nature communications

Article

https://doi.org/10.1038/s41467-023-37510-z

Meta-optics empowered vector visual cryptography for high security and rapid decryption

Received: 17 October 2022

Accepted: 17 March 2023

Published online: 07 April 2023

Check for updates

Fei Zhang[1,2,5], Yinghui Guo[1,2,3,5], Mingbo Pu[1,2,3] ✉, Lianwei Chen[1], Mingfeng Xu[1,2], Minghao Liao[1,3], Lanting Li[4], Xiong Li[1,3], Xiaoliang Ma[1,3] & Xiangang Luo[1,3] ✉

Optical encryption is a promising approach to protecting secret information owing to the advantages of low-power consumption, parallel, high-speed, and multi-dimensional processing capabilities. Nevertheless, conventional strategies generally suffer from bulky system volume, relatively low security level, redundant measurement, and/or requirement of digital decryption algorithms. Here, we propose a general optical security strategy dubbed meta-optics-empowered vector visual cryptography, which fully exploits the abundant degrees of freedom of light as well as the spatial dislocation as key parameters, significantly upgrading the security level. We also demonstrate a decryption meta-camera that can implement the reversal coding procedure for real-time imaging display of hidden information, avoiding redundant measurement and digital post-processing. Our strategy features the merits of a compact footprint, high security, and rapid decryption, which may open an avenue for optical information security and anti-counterfeiting.

Information security is critical for a great number of applications ranging from anti-counterfeiting to telecommunications. Various digital cryptography techniques have been investigated to prevent information leakage, pursuing a high-security level of information. For computer-based techniques, long latency and high computational power are two main challenges. Compared with their electronic counterparts, optical cryptography techniques generally have the advantages of low-power consumption, high-speed parallel processing, and multi-dimensional capabilities, opening up a gate for securing information[1,2]. The past decades have seen significant advances in optical cryptography, including optical watermarking[3], steganography[4], and visual cryptography (VC)[5,6]. Nevertheless, the early efforts rely on the complex combination of multiple optical components for signal processing in the Fourier realm[7], leading to a large form factor. Furthermore, owing to the limited vector optical-field manipulation capabilities of conventional optical devices, the abundant degrees of freedom of light, such as amplitude, phase, frequency, polarization, etc., have not been fully exploited in early optical cryptography, leading to a limited safety performance[8–11].

In recent years, metasurfaces, one kind of ultrathin optical elements consisting of an array of subwavelength nanostructures, have been developed to manipulate all the fundamental properties of light[12–24]. By combining multiple meta-atoms[25–27] or different phase shift mechanisms[28–32], a single metasurface can be engineered to achieve independent multi-dimensional optical-field manipulation[33–35]. The compactness and versatile functionalities make metasurfaces perfect candidates for optical encryption[36–42], through various mechanisms such as multichannel vector hologram by exploiting Malus's law[43–45], the combination of grayscale/color printing and the holographic image[46–50], as well as tunable meta-holograms based on phase-change materials or spatial light modulators[51–54]. However, the spatially varying polarization property of vector light is not well

[1]State Key Laboratory of Optical Technologies on Nano-Fabrication and Micro-Engineering, Institute of Optics and Electronics, Chinese Academy of Sciences, Chengdu 610209, China. [2]Research Center on Vector Optical Fields, Institute of Optics and Electronics, Chinese Academy of Sciences, Chengdu 610209, China. [3]School of Optoelectronics, University of Chinese Academy of Sciences, Beijing 100049, China. [4]Tianfu Xinglong Lake Laboratory, Chengdu 610299, China. [5]These authors contributed equally: Fei Zhang, Yinghui Guo. ✉e-mail: pmb@ioe.ac.cn; lxg@ioe.ac.cn

exploited in optical cryptography until now, leading to a limited security level. The vast majority of holographic cryptography techniques can be potentially cracked by adjusting the polarization state of the input and output light or the incidence wavelength[38,41,44,46]. A pioneering work that combines metasurface with ghost imaging or single-pixel imaging provides a framework to solve the integration problem and enhance the security level[55]. In recent investigations, the security level has been improved by integrating metasurface imaging, visual cryptography, and computational imaging[56,57]. Generally, owing to the indirect imaging manner of computational imaging, multiple optical measurements or additional digital post-processing are required for hidden image restoration. Essentially, these approaches deviate from the original intention of all-optical encryption, leading to the loss of the merits of parallel, high-speed, and low-power consumption properties to some extent.

Here, we propose the concept of high-security vector VC, whose ciphertexts are coded based on the vector imaging process of a spin-decoupled dual-axis metalens. Since the spatial degree is theoretically unlimited and the encryption is combined with other degrees (e.g., incident wavelength, polarization, orbital angular momentum, and spatial dislocation of spin states), our approach enables much higher security. Benefiting from the metasurface-based vector optical manipulation[58], the complex encryption process can be reversely decrypted via a compact meta-camera. Once these optical key parameters are all matched perfectly, the hidden vector optical information is converted into detectable intensity patterns, enabling secure decryption in real-time without additional measurement and digital post-processing. Owing to the advantages of a compact footprint, high-security level, and real-time security display (see Supplementary Note 1 for a comprehensive comparison among different optical cryptography techniques), the proposed vector VC is favorable for optical information security and anti-counterfeiting. These properties are of significance in the future development of optical security[1,59,60], especially in monitored/peeped environments[5,61].

Results

Concept and operation principle of the decryption camera

Most conventional VC devices decompose secret images into multiple binary amplitude or phase shares, which are then digitally or physically overlapped to recover the original secret image. Compared with existing intensity- and phase-only scalar VC, our proposed vector VC exhibits a higher security level since it fully exploits abundant degrees of freedom of light as key parameters, including wavelength, phase, amplitude, polarization, and spatial dislocation. Therefore, the hidden image in a ciphertext cannot be directly decrypted by simply rotating the polarization state of the input and output light[54], ensuring a high-security level. To decrypt the optical ciphertext images, we construct a user-defined meta-camera based on the vector imaging principle, which could realize real-time decryption without complex mathematical operations or additional computational hardware resources. As indicated in Fig. 1, the decryption meta-camera contains two unique decryption elements: a) spin-decoupled dual-axis metalens generating pixel-wise spatial dislocation and overlap between two spin replicas of a ciphertext image and b) a vector sensor comprising a vector polarization analyzer attached to a photodetector for rapid security display.

Specifically, the spin-decoupled metalens equivalently operates as two independent devices with full-aperture utilization, owing to the conjugate symmetry breaking of photonic spin-orbit interactions via combining both propagation and geometric phases in a single metasurface[25,28]. Here, the spin-decoupled metalens is designed as a dual-axis planar lens to respectively respond to the left-handed and right-handed circularly polarized (LCP and RCP) light coming from the

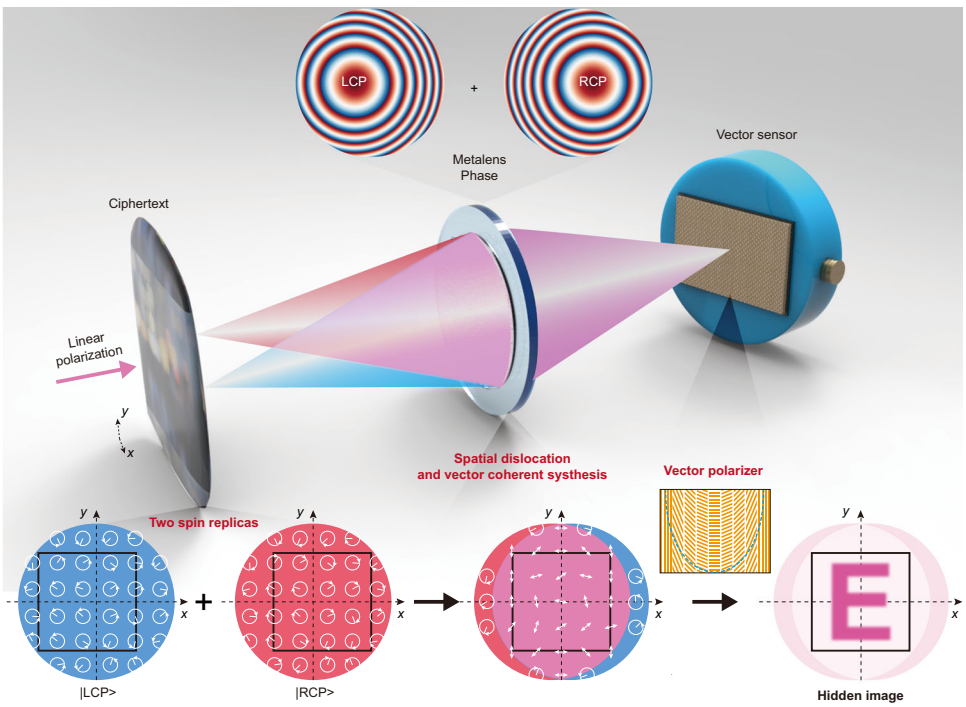

Fig. 1 | Schematics of a meta-optics-empowered decryption camera for vector VC. The decryption camera is composed of spin-decoupled dual-axis metalens (the phase profile is schematically shown in the top panel) and a vector polarization-analyzer sensor (indicated in the inset). The spin-decoupled dual-axis metalens divides the coded phase-type ciphertexts into two replicas with opposite circular polarized states and projects them to the image plane with spatial dislocation and overlap (bottom panel). The handedness and phase at each pixel are represented by the direction of the circle arrows and the azimuthal angle of short wires, respectively. As a reversal process of the coding procedure, the vector optical field synthesized at the spatially overlapping region on the image plane reproduces the hidden image in the optical ciphertexts with the help of a matched vector polarization analyzer.

https://doi.org/10.1038/s41467-023-37510-z

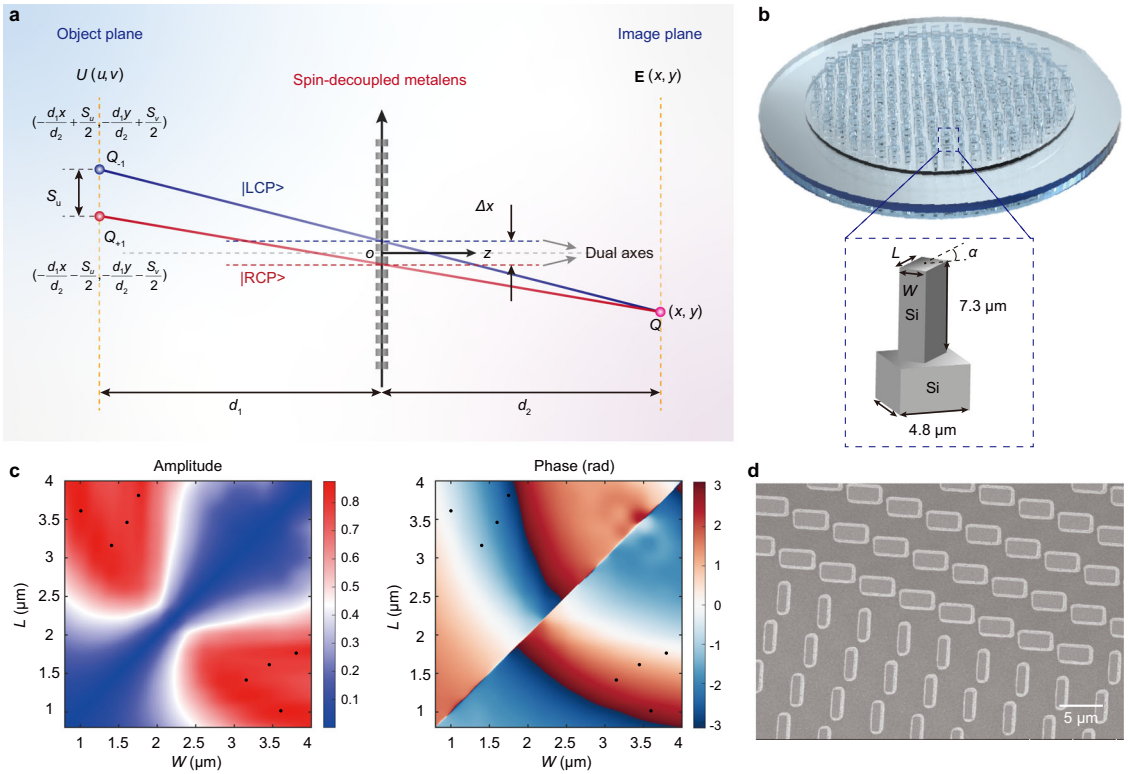

Fig. 2 | Spatial mapping relationship of the spin-decoupled metalens. **a** Opposite spin components of pixels Q_{+1} and Q_{-1} at the object plane are imaged by the spin-decoupled dual-axis metalens and coherently synthesized at the pixel Q on the image plane. **b** Schematics of the spin-decoupled metalens with the nanopillar building block shown in the inset. The width W, length L, and spatial orientation α are spatially engineered according to the phase profiles of LCP and RCP. **c** Polarization conversion amplitude and the phase shift as functions of W and L. The black dots represent the selected eight unit cells with high conversion efficiency and equal phase step. **d** Scanning electron microscope (SEM) images of the metalens consisting of all-silicon nanopillars with different geometries and orientations.

optical ciphertext. Consequently, the single-to-single point mapping of a conventional lens is transformed into dual-to-single or single-to-dual mapping. As shown in the bottom of Fig. 1, when an optical ciphertext is placed at a proper distance from the spin-decoupled metalens, it divides the optical ciphertext into two replicas with opposite spin states and projects them to the image plane with a certain spatial dislocation and overlap. The optical ciphertext exhibits a spatially inhomogeneous phase, resulting in the inherent phase difference between two points of the ciphertext. In addition, there will be a spatial variation between the propagation phases accumulated along distinct optical paths, when two separated pixels on the ciphertext respectively pass through the dual-axis centers of the metalens and intersect at one point on the image plane. Furthermore, the linear polarization direction of incidence will introduce a uniform phase difference between the two spin replicas. Owing to the inhomogeneous distribution (phase, amplitude, or both) of two spin replicas caused by the aforementioned factors, a complex vector optical field is generated in their overlapping region at the image plane. For ease of understanding, Fig. 1 shows a case of the phase-type ciphertext. Since conventional cameras cannot directly characterize the distribution of vector light fields, another vital decryption element called vector sensor is constructed by tightly attaching a vector polarization analyzer to a normal photodetector. The vector polarization analyzer is composed of meta-gratings with spatially varying orientations. It converts the synthesized vector optical field into intensity patterns, wherein the intensity value is determined by both the aforementioned phase difference and the orientations of meta-gratings.

The imaging mechanism of our decryption camera is equivalent to the reversal process of the coding procedure. As shown in Fig. 2a, under the illumination of linearly polarized light (composed of two spin states represented by $\sigma = \pm 1$), any pixel (denoted as Q) located at the overlapping region on the image plane is the vector coherent synthesis of RCP and LCP components coming from two separated points (denoted as Q_{+1} and Q_{-1}) on the object plane via the spin-decoupled dual-axis metalens. The design of the spin-decoupled metalens is shown in Supplementary Note 2. Without loss of generality, we assume that the camera operates with a distortion-free magnification factor of d_2/d_1, where d_1 and d_2 are the object and image distances, respectively. If the pixel size of the ciphertext is sufficiently larger than the detection resolution, the image can be approximated to a point-to-point projection from (u, v) to (x, y) (the diffraction effect along the optical path is ignored). Under a circularly polarized basis, the output electric fields distribution can be approximately written as:

$$\begin{aligned}\mathbf{E}(x,y) &\propto \sum_{\sigma} e^{i(k\overline{Q_\sigma Q}-\sigma\theta)} U(u,v)\begin{bmatrix}1\\-\sigma i\end{bmatrix}\\ &= \sum_{\sigma} e^{i(k\overline{Q_\sigma Q}-\sigma\theta)} U\left(-\frac{d_1 x}{d_2}-\frac{\sigma S_u}{2},-\frac{d_1 y}{d_2}-\frac{\sigma S_v}{2}\right)\begin{bmatrix}1\\-\sigma i\end{bmatrix},\end{aligned} \tag{1}$$

and

$$k=\frac{2\pi}{\lambda}, S_u=\Delta x\left(\frac{d_1}{d_2}+1\right), S_v=\Delta y\left(\frac{d_1}{d_2}+1\right), \tag{2}$$

where $k\overline{Q_\sigma Q}$ represents the propagation phase along the optical path, $(\Delta x, \Delta y)$ is the lateral displacement between the two axes at the metalens plane, (S_u, S_v) is the lateral displacement between points Q_{+1} and Q_{-1}, and λ indicates the wavelength. Furthermore, $-\sigma\theta$ represents the polarization-dependent phase delay of two spin components for a linearly polarized incidence with an azimuthal angle θ, while

$U(u,v) = A(u,v)\exp[i\varphi(u,v)]$ is the complex-amplitude distribution function of the ciphertext (A is the amplitude and φ is the phase). There are three phase factors in the right-hand of Eq. (1) contributing to the phase differences between two spin replicas, which respectively depend on the different propagation phase, the azimuthal angle of the incident polarization, and the inherent phase of the ciphertext.

When the size of the ciphertext is much smaller than the focal length, the paraxial approximation holds and $\mathbf{E}(x,y)$ can be approximately simplified with the spin-independent phase being ignored:

$$\mathbf{E}(x,y) \approx \sum_{\sigma} e^{i[\sigma\chi(x,y)-\sigma\theta]} U\left(-\frac{d_1 x}{d_2}-\frac{\sigma S_u}{2}, -\frac{d_1 y}{d_2}-\frac{\sigma S_v}{2}\right)\begin{bmatrix}1\\ -\sigma i\end{bmatrix}, \quad (3)$$

where χ indicates the halved propagation phase difference between two distinct optical paths and can be written as:

$$\chi(x,y) = k\frac{xS_u + yS_v}{2d_2} = \frac{k(x\cdot\Delta x + y\cdot\Delta y)(d_1+d_2)}{2{d_2}^2}. \quad (4)$$

Since the complex-amplitude of the ciphertext and the optical-path-determined propagation phase difference are changed among the spatial pixels, the final polarization distribution is inhomogeneous and complex, as illustrated in Supplementary Note 3. Since the polarization states of the two spin replicas are orthogonal, there will be no interference-induced intensity change after synthesis. To address this issue, a vector linear polarization analyzer with a spatially varying orientation of $\gamma(x, y)$ is required at the front of sensors to form the complex interference effect between the two dislocated replicas and then convert the phase difference and amplitude into detectable intensity patterns, which can be written as:

$$I(x,y) = \left|\sum_{\sigma} e^{i\sigma[\chi(x,y)-\theta-\gamma(x,y)]} U\left(-\frac{d_1 x}{d_2}-\frac{\sigma S_u}{2}, -\frac{d_1 y}{d_2}-\frac{\sigma S_v}{2}\right)\right|^2. \quad (5)$$

In principle, the more complex the orientation distribution of γ, the higher the security. For simplicity, we utilize a catenary-like vector polarization analyzer with its spatial orientation $\gamma(x,y) = \chi(x,y) - \theta + \pi/2$, as discussed in Supplementary Note 4. Since its orientation profile linearly changes with the coordinates, its structural streamline, illustrated as the blue dash curve in Fig. 1, forms the catenary of equal strength[14]. Under this condition, the final intensity pattern through the vector polarization analyzer is obtained:

$$I(x,y) = \left|\sum_{\sigma} \sigma U\left(-\frac{d_1 x}{d_2}-\frac{\sigma S_u}{2}, -\frac{d_1 y}{d_2}-\frac{\sigma S_v}{2}\right)\right|^2. \quad (6)$$

As illustrated by Eq. (4–6), the imaging result of our decryption meta-camera is the interference result between different spatial pixels in the ciphertext, accompanied by a phase difference of π. The final intensity distribution is determined by several critical key parameters (λ, Δx, Δy, d_1, d_2, θ, and γ). The abundance of key parameters ensures a high-security level of the complex-amplitude vector VC. Therefore, it is unlikely to decrypt the vector VC by try-and-error attack within a reasonable time if these key parameters are unknown.

Subsequently, we show how to encrypt an arbitrary hidden intensity image I into the ciphertext U. Without loss of generality and for simplicity, it is assumed that $\Delta y = 0$, I has a pixel number of $q_1 \times q_2$ with a pixel size of $\Delta x \times \Delta x$, and $S_u = n\Delta x$, where n is a positive integer. To realize dislocation encryption between different columns, U requires at least $q_1 \times (q_2 + n)$ pixels for complete image restoration. The first n columns of U are random complex numbers, therefore, the same hidden image I can be encrypted into many different ciphertexts. An example of the same information hidden in multiple different ciphertexts is presented in Supplementary Note 5.

In general, the lth row and mth column of U is given by:

$$U(l,m) = \begin{cases} U(l,m-n) - \sqrt{I(l,m-n)}e^{i\psi_1} \\ \qquad\qquad or \\ U(l,m-n) + \sqrt{I(l,m-n)}e^{i\psi_1} \end{cases}, \; m > n \geq 1 \quad (7)$$

where the one with the smaller modulus is selected. For $m \leq n$, there are:

$$U(l,m) = ae^{i\psi_2} \quad (8)$$

Here, ψ_1 and ψ_2 are random phases ranging from 0 to 2π and a is a random number ranging from 0 to 1. In our design, ψ_1 is equal to zero for simplicity. These random codes in the ciphertexts (the first n columns of U) and hidden image (its phase profile) can reduce the probability that directly inferring the hidden image I from the complex amplitude of the ciphertext.

Experimental demonstration and security verification of the vector VC

In the decryption meta-camera, the phase coefficients and profiles of the spin-decoupled metalens for RCP and LCP components are given in Supplementary Note 2. The distinct phase profiles of LCP and RCP are implemented by merging the propagation phase (β) and geometric phase ($-2\sigma\alpha$) in a single metasurface, which is composed of high-index dielectric rectangular nanopillars with various geometries and orientations (α). Among them, the propagation phase is spin-insensitive and utilized to generate the focusing wavefront, while the spin-dependent geometric phase introduces an opposite linear phase gradient to the focusing wavefront, leading to the generation of the dual-axis metalens. These phases can be independently controlled by the spatial geometries and orientations of the nanopillar. Under the normal illumination of circularly polarized light of $[1, -\sigma i]^{\mathrm{T}}$, the output field from the nanopillars follows an analytical model based on the Jones matrix given by (see Supplementary Note 2 for details)[28,31]:

$$\mathbf{E}_{atom} = \cos\frac{\delta}{2}e^{i\beta}\begin{bmatrix}1\\ -\sigma i\end{bmatrix} + i\sin\frac{\delta}{2}e^{i(-2\sigma\alpha+\beta)}\begin{bmatrix}1\\ \sigma i\end{bmatrix}, \quad (9)$$

where $\beta + \delta/2$ and β-$\delta/2$, respectively, denote the phase shifts along the two main axes of the nanopillar and α is its orientation angle. The first term in Eq. (9) is determined by the propagation phase and shares the same polarization with the incidence. In contrast, the second term reverses the handedness of the incidence and imparts not only the geometric phase but also the propagation phase. These phases can be independently controlled by the spatial orientation and geometries of the nanopillars, which are required in constructing the spin-decoupled metalens[25,28]. Note that the phase difference of δ between two anisotropic axes generally equals to π for high energy efficiency.

For proof-of-concept demonstrations, the vector VC is demonstrated at the wavelength of 10.6 μm. We utilized all-silicon nanopillars with high transmissivity at this wavelength as meta-atoms, which are arranged in a square lattice with the period and height being kept ($p_x = p_y = 4.8$ μm and $h = 7.3$ μm), as indicated in Fig. 2b. The amplitude and phase of the spin-reversed light as functions of width W and length L are determined through the finite-element method and the simulation results are presented in Fig. 2c. As indicated by the black points in Fig. 2c, a set of eight nanopillars with proper W and L (the geometries are listed in Supplementary Table 3), including eight basic structures are utilized to provide eight phase levels covering the 2π phase range with high average polarization conversion amplitude (higher than 0.8). Then, the geometries and spatial orientation of the meta-atoms at each pixel can be determined by the required phase profiles for RCP and

https://doi.org/10.1038/s41467-023-37510-z

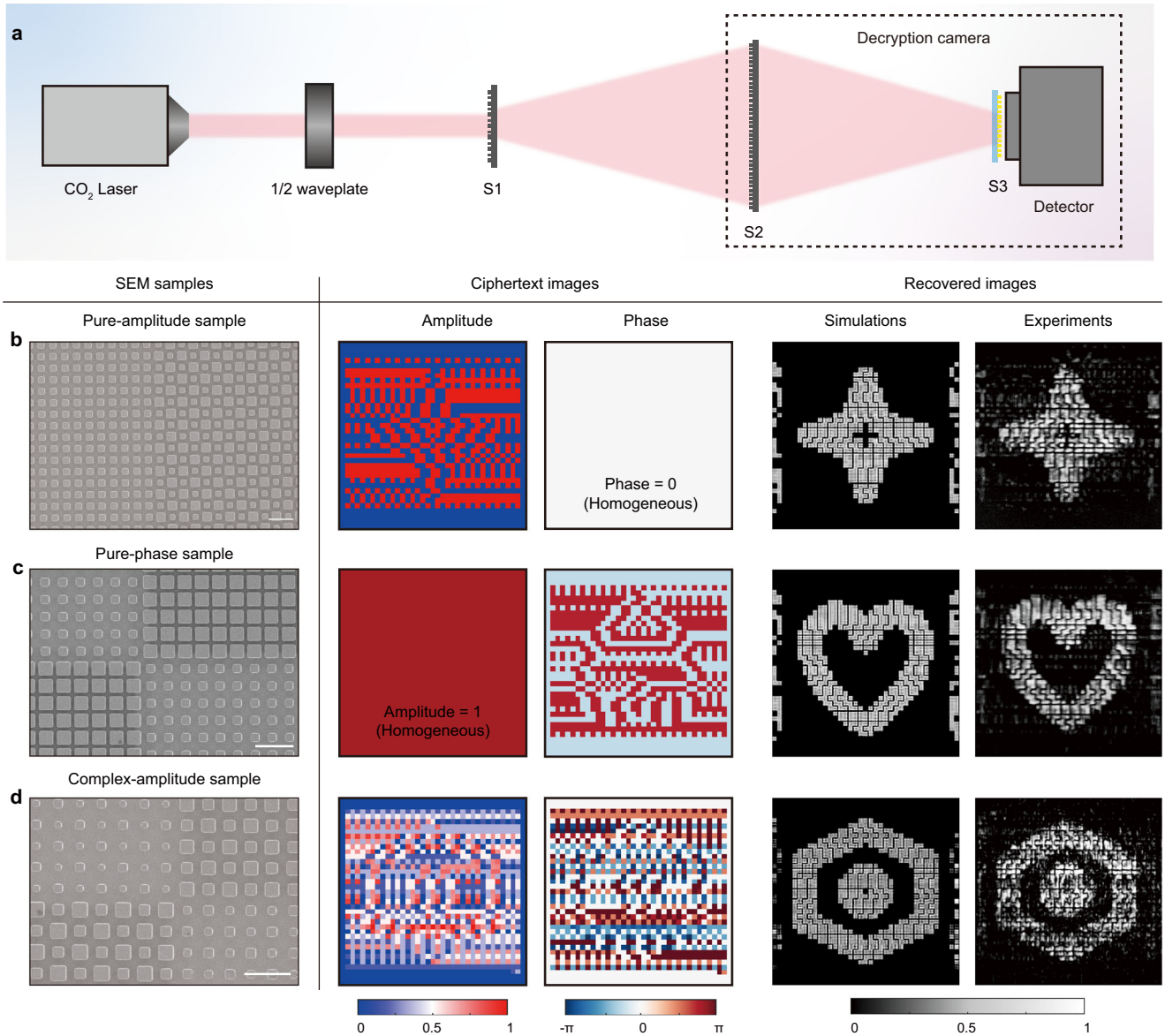

Fig. 3 | Experimental setup and decryption results. a Experimental setup. S1 to S3 represent the optical ciphertext, spin-multiplexed metalens, and the vector polarizer, respectively. **b**–**d** Simulated and experimental imaging results of three kinds of optical ciphertexts with binary pure-amplitude, binary pure-phase, or grayscale complex-amplitude modulation. Left panel: SEM images of the optical ciphertexts. Middle panel: complex-amplitude distributions of the optical ciphertexts. Right panel: Simulated and measured imaging results. Scale bar: 10 μm.

LCP (ζ_{+1} and ζ_{-1})[25,28]. The designed metalens are fabricated by direct laser writing (see Methods for details), and the SEM image is presented in Fig. 2d, demonstrating high fabrication quality. Note that, our vector VC can be extended to the near-infrared and the visible band. The direct laser writing can be replaced by electron-beam lithography for smaller feature fabrication. The spin-decoupled metalens and corresponding meta-atoms operating at the communication band of 1.55 μm are presented in Supplementary Note 2.

Figure 3a shows our experimental setup. A proper incident linear polarization is critical to illuminate the steganographic ciphertext (S1), which serves as the first key in the decryption process. S2 and S3 represent the spin-decoupled metalens and vector polarization analyzer, respectively. The imaging system parameters are summarized as follows: $d_1 = d_2 = 130$ mm (the focal length is 65 mm), $\Delta x = 100$ μm, $\Delta y = 0$, $\theta = 0$, and $S_u = 2\Delta x$ (i.e., n in Eq. (7) is equal to 2). The simulation results shown in Supplementary Note 4 indicate our vector polarizer supports a high extinction ratio of ~1000:1 and transmissivity of ~85%, which can be further improved by decreasing the period and structural height. To demonstrate the robustness of our system, three kinds of optical ciphertexts with binary pure-amplitude (Fig. 3b), binary pure-phase (Fig. 3c), and grayscale complex-amplitude (Fig. 3d) encryption are fabricated and characterized. Multiple meta-atom interference approach proposed in our previous work[25] is employed to generate such an optical ciphertext with arbitrary complex-amplitude distributions U (see Supplementary Note 6 for details), which can be directly decrypted by the proposed decryption meta-camera with proper design and a set of matched key parameters. The SEM images, complex-amplitude distributions of these optical ciphertexts, and simulated and measured imaging results are shown in the left, middle, and right panels of Fig. 3b–d. The measured results are consistent with simulation results, which indicates the encrypted information can be effectively retrieved by our system due to its capability to detect and analyze vector optical fields. Supplementary Movie 1 shows a rapid decryption process.

As discussed above, the optical decryption requires a specially equipped meta-camera with proper designs and key parameters: i.e., a

https://doi.org/10.1038/s41467-023-37510-z

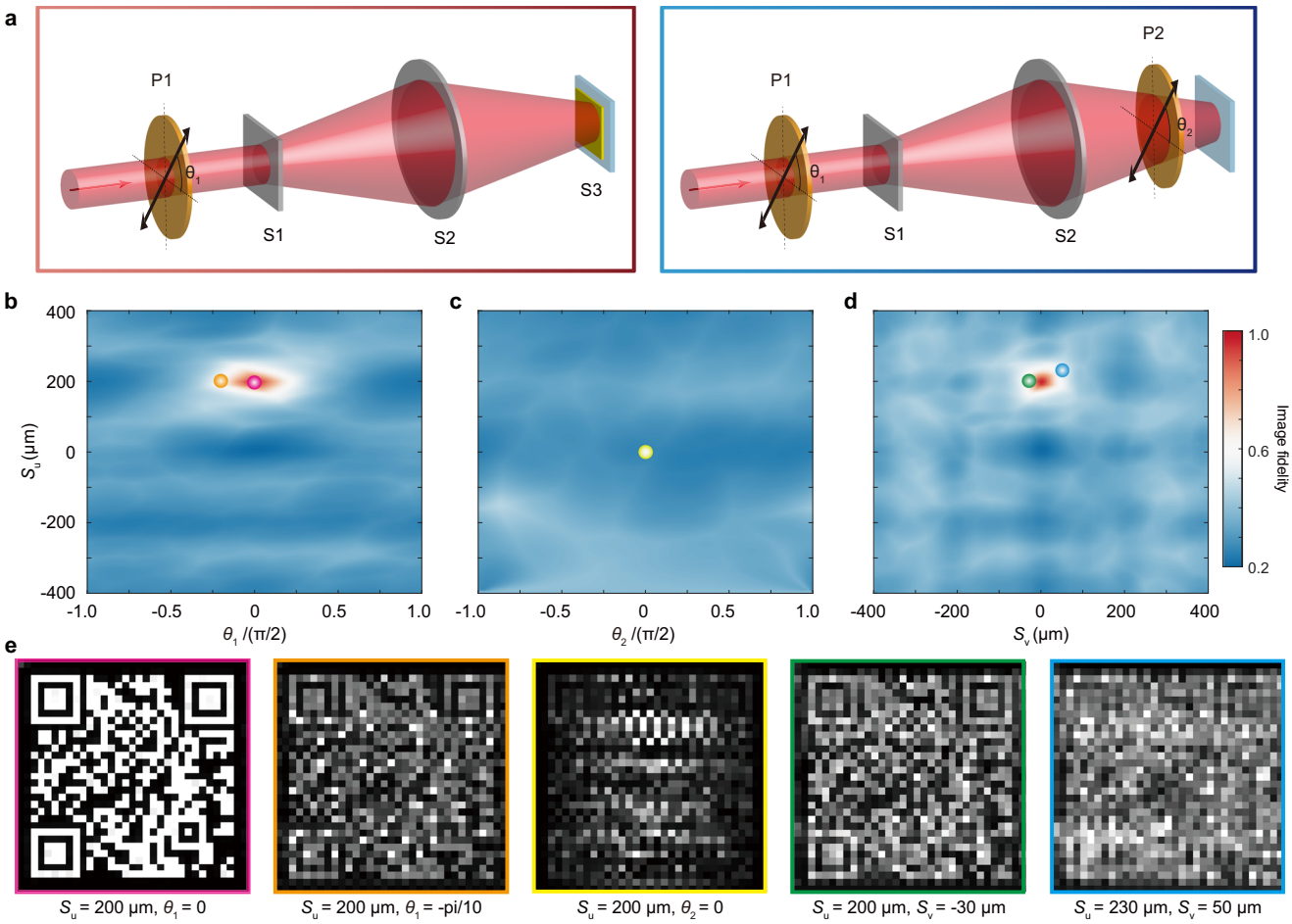

Fig. 4 | Security verification of the vector VC. a Schematic of optical setups for sensitivity check. Left panel: changing the incident polarization direction by rotating a normal linear polarizer 1 (P1). Right panel: changing the detection polarization direction by rotating a normal linear polarizer 2 (P2) that replaces the vector polarization analyzer (S3). Two-dimensional map of image fidelity as a function of the horizontal dislocation of S_u and incident polarization angle of θ_1 (**b**), detection polarization angle of θ_2 (**c**), or vertical dislocation of S_v (**d**). **e** Simulated imaging results of a hidden QR code at different key parameters, represented by circles of different colors in (**b**–**d**).

spin-decoupled dual-axis metalens with matched key parameters (S_u and S_v determined by Δx, Δy, d_1, and d_2), a vector polarization analyzer with a matched spatial orientation $\gamma = \chi - \theta + \pi/2$, and a correct incident polarization state (linear polarization with an azimuthal angle of θ). Missing any of these secret keys will result in a failed decryption. The following simulations are carried out for security verification of the vector VC under different physical parameters. Figure 4a displays schematic diagrams of optical setups for characterizing the sensitivity of image fidelity to the incident and detection polarization directions, which are controlled by rotating two normal linear polarizers P1 and P2, respectively. The vector polarization analyzer (S3) is utilized in the left panel case but is replaced by the linear polarizer (P2) in the right panel case. The image fidelity is defined as $1 - \sum|\bar{I} - \bar{I}_o| / \sum|\bar{I} + \bar{I}_o|$ to measure the similarity between the retrieved image and hidden image, where $\bar{I}$ and $\bar{I}_o$, respectively represent the normalized intensity of the measured pattern and hidden pattern. Figure 4b–d shows the two-dimensional map of image fidelity as a function of the horizontal dislocation of S_u and incident polarization angle of θ_1, detection polarization angle of θ_2, and vertical dislocation of S_v. It can be seen that confidential information can only be retrieved with relatively high image fidelity in a small area, where the key parameters exactly approach the designed system parameters. Note that, the actual selectable parameter space is larger than the simulation range. For example, dislocation parameters of S_u and S_v can go well beyond ±400 μm, and both incident and detection polarizations can be at any point on the Poincaré sphere (e.g., security verifications under circularly polarized incidences are presented in Supplementary Note 7). Figure 4e shows the simulated imaging results of a hidden QR code at different key parameters, represented by circles of different colors in Fig. 4b-d. We can see the hidden QR code can be reconstructed precisely at the center of the hot spots.

To retrieve the hidden image, a matched vector polarization analyzer is necessary but insufficient. Especially when the vector polarization analyzer (S3) is replaced by a normal linear-polarization analyzer (P2) in the camera, the image fidelity is always low. In other words, confidential information cannot be obtained, no matter what the incidence polarization is. If other parameters have been known by the attacker and the hidden imaging is relatively simple, normal polarization filters jointly with physics-driven machine-learning modeling could extract relevant information through multiple measurements. However, this potential attack can be readily reduced by using a hybrid vector polarization analyzer during the encoding of ciphertexts. For example, the catenary-like vector linear polarization analyzer could be replaced by a full-Poincaré vector polarization analyzer based on the local interference principle[25,27].

Discussion

To summarize, we present a decryption meta-camera and a general approach for real-time extraction of hidden images in coded complex-amplitude ciphertexts. Three kinds of optical ciphertexts with binary

pure-amplitude, binary pure-phase, and grayscale complex-amplitude encryption are designed and fabricated to demonstrate the flexibility of this method for vector VC. Furthermore, the high-security level of the meta-optics-based vector VC is examined, which simultaneously requires a proper incidence polarization, a correct imaging configuration, and a matched vector polarization analyzer. Inspired by the spatial vector coding empowered by spin-decoupled metasurfaces[62,63], we expect the meta-optics-based camera to obtain all-optical sensing-computing capability in the near future, which combines the sensing and computing in a single meta-device without any electronic post-processing. The capabilities of parallel high-speed processing and multi-dimensional manipulation may open an avenue for vector optical field research as well as intelligent perception and recognition.

The proposed vector VC has good scalability to further enhance its security without the sacrifice of responding time and convenience. For example, the incident polarization state can be coded to apply to a special elliptical polarization or even a vector field. The cryptography complexity can also be increased by using hybrid vector depolarizers or extending the dual-axis metalens to multi-axis metalenses (e.g., each circular polarization corresponds to multiple focus points enabled by complex-amplitude superposition[64]) for complicated spatial dislocation among multiple replicas. Furthermore, owing to the advantage of rapid decryption, one can design meta-ciphertexts containing volatile materials to maintain the correct complex amplitude in a given condition, while the device can be destroyed under unauthorized try-and-error attack. In addition, combined with the recent advance in spatial nonlinear optics[10], one can develop a nonlinear vector VC encryption system to reduce the risks caused by the fixed linear relationship between the ciphertext and hidden image, including known-plaintext attack, chosen-plaintext attack, and deep-learning-based attack.

Methods

The metalens and ciphertexts were fabricated through direct laser writing (Heidelberg DWL66+). The minimum feature size is about 0.6 μm, which is smaller than the geometries of the meta-atoms. First, ~700 nm thick photoresist is spin-coated on a double-sided polished silicon wafer with a thickness of 0.5 mm. An inductively coupled plasma etching combined with the Bosch process was subsequently employed to transfer photoresist patterns into the silicon wafer to form silicon structures. For the vector polarization analyzer, a double-sided polished barium fluoride wafer was deposited with a 600-nm gold layer using magnetron sputtering. After laser direct writing, ion beam etching was applied to transfer photoresist patterns into gold patterns, and the remaining photoresist was removed by reactive ion etching.

Data availability

The source data are available from the corresponding author upon request. All data needed to evaluate the conclusion are present in the manuscript and/or the Supplementary Information.

References

1. Chen, W., Javidi, B. & Chen, X. Advances in optical security systems. *Adv. Opt. Photonics* **6**, 120–155 (2014).
2. Matoba, O., Nomura, T., Perez-Cabre, E., Millan, M. S. & Javidi, B. Optical techniques for information security. *Proc. IEEE* **97**, 1128–1148 (2009).
3. Jiao, S., Zhou, C., Shi, Y., Zou, W. & Li, X. Review on optical image hiding and watermarking techniques. *Opt. Laser Technol.* **109**, 370–380 (2019).
4. Unnikrishnan, G., Joseph, J. & Singh, K. Optical encryption by double-random phase encoding in the fractional Fourier domain. *Opt. Lett.* **25**, 887–889 (2000).
5. Yamamoto, H., Hayasaki, Y. & Nishida, N. Securing information display by use of visual cryptography. *Opt. Lett.* **28**, 1564–1566 (2003).
6. Papas, M., Houit, T., Nowrouzezahrai, D., Gross, M. & Jarosz, W. The magic lens: refractive steganography. *ACM Trans. Graph.* **31**, 1–186 (2012). 10.
7. Refregier, P. & Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **20**, 767–769 (1995).
8. Carnicer, A., Montes-Usategui, M., Arcos, S. & Juvells, I. Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys. *Opt. Lett.* **30**, 1644–1646 (2005).
9. Peng, X., Zhang, P., Wei, H. & Yu, B. Known-plaintext attack on optical encryption based on double random phase keys. *Opt. Lett.* **31**, 1044–1046 (2006).
10. Hou, J. & Situ, G. Image encryption using spatial nonlinear optics. *eLight* **2**, 3 (2022).
11. Liao, M. et al. Deep-learning-based ciphertext-only attack on optical double random phase encryption. *Opto-Electron. Adv.* **4**, 200016–12 (2021).
12. Yu, N. et al. Light propagation with phase discontinuities: generalized laws of reflection and refraction. *Science* **334**, 333–337 (2011).
13. Luo, X. Principles of electromagnetic waves in metasurfaces. *Sci. China-Phys. Mech. Astron.* **58**, 594201 (2015).
14. Pu, M. et al. Catenary optics for achromatic generation of perfect optical angular momentum. *Sci. Adv.* **1**, e1500396 (2015).
15. Li, G., Zhang, S. & Zentgraf, T. Nonlinear photonic metasurfaces. *Nat. Rev. Mater.* **2**, 17010 (2017).
16. Arbabi, E., Kamali, S. M., Arbabi, A. & Faraon, A. Full Stokes imaging polarimetry using dielectric metasurfaces. *ACS Photonics* **5**, 3132–3140 (2018).
17. Faraji-Dana, M. et al. Compact folded metasurface spectrometer. *Nat. Commun.* **9**, 4196 (2018).
18. Lin, R. J. et al. Achromatic metalens array for full-colour light-field imaging. *Nat. Nanotechnol.* **14**, 227–231 (2019).
19. Xie, X. et al. Generalized Pancharatnam-Berry phase in rotationally symmetric meta-atoms. *Phys. Rev. Lett.* **126**, 3902 (2021).
20. Ni, J. et al. Multidimensional phase singularities in nanophotonics. *Science* **374**, eabj0039 (2021).
21. He, C., Shen, Y. & Forbes, A. Towards higher-dimensional structured light. *Light Sci. Appl.* **11**, 205 (2022).
22. Zhang, X., Liu, Y., Han, J., Kivshar, Y. & Song, Q. Chiral emission from resonant metasurfaces. *Science* **377**, 1215–1218 (2022).
23. Liu, S., Chen, S., Wen, S. & Luo, H. Photonic spin Hall effect: fundamentals and emergent applications. *Opto-Electron. Sci.* **1**, 220007–220032 (2022).
24. Meng, W. et al. 100 Hertz frame-rate switching three-dimensional orbital angular momentum multiplexing holography via cross convolution. *Opto-Electron. Sci.* **1**, 220004–220010 (2022).
25. Zhang, F. et al. All-dielectric metasurfaces for simultaneous giant circular asymmetric transmission and wavefront shaping based on asymmetric photonic spin–orbit interactions. *Adv. Funct. Mater.* **27**, 1704295 (2017).
26. Deng, L. et al. Malus-metasurface-assisted polarization multiplexing. *Light Sci. Appl.* **9**, 101 (2020).
27. Fan, Q. et al. Independent amplitude control of arbitrary orthogonal states of polarization via dielectric metasurfaces. *Phys. Rev. Lett.* **125**, 267402 (2020).
28. Zhang, F., Pu, M., Luo, J., Yu, H. & Luo, X. Symmetry breaking of photonic spin-orbit interactions in metasurfaces. *Opto-Electron. Eng.* **44**, 319–325 (2017).
29. Balthasar Mueller, J. P., Rubin, N. A., Devlin, R. C., Groever, B. & Capasso, F. Metasurface polarization optics: independent phase

control of arbitrary orthogonal states of polarization. *Phys. Rev. Lett.* **118**, 113901 (2017).
30. Devlin, R. C., Ambrosio, A., Rubin, N. A., Mueller, J. P. B. & Capasso, F. Arbitrary spin-to-orbital angular momentum conversion of light. *Science* **358**, 896–901 (2017).
31. Guo, Y. et al. Spin-decoupled metasurface for simultaneous detection of spin and orbital angular momenta via momentum transformation. *Light Sci. Appl.* **10**, 63 (2021).
32. Liu, M. et al. Broadband generation of perfect Poincaré beams via dielectric spin-multiplexed metasurface. *Nat. Commun.* **12**, 2230 (2021).
33. Liu, L. et al. Broadband metasurfaces with simultaneous control of phase and amplitude. *Adv. Mater.* **26**, 5031–5036 (2014).
34. Overvig, A. C. et al. Dielectric metasurfaces for complete and independent control of the optical amplitude and phase. *Light Sci. Appl.* **8**, 92 (2019).
35. Arbabi, A., Horie, Y., Bagheri, M. & Faraon, A. Dielectric metasurfaces for complete control of phase and polarization with subwavelength spatial resolution and high transmission. *Nat. Nanotechnol.* **10**, 937 (2015).
36. Ren, H. et al. Metasurface orbital angular momentum holography. *Nat. Commun.* **10**, 2986 (2019).
37. Fang, X., Ren, H. & Gu, M. Orbital angular momentum holography for high-security encryption. *Nat. Photonics* **14**, 102–108 (2020).
38. Zhao, R. et al. Nanoscale polarization manipulation and encryption based on dielectric metasurfaces. *Adv. Opt. Mater.* **6**, 1800490 (2018).
39. Georgi, P. et al. Optical secret sharing with cascaded metasurface holography. *Sci. Adv.* **7**, eabf9718 (2021).
40. Li, Z. et al. Cryptography metasurface for one-time-pad encryption and massive data storage. *Laser Photonics Rev.* **16**, 2200113 (2022).
41. Zhao, R. et al. Multichannel vectorial holographic display and encryption. *Light Sci. Appl.* **7**, 95 (2018).
42. Guo, X. et al. Stokes meta-hologram toward optical cryptography. *Nat. Commun.* **13**, 6687 (2022).
43. Yue, F. et al. High-resolution grayscale image hidden in a laser beam. *Light Sci. Appl.* **7**, 17129 (2018).
44. Deng, Z.-L. et al. Vectorial compound metapixels for arbitrary nonorthogonal polarization steganography. *Adv. Mater.* **33**, 2103472 (2021).
45. Ren, R. et al. Non-orthogonal polarization multiplexed metasurfaces for tri-channel polychromatic image displays and information encryption. *Nanophotonics* **10**, 2903–2914 (2021).
46. Lim, K. T., Liu, H., Liu, Y. & Yang, J. K. Holographic colour prints for enhanced optical security by combined phase and amplitude control. *Nat. Commun.* **10**, 25 (2019).
47. Zhang, F. et al. Simultaneous full-color printing and holography enabled by centimeter-scale plasmonic metasurfaces. *Adv. Sci.* **7**, 1903156 (2020).
48. Li, J. et al. From lingering to rift: metasurface decoupling for near- and far-field functionalization. *Adv. Mater.* **33**, 2007507 (2021).
49. Song, Q. et al. Printing polarization and phase at the optical diffraction limit: near- and far-field optical encryption. *Nanophotonics* **10**, 697–704 (2021).
50. Song, Q. et al. Broadband decoupling of intensity and polarization with vectorial Fourier metasurfaces. *Nat. Commun.* **12**, 3631 (2021).
51. Li, J. et al. Addressable metasurfaces for dynamic holography and optical information encryption. *Sci. Adv.* **4**, eaar6768 (2018).
52. Zhang, F. et al. Multistate switching of photonic angular momentum coupling in phase-change metadevices. *Adv. Mater.* **32**, 1908194 (2020).
53. Qu, G. et al. Reprogrammable meta-hologram for optical encryption. *Nat. Commun.* **11**, 5484 (2020).
54. Choi, C. et al. Hybrid state engineering of phase-change metasurface for all-optical cryptography. *Adv. Funct. Mater.* **31**, 2007210 (2021).
55. Liu, H.-C. et al. Single-pixel computational ghost imaging with helicity-dependent metasurface hologram. *Sci. Adv.* **3**, e1701477 (2017).
56. Zheng, P. et al. Metasurface-based key for computational imaging encryption. *Sci. Adv.* **7**, eabg0363 (2021).
57. Zheng, P. et al. Compressive imaging encryption with secret sharing metasurfaces. *Adv. Opt. Mater.* **10**, 2200257 (2022).
58. Luo, X. et al. Vector optical field manipulation via structural functional materials: tutorial. *J. Appl. Phys.* **131**, 181101 (2022).
59. Javidi, B. et al. Roadmap on optical security. *J. Opt.* **18**, 083001 (2016).
60. Liu, S., Guo, C. & Sheridan, J. T. A review of optical image encryption techniques. *Opt. Laser Technol.* **57**, 327–342 (2014).
61. Matoba, O. & Javidi, B. Optical retrieval of encrypted digital holograms for secure real-time display. *Opt. Lett.* **27**, 321–323 (2002).
62. Dorrah, A. H., Rubin, N. A., Zaidi, A., Tamagnone, M. & Capasso, F. Metasurface optics for on-demand polarization transformations along the optical path. *Nat. Photonics* **15**, 287–296 (2021).
63. Zhang, F. et al. Synthetic vector optical fields with spatial and temporal tunability. *Sci. Chin. Phys. Mech. Astron.* **65**, 254211 (2022).
64. Jin, J. et al. Multi-channel vortex beam generation by simultaneous amplitude and phase modulation with two-dimensional metamaterial. *Adv. Mater. Technol.* **2**, 1600201 (2017).

Acknowledgements

F.Z. acknowledges the funding provided by the National Natural Science Foundation of China (NSFC) (62175242), Sichuan Science and Technology Program (2021ZYCD002), and China Postdoctoral Science Foundation (2021T140670). Y.-H.G. acknowledges the funding provided by the National Natural Science Foundation of China (NSFC) (62222513), National key research and development program (SQ2021YFA1400121), and Youth Innovation Promotion Association of the Chinese Academy of Sciences (2019371). M.-B.P. acknowledges the funding provided by the National Natural Science Foundation of China (NSFC) (U20A20217). The authors would like to thank Jin Tang, Chaolong Feng, and Yujia Ma for their help with sample fabrication.

Author contributions

F.Z., Y.-H.G., M.-B.P., and X.-G.L. conceived the principle. F.Z. performed the simulations. F.Z., Y.-H.G., M.-H. L., and L.-T. L. designed and conducted experiments. Y.-H.G., L.-W.C., and F.Z. wrote the manuscript and plotted the figures. Y.-H.G., F.Z., M.-F.X., X.L., and X.-L.M. revised the manuscript. All authors discussed and analyzed the data and results. M.-B.P. and X.-G.L. co-supervised the project.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41467-023-37510-z.

Correspondence and requests for materials should be addressed to Mingbo Pu or Xiangang Luo.

Peer review information *Nature Communications* thanks Sunae So, Haoran Ren, and the other, anonymous, reviewer(s) for their contribution to the peer review of this work.