nature communications

Article

https://doi.org/10.1038/s41467-022-34542-9

Stokes meta-hologram toward optical cryptography

Received: 30 March 2022

Accepted: 28 October 2022

Published online: 05 November 2022

Check for updates

Xuyue Guo[1], Peng Li[1] ✉, Jinzhan Zhong[1], Dandan Wen[1], Bingyan Wei[1], Sheng Liu[1], Shuxia Qi[1] & Jianlin Zhao[1] ✉

Optical cryptography manifests itself a powerful platform for information security, which involves encrypting secret images into visual patterns. Recently, encryption schemes demonstrated on metasurface platform have revolutionized optical cryptography, as the versatile design concept allows for unrestrained creativity. Despite rapid progresses, most efforts focus on the functionalities of cryptography rather than addressing performance issues, such as deep security, information capacity, and reconstruction quality. Here, we develop an optical encryption scheme by integrating visual cryptography with metasurface-assisted pattern masking, referred to as Stokes meta-hologram. Based on spatially structured polarization pattern masking, Stokes meta-hologram allows multichannel vectorial encryption to mask multiple secret images into unrecognizable visual patterns, and retrieve them following Stokes vector analysis. Further, an asymmetric encryption scheme based on Stokes vector rotation transformation is proposed to settle the inherent problem of the need to share the key in symmetric encryption. Our results show that Stokes meta-hologram can achieve optical cryptography with effectively improved security, and thereby paves a promising pathway toward optical and quantum security, optical communications, and anticounterfeiting.

Over the years, information security has always been of vital importance in communication. Especially in the digital era of contemporary society, securely preserving private information is necessary and urgent to alleviate the concerns about data sharing and data misuse. Diverse cryptographic techniques[1–6] have been sparked to store information and protect them from attack. Among them, optical cryptography[7–11] delineates a distinctive and excellent framework to advance such domain forward, with regard to the unique features such as high speed, parallel processing, and abundant degrees of freedom (DoFs, e.g., amplitude, phase, polarization, frequency, and orbital angular momentum)[12]. Generally, optical cryptography involves encrypting secret images into visual patterns (as ciphertext), in which no encrypted information can be directly extracted unless decrypting with specific secret keys. Therefore, the secret information can be highly secured and communicated to the intended recipients and remain invisible to unauthorized users. Nevertheless, the bulky size resulting from increasing cryptographic complexity hinders the application of optical cryptography in compact systems.

The pioneering work that combines metasurface with ghost imaging[13] attracts considerable attention for optical cryptography and can be achieved through meta-hologram, providing a new framework to solve the integration problem and enhance the security level. Thanks to the unparalleled modulation capability on multiple DoFs[14,15], metasurface-based optical cryptography[16–21] has subsequently attracted considerable attention, because of the potential in boosting multi-image[22,23] and color image encryption[24,25], as well as multi-dimensional key design[26–28]. In addition, the subwavelength-pixel light field manipulation enables metasurface dense data processing. So far, the metasurface-based encryption frameworks are commonly

[1]Key Laboratory of light field manipulation and information acquisition, Ministry of Industry and Information Technology, and Shaanxi Key Laboratory of Optical Information Technology, School of Physical Science and Technology, Northwestern Polytechnical University, Xi'an 710129, China.
✉e-mail: pengli@nwpu.edu.cn; jlzhao@nwpu.edu.cn

concentrating on the expansion of encryption capacity, that is, using innovative vectorial-[29,30], multichromatic-[31,32], and OAM (orbital angular momentum)-holograms[33–35] to exploit encrypting channels. For instance, encrypting secret images (attached on phase[36], amplitude[37] or complex amplitude[38] of light fields) into independent polarization channels (orthogonal polarization pairs[36], nonorthogonal polarization pairs[39,40], or arbitrary polarization combination[41–43]), or hiding images in nonuniform polarization distribution by exploiting Malus' law[44,45] and its orientation degeneracy[46,47]. Despite the tremendous developments in this emerging platform in past years, the security issues have not been well addressed. The above multichannel encryption schemes are vulnerable to brute force attacks (e.g., undifferentiated polarization analysis), leaving hidden risks for information security. Zheng et al. recently demonstrated a high-security encryption scheme by integrating metasurface imaging and computational imaging[48], whereas the information capacity is related to and limited by the shift matrix.

In this work, we revisit the capability of metasurface to construct fully-polarized structured light fields and develop a Stokes meta-hologram based on vectorial encryption toward both the security and capacity of optical cryptography. We provide complete design rules on how to design a Stokes meta-hologram with different security levels, of which the principle is illustrated in Fig. 1. The fundamental-level encryption, namely, vectorial encryption based on Stokes parameters, generates a fully-polarized structured light field, as visual ciphertext, in which three secret images are masked into Stokes vector $\mathbf{S} = (S_1, S_2, S_3)^T$. In this scheme, decrypting the ciphertext according to the measured polarization component patterns via the Stokes method can directly retrieve the secret images (Fig. 1b). However, this primary masked ciphertext is easy to be cracked since the attacker can obtain multiple images through polarization analysis and perform further operations according to the visible pattern in the ciphertext. Therefore, a pixeled polarization mask is introduced as the secret key by Mueller matrix transformation (Fig. 1c). Double polarization pattern masking improves

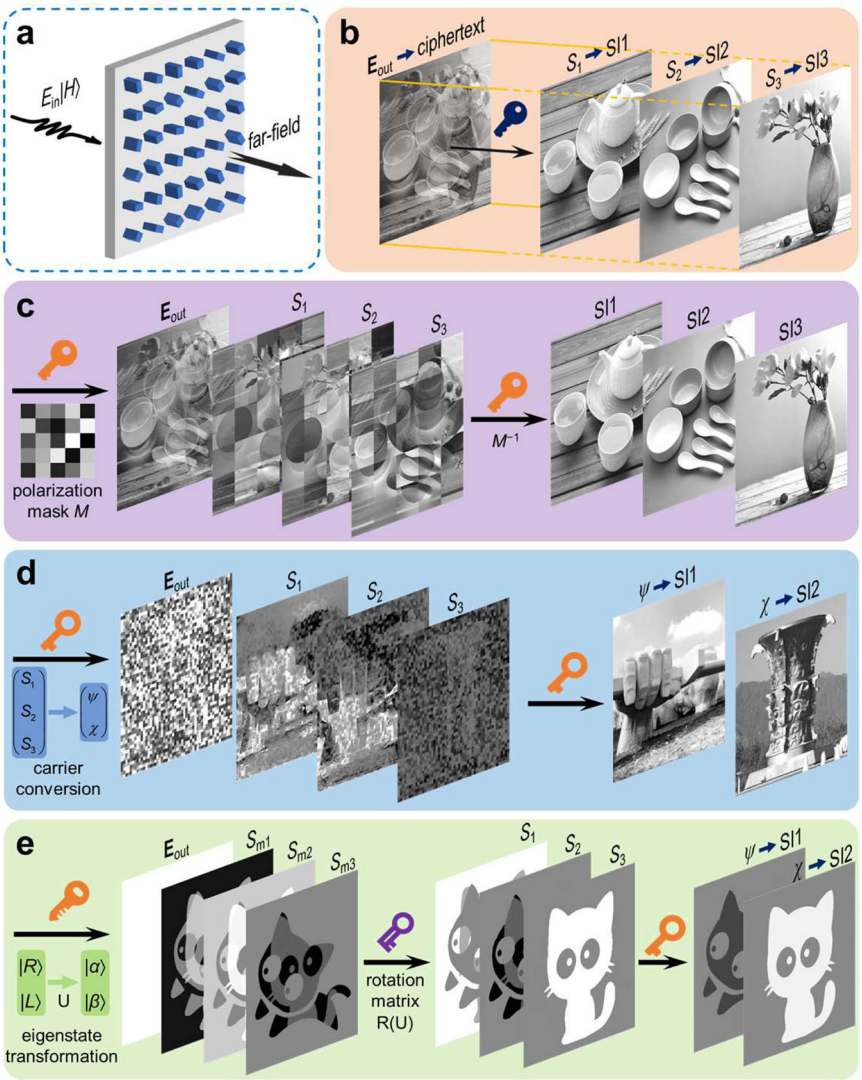

Fig. 1 | Conceptual illustration of Stokes meta-hologram. a, **b** Fundamental Stokes vector encryption. The meta-hologram generates a fully-polarized far-field $\mathbf{E}_{out}$ (as ciphertext) encrypted with secret images (SI) in Stokes vector, i.e., $(SI1, SI2, SI3)^T = (S_1, S_2, S_3)^T$, when it is illuminated with a uniform light beam of $|H\rangle$ polarization state. **c** Mueller matrix encryption. A pixeled polarization mask (depicted as Mueller matrix M) is used to perform the second-level encryption, in which the Stokes distribution will be unrecognizable, and a specific secret key is required to decrypt secret images. **d** Angular vector encryption. To eliminate the visible pattern in ciphertext, the vector consisting of azimuth (ψ) and elliptical (χ) angles on the Poincaré sphere is used as extended secret keys for further-level encryption. The two images are photographs of architecture on the campus of Northwestern Polytechnical University and are used with the permission of Northwestern Polytechnical University. **e** Asymmetric encryption. A rotation transformation of the Stokes vector corresponding to the eigenstate transformation (public key) is introduced as a private key for asymmetric encryption.

the security level and the robustness of ciphertext, while in which, the visible pattern is yet prone to leak some information. In this respect, an information carrier conversion based on the Poincaré sphere angular vector is then introduced in the polarization pattern masking process (Fig. 1d). Owing to the multiple encryption processes and more DoFs, visible pattern in the ciphertext can be effectively eliminated. In order to further improve the encryption level, Stokes vector rotation transformation R(U), as a private key, is introduced to break the symmetry relationship of the secret keys in encrypting and decrypting processes (Fig. 1e). The asymmetric scheme can isolate an encrypted image from the mask (public key) holders, creating extreme improvement in information security.

Results

Stokes meta-hologram

As shown in Fig. 1a, the Stokes meta-hologram is desired to yield the ciphertext in the far-field under the illumination of an incident beam with uniform amplitude ($E_{in}=1$) and definite polarization, e.g., the horizontal polarization $|H\rangle$. To construct fully-polarized information $\mathbf{E}_{out}$, the amplitude, phase, and polarization of the transmitted light beam are supposed to experience a completely decoupled modulation through the meta-hologram. Meanwhile, suitable multiplexing methods are as well necessary in favor of the improvement of information capacity. Consequently, we design a dual-channel meta-hologram in which the amplitude, phase, and polarization can be simultaneously and independently modulated on each spatial channel.

The metasurface is composed of birefringent dielectric nanopillars with a tetratomic macro-pixel arrangement, of which each meta-atom behaves as a half-wave plate and has varying geometrical size and rotation angle, i.e., D_{io}, D_{ie}, and θ_i, ($i=a_1, a_2, a_3, a_4$), as shown in Fig. 2a. By skillfully tailoring the polarization-dependent interference[49], the far-field distributions in two completely decoupled channels can be achieved as

$$\begin{aligned}\mathbf{E}^1_{out} &= \mathcal{F}\{2\cos(\xi_{11})\exp(i\phi_{11})|R\rangle + 2\cos(\xi_{12})\exp(i\phi_{12})|L\rangle\}\\ \mathbf{E}^2_{out} &= \mathcal{F}\{2\cos(\xi_{21})\exp(i\phi_{21})|R\rangle + 2\cos(\xi_{22})\exp(i\phi_{22})|L\rangle\},\end{aligned} \quad (1)$$

where, $|R\rangle$ and $|L\rangle$ represent the right- (RCP) and left-hand circularly polarized (LCP) bases, and ξ_{11}, ξ_{12}, ξ_{21}, ξ_{22}, ϕ_{11}, ϕ_{12}, ϕ_{21}, ϕ_{22} are preestablished phase patterns. The detailed derivation is shown in Supplementary Note 1. A dual-channel Malus meta-hologram is first implemented to testify the performance, as shown in Fig. 2b. Two sets of complementary images are separately encrypted into the horizontal $|H\rangle$ and vertical $|V\rangle$ states on each channel, i.e., four independent images are encrypted into a meta-hologram. The scanning electron microscope image and experiment results of the meta-hologram are shown in Fig. 2c, d, respectively. Under linear polarization incidence, each channel displays a uniform holographic pattern composed of $|H\rangle$ and $|V\rangle$ polarization multiplexed images, which can be observed by changing the orientation of the polarization analyzer.

We further design the Stokes meta-hologram by using this dual-channel configuration, to create spatial polarization pattern masked ciphertexts with high capacity. The fundamental-level encryption, that is, masking three arbitrary images into Stokes vector $\mathbf{S}=(S_1, S_2, S_3)^T$, is illustrated in Fig. 2e. Firstly, the secret images (SI1, SI2, and SI3) are mapped to S_1, S_2, and S_3 through a linear transformation ($2X/255-1$), where X represents the original grayscale value. Sophisticated transformation methods, such as nonlinear transformation and matrix shift operation[48], can be used for high-security encryption. Second, according to the Stokes vector, we retrieve the Jones vector, with

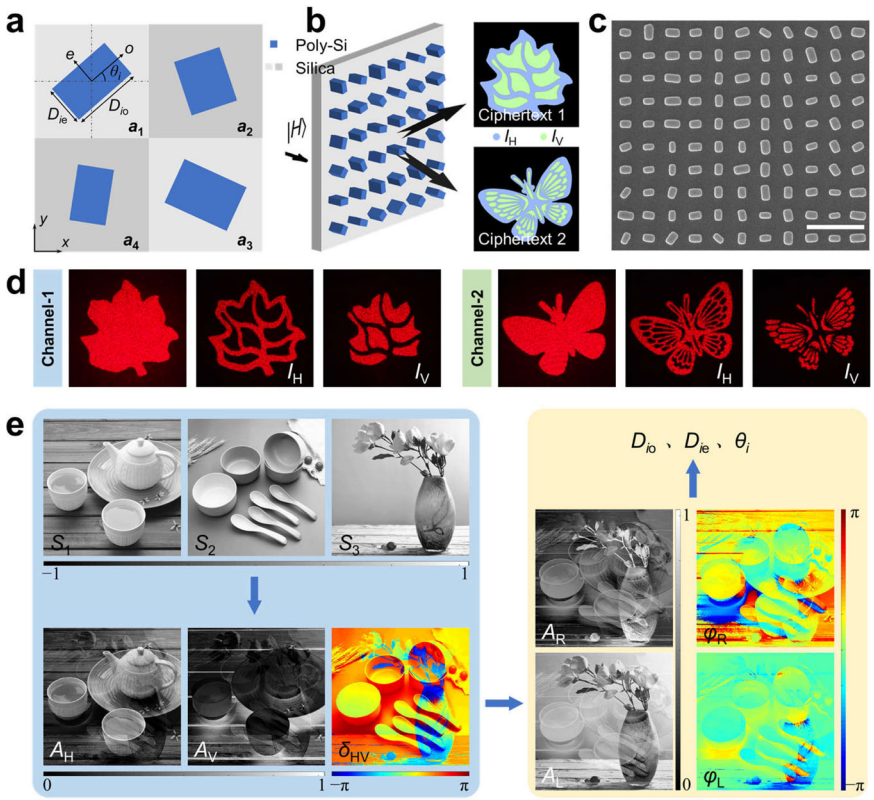

Fig. 2 | Design principle of Stokes meta-hologram. a Schematic illustration of the tetratomic macro-pixel unit cell, which comprises four types of rectangular nanopillars denoted as meta-atoms a_1, a_2, a_3, and a_4 with variant geometrical sizes D_{io} and D_{ie}, and orientation angles θ_i, ($i=a_1, a_2, a_3, a_4$). The period and height of the macro-pixel unit cell are 900 and 550 nm, respectively. **b** Working principle of dual-channel meta-hologram. **c** Scanning electron microscope image of the metasurface. The scale bar is 1 μm. **d** Experiment results of the dual-channel polarization-switchable holographic display to testify the vectorial encryption performance of the designed meta-hologram. **e** Designing process of Stokes meta-hologram for masking three arbitrary image information into Stokes vector $(S_1, S_2, S_3)^T$.

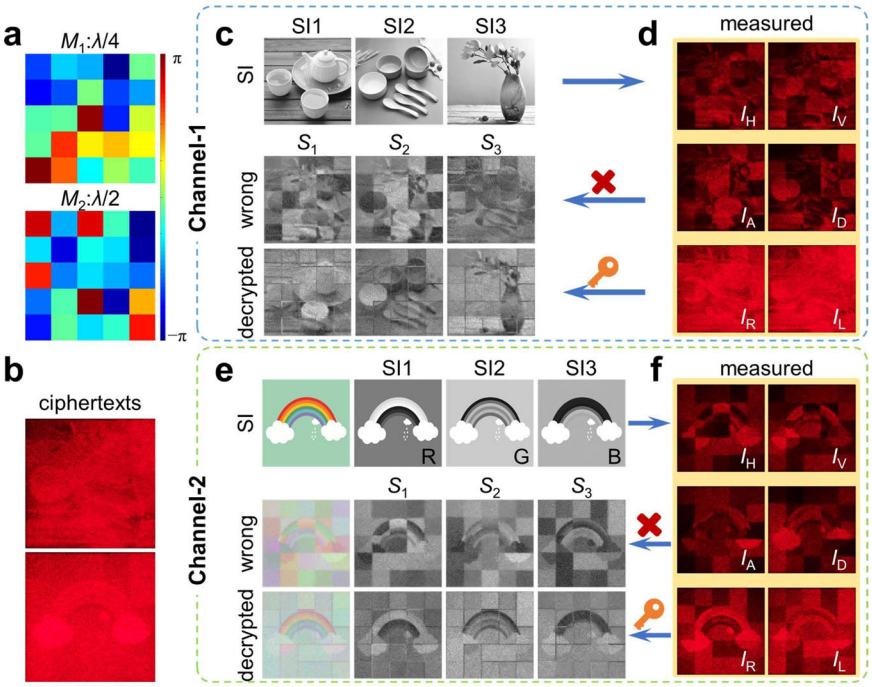

Fig. 3 | Mueller matrix encryption. a Random direction in Mueller matrices of pixelated wave plates. **b** Measured ciphertext (total intensity) patterns. **c**–**f** Decrypted results with and without the secret key. Three grayscale images and an RGB color image are encrypted into Stokes vectors (SI1, SI2, SI3)^T (first rows of **c** and **e**) and then transformed into vectorial ciphertexts after a pixelated polarization mask, which is equivalent to the cascaded Mueller matrices M_2M_1. For this two-level vectorial encryption, any measured polarization components (**d** and **f**) and the directly decrypted results by Stokes vector $(S_1, S_2, S_3)^T$ (second rows of **c** and **e**) can not present secret images. Whereas, through decryption with a secret key, the secret images can be extracted accurately (third rows of **c** and **e**).

linearly polarized basic states:

$$\begin{aligned} S_1 &= A_H^2 - A_V^2 \\ S_2 &= 2A_H A_V \cos(\delta_{HV}) \\ S_3 &= 2A_H A_V \sin(\delta_{HV}). \end{aligned} \tag{2}$$

Therefore, the desired fully-polarized field is decomposed to the amplitude (A_H, A_V) and phase difference (δ_{HV}) of the $|H\rangle$ and $|V\rangle$ components and then transformed into the complex amplitudes of RCP and LCP. Then, the preestablished phase patterns are generated according to Supplementary Eqs. (8–10), and the required phase responses and orientation angles (θ_i) can be obtained from Supplementary Eq. (6). Finally, matching geometries (D_{io}, D_{ie}) are selected to map the meta-hologram according to phase responses. In the decryption of each channel, the secret images masked in the Stokes vector can be obtained as

$$\begin{aligned} S_1 &= |\langle H|\mathbf{E}_{out}|^2 - |\langle V|\mathbf{E}_{out}|^2 \\ S_2 &= |\langle A|\mathbf{E}_{out}|^2 - |\langle D|\mathbf{E}_{out}|^2 \\ S_3 &= |\langle R|\mathbf{E}_{out}|^2 - |\langle L|\mathbf{E}_{out}|^2. \end{aligned} \tag{3}$$

Where, $|A\rangle$ and $|D\rangle$ correspond to the antidiagonal and diagonal polarization states, respectively.

Mueller matrix encryption

A two-dimensional polarization mask is a common selection to enhance the security of ciphertext in Stokes vector encryption, whose encrypting process can be described by the pixeled Mueller matrix as

$$\begin{pmatrix} S_0^{out} \\ S_1^{out} \\ S_2^{out} \\ S_3^{out} \end{pmatrix} = M_n(\theta) \cdots M_1(\theta) \begin{pmatrix} S_0^{in} \\ S_1^{in} \\ S_2^{in} \\ S_3^{in} \end{pmatrix}, \tag{4}$$

where, $M(\theta)$ represents the 4×4 Mueller matrix with spatially varying modulation, which can be a polarizer, a phase retarder, and so on. One can regard the cascaded modulation effect $M_1(\theta)\cdots M_n(\theta)$ as the secret key, or create multiple secret keys by separating the modulation effect and cascade order. Both the modulation effect and the cascade order are unlimited, therefore, the possibility of the attacker decrypting an unknown image is thus strongly reduced[50].

In the experimental demonstration, we exhibit two types of encryptions in two channels, e.g., simultaneously encoding arbitrary three grayscale images and an RGB color image into the Stokes meta-hologram, i.e., up to six images can be encrypted at the same time. The Mueller matrices of cascaded quarter- and half-wave plates with random directions (Fig. 3a) both have 5×5 pixels (the security level can be further enhanced with more pixels, which is shown in Supplementary Fig. 15). Compared with the fundamental-level ones (Supplementary Fig. 1), the dual-channel ciphertext patterns (Fig. 3b), measured intensity patterns of different polarization components (Fig. 3d, f), as well as the directly Stokes vector decrypted results (second rows of Fig. 3c, e) all present chaotic information. For accurate decryption, a secret key corresponding to these cascaded Mueller matrices is required to reorder the chaotic distributions, as shown in the third rows of Fig. 3c, e. Obviously, the secret images are stored intactly, and cannot be directly obtained from any single polarization measurement. The experiment and simulation details are shown in Supplementary Figs. 3, 4, respectively. Since the captured images are slightly distorted due to the far-field projection, a misalignment of the

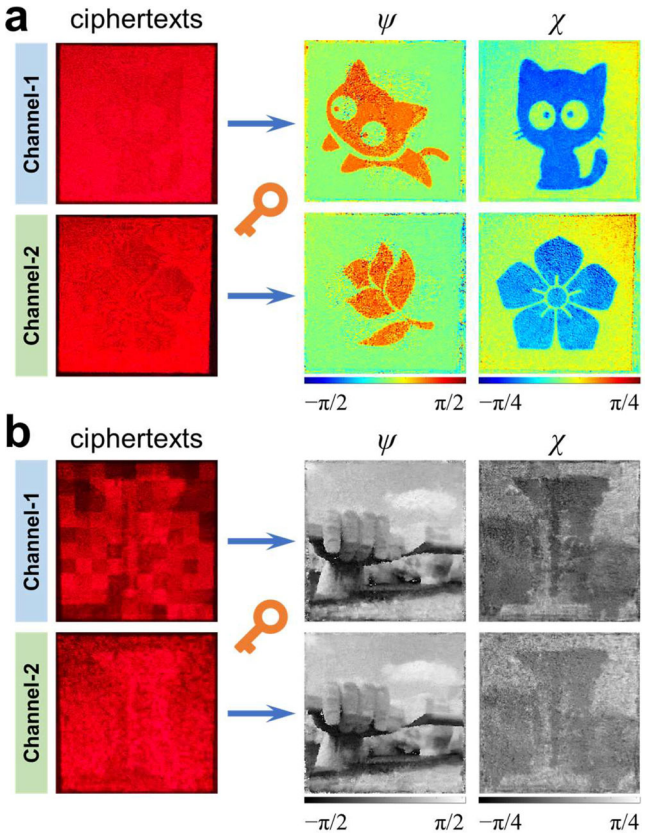

Fig. 4 | Angular vector encryption on Poincaré sphere. a, **b** Uniform and ununiform ciphertext (total intensity I_T) encryptions. In **a**, two secret images are decrypted by characterizing an angular vector (ψ, χ) on the Poincaré sphere. In contrast, in **b**, two random intensity patterns (10 × 10 pixels for channel-1 and 50 × 50 pixels for channel-2) are used to improve the confidentiality of the measurement of circularly polarized components. The two images are photographs of architecture on the campus of Northwestern Polytechnical University and are used with permission of Northwestern Polytechnical University.

pixelated polarization mask will be introduced when decrypting. The slight distortion in decrypted images is due to the imperfect fabrication of metasurfaces, and intensity measurement error caused by off-axis aberration and manual capture.

Angular vector encryption on Poincaré sphere

The above scheme can mask multiple secret images into the Stokes vector. However, the released S_0 results in that the generated ciphertext (total intensity) still presents some plaintext (secret images) information, namely, visible pattern (see the total intensities in Fig. 3b and Supplementary Fig. 1b, e). Despite no secret images can be directly extracted, this scheme still leaves some safety concerns. To address this risk, i.e., to realize a further level of secured encryption, the information carrier can be extended to an angular vector on the Poincaré sphere, which is characterized by the azimuthal and elliptical angles, due to the inherent relationship between the spherical coordinates (namely angular vector) on Poincaré sphere and the Stokes vector in Cartesian coordinates:

$$\begin{aligned} \tan 2\psi &= S_2/S_1 \\ \sin 2\chi &= S_3/S_0. \end{aligned} \tag{5}$$

Therefore, by sacrificing some capacity, the security of ciphertext can be enhanced. Figure 4a shows an experimental verification, for clarity, no Mueller matrix is introduced (simulation results with the Mueller matrix are shown in Supplementary Fig. 16). Clearly, a uniform ciphertext is observed (left panel), but two secret images can be decrypted when characterizing the spatially structured polarization pattern in the azimuth and elliptical angle (right panel).

Theoretically, under the circular polarization eigenstates, the ellipticity only depends on the amplitude ratio of the RCP and LCP states. Therefore, when the ciphertext has a uniform intensity profile, the secret image encrypted on the elliptical angle can be directly observed by merely measuring the RCP or LCP component (see the I_R and I_L shown in Supplementary Fig. 5b, d). To eliminate such security risk, we introduce a random intensity distribution to the circular polarization eigenstates with a guaranteed amplitude ratio. Two photographs of architecture on our campus are chosen as secret images. The experiment results are shown in Fig. 4b, and the random intensity patterns are 10 × 10 (upper) and 50 × 50 (lower) pixels in different channels, respectively (details are shown in Supplementary Fig. 6). Clearly, random intensities attached on the LCP dilute the information that can be directly observed. The noise in the decrypted image on an elliptical angle comes from the measurement error of the random intensity distribution. It is worth noting that, the secret images encrypted on azimuth associated with phase can always be recovered well (see decrypted ψ in Fig. 4b), whereas, errors in intensity measurement result in some unevenly distributed grids in elliptical angle decryption (see decrypted χ in Fig. 4b), which corresponds to the lower values of random intensity. These errors can be averaged by increasing the pixel number of the random intensity pattern, or the secret image can be set to the same pixel number as the random intensity pattern to avoid the loss of grayscale in a continuous gray image, the corresponding demonstration is shown in Supplementary Fig. 7.

Asymmetric encryption

The above presentations all belong to symmetric encryption, in which the secret key works in both encryption and decryption processes. Whereas, asymmetric encryption uses two keys to boost security, i.e., the public key for encryption and the private key for decryption, eliminating the need to share the key. To break such a symmetry relationship, we introduce an eigenstate transformation on the Poincaré sphere to reconstruct the Stokes vector.

On a normal Poincaré sphere, any polarization state $|\alpha\rangle$ can be characterized by a special angular vector $(2\psi, 2\chi)^T$ with respect to two eigenstates of RCP and LCP (i.e., the north and south poles) as

$$|\alpha\rangle = \cos(\varphi)\exp(i\theta)|R\rangle + \sin(\varphi)\exp(-i\theta)|L\rangle. \tag{6}$$

where, φ and θ represent spherical coordinates. Its orthogonal polarization state $|\beta\rangle$, located on the sphere that is symmetrical about the origin, as shown in the left panel of Fig. 5a. In our asymmetric encryption scheme, the secret images (middle panel of Fig. 5a) are still encrypted into the angular vector, but an eigenstate transformation is introduced to break the symmetry, that is, implementing the complex amplitude distribution on the original circular polarization eigenstates (in Supplementary Eq. (1)) to any other pair of orthogonal eigenstates (as public key), as

$$A_R\exp(i\varphi_R)|\alpha\rangle + A_L\exp(i\varphi_L)|\beta\rangle, \tag{7}$$

where, $A_R\exp(i\varphi_R)$ and $A_L\exp(i\varphi_L)$ are the complex amplitudes from decomposing the desired fully-polarized field under circular polarization eigenstates. After such transformation, the spatially structured polarization of the field will be redefined. The right panel in Fig. 5a shows the Poincaré sphere constructed by the $|\alpha\rangle$ and $|\beta\rangle$ eigenstates, in which all the coordinates of original polarization states are changed, that is, the angular vector of any polarization state rotates a special angle associated with the angular vector of the $|\alpha\rangle$ state on the normal Poincaré sphere. Whereas, in practice, the measured Stokes vector is

https://doi.org/10.1038/s41467-022-34542-9

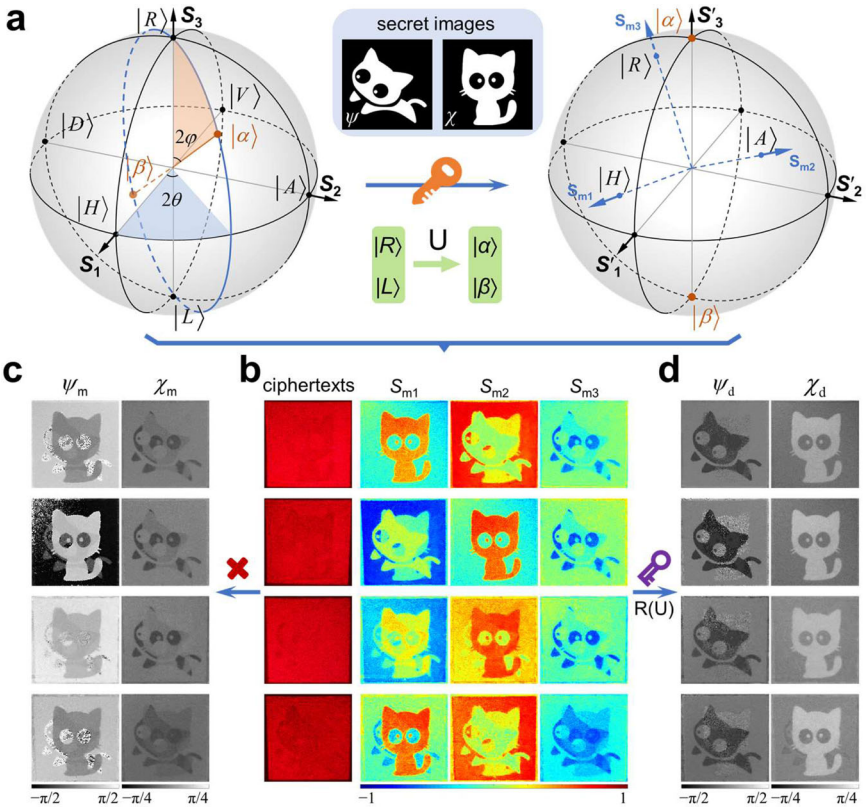

Fig. 5 | Asymmetric encryption scheme. a Rotation transformation of the Poincaré sphere corresponding to the transformation of eigenstates from originally circular polarizations to an arbitrary eigenstate pair $|\alpha\rangle$ and $|\beta\rangle$. Inset (upper): The secret images are encrypted in azimuth and elliptical angles. Inset (bottom): Transformation of eigenstates. **b** Measured ciphertexts and Stokes vectors (S_{m1}, S_{m2}, S_{m3}). **c**, **d** Decrypted images from measured information without and with the private key. The results shown in the first to fourth rows of **b**–**d** correspond to the Poincaré sphere with different eigenstates: $|H\rangle$-$|V\rangle$, $|A\rangle$-$|D\rangle$, $|\alpha_1\rangle$-$|\beta_1\rangle$, $|\alpha_2\rangle$-$|\beta_2\rangle$, and the coordinates of $|\alpha_1\rangle$ and $|\alpha_2\rangle$ are (π/3, π/2) and (0, π/3), respectively.

still conventionally determined in terms of six polarization components $|H\rangle$, $|V\rangle$, $|A\rangle$, $|D\rangle$, $|R\rangle$, $|L\rangle$, which results in that the measured Stokes vector $\mathbf{S}_m = (S_{m1}, S_{m2}, S_{m3})^T$ do not coincide with the transformed Stokes vector $\mathbf{S}' = (S'_1, S'_2, S'_3)^T$ and redefined axes. Because the Stokes vector is equivalent to the angular vector, these secret images cannot be decrypted.

To decrypt, the relationship between eigenstate and Stokes vector transformation can be interpreted by the homomorphic correspondence between SU(2) and SO(3) groups in group theory[51]. The eigenstate transformation can be expressed by the Jones matrix as $(\alpha, \beta)^T = U(R, L)^T$, obviously, U∈SU(2). Meanwhile, the transformation variation of the Stokes vector can be expressed as the modulation of a Mueller matrix $\mathbf{S}' = M_{st}\mathbf{S}$. Noting that, since only variation in polarization is involved and the total intensity remains the same, S_0 needs no consideration. Therefore, the transformation of the Mueller matrix is equivalent to the rotation of the Stokes vector by a certain angle, i.e., $\mathbf{S}' = R(U)\mathbf{S}$, where 3×3 matrix R(U)∈SO(3) represents the three-dimensional rotation matrix. According to the homomorphic correspondence between SU(2) and SO(3), the rotation matrix can be derived as[52,53]

$$R(U)_{ij} = \frac{1}{2}\mathrm{Tr}(\sigma_i U \sigma_j U^{\dagger})\,(i,j = 1,2,3), \tag{8}$$

where, Tr() is the trace of matrix, $\sigma_{i/j}$ is Pauli spin matrix, and † stands for the Hermitian conjugate. Further, considering the special symmetry of the Poincaré sphere, the above relationship can be regarded as the private key in the decryption process to extract the secret images masked in the original Stokes vector.

In the experimental demonstration, we select $|H\rangle$-$|V\rangle$ and $|A\rangle$-$|D\rangle$ eigenstates as the public keys to perform the asymmetric encryption, the transformation relationships are shown in Supplementary Fig. 8. According to these relationships, the rotation matrix can be obtained as

$$R_{HV} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, R_{AD} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}. \tag{9}$$

The measured Stokes vector $(S_{m1}, S_{m2}, S_{m3})^T$ and the angular vector $(\psi_m, \chi_m)^T$ directly calculated without private key are shown in the first two rows of Fig. 5b, c. Obviously, the encrypted information cannot be directly obtained from ψ_m and χ_m. By performing the asymmetric decryption process in Fig. 1e, the secret images can be ultimately extracted from the angle vector $(\psi_d, \chi_d)^T$, as shown in the first two rows of Fig. 5d. Further, experimental demonstrations based on the Poincaré sphere under a pair of linear polarizations on equator line and elliptical polarizations on zero meridian eigenstates are performed, as shown in the last two rows of Fig. 5b–d. Simulation results are shown in Supplementary Figs. 9, 10.

Discussion

It is foreseeable that with the speedy development and multifaceted applications of advanced technologies, such as big data, artificial intelligence (AI), cloud computing, and the like, information security will always be an important challenge. To eliminate the threat of information theft and misuse, it is relatively easier to find attackers in the optical domain rather than on the digital internet. Therefore,

developing novel optical cryptographic techniques are highly desirable to meet the challenges in the information security domain.

Security and capacity are timeless goals in optical cryptography, but here's a caveat that most efforts focus on the functionalities rather than fundamental performance. In our proposal, multi-dimensional and multichannel optical encryption is realized by manipulating the light field with multiple DoFs, and an asymmetric encryption scheme is exploited, in which both security and capacity are well addressed. As proofs of principle, ciphertext-only attack (COA)[54,55], and known-plaintext attack (KPA)[56,57] are employed to evaluate the security performance (detailed in Supplementary Note 7), of which the results show that the Stokes meta-hologram can effectively avoid brute force attack and the security level can be increasingly improved by polarization mask, carrier conversion, and eigenstate transformation.

In addition, the reconstruction quality is another crucial factor in terms such as storage and encryption of biological information (e.g., fingerprint, face image). Usually, in order to accurately identify biological information, there is always a trade-off between recognition performance and security[58,59]. While in the Stokes meta-hologram, the complete decoupled modulation of amplitude, phase, and polarization can encrypt and reconstruct the secret images accurately compared with other holograms (e.g., phase-only and amplitude-only holograms), which ensures that biometric information can be stored in high security and identified accurately[60,61]. Here, the robustness performance is also analyzed, and it is proved that the Stokes meta-hologram has great anti-shearing and certain anti-noise capacities (detailed in Supplementary Note 8). Furthermore, the Stokes operators are the direct extension of their classical counterparts, Stokes meta-hologram may open a new avenue for encoding quantum information via polarization manipulation[62].

To summarize, we proposed and demonstrated an optical encryption scheme, referred to as Stokes meta-hologram, to address the performance issues of optical cryptography. By integrating visual cryptography with a metasurface-assisted encoding technique, the secret images can be vectorially encrypted into unrecognizable visual patterns with spatially distributed polarization based on polarization pattern masking. In experimental verifications, we designed a dual-channel meta-hologram, which introduces polarization-dependent interference through a tetratomic macro-pixel arrangement to construct dual-channel far-field fully-polarized light fields. Hierarchical encryption strategies were exhibited, including Stokes vector encryption, Mueller matrix encryption, and angular vector encryption. Moreover, we presented an asymmetric encryption scheme based on Stokes vector rotation transformation to further boost security. The inherent invisible property of polarization, together with multichannel vectorial encryption, can effectively improve security and capacity. In addition, our scheme largely enriches the functionality breadth of metasurface-based optical cryptography, and could offer an unprecedented information security solution for data transfer and exchange in optical communication.

Methods

Fabrication

The metasurfaces were fabricated based on the process of deposition, patterning, and etching. At first, a 550-nm-thick Poly-Si film was deposited on a 500-μm-thick fused silica substrate by inductively coupled plasma enhanced chemical vapor deposition (ICPECVD), and then a 100-nm-thick Hydrogen silsesquioxane electron beam spin-on resist (HSQ, XR-1541) was spin-coated onto the Poly-Si film. Next, the desired structures were imprinted by using standard electron beam lithography (EBL, Nanobeam Limited, NB5) and subsequently developed in NMD-3 solution (concentration 2.38%) for 2 minutes. Finally, by using inductively coupled plasma etching (ICP, Oxford Instruments, Oxford Plasma Pro 100 Cobra300), the desired structures were transferred from resist to the Poly-Si film.

Experimental characterization

The fabricated metasurfaces were illuminated by a laser beam at $\lambda = 633$ nm, which has uniform intensity and polarization state of $|H\rangle$. The transmitted light beam propagated freely (enough away from the metasurface) and its far-field was projected onto a white screen, then captured by a camera (Supplementary Fig. 11). In Stokes vector measurement, a linear polarizer and a cascade of a linear polarizer and quarter-wave plate were used to obtain the linear polarization components $|H\rangle$, $|V\rangle$, $|A\rangle$, $|D\rangle$, and circular polarization components $|R\rangle$, $|L\rangle$, respectively. Off-axis configuration was adopted to separate dual channels and avoid unmodulated components. The measured efficiencies of metasurfaces were about 60%, the loss mainly stemmed from the absorption of the material and imperfect fabrication, which caused the absorptivity and unmodulated components about 32 and 8% in our experiment.

Data availability

The data that support the findings of this study are available from the corresponding author upon request.

References

1. Katz, J. & Lindell, Y. *Introduction to Modern Cryptography* (CRC Press, 2020).
2. Waks, E. et al. Quantum cryptography with a photon turnstile. *Nature* **420**, 762–762 (2002).
3. Yin, J. et al. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature* **582**, 501–505 (2020).
4. Li, J., Zhang, Y., Chen, X. & Xiang, Y. Secure attribute-based data sharing for resource-limited users in cloud computing. *Comput. Secur.* **72**, 1–12 (2018).
5. Alrawais, A., Alhothaily, A., Hu, C., Xing, X. & Cheng, X. An attribute-based encryption scheme to secure fog communications. *IEEE Access* **5**, 9131–9138 (2017).
6. Li, J., Shi, Y. & Zhang, Y. Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage. *Int. J. Commun. Syst.* **30**, e2942 (2017).
7. Chen, W. & Chen, X. Optical cryptography topology based on a three-dimensional particle-like distribution and diffractive imaging. *Opt. Express* **19**, 9008–9019 (2011).
8. Erven, C. et al. An experimental implementation of oblivious transfer in the noisy storage model. *Nat. Commun.* **5**, 3418 (2014).
9. Li, N. et al. Chaotic optical cryptographic communication using a three-semiconductor-laser scheme. *J. Opt. Soc. Am. B* **29**, 101–108 (2012).
10. Liao, M., He, W., Lu, D. & Peng, X. Ciphertext-only attack on optical cryptosystem with spatially incoherent illumination: from the view of imaging through scattering medium. *Sci. Rep.* **7**, 41789 (2017).
11. Yan, A. et al. Optical cryptography with biometrics for multi-depth objects. *Sci. Rep.* **7**, 12933 (2017).
12. Matoba, O., Nomura, T., Perez-Cabre, E., Millan, M. S. & Javidi, B. Optical techniques for information security. *Proc. IEEE* **97**, 1128–1148 (2009).
13. Liu, H. et al. Single-pixel computational ghost imaging with helicity-dependent metasurface hologram. *Sci. Adv.* **3**, e1701477 (2017).
14. Bao, Y., Ni, J. & Qiu, C. A minimalist single-layer metasurface for arbitrary and full control of vector vortex beams. *Adv. Mater.* **32**, 1905659 (2020).
15. Chen, S., Li, Z., Liu, W., Cheng, H. & Tian, J. From single-dimensional to multidimensional manipulation of optical waves with metasurfaces. *Adv. Mater.* **31**, 1802458 (2019).
16. Choi, C. et al. Hybrid state engineering of phase-change metasurface for all-optical cryptography. *Adv. Funct. Mater.* **31**, 2007210 (2021).
17. Jang, J., Badloe, T. & Rho, J. Unlocking the future of optical security with metasurfaces. *Light Sci. Appl.* **10**, 144 (2021).

18. Georgi, P. et al. Optical secret sharing with cascaded metasurface holography. *Sci. Adv.* **7**, eabf9718 (2021).
19. Qu, G. et al. Reprogrammable meta-hologram for optical encryption. *Nat. Commun.* **11**, 5484 (2020).
20. Song, Q. et al. Broadband decoupling of intensity and polarization with vectorial Fourier metasurfaces. *Nat. Commun.* **12**, 3631 (2021).
21. Li, J. et al. Addressable metasurfaces for dynamic holography and optical information encryption. *Sci. Adv.* **4**, eaar6768 (2018).
22. Zhao, R. et al. Multichannel vectorial holographic display and encryption. *Light Sci. Appl.* **7**, 95 (2018).
23. Zhang, C. et al. Multichannel metasurfaces for anticounterfeiting. *Phys. Rev. Appl.* **12**, 034028 (2019).
24. Guo, X. et al. Full-color holographic display and encryption with full-polarization degree of freedom. *Adv. Mater.* **34**, 2103192 (2022).
25. Zang, X. et al. Polarization encoded color image embedded in a dielectric metasurface. *Adv. Mater.* **30**, 1707499 (2018).
26. Jin, L. et al. Noninterleaved metasurface for (26-1) spin-and wavelength-encoded holograms. *Nano Lett.* **18**, 8016–8024 (2018).
27. Luo, X. et al. Integrated metasurfaces with microprints and helicity-multiplexed holograms for real-time optical encryption. *Adv. Opt. Mater.* **8**, 1902020 (2020).
28. Tang, Y. et al. Nonlinear vectorial metasurface for optical encryption. *Phys. Rev. Appl.* **12**, 024028 (2019).
29. Arbabi, E., Kamali, S. M., Arbabi, A. & Faraon, A. Vectorial holograms with a dielectric metasurface: ultimate polarization pattern generation. *ACS Photonics* **6**, 2712–2718 (2019).
30. Zhou, H. et al. Polarization-encrypted orbital angular momentum multiplexed metasurface holography. *ACS Nano* **14**, 5553–5559 (2020).
31. Zhang, X. et al. Helicity multiplexed spin-orbit interaction in metasurface for colorized and encrypted holographic display. *Ann. Phys.* **529**, 1700248 (2017).
32. Kim, I. et al. Pixelated bifunctional metasurface-driven dynamic vectorial holographic color prints for photonic security platform. *Nat. Commun.* **12**, 3614 (2021).
33. Ren, H. et al. Metasurface orbital angular momentum holography. *Nat. Commun.* **10**, 2986 (2019).
34. Yu, P. et al. Generation of switchable singular beams with dynamic metasurfaces. *ACS Nano* **13**, 7100–7106 (2019).
35. Fang, X., Ren, H. & Gu, M. Orbital angular momentum holography for high-security encryption. *Nat. Photonics* **14**, 102–108 (2020).
36. Mueller, J. B., 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).
37. Fan, Q. et al. Independent amplitude control of arbitrary orthogonal states of polarization via dielectric metasurfaces. *Phys. Rev. Lett.* **125**, 267402 (2020).
38. Liu, M. et al. Multifunctional metasurfaces enabled by simultaneous and independent control of phase and amplitude for orthogonal polarization states. *Light Sci. Appl.* **10**, 107 (2021).
39. Deng, Z. et al. Vectorial compound metapixels for arbitrary nonorthogonal polarization steganography. *Adv. Mater.* **33**, 2103472 (2021).
40. Ren, R. et al. Non-orthogonal polarization multiplexed metasurfaces for tri-channel polychromatic image displays and information encryption. *Nanophotonics* **10**, 2903–2914 (2021).
41. Deng, Z. et al. Full-color complex-amplitude vectorial holograms based on multi-freedom metasurfaces. *Adv. Funct. Mater.* **30**, 1910610 (2020).
42. Deng, Z. et al. Diatomic metasurface for vectorial holography. *Nano Lett.* **18**, 2885–2892 (2018).
43. Song, Q. et al. Ptychography retrieval of fully polarized holograms from geometric-phase metasurfaces. *Nat. Commun.* **11**, 2651 (2020).
44. Yue, F. et al. High-resolution grayscale image hidden in a laser beam. *Light Sci. Appl.* **7**, 17129 (2018).
45. Zhao, R. et al. Nanoscale polarization manipulation and encryption based on dielectric metasurfaces. *Adv. Opt. Mater.* **6**, 1800490 (2018).
46. Deng, J. et al. Multiplexed anticounterfeiting meta-image displays with single-sized nanostructures. *Nano Lett.* **20**, 1830–1838 (2020).
47. Deng, L. et al. Malus-metasurface-assisted polarization multiplexing. *Light.: Sci. Appl.* **9**, 101 (2020).
48. Zheng, P. et al. Metasurface-based key for computational imaging encryption. *Sci. Adv.* **7**, eabg0363 (2021).
49. Guo, X. et al. Metasurface-assisted multidimensional manipulation of a light wave based on spin-decoupled complex amplitude modulation. *Opt. Lett.* **47**, 353–357 (2022).
50. Dubreuil, M., Alfalou, A. & Brosseau, C. Robustness against attacks of dual polarization encryption using the Stokes–Mueller formalism. *J. Opt.* **14**, 094004 (2012).
51. Sternberg, S. *Group Theory and Physics* (Cambridge Univ. Press, 1995).
52. Takenaka, H. A unified formalism for polarization optics by using group theory. *Nouv. Rev. Opt.* **4**, 37 (1973).
53. Takenaka, H. A unified formalism for polarization optics by using group theory I (Theory). *Jpn. J. Appl. Phys.* **12**, 226 (1973).
54. Li, G., Yang, W., Li, D. & Situ, G. Cyphertext-only attack on the double random-phase encryption: experimental demonstration. *Opt. Express* **25**, 8690–8697 (2017).
55. Jiao, S., Lei, T., Gao, Y., Xie, Z. & Yuan, X. Known-plaintext attack and ciphertext-only attack for encrypted single-pixel imaging. *IEEE Access* **7**, 119557–119565 (2019).
56. 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).
57. Hou, J. & Situ, G. Image encryption using spatial nonlinear optics. *eLight* **2**, 3 (2022).
58. Rathgeb, C. & Uhl, A. A survey on biometric cryptosystems and cancelable biometrics. *Eurasip J. Inf. Secur.* **2011**, 3 (2011).
59. Nagar, A., Nandakumar, K. & Jain, A. K. A hybrid biometric cryptosystem for securing fingerprint minutiae templates. *Pattern Recogn. Lett.* **31**, 733–741 (2010).
60. Guo, X. et al. On-demand light wave manipulation enabled by single-layer dielectric metasurfaces. *APL Photonics* **6**, 086106 (2021).
61. Overvig, A. C. et al. Dielectric metasurfaces for complete and independent control of the optical amplitude and phase. *Light Sci. Appl.* **8**, 92 (2019).
62. Solntsev, A. S., Agarwal, G. S. & Kivshar, Y. S. Metasurfaces for quantum photonics. *Nat. Photonics* **15**, 327–336 (2021).

Acknowledgements

This work was supported by the National Key Research and Development Program of China (Grant Nos. 2022YFA1404800 and 2017YFA0303800), the National Natural Science Foundation of China (Grant Nos. 12174309, 11634010, 91850118, 12074312, 12074313, and 11804277), the Natural Science Basic Research Program of Shaanxi (2020JM-104, 2021JQ-895), the Fundamental Research Funds for the Central Universities (Grant No. 3102019JC008), the Innovation Foundation for Doctor Dissertation of Northwestern Polytechnical University (Grant Nos. CX202046, CX202047, CX202048). We thank the Zhiwei Song of the National Center for Nanoscience and Technology for supplying the materials, as well as the Analytical and Testing Center of Northwestern Polytechnical University.

Author contributions

X.G. and P.L. conceived the idea and wrote the manuscript. X.G. conducted the numerical simulations and fabricated the samples. X.G and J.Z. performed the measurements. D.W., S.L., B.W., and S.Q. contributed to data analysis and manuscript revision. P.L. and J.Z. Supervised the work. All the authors analyzed the data and discussed the results. The authors read and approved the final manuscript.

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/s41467-022-34542-9.

Correspondence and requests for materials should be addressed to Peng Li or Jianlin Zhao.

Peer review information *Nature Communications* thanks Shuang Zhang and the other anonymous reviewer(s) for their contribution to the peer review of this work.