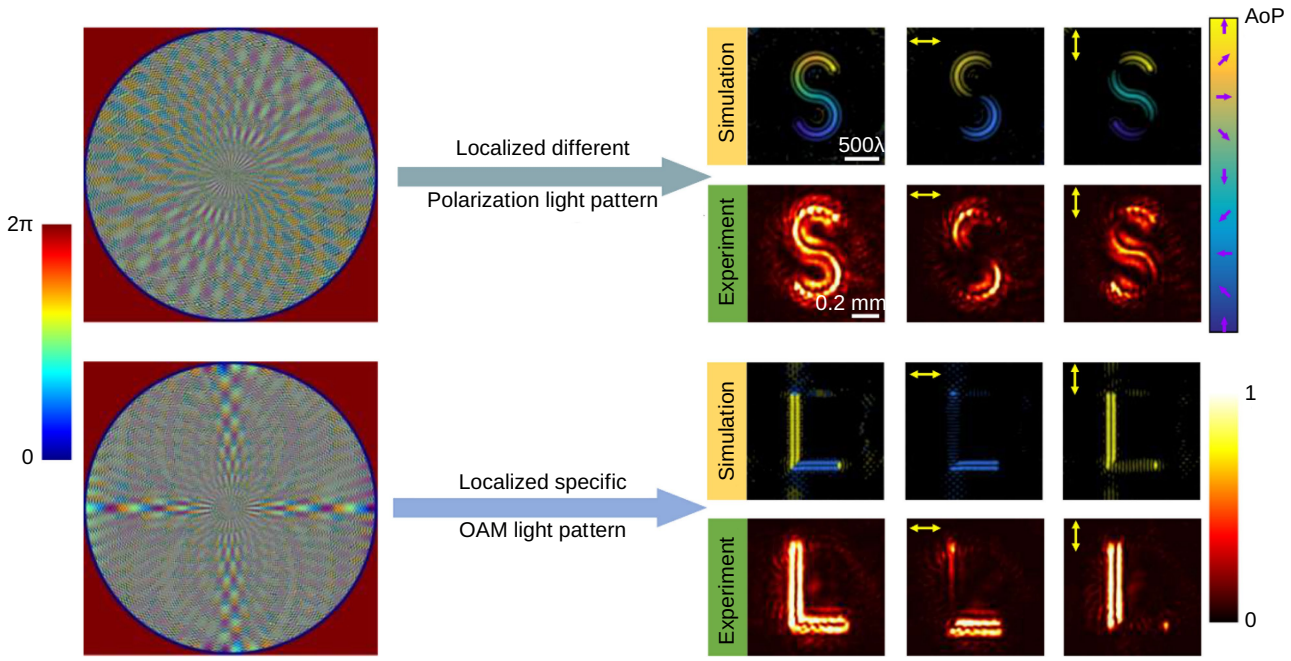

Fig. 2 | Simulation and experimental realization of pixel-level patterns. By employing the modulation capability of the VOP, the light patterns "S" and "L" are successfully generated on the imaging plane, which are constituted by optical foci with different polarization states and foci carrying specific OAM, respectively. The colored simulation maps indicate the polarization angles of the "S" and "L" patterns, and the purple arrows within the polarization colorbar represent the corresponding polarization directions. Concurrently, the experimental results represent the intensity distributions of the patterns. The yellow arrows denote the transmission axes of the polarizers. The intensity is normalized to unity, and the phase is scaled from 0 to 2π.

Table 1 | Uppercase letters and their corresponding ASCII codes. We exploit the SZU, CUTE, PUPPY and their codes for the concealed ciphertext in the subsequent experiment.

Character	ASCII	Character	ASCII	Character	ASCII
A	65	J	74	**S**	**83**
B	66	K	75	**T**	**84**
C	**67**	L	76	**U**	**85**
D	68	M	77	V	86
E	**69**	N	78	W	87
F	70	O	79	X	88
G	71	**P**	**80**	**Y**	**89**
H	72	Q	81	**Z**	**90**
I	73	R	82		

which correspond to the ASCII codes 83, 90, and 85, respectively. By precisely modulating the VOP, we generated a series of light patterns composed of specific optical foci corresponding to $\exp \mathrm{i}(-\varphi-\beta)|\boldsymbol{L}\rangle$ (denotes a left circularly polarized mode with a topological charge of -1 and a polarization direction of β), $|\boldsymbol{RVVB}_{-1,0}\rangle$, and $|\boldsymbol{RVVB}_{-1,\pi}\rangle$. The ASCII codes were split, with the tens digit displayed in the horizontal polarization direction and the units digit in the vertical polarization direction. The corresponding decryption results (see Fig. 3(c) and 3(d)) demonstrate that the correct ASCII information can only be retrieved when a 32-order VVB is used as the incident light and its polarization state matches the encoding condition. The specific OP holographic phase parameters used to encrypt the uppercase letters “SZU”, “CUTE”, and “PUPPY” are provided in Supplementary Section 6.

2.4 Security analysis of the encryption system

In Fig. 3(b), we present the simulation results obtained when the OAM and polarization conditions do not meet the correct decryption conditions. For instance, when no polarizer is used in the decryption path, the observer can only see an ambiguous number "8", failing to retrieve the actual

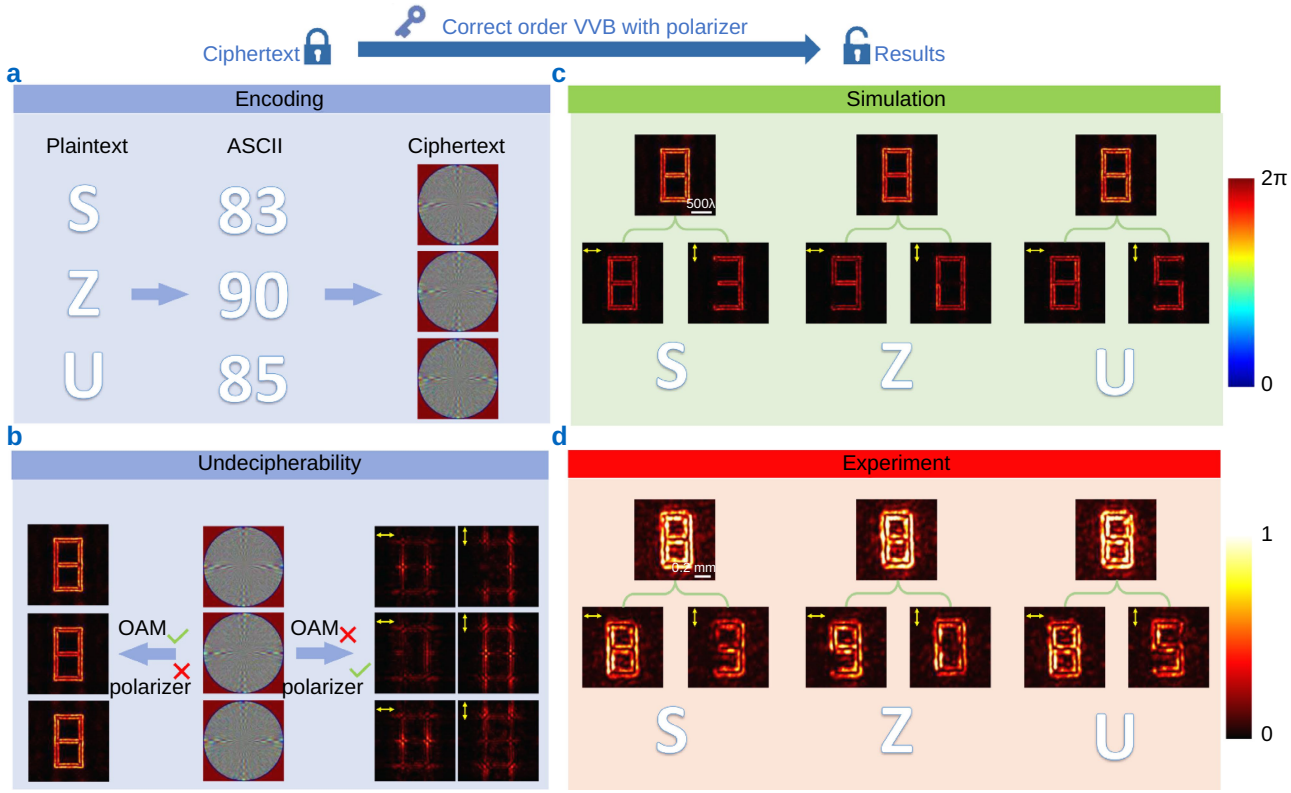

Fig. 3 | Demonstration of the high-security optical encryption system. (a) Flow diagram illustrating the conversion of plaintext into ciphertext. The ASCII codes of the uppercase letters "S", "Z", and "U" are 83, 90, and 85, respectively, and these codes can be encrypted via the OP holographic phase. (b) When incorrect parameters of incident light are applied to the holographic phase, the encrypted results are undecipherable, which proofs the capacity of high security of the proposed encryption system. (c) Simulation results by using the correct incident light. Under the proper orthogonal polarization states, the encrypted information "S", "Z", and "U" can be correctly decrypted. (d) Experimental results in accordance with the simulations. The intensity is normalized to unity, and the phase is scaled from 0 to 2π.

encrypted information. When the OAM of the incident light does not meet the required condition, different topological charges result in distinct light patterns. For instance, an 11-order beam generates a pattern composed of optical foci corresponding to $\exp \mathrm{i}(-20\varphi-\beta)|\boldsymbol{L}\rangle$, $|\boldsymbol{RVVB}_{-20,0}\rangle$, $|\boldsymbol{RVVB}_{-20,\pi}\rangle$, whereas a 21-order beam produces a pattern composed of optical foci corresponding to $\exp \mathrm{i}(-10\varphi-\beta)|\boldsymbol{L}\rangle$, $|\boldsymbol{RVVB}_{-10,0}\rangle$, $|\boldsymbol{RVVB}_{-10,\pi}\rangle$. These patterns from incorrect keys are meaningless, preventing unauthorized extraction of correct information. To quantitatively evaluate the security of this encryption system, we introduce a morphological crossing-feature extraction algorithm[80,81], designed to recognize structural features and identify the category of the decoded digits, to directly calculate the recognition probability of the decrypted results. (The detailed principles and mathematical models of this algorithm are provided in the Supplementary Note 4.) We independently perform morphological crossing-feature extraction on the specific optical simulation results generated by the 11-order, 21-order, 31-order (incorrect keys), and 32-order (correct key) incident light, as shown in Fig. 4(a), and present the recognition probability distributions of different digits in the x and y polarization directions in Fig. 4(b) and 4(c). Since the complete ASCII information is encoded in two orthogonal polarization states and requires simultaneous decoding, we multiply the predicted probabilities of the target features in these two directions to obtain the ultimate joint decoding probability, as quantitatively summarized in Fig. 4(d). The results reveal that the joint probabilities for the 11-order, 21-order, and 31-order keys are nearly 0.0%, whereas the joint probability for the 32-order key reaches 96.8%. This indicates that the proposed system possesses extreme sensitivity to the OAM order of the incident vortex light. Even if the incorrect key differs from the correct key by only 1 order, an unauthorized access is highly unlikely to extract the correct structural information from the distorted results. These tests confirm that no information leakage occurs when the incident light OAM order is incorrect, thus validating the high security of the proposed encryption scheme.

3 Conclusions

The encryption method proposed in this paper enhances the

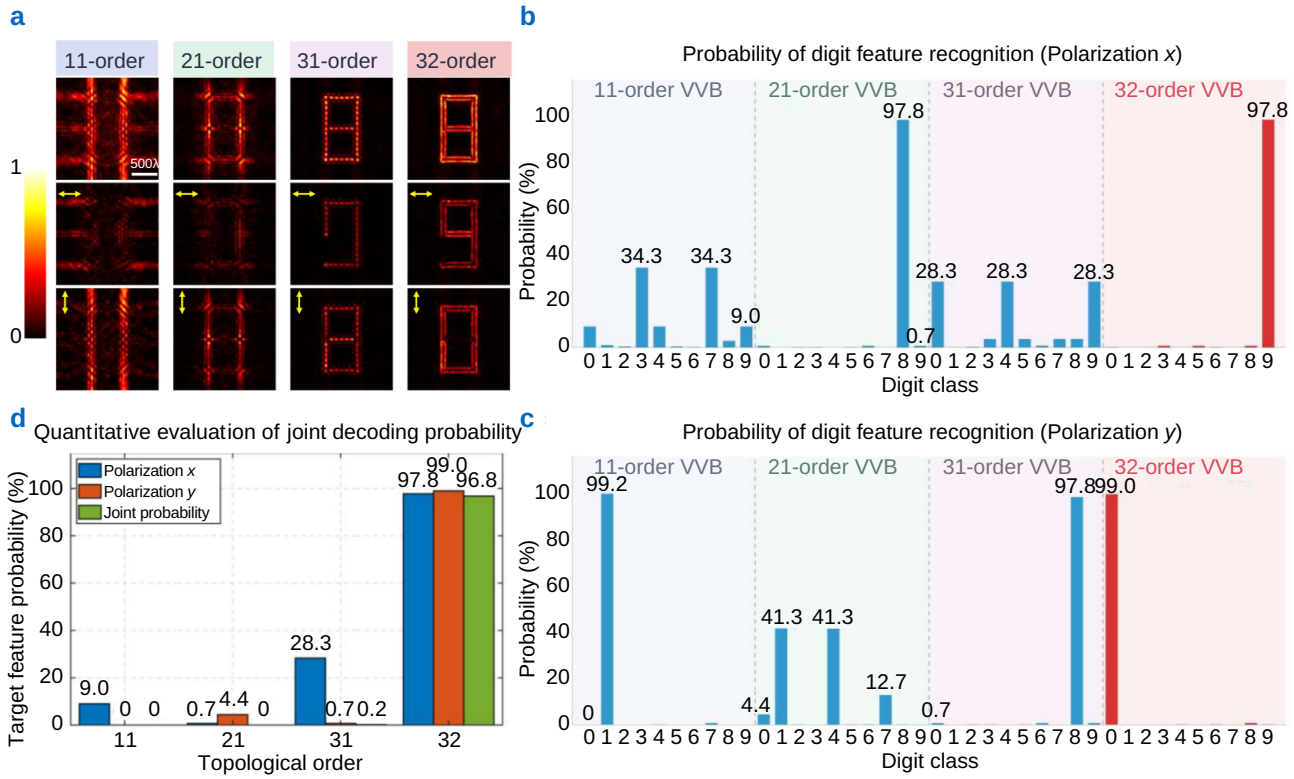

Fig. 4 | Security analysis of the optical encryption system. (a) Distinguishable visual results. Simulation results under 11, 21, 31, and 32-order OAM incident light conditions, where the yellow arrows represent the simulation results obtained after adding polarizers in the corresponding polarization directions. The intensity is normalized to unity. (b, c) Quantitative probability analysis. The recognition probability distributions of different digit classes (0–9) for the decrypted results in the (b) *x* polarization direction and (c) *y* polarization direction. The probabilities are independently calculated using the morphological crossing-feature extraction algorithm. (d) Joint decoding probability analysis. The target recognition probabilities in the *x* and *y* polarization directions and the calculated ultimate joint decoding probabilities under 11, 21, 31, and 32-order OAM incident light conditions.

modulation resolution of the encryption system to the scale of the focal spot size, achieving high spatial resolution and pixel-resolved precision. By enabling independent control of multiple DoFs for each focus, the encryption key space is expanded into multiple physical dimensions, thereby effectively resisting unauthorized decryption attempts. Security analysis demonstrates that correct information cannot be retrieved when using incident light with incorrect polarization or OAM modes. Cross-correlation analysis further quantitatively verifies the remarkably low similarity between the information decrypted with incorrect keys and the original data, robustly affirming the high security of the proposed system.

A key advantage of this encryption scheme is its implementational diversity, allowing encryption through different focal spot combinations (see Figs. S5–S8), providing user flexibility. Both simulated and experimental results confirm that different combinations yield different encryption outcomes, allowing users to select suitable combinations based on specific needs.

In the demonstration system designed in this work, encryption was validated specifically for the case where the tens and units digits of the ASCII code combine to form the numeral "8" under orthogonal polarization states. If the combination does not result in "8", the decryption appearance under incorrect polarization might differ from other characters, potentially compromising stealth. It is noteworthy that our demonstration serves as a proof of concept; the system's capability extends far beyond this specific case. Leveraging the flexibility of the VOP, users can design more sophisticated schemes. For instance, a computational random seed can be used to drive the VOP to generate an optical white-noise field composed of multi-mode foci, within which information is concealed. Authorized users can decrypt the message by applying the same seed for filtering. This approach of "actively engineering" noise offers security superior to conventional methods of randomly adding noise. Furthermore, the system's security and information capacity can be significantly enhanced by incorporating additional DoFs (e.g., wavelength, angle of incidence) or employing more polarization channels.

To explicitly delineate the conceptual advancement of the proposed work relative to typical and state-of-the-art optical encryption schemes, a systematic comparison is

summarized in Table S1. While the proposed VOP framework presents a highly secure and dynamically programmable pixel-resolved encryption system, the current experimental validation is performed using a conventional SLM-based architecture. Because the fundamental physical mechanism of the VOP is being demonstrated for the first time, the SLM serves as an ideal and highly flexible testbed, enabling the rapid and intuitive verification of the modulation effects of localized multi-dimensional physical parameters. However, it is important to objectively acknowledge the inherent limitations of this initial architecture. Compared to state-of-the-art integrated photonics and metasurfaces, the SLM system inevitably encounters challenges such as a bulky optical footprint, reduced diffraction efficiency, and lower dynamic refresh rates. To overcome these limitations, subsequent research will consider employing integrated platforms or metasurfaces to implement this mechanism, thereby achieving both extreme device miniaturization and high-efficiency dynamic programmability.

In conclusion, we propose a multi-DoFs optical encryption via pixel-level vectorial holography. By leveraging the powerful modulation capability of the VOP, pixel-resolved of optical patterns with tunable polarization, spatial location and OAM can be generated. By flexibly combining these foci into complex information carrying patterns, we enable locally adjustable, multi-DoF holographic displays. This approach overcomes the pixel-level dynamic control limitations of existing technologies and significantly boosts the system's security and information capacity. Utilizing this powerful tool, we design and implement a straightforward optical encryption system, successfully encrypting various letters and words. Correlation analysis confirms the system's robustness against unauthorized decryption, unequivocally validating the powerful functionality of this method for advanced optical encryption applications.

4 Materials and methods

4.1 Scheme for encoding multiple DoFs

As shown in Fig. 1, the VOP is the core component for multi-DoF encoding in the encryption system, which is composed of OP and VP. Therefore, the light beam carrying the encrypted multi-dimensional optical information emerging from the VP can be expressed as[78]

$$\boldsymbol{E}_{\mathrm{VOP}} = T_{\mathrm{op}} \cdot \boldsymbol{E}_{\mathrm{VVB}} \ , \tag{1}$$

where $\boldsymbol{E}_{\mathrm{VVB}} = \left[\begin{array}{cc} \cos(m\varphi + \sigma_0) & \sin(m\varphi + \sigma_0) \end{array} \right]^{\mathrm{t}}$ denotes the appropriate incident m-order VVB used to decrypt the multi-dimensional optical information in the focal region of OL, φ is the azimuthal angle, and t denotes the matrix transpose operator. In this paper, $\sigma_0 = 0$.

T_{op} represents the transmittance of OP, and can be written as

$$T_{\mathrm{op}} = \sum_{j=1}^{N} \left[\mathrm{PF}(s_j, x_j, y_j, z_j, \delta_j) \cdot \exp(\mathrm{i}\phi_j) \right] \ . \tag{2}$$

According to Eq. (2), there are two key pieces of information contained in the incident m-order VVB. One is the scalar mode modulation function $\mathrm{PF}(s_j, x_j, y_j, z_j, \delta_j)$, which is derived using optical path compensation, where x_j, y_j, z_j denote the position of the j-th focus in the focal region, the maximum of j being the total number of foci N; and s_j and δ_j are the parameters that can be used to adjust the amplitude and phase of the j-th focus, respectively. The other is the vector mode modulation function factor of polarization modes $T_j = \exp(\mathrm{i}\phi_j)$.

In the case of encoding scalar DoFs, the spatial location of each focus can be adjusted by the parameters N, x_j, y_j, z_j, while their respective OAM can be independently modulated by $\delta_j = l_j\varphi$, where l_j is the topological charge of the j-th focus. In the case of encoding vector DoF, when modulating by $T_j = \exp(\mathrm{i}\phi_j)$ in Eq. (2) induces different polarization response in the focal region of OL. One can simply extract a single polarization mode from the incident m-order VVB in Eq. (1). In this way, the relationship between the phase in Eq. (3) and the polarization of the j-th focus in Eq. (4) can be established (More details can be found in ref.[79]).

$$\begin{aligned} \phi_j = & \mathrm{Phase} \left\{ \cos\varphi_0 \exp \mathrm{i} \left(m\varphi - \beta_j \right) \right. \\ & \left. + \sin\varphi_0 \exp \left[-\mathrm{i} \left(m\varphi_j - \beta_j \right) \right] \right\} \ , \end{aligned} \tag{3}$$

$$\boldsymbol{E}_{\mathrm{PA}} = \cos\varphi_0 \exp(-\mathrm{i}\beta_j) \left| \boldsymbol{L} \right\rangle + \sin\varphi_0 \exp(\mathrm{i}\beta_j) \left| \boldsymbol{R} \right\rangle \ , \tag{4}$$

where φ_0 is a weight factor that adjusts the relative contributions of left and right circular polarization mode $|\boldsymbol{L}\rangle$ and $|\boldsymbol{R}\rangle$. That is, the polarization of each focus can be encoded by the phase applied to the wavefront of OL in Eq. (3).

Theoretically speaking, the phase encodings for OAM, spatial position, and polarization in Eq. (2) correspond to three distinct phase components, denoted as ψ_1, ψ_2, ψ_3, respectively. Although these encodings are superimposed into the overall OP holographic phase, they possess independent transmittance coefficients, which can be expressed as $\exp(\mathrm{i}\psi_1)$, $\exp(\mathrm{i}\psi_2)$, and $\exp(\mathrm{i}\psi_3)$. Consequently, the control of these three corresponding DoFs operates independently without mutual interference.

4.2 Realization of VOP based on mode extraction

As mentioned, the multiple DoFs—including OAM, spatial position, and polarization are superimposed into the overall OP holographic phase. However, Eq. (2) constitutes a complex-valued function, which encompasses not only the phase factor but also the amplitude. In this section, we aim to convert the complex function in Eq. (2) into a holographic phase while preserving the concealed information

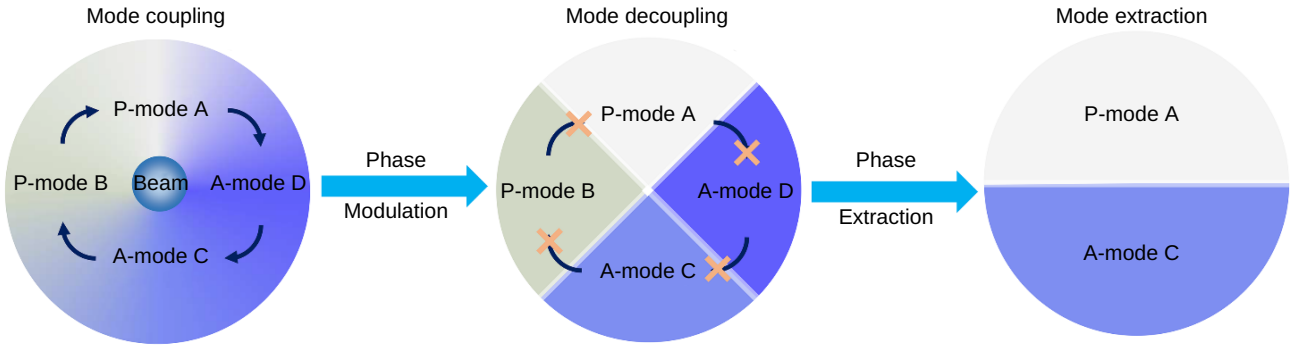

Fig. 5 | Schematic of vectorial holography based on the polarization-amplitude decoupling. The intrinsic polarization and amplitude modes of the beam always maintain mode coupling in free space, ensuring stable propagation. When special phase modulation is applied, this mode coupling is broken, achieving mode decoupling and enabling the separation between polarization and amplitude modes. Through mode extraction, the desired polarization and amplitude modes can be selectively obtained at the image plane, thereby achieving independent control of multiple DoFs including polarization, spatial location, and OAM.

encoded by the OAM, spatial position, and polarization of light beam. In general, Eq. (2) can be simplified as

$$T_{\mathrm{op}} = \cos\sigma_{\mathrm{amp}} \cdot \exp(\mathrm{i}\eta)\ , \tag{5}$$

where $\cos\sigma_{\mathrm{amp}}$ and η denote the amplitude and phase of Eq. (2), respectively.

From Eq. (5), the phase η can be directly obtained using a phase-only SLM. However, the amplitude $\cos\sigma_{\mathrm{amp}}$ cannot be directly obtained using a phase-only SLM. To address this issue, the amplitude $\cos\sigma_{\mathrm{amp}}$ is treated as a desired amplitude mode within the m-order VVB. Based on the principle of mode extraction, the desired amplitude mode A-Mode C and the undesired amplitude mode A-Mode D correspond to the real and imaginary components of the complex space, respectively. A 0–π binary phase pupil filter can be employed to selectively modulate these two modes, enabling the retention of the desired A-Mode C while eliminating the undesired A-Mode D. Therefore, the overall transmittance function of the SLM can be expressed as

$$T = \exp(\mathrm{i}\eta) \cdot (\cos\sigma_{\mathrm{amp}} + \mathrm{i}T_{\mathrm{imag}}\sin\sigma_{\mathrm{amp}})\ , \tag{6}$$

where $\exp(\mathrm{i}\delta_{\mathrm{phase}})\cos\phi_{\mathrm{amp}}$ and $\exp(\mathrm{i}\delta_{\mathrm{phase}})\sin\phi_{\mathrm{amp}}$ represent the desired and undesired amplitude modes, respectively. In the equation (6), $T_{\mathrm{imag}} = \exp(\mathrm{i}\varphi_{\mathrm{imag}})$, and φ_{imag} is a binary phase of 0–π. To eliminate the undesired mode, the phase of T_{imag} is adjusted to

$$\varphi_{\mathrm{imag}} = \mathrm{phase}\left[J_{10}\left(pk\sin\theta/NA\right) \cdot \cos\left(q\varphi\right)\right]\ , \tag{7}$$

where θ and NA denote the convergence angle and numerical aperture of the OL, respectively. The parameters p and q are adjustable, represent the radial scaling factor and the azimuthal modulation frequency, respectively, which physically disperse the undesired amplitude modes into the background. $J(\cdot)$ is the Bessel function of the first kind with order 10. While amplitude extraction inherently involves a certain degree of energy loss, it serves as a necessary approach to establish the strict correspondence between phase and amplitude, thereby laying a solid foundation for the realization of the proposed encryption system. Likewise, polarization mode extraction can also be achieved through a similar procedure as illustrated in Fig. 5, using the phase in Eq. (3). More details can be found in ref.[79].

4.3 Optical setup

We apply the proposed a VOP for high-security optical encryption system (see Fig. S1). A continuous-wave light source with a wavelength of 633 nm is used in the system. The beam is expanded threefold by a beam expander and passes through a polarizer, which is aligned with the liquid crystal arrangement of the SLM for polarization preparation. Upon incidence on the SLM, the beam carrys the holographic phase encoding generated by the VOP and is subsequently converted into a m= 32-order VVB by a VP. Finally, the beam is focused by an objective lens, and the decoded information at the image plane is recorded by a CMOS camera. In this optical setup, the SLM is conjugated with the VP via a 4f system consisting of two lenses (L1 and L2), and both devices are also conjugated with the CMOS imaging plane. The VP is implemented using q-plate technology[82–84].

References

1. Li XJ, Liu Y, Sun MZ et al. Computational ghost image encryption method based on sparse speckles. *Phys Scr* **99**, 025114 (2024).
2. Qiu MC, Chen JM, Chai XC et al. Optical image encryption with photo-thermoelectric device. *Opt Express* **33**, 29689–29700 (2025).
3. Hou JF, Situ GH. Image encryption using spatial nonlinear optics. *eLight* **2**, 3 (2022).
4. Pi DP, Gao L, Ye YQ et al. Direct laser writing 3D carbon dot array for orbital angular momentum holographic encryption. *Laser Photonics Rev* **20**, e01648 (2026).
5. Shang JY, Fang GQ, Yin XM et al. Dynamic multicolor upconversion through excitation pulse duration modulation toward machine learning assisted optical encryption. *Laser Photonics Rev* **19**, 2500465 (2025).

6. Zhang F, Guo YH, Pu MB et al. Meta-optics empowered vector visual cryptography for high security and rapid decryption. *Nat Commun* **14**, 1946 (2023).
7. Wang J, Lu X, Zeng QJ et al. High-security optical encryption using spin-orbital angular momentum matched structure light beam modes. *J Opt* **27**, 055101 (2025).
8. Chen W, Javidi B, Chen XD. Advances in optical security systems. *Adv Opt Photonics* **6**, 120–155 (2014).
9. Yang H, Ou K, Wan HY et al. Metasurface-empowered optical cryptography. *Mater Today* **67**, 424–445 (2023).
10. Bian LH, Chang XY, Jiang SW et al. Large-scale scattering-augmented optical encryption. *Nat Commun* **15**, 9807 (2024).
11. Zheng SJ, Tan JR, Liu HJ et al. Orthogonal matrix of polarization combinations: concept and application to multichannel holographic recording. *Opto-Electron Adv* **7**, 230180 (2024).
12. Refregier P, Javidi B. Optical image encryption based on input plane and fourier plane random encoding. *Opt Lett* **20**, 767–769 (1995).
13. Hazer A, Yıldırım R. A review of single and multiple optical image encryption techniques. *J Opt* **23**, 113501 (2021).
14. Cao B, Li J, Huang ZH. Phase-only asymmetric encryption based on coherent superposition and phase-truncated fourier transforms. *Opt Commun* **347**, 118–122 (2015).
15. Wang XG, Zhao DM. Amplitude-phase retrieval attack free cryptosystem based on direct attack to phase-truncated fourier-transform-based encryption using a random amplitude mask. *Opt Lett* **38**, 3684–3686 (2013).
16. Chen W, Chen XD, Sheppard CJR. Optical image encryption based on diffractive Imaging. *Opt Lett* **35**, 3817–3819 (2010).
17. Qin Y, Wang ZP, Wang HJ et al. Robust information encryption diffractive-imaging-based scheme with special phase retrieval algorithm for a customized data container. *Opt Lasers Eng* **105**, 118–124 (2018).
18. Zhang Y, Wang B. Optical image encryption based on interference. *Opt Lett* **33**, 2443–2445 (2008).
19. Liao MH, Zheng SS, Pan SX et al. Deep-learning-based ciphertext-only attack on optical double random phase encryption. *Opto-Electron Adv* **4**, 200016 (2021).
20. Fan XH, Xiong W, Xu K et al. Spatial light modulator via optically addressed metasurface. *Nat Nanotechnol* **21**, 561–570 (2026).
21. Yao YW, Zhang YP, He HR et al. Scale-invariant 3D face recognition using computer-generated holograms and the Mellin transform. *Opto-Electron Adv* **8**, 250095 (2025).
22. Yu X, Teng ZL, Fan XH et al. IncepHoloRGB: multi-wavelength network model for full-color 3D computer-generated holography. *Opto-Electron Adv* **8**, 250130 (2025).
23. Li KY, Wang YM, Pi DP et al. Multi-dimensional multiplexing optical secret sharing framework with cascaded liquid crystal holograms. *Opto-Electron Adv* **7**, 230121 (2024).
24. Xu X, Zhang RZ, Guo YH et al. Reprogrammable vector optical field meets planar liquid crystal elements for enhanced security in holography. *Laser Photonics Rev* **19**, 2401962 (2025).
25. Ma JY, Li Z, Zhao SM et al. Encrypting orbital angular momentum holography with ghost imaging. *Opt Express* **31**, 11717–11728 (2023).
26. Laxminarayan, Tripathi KK, Kumar P et al. Single-phase modulated optical skyrmions for information security applications. *Opt Express* **33**, 51116–51141 (2025).
27. Liu R, Li Y, Liu Y et al. Spatially varying polarization-structured optical fields via multi-focus synthesis for multidimensional image encryption. *Laser Photonics Rev* **20**, e01944 (2026).
28. Peng DM, Huang ZF, Liu YL et al. Optical coherence encryption with structured random light. *PhotoniX* **2**, 6 (2021).
29. Lin C, Wang L, Zhao SM. Petal orbital angular momentum multiplexing holography for two-dimensional optical encryption. *Appl Opt* **64**, 5407–5415 (2025).
30. Ding CX, Shao RJ, Qu Y et al. Spatial full degree-of-freedom scattered optical field modulation. *Laser Photonics Rev* **17**, 2300104 (2023).
31. Wang XC, Díaz-Rubio A, Tretyakov SA. Independent control of multiple channels in metasurface devices. *Phys Rev Appl* **14**, 024089 (2020).
32. He DJ, Wan YJ, Dong YJ et al. Ultra-high-capacity full-vectorial meta-holography. *Opto-Electron Adv* **9**, 250281 (2026).
33. Yang H, He HR, Hu YQ et al. Metasurface-empowered vector light field regulation, detection and application. *Opto-Electron Eng* **51**, 240168 (2024).
34. Liu X, Huang Z, Zang JF. All-dielectric silicon nanoring metasurface for full-color printing. *Nano Lett* **20**, 8739–8744 (2020).
35. Wang B, Dong FL, Li QT et al. Visible-frequency dielectric metasurfaces for multiwavelength achromatic and highly dispersive holograms. *Nano Lett* **16**, 5235–5240 (2016).
36. Wei QS, Sain B, Wang YT et al. Simultaneous spectral and spatial modulation for color printing and holography using all-dielectric metasurfaces. *Nano Lett* **19**, 8964–8971 (2019).
37. Zhang SF, Huang LL, Li X et al. Dynamic display of full-stokes vectorial holography based on metasurfaces. *ACS Photonics* **8**, 1746–1753 (2021).
38. Xiong B, Liu Y, Xu YH et al. Breaking the limitation of polarization multiplexing in optical metasurfaces with engineered noise. *Science* **379**, 294–299 (2023).
39. Hu YQ, Wang XD, Luo XH et al. All-dielectric metasurfaces for polarization manipulation: principles and emerging applications. *Nanophotonics* **9**, 3755–3780 (2018).
40. Ding F, Tang SW, Bozhevolnyi SI. Recent advances in polarization-encoded optical metasurfaces. *Adv Photonics Res* **2**, 2000173 (2021).
41. Dorrah AH, Rubin NA, Zaidi A et al. Metasurface optics for on-demand polarization transformations along the optical path. *Nat Photonics* **15**, 287–296 (2021).
42. Deng ZL, Tu QA, Wang YJ et al. Vectorial compound metapixels for arbitrary nonorthogonal polarization steganography. *Adv Mater* **33**, 2103472 (2021).
43. Bao YJ, Wen L, Chen Q et al. Toward the capacity limit of 2D planar jones matrix with a single-layer metasurface. *Sci Adv* **7**, eabh0365 (2021).
44. Bao YJ, Nan F, Yan JH et al. Observation of full-parameter jones matrix in bilayer metasurface. *Nat Commun* **13**, 7550 (2022).
45. Zhang X, Huang LL, Zhao RZ et al. Basis function approach for diffractive pattern generation with dammann vortex metasurfaces. *Sci Adv* **8**, eabp8073 (2022).
46. Zhang RZ, Guo YH, Zhang F et al. Dual-layer metasurface enhanced capacity of polarization multiplexing. *Laser Photonics Rev* **18**, 2400126 (2024).
47. Ren HR, Fang XY, Jang J et al. Complex-amplitude metasurface-based orbital angular momentum holography in momentum space. *Nat Nanotechnol* **15**, 948–955 (2020).
48. Fang XY, Ren HR, Gu M. Orbital angular momentum holography for high-security encryption. *Nat Photonics* **14**, 102–108 (2020).
49. Jin L, Dong ZG, Mei ST et al. Noninterleaved metasurface for (2^6-1) spin- and wavelength-encoded holograms. *Nano Lett* **18**, 8016–8024 (2018).
50. Yang B, Liu WW, Li ZC et al. Polarization-sensitive structural colors with hue- and-saturation tuning based on all-dielectric nanopixels. *Adv Opt Mater* **6**, 1701009 (2018).

51. Song MW, Wang D, Kudyshev ZA et al. Enabling optical steganography, data storage, and encryption with plasmonic colors. *Laser Photonics Rev* **15**, 2000343 (2021).
52. Feng R, Wang H, Cao YY et al. A modular design of continuously tunable full color plasmonic pixels with broken rotational symmetry. *Adv Funct Mater* **32**, 2108437 (2022).
53. Kim J, Jeon D, Seong J et al. Photonic encryption platform *via* dual-band vectorial metaholograms in the ultraviolet and visible. *ACS Nano* **16**, 3546–3553 (2022).
54. Wang B, Dong FL, Yang D et al. Polarization-controlled color-tunable holograms with dielectric metasurfaces. *Optica* **4**, 1368–1371 (2017).
55. Zang XF, Dong FL, Yue FY et al. Polarization encoded color image embedded in a dielectric metasurface. *Adv Mater* **30**, 1707499 (2018).
56. Guo XY, Zhong JZ, Li BJ et al. Full-color holographic display and encryption with full-polarization degree of freedom. *Adv Mater* **34**, 2103192 (2022).
57. Deng ZL, Jin MK, Ye X et al. Full-color complex-amplitude vectorial holograms based on multi-freedom metasurfaces. *Adv Funct Mater* **30**, 1910610 (2020).
58. Luo XH, Hu YQ, Li X et al. Integrated metasurfaces with microprints and helicity-multiplexed holograms for real-time optical encryption. *Adv Opt Mater* **8**, 1902020 (2020).
59. Zhou HQ, Sain B, Wang YT et al. Polarization-encrypted orbital angular momentum multiplexed metasurface holography. *ACS Nano* **14**, 5553–5559 (2020).
60. Fang XY, Yang HC, Yao WZ et al. High-dimensional orbital angular momentum multiplexing nonlinear holography. *Adv Photonics* **3**, 015001 (2021).
61. Zhu L, Wei JX, Dong L et al. Multi-dimensional meta-holography encrypted by orbital angular momentum, frequency, and polarization. *Laser Photonics Rev* **18**, 2301362 (2024).
62. Bao YJ, Yu Y, Xu HF et al. Coherent pixel design of metasurfaces for multidimensional optical control of multiple printing-image switching and encoding. *Adv Funct Mater* **28**, 1805306 (2018).
63. Cui TJ, Qi MQ, Wan X et al. Coding metamaterials, digital metamaterials and programmable metamaterials. *Light Sci Appl* **3**, e218 (2014).
64. Zhang L, Chen XQ, Liu S et al. Space-time-coding digital metasurfaces. *Nat Commun* **9**, 4334 (2018).
65. Tian J, Li ZF, He C et al. Multi-channel secret sharing and camouflage in programmable metasurface-based wireless communication. *Laser Photonics Rev* **19**, 2500395 (2025).
66. Chen TL, Ni C, Li XR et al. Dual-encrypted chiral imaging based on VO_2 thermal metasurfaces. *Laser Photonics Rev* **16**, e03122 (2026).
67. Guo MC, Wang Q, Bi RB et al. Dynamically programmable GST-based metasurface for multi-channel holography and optical encryption. *Opt Express* **34**, 1896–1904 (2026).
68. Zhu LY, Wei HR, Wu BH et al. Terahertz holographic image encryption via thermally tunable directional Janus metasurface. *SmartMat* **6**, e70049 (2025).
69. Cui TJ, Liu S, Zhang L. Information metamaterials and metasurfaces. *J Mater Chem C* **5**, 3644–3668 (2017).
70. Liu X, Duan X, Li BY et al. Liquid crystal on metasurfaces toward dynamic photonic control. *Adv Funct Mater* **36**, e29188 (2026).
71. Lu HY, Liu CX, Peng S et al. Highly integrated liquid crystal metasurface for dynamic and independent transmission-reflection manipulation. *Adv Opt Mater* **13**, e02217 (2025).
72. Qiu TS, Shi X, Wang JF et al. Deep learning: a rapid and efficient route to automatic metasurface design. *Adv Sci* **6**, 1900128 (2019).
73. An SS, Fowler C, Zheng BW et al. A deep learning approach for objective-driven all-dielectric metasurface design. *ACS Photonics* **6**, 3196–3207 (2019).
74. Yu ZP, Li HH, Zhao WN et al. High-security learning-based optical encryption assisted by disordered metasurface. *Nat Commun* **15**, 2607 (2024).
75. Liu YC, Xu K, Fan XH et al. Dynamic interactive bitwise meta-holography with ultra-high computational and display frame rates. *Opto-Electron Adv* **7**, 230108 (2024).
76. Peng X, Wei HZ, Zhang P. Chosen-plaintext attack on lensless double-random phase encoding in the fresnel domain. *Opt Lett* **31**, 3261–3263 (2006).
77. Weng XY, Song Q, Li XM et al. Free-space creation of ultralong anti-diffracting beam with multiple energy oscillations adjusted using optical pen. *Nat Commun* **9**, 5035 (2018).
78. Weng XY, Miao Y, Zhang QL et al. Extraction of inherent polarization modes from an *m*-order vector vortex beam. *Adv Photonics Res* **3**, 2100194 (2022).
79. Xia ZY, Weng XY, Liu LW et al. Extraction of inherent amplitude mode from a light beam. *Adv Photonics Res* **6**, 2400198 (2025).
80. Heutte L, Paquet T, Moreau JV et al. A structural/statistical feature based vector for handwritten character recognition. *Pattern Recognit Lett* **19**, 629–641 (1998).
81. Due Trier Ø, Jain AK, Taxt T. Feature extraction methods for character recognition-A survey. *Pattern Recognit* **29**, 641–662 (1996).
82. Sánchez-López MM, Davis JA, Hashimoto N et al. Performance of a *q*-plate tunable retarder in reflection for the switchable generation of both first- and second-order vector beams. *Opt Lett* **41**, 13–16 (2016).
83. Marrucci L, Manzo C, Paparo D. Optical spin-to-orbital angular momentum conversion in inhomogeneous anisotropic media. *Phys Rev Lett* **96**, 163905 (2006).
84. Chen P, Ji W, Wei BY et al. Generation of arbitrary vector beams with liquid crystal polarization converters and vector-photoaligned q-plates. *Appl Phys Lett* **107**, 241102 (2015).
85. Wang D. Hologram codes of VOP. Github. https://github.com/dapengwang077-create/OPTICS-CODES. Deposited 12 December 2025.

Acknowledgements

We are grateful for financial supports from the National Key R&D Program of China (No. 2024YFF0507202); National Natural Science Foundation of China (Nos. 62550186, 62375183, T2421003, 62127819); Shenzhen Key Laboratory of Photonics and Biophotonics (No. ZDSYS20210623092006020) and Biomedical Optics Micro-Nano Detection and Imaging (No. ZDSY20130329101226215); Shenzhen Science and Technology Program (Nos. JCYJ20241202124801002, JCYJ20230807153500001).

Author contributions

All authors commented on the manuscript. X. Weng and D. Wang conceived the research and designed the experiments. J. Peng conducted the experiments with assistance from H. Zhou and M. Shen, J. Peng, Y. Chen, R. Zhang, and F. Lin analyzed the data and performed numerical simulations. J. Peng and D. Wang co-wrote the manuscript with support from all other authors. X. Weng and J. Qu provided valuable guidance throughout the development of the study. J. Qu supervised the entire project. All of the authors participated in the analysis.

Competing interests

The authors declare no competing financial interests.

Data availability

All data supporting the findings of this study are available from the corresponding

author on request. The code to write as an hologram example will be made publicly available at https://github.com/dapengwang077-create/OPTICS-CODES[85]. Additional codes are available from the corresponding authors upon reasonable request.

Supplementary information

Supplementary information for this paper is available at https://doi.org/10.29026/oet.2026.260018.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. To view a copy of this license, visit http://creativecommons.org/licenses/by/4.0/
©The Author(s) 2026.
Published by Editorial Office of *Opto-Electronic Technology*, Institute of Optics and Electronics, Chinese Academy of Sciences.

Opto-Electronic Journals Group
www.oejournal.org
Scan for Article PDF