ACS Photonics

pubs.acs.org/journal/apchd5

Article

Cryptographic Metasurface Enabled High-Security Information Authentication Using Dual-Beam Off-Axis Illumination

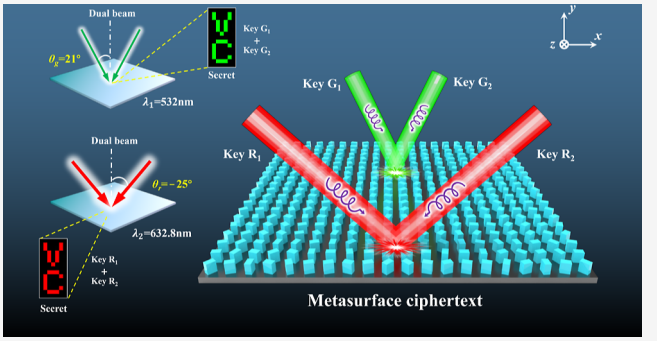
Zhenfei Li, Yuhang Zhang, Shaojie Liu, Jiaru Lin, Xianfeng Wu, Shuo Du, Xudong Bai, Kun Song,* Yahong Liu, Ruonan Ji, Weiren Zhu, Guangzhou Geng,* and Xiaopeng Zhao

Cite This: https://doi.org/10.1021/acsphotonics.5c00770

Read Online

ACCESS | Metrics & More | Article Recommendations | Supporting Information

ABSTRACT: Optical information security has become paramount in data-driven technological systems, where metasurface holography has emerged as a transformative paradigm for high-density optical encryption. However, conventional methods remain constrained by fundamental limitations: multiplexed architectures suffer from inherent interchannel crosstalk, while complex cryptographic algorithms introduce impractical computational overhead. Here, we present a breakthrough visual cryptography platform that utilizes a metasurface hologram with dual-beam off-axis illumination for shared information encryption. The cryptographic scheme physically encodes secret information into the geometric phase profile of metasurface-engineered ciphertexts, with decryption strictly requiring synchronized dual-beam off-axis illumination at predetermined angular configurations. Crucially, single-beam interrogation yields only stochastic speckle-like patterns through partial phase retrieval, providing inherent security against unauthorized access. This architecture achieves channel-independent encryption through angular freedom manipulation, eliminating interchannel crosstalk while preventing potential information leakage through spatial frequency separation mechanisms. The off-axis design not only increases the information capacity, but also establishes a multilayered security framework through the angular degrees of freedom. Both numerical simulations and experimental results validate the effectiveness of the proposed method and demonstrate robust encryption and decryption performance. Our method balances encryption complexity and security, providing a promising solution for next-generation optical encryption devices.



KEYWORDS: *optical metasurface, wavefront manipulation, information authentication, holography*

1. INTRODUCTION

Optical information security has become a critical area due to the increasing reliance on optical technologies for data transmission and storage.[1−3] In an era where data breaches and unauthorized access are rampant, ensuring the security of optical information is paramount. Metasurface holography,[4−7] a pioneering approach, provides a highly controlled and efficient means of encrypting information by manipulating light at the subwavelength scale. This technique exploits the unique properties of engineered surfaces to encode secret information into different structural units of the metasurface, allowing for high-density data storage and complex encryption modes.[8−13] The primary advantage of metasurface holography lies in its ability to hide information within the intricate patterns of the metasurface, making unauthorized access extremely difficult. However, a significant challenge is to balance the security level of the system with the number of metasurface channels.[14−16] As the number of channels increases, the potential for higher levels of security also increases. However, this increased complexity complicates the design process, making it difficult to develop highly secure metasurfaces without introducing significant engineering difficulties.

The integration of traditional encryption algorithms with metasurface holography has significantly improved the security of information transmission. In recent years, numerous innovations have been developed in this field. For example, a multichannel metasurface-based secret sharing encryption mechanism has been proposed in which a single piece of secret information is hidden in three different frequency channels. This approach enables multifrequency shared encryption, which requires simultaneous decryption of all three channels to reconstruct the original secret, thus greatly improving information security.[17] Based on the principles of

Received: April 2, 2025
Revised: August 1, 2025
Accepted: August 4, 2025

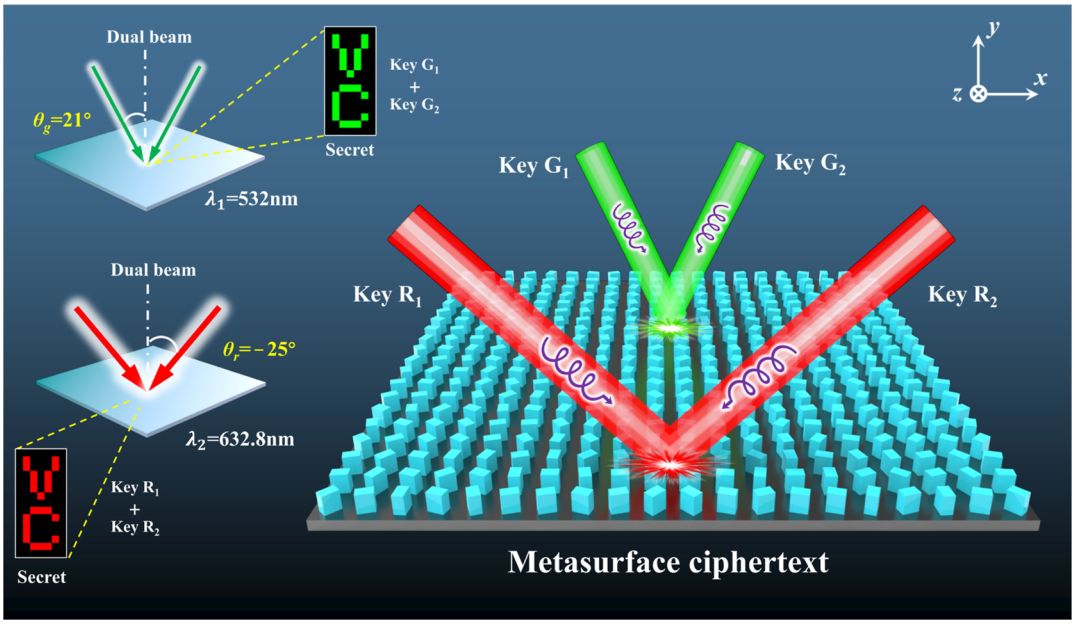


Figure 1. Schematic of information authentication via dual-beam off-axis illumination on cryptographic Metasurface. The metasurface ciphertext is decrypted using 532 nm CP light at off-axis angles of ±21° or 632.8 nm CP light at off-axis angles of ±25°.

secret sharing algorithms, a cascaded metasurface phase sharing encryption strategy was later introduced.[18] In this method, the secret image can only be recovered by cascading and superimposing two metasurfaces. Other innovations include a one-time-pad and high-capacity information encryption scheme based on polarization key sequence sharing, which significantly increases both encryption capacity and security.[19,20] In addition, a hybrid approach combining metasurface imaging, computational ghost imaging, and visual cryptography has been developed that allows keys and ciphertext to be simultaneously embedded in a single metasurface.[21] Recent advances also include the use of single-pixel image reconstruction as an addressing key, allowing the matching of arbitrary letters and numbers on holograms, thereby increasing the capacity and flexibility of information transmission.[22] Another breakthrough is the integration of visual cryptography with optical metasurfaces, resulting in a novel holographic optical encryption method based on stokes vector coding.[23] More recently, a universal optical security strategy using vector visual cryptography has been proposed, which utilizes the polarization degree of freedom and the spatial displacement of electromagnetic waves as key parameters to significantly enhance the security level.[24] Furthermore, orbital angular momentum (OAM) has emerged as a powerful degree of freedom for high-security encryption. Recent work has demonstrated 118 independent channels via wavelength-OAM multiplexing and ultranarrow line widths (2 nm) using sparse *k*-vector filtering.[25] This approach achieves information rates that are over 2500 times higher than those of traditional visual cryptography.

Despite these advances, the reported encryption schemes still face significant challenges. On the one hand, crosstalk or interference between different information channels during decryption can lead to unintended leakage of secret information. On the other hand, the complexity of encryption algorithms often results in cumbersome decryption processes, limiting their practicality. Even with progress in algorithmic optimizations such as cascaded metasurfaces[18] and vector visual cryptography[24] for crosstalk mitigation, inherent computational overhead and potential vulnerabilities remain. To address these limitations, we propose a novel two-beam off-axis illumination method for joint encryption in metasurface holography, which leverages physical angular multiplexing to deliver unique antieavesdropping advantages. This approach encodes secrets into the metasurface's geometric phase through physics-driven mechanisms, avoiding algorithmic complexities. By exploiting spatial frequency separation via off-axis illumination, each channel maps to a unique angular subspace, eliminating crosstalk physically rather than through computational decoupling. In our design, two visual keys (VKs) are encoded in a phase hologram, and successful decryption requires strict adherence to dual-beam off-axis illumination conditions with strict angular tolerance (<1°) for specific wavelengths, such as ± 21° under 532 nm green light or ±25° under 632.8 nm red light. Any misalignment yields only chaotic speckle patterns, preventing decryption via computational means alone, while single-beam or misaligned illumination retrieves only stochastic patterns to avoid partial leakage. Unlike conventional multichannel approaches, our method optimizes decryption within a single holographic channel, conserving resources and eliminating crosstalk through spatial/angular orthogonality. Relying on the metasurface's stable optical response, it resists environmental and computational attacks, suiting high-security scenarios. The proposed off-axis dual-beam encryption strategy offers significant advantages in encryption efficiency, information capacity, security level, and image quality. By striking an optimal balance between encryption robustness and system complexity, this work paves the way for next-generation optical encryption devices with enhanced performance and practicality.

2. RESULTS AND DISCUSSION

2.1. Theoretical Concept and Metasurface Ciphertext Design. Off-axis illumination is pivotal in holographic imaging, as it introduces a spatial phase shift that directly

https://doi.org/10.1021/acsphotonics.5c00770
ACS Photonics XXXX, XXX, XXX−XXX

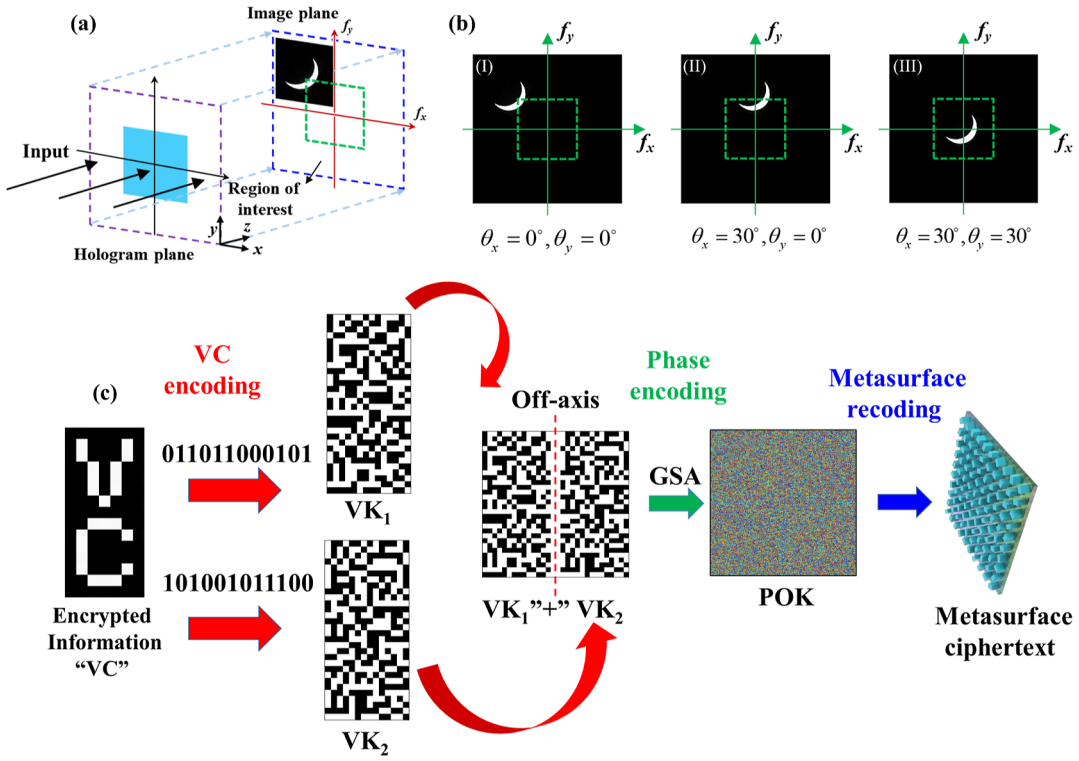


Figure 2. Design principles for off-axis encryption. (a) Correspondence between the hologram plane and the imaging plane. (b) Examples of imaging plane under different off-axis angles of illumination. (c) Schematic for secret shared off-axis encryption process.

manifests as a corresponding shift in the frequency spectrum.[26−28] This unique property allows the off-axis design to dynamically alter the displayed image within the region of interest, making it a powerful tool for optical encryption. The schematic in Figure 1 presents a novel decryption framework for metasurface-encrypted information through precisely controlled off-axis dual-beam illumination. The secret information "VC" (abbreviation for visual cryptography) is embedded in the phase coding of the metasurface, and successful decryption requires precise dual-beam illumination at specific off-axis angles. Any deviations from these specified conditions, including near-axis illumination, single-beam off-axis configurations, or dual-beam illumination with improper angular alignment, invariably lead to the generation of chaotic and unintelligible image patterns, thereby providing an inherent layer of high security. Taking advantage of the metasurface's broadband operating capability, decryption can be performed using either dual 532 nm green circularly polarized (CP) beams with symmetric incident angles of ±21° or 632.8 nm red CP beams with incident angles of ±25° along the x axis. This flexibility further enhances the practicality and robustness of the proposed encryption scheme.

Figure 2 schematically depicts the operational mechanism of off-axis angular spectrum-based shared encryption through dual-beam interference. In holographic imaging, when light is normally incident on a sample, the far-field (Fraunhofer region) holographic image can be expressed as $G(f_x, f_y) = \mathcal{F}\{g(x, y)\}$. Therein, (x, y) represents the coordinates of the metasurface hologram, (f_x, f_y) denotes the coordinates in the frequency domain, $g(x, y)$ is the electromagnetic field distribution just after the sample, and $\mathcal{F}$ represents the Fourier transform. This forms the basis for encoding information into the hologram, as shown in Figure 2a. When the hologram is illuminated by light incident at an angle $\theta(\theta_x, \theta_y)$, the far-field image is modified as

$$G(f_x - \cos(\theta_x)/\lambda - \cos(\theta_y)/\lambda) = \mathcal{F}\{g(x, y)\exp[i2\pi(x\cos(\theta_x) + y\cos(\theta_y))/\lambda]\} \quad (1)$$

here, θ_x and θ_y are the angles between the incident direction and the positive x- and y-axes, respectively. It is obvious that phase modulation in the spatial domain induces predictable spectral translations in the corresponding Fourier plane, with the displacement magnitude satisfying $\Delta k = 2\pi/\lambda\Delta x$, where Δx represents the spatial displacement. In particular, by applying an appropriate angle of incidence, any segment of the hologram can be strategically positioned within a predetermined area (as shown in Figure 2b).[28,29] For example, under the off-axis condition where $\theta_x = 30°$, $\theta_y = 0°$, the crescent-shaped image initially located in the second quadrant (Figure 2b, I) undergoes a translational shift along the x-axis (Figure 2b, II). Furthermore, when the off-axis condition is set to $\theta_x = 30°$, $\theta_y = 30°$, the crescent image moves to the designated region of interest (Figure 2b, III). Based on this theoretical framework, we introduce an off-axis illumination method for shared encryption in metasurface holography. This approach allows for the effective translocation of encoded information from peripheral nontransport regions to the central region of interest, thereby enhancing the visualization and accessibility of critical holographic data.

We then used a visual cryptography encryption scheme to encrypt the secret image "VC", generating two visual keys (VKs).[29−33] The original image can be decrypted by completely overlaying these two keys. According to the (2,2) VSS encryption principle, each pixel of the original image is expanded into a 2 × 2 pixel array, which is then divided into

https://doi.org/10.1021/acsphotonics.5c00770
ACS Photonics XXXX, XXX, XXX−XXX

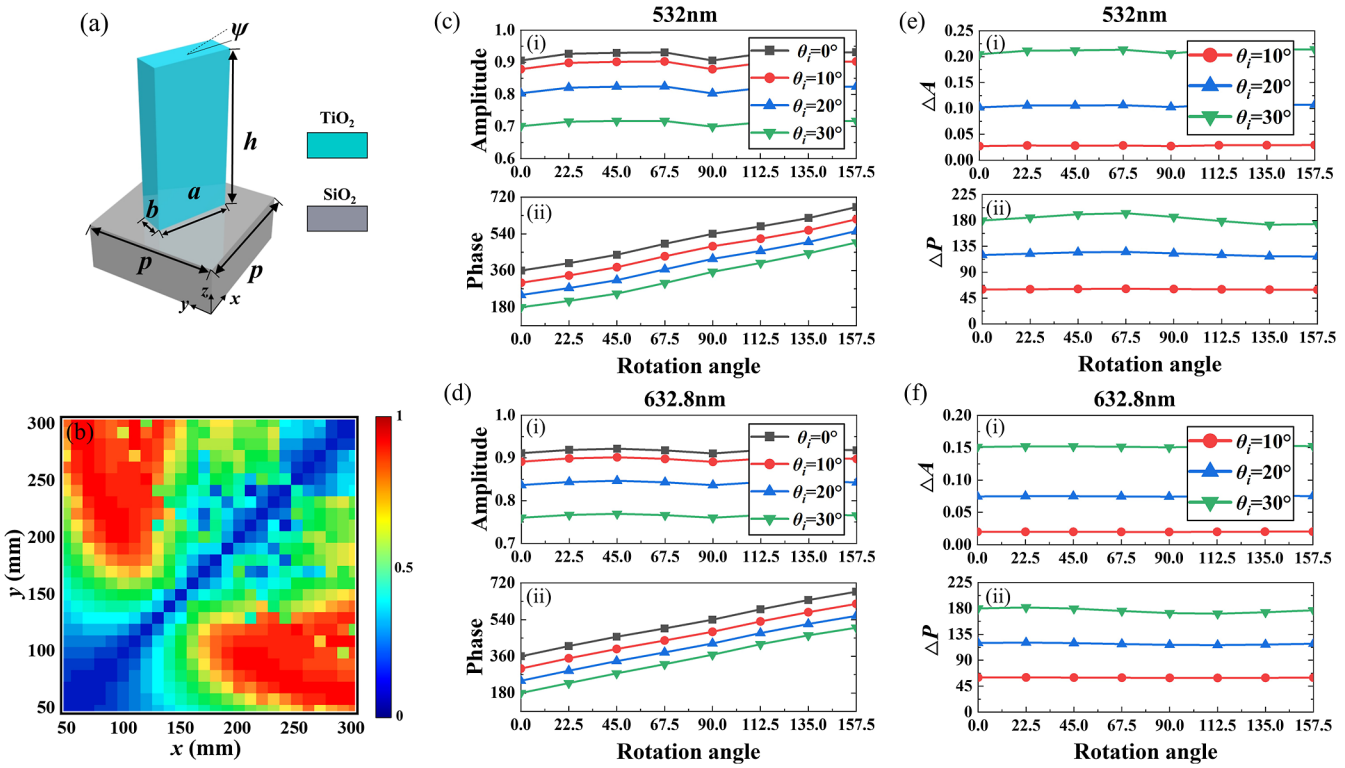


Figure 3. Unit cell design and numerical simulation results. (a) Schematic of the unit cell with optimized parameters: P = 390 nm, h = 600 nm, a = 230 nm, b = 80 nm. ψ Represents the orientation angle of the nanobrick. (b) Simulated cross-polarized transmission coefficients for unit cells with varying nanobrick dimensions under normal incidence of circularly polarized (CP) light. The nanobrick dimensions a = 230 nm, b = 80 nm were selected for subsequent designs due to their optimal transmittance. (c) Amplitude and phase distribution spectra under 532 nm illumination and (d) under 632.8 nm illumination, as the rotation angle of the metasurface unit varies from 0° to 180°. (e) Amplitude and phase differences between various incident angles and the 0° incident condition under 532 nm illumination, and (f) under 632.8 nm illumination, as the rotation angle of the metasurface unit varies from 0° to 180°.

two 2 × 2 subpixel arrays and assigned to the two keys, respectively. The original pixel information can be recovered by superimposing these two keys. For example, a black pixel (denoted as 0) in "VC" is encoded as "0101" in VK_1 and "1010" in VK_2. After overlaying the two keys, the black pixel is decoded as "1111". Similarly, a white pixel (marked as 1) is encoded as "0101" in both VK_1 and VK_2, and the superposition of the two keys decodes the white pixel as "0101" (The detailed encoding process can be found in Note S1 of Supporting Information).

Next, these VKs must be concatenated into a single image for subsequent dual-beam off-axis decryption. Notably, when concatenating the two VKs, we chose a distance of one pixel between the two keys and arranged them symmetrically along the central perpendicular. This arrangement will also result in the angles of the two off-axis beams being symmetrically distributed along the normal line (a discussion of asymmetry will be mentioned below). Then, based on the Gerchberg–Saxton (GS) phase variation algorithm, the phase of the designed ciphertext image was calculated, i.e., it was transformed into phase information suitable for metasurface recording, which also becomes a phase key that cannot directly recognize amplitude information.[34−36] Finally, the calculated phase information was encoded into the metasurface to complete the final information encryption, as shown in Figure 2c. The original information can be decoded by the principle of dual-beam off-axis illumination

$$G_{\text{secret}} = F(\theta_{x_1}, \theta_{y_1}) + F(\theta_{x_2}, \theta_{y_2}) \quad (2)$$

where $\theta_{x_1} = -\theta_{x_2}$ and $\theta_{y_1} = \theta_{y_2} = 0$. This symmetric angular configuration ensures that the two beams constructively overlap in the central region, enabling precise reconstruction of the original information.

2.2. Metasurface Design and Experimental Validation. The unit cell of the metasurface is designed as a TiO_2 nanobrick fabricated on a SiO_2 substrate (Figure 3a), with a period of P = 390 nm, a nanobrick height of h = 600 nm, a length of a = 230 nm, and a width of b = 80 nm. To achieve the desired polarization conversion efficiency, the nanobrick is engineered to function as a half-waveplate, as shown in Figure 3b). By controlling the in-plane orientation angle of the nanobrick from 0° to 180°, the Pancharatnam–Berry (PB) phase[37,38] is tuned to cover a range of 0°−360°.

Figure 3c,d illustrate the simulated amplitude and phase distributions of the unit cells under oblique illumination at wavelengths of 532 and 632.8 nm, respectively, for varying orientation angles. Figure 3e,f depict the amplitude and phase differences between off-axis illumination at 10°, 20°, and 30° and the normal incidence condition. It is evident that, for a fixed off-axis angle, the amplitude and phase variations of the unit cells remain nearly constant across different orientation angles. Additionally, when the off-axis angle is altered, these values exhibit only minor fluctuations. This suggests that, within a certain range of off-axis illumination angles, the amplitude and phase characteristics of the unit cells are largely unaffected by the incident angle, demonstrating optical responses that are nearly equivalent to those under normal

https://doi.org/10.1021/acsphotonics.5c00770
ACS Photonics XXXX, XXX, XXX−XXX

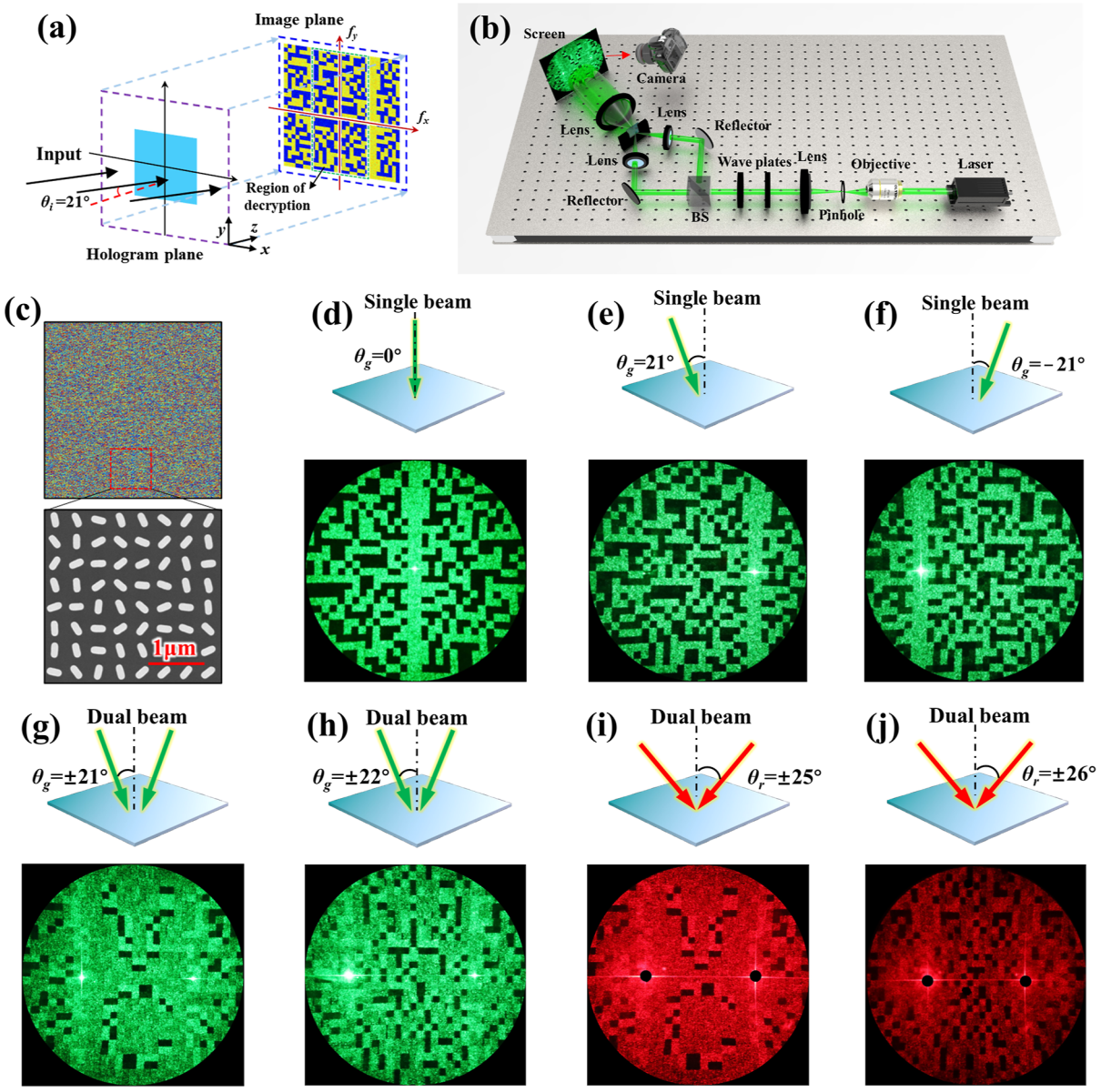


Figure 4. Experimental demonstration of decrypting metasurface ciphertext via dual off-axis illumination (a) Schematic of single-beam irradiation at an off-axis angle. (b) Off-axis dual-beam decryption system, where BS denotes the beam splitter. (c) Phase hologram and corresponding scanning electron microscopy image of the metasurface. (d−f) Far-field holographic images of the metasurface ciphertext under single-beam illumination: (d) normal incidence, (e) off-axis angle of 21°, and (f) off-axis angle of −21°. (g) Decrypted image obtained under 532 nm dual-beam illumination at off-axis angles of ±21°. (h) Chaotic image obtained under 532 nm dual-beam illumination at off-axis angles of ±22°. (i) Decrypted image obtained under 632.8 nm dual-beam illumination at off-axis angles of ±25°. (j) Chaotic image obtained under 632.8 nm dual-beam illumination at off-axis angles of ±26°.

incidence. However, as the off-axis angle increases, the amplitude experiences a slight reduction while maintaining relatively high efficiency, whereas the phase remains virtually unchanged. Furthermore, based on the PB phase principle and the simulation results presented above, it can be concluded that the selected unit cell exhibits broadband operational characteristics. Upon completing the unit cell design, the off-axis encrypted image is converted into a holographic phase using the classical GS algorithm, and the orientation angles of the nanobricks are correspondingly assigned.

Based on the designed broadband characteristics and off-axis response stability of the metasurface unit cells demonstrated above, we experimentally demonstrate the feasibility of the proposed encryption and decryption functionalities. To begin with, it is essential to further clarify the key aspects of dual-beam off-axis illumination for decryption. As shown in Figure 4a, VK_1 becomes visible in the decryption region when illuminated with 532 nm light at an off-axis angle of 21°. Simultaneously, VK_2 also appears in the decryption region when another beam is incident at an off-axis angle of −21°, allowing the encrypted image to be decrypted by superimposing VK_1 and VK_2. A 600 × 600 metasurface array was then fabricated using electron beam lithography (EBL) and atomic layer deposition (ALD). Subsequently, an off-axis dual-beam decryption system was constructed for experimental validation, as shown in Figure 4b. Figure 4c shows the phase hologram and scanning electron microscopy (SEM) image of the metasurface, highlighting a localized region. Under normal

https://doi.org/10.1021/acsphotonics.5c00770
ACS Photonics XXXX, XXX, XXX−XXX

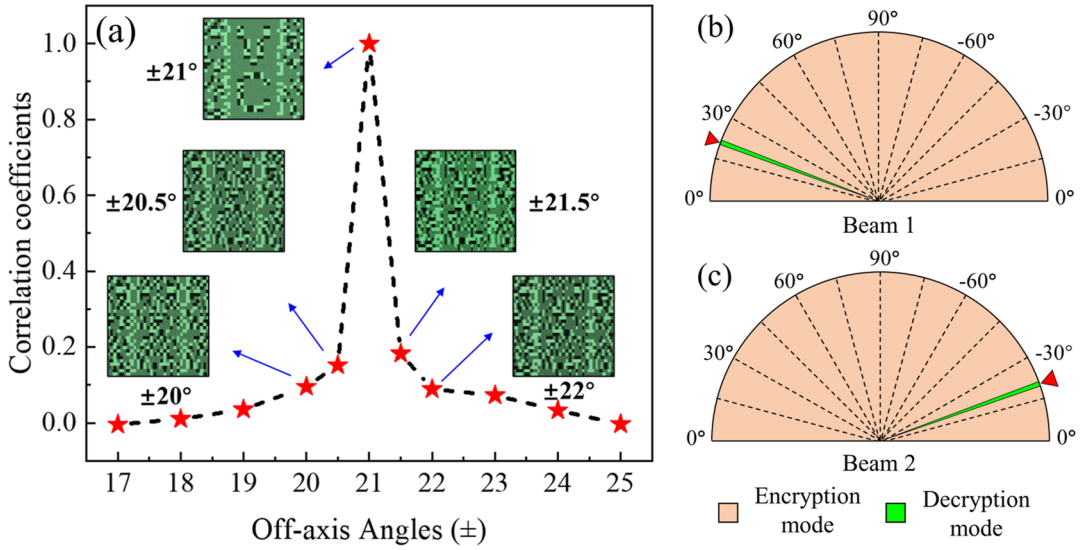


Figure 5. (a) Decryption analysis of the proposed encryption scheme. Encryption and decryption modes of off-axis dual-beam at 532 nm wavelength for (b) beam 1 and (c) beam 2.

incidence at 532 nm, the original amplitude keys VK_1 (left) and VK_2 (right) are observed in the imaging plane, as shown in Figure 4d. When a single beam is incident at an off-axis angle of 21°, the image of the VKs shifts to the right, positioning VK_1 in the center of the imaging plane, as shown in Figure 4e. Similarly, when a single beam is incident at an off-axis angle of −21°, the amplitude key shifts to the left, placing VK_2 in the center of the imaging plane (Figure 4f). When two beams are simultaneously incident at off-axis angles of ±21°, VK_1 and VK_2 are perfectly superimposed, successfully decoding the image "VC" in the imaging plane (Figure 4g). These experimental results robustly validate the correctness and feasibility of the theoretical design. Notably, off-axis illumination spatially separates the zero-order diffraction terms from the first-order terms in the frequency domain. This separation effectively filters out unwanted zero-order components, enabling clearer and more accurate image reconstruction. This advantage is evident in the high-quality decrypted images obtained under precise off-axis illumination conditions.

Additional experiments show that only a chaotic image can be extracted at off-axis angles of ±22°, indicating the sensitivity of the off-axis dual-beam encryption scheme to the angle of incidence, thereby demonstrating its security, as shown in Figure 4h. Furthermore, the metasurface ciphertext is capable of broadband encryption operations. For example, under 632.8 nm illumination, the information can only be decrypted at off-axis angles of ±25°, as shown in Figure 4i. A deviation of only 1° leads to decryption failure, as illustrated in Figure 4j.

It should be noted that in multiwavelength operation, the TiO_2 nanobrick unit cell maintains stable signal-to-noise ratio (SNR) performance without redesign. Its cross-polarized transmission efficiency exceeds 85% at both 532 and 632.8 nm, with <5% amplitude fluctuation across 0°−180° orientation angles, ensuring strong signal strength. Off-axis illumination spatially separates the two wavelengths via distinct decryption angles (±21° for 532 nm, ±25° for 632.8 nm), eliminating crosstalk and keeping SNR >30 dB, comparable to single-wavelength operation. This stability arises from broadband PB phase coverage (0°−360° phase tuning via 0°−180° orientation) and robust optical responses, where amplitude/phase vary minimally with wavelength, supporting reliable multiwavelength operation inherently.

In this study, we show that the images of VK_1 and VK_2 are symmetrically distributed along the central perpendicular axis, which inherently results in a symmetrical distribution of the off-axis illumination angles required for dual-beam decryption. This symmetrical arrangement simplifies the alignment and decryption process under controlled conditions. However, to further enhance the security level of the encryption system, we explore the scenario where VK_1 and VK_2 are not symmetrically positioned. In such cases, the decryption angles have an asymmetric distribution, which significantly complicates the decryption angle key. This added complexity provides an additional layer of security, making it more difficult for unauthorized access. To validate this concept, we performed simulations for the asymmetric arrangement of VK_1 and VK_2. The detailed discussion and results can be found in Note S2 of Supporting Information. This asymmetric angular requirement further enhances the security of the system by introducing additional complexity into the decryption process. In addition, this study overcomes the limitations of conventional holographic imaging, which are constrained by small emission angles to avoid distortion. This significantly enhances data storage capacity. A detailed discussion and results can be found in Note S3 of the Supporting Information. Note that the optical path difference (OPD) between the two incident beams does not affect the performance of the decryption process. This is because the mechanism relies on the incoherent superposition of the diffracted beams' intensities rather than on coherent interference. To quantify this, we conducted additional analyses in Note S4 of the Supporting Information, in which we intentionally introduced an OPD between the two beams.

2.3. Angle-Dependent Security and Image Reconstruction Quality. To quantitatively evaluate the quality of the decrypted images and the security of the proposed off-axis decryption scheme, the correlation coefficients (Co) between the original secret image and the reconstructed image are employed as the primary analysis metric. The correlation coefficient is defined as[39,40]

https://doi.org/10.1021/acsphotonics.5c00770
ACS Photonics XXXX, XXX, XXX−XXX

$$\mathrm{Co}(S_v, U_v) = \frac{E\{[S - E[S]][U - E[U]]\}}{\{E\{[S - E[S]]^2\}E\{[U - E[U]]^2\}\}^{1/2}} \quad (3)$$

where $E[.]$ represents the expectation value, S is the original secret image, U is the reconstructed image.

The decryption system exhibits high sensitivity to the incident angle. Experimental results demonstrate that for light with a wavelength of 532 nm, when dual beams are incident at the precise off-axis angles of ±21°, the amplitude keys VK_1 and VK_2 are perfectly superimposed. This spatial overlap successfully decrypts the target image on the imaging plane, validating the angular alignment mechanism. Under these conditions, the correlation coefficient Co reaches its maximum value of 1, indicating a high reconstruction quality of the original secret image. However, as shown in Figure 5a, when the incident angle deviates from ±21° by more than ±0.5°, the Co value drops significantly, especially when the deviation exceeds ±1°, where the Co value approaches zero. This confirms that the decryption system is highly sensitive to the incident angle, and successful decryption can only be achieved within an extremely narrow angular range of ±21°. Outside this range, the decrypted results show no significant correlation with the original image, thereby ensuring the security of the encrypted information. In Figure 5a, we also present simulated images of the decryption results corresponding to different Co values. It can be observed that as the angle gradually deviates slightly from the decryption angle, the Co value exhibits an exponential decline, accompanied by a sharp drop in the recovery degree of the decrypted images. This further proves the sensitivity of the encryption system to angle variations and its high level of security. To ensure robustness in the face of source jitter or mechanical misalignment while maintaining high security, the system can be integrated with closed-loop active feedback control, such as piezo-driven mounts guided by real-time image correlation, as well as passive stabilization via rigid optomechanical mounts. Together, these strategies mitigate angular deviations to within the critical (±0.5°) tolerance window. These engineering strategies guarantee reliable decryption performance in real-world, high-security scenarios without compromising the system's encryption strength.

Similarly, for beam with a wavelength of 632.8 nm, the system demonstrates comparable sensitivity to the incident angles. Successful decryption occurs only when dual beams are incident at off-axis angles of ±25°. However, any deviation beyond this range, such as ± 1°, leads to a sharp decline in the Co value, rendering the decrypted information unrecognizable. This further underscores the robustness and angle-dependent nature of the encryption scheme, ensuring that the decrypted information remains secure against unauthorized access. Additionally, we further emphasize the security of the proposed encryption system through the following two decryption schematic diagrams (Figure 5b for beam 1 and Figure 5c for beam 2). As shown in Figure 5b,c, we define the decryptable spatial region of our metasurface as a semicircular area ranging from 0° to ±90°. The light red area represents the encryption mode, while the green region denotes the decryption mode. The red triangular symbols indicate the decryption angles involved. For our encryption system, decryption can only be achieved when dual beams simultaneously illuminate within the extremely narrow green range. Outside this range, correct decryption is impossible.

As a result, the quantitative evaluation confirms that the off-axis decryption scheme is highly sensitive to the incident angle, with successful decryption achievable only within precise angular ranges. For 532 nm light, this range is limited to ±21°, while for 632.8 nm light, it is restricted to ±25°. These findings highlight the accuracy and security of the proposed encryption system, making it suitable for high-confidentiality applications. To further demonstrate the versatility and precision of the proposed encryption scheme, we extended its application to encrypt different types of secret information. The detailed discussion and results can be found in Note S5 of Supporting Information. Additionally, to address the security requirements of the system, we implemented a (3, 3) threshold visual cryptography scheme with triple-beam angular multiplexing. A detailed discussion and results can be found in Note S6 of the Supporting Information.

3. CONCLUSION

In summary, we propose a novel cryptographic metasurface based on a visual cryptography scheme enabled by dual-beam off-axis illumination for shared encryption. The decryption process relies on precise off-axis dual-beam illumination at specific incident angles, with a decryption tolerance of less than 1°, ensuring both high encryption accuracy and enhanced security. First, dual off-axis illumination enables the encoding and decoding of distinct information sets at varying incident angles. This angle-dependent access allows for shared information retrieval without the need for complex multi-channel designs. By utilizing different illumination angles, multiple users can independently access their respective data, simplifying system architecture and reducing hardware complexity. Second, off-axis illumination effectively captures high-frequency spatial information typically confined to obscured wave regions. This capability not only significantly increases data storage capacity but also enhances the security of encrypted information, as hidden components remain accessible only under specific illumination conditions. Third, off-axis illumination spatially separates zero-order diffraction terms from first-order terms in the frequency domain. This separation enables efficient filtering of unwanted zero-order components, resulting in clearer and more accurate image reconstruction. By integrating these advantages, our proposed method provides a robust and versatile solution for secure and efficient optical information encryption. It addresses the challenges of multichannel metasurface holography while significantly enhancing both security and image quality. As a result, dual-beam off-axis illumination metasurface holography emerges as a powerful technique for advancing optical information security, with broad applicability across diverse fields.

4. SAMPLE FABRICATION

The metasurface was fabricated on 500 μm quartz substrates that underwent sequential cleaning with acetone and isopropyl alcohol, followed by spin-coating of 600 nm PMMA 495A5 positive e-beam resist and baking at 180 °C for 1 min. A conductive Espacer polymer layer was subsequently applied to prevent charging during electron beam lithography (EBL). Nanostructures were patterned using a JEOL 6300FS EBL system (100 kV, 100 pA) with a dose of 1100 $\mu C/cm^2$ over 200 × 200 μm^2 areas (30 min/area exposure). Postpatterning, the spacer layer was removed via development in 1:3 MIBK/

https://doi.org/10.1021/acsphotonics.5c00770
ACS Photonics XXXX, XXX, XXX−XXX

IPA for 3 min and water rinsing. TiO_2 deposition was then performed by atomic layer deposition (ALD) at 105 °C using alternating H_2O and TDMAT precursor pulses (0.015 s/0.4 s respectively) with 20 s delays between pulses, achieving 0.6 nm/cycle growth over 16 h under 20 sccm N_2 flow. Reactive ion etching with Cl_2 (20 sccm), BCl_3 (6 sccm), and Ar (5 sccm) at 4 mTorr, 400 W plasma power, and 150 V bias removed excess TiO_2 at 1.3−1.6 nm/s for 2 min. Finally, residual resist was dissolved in PG Remover for 24 h, followed by a 2:1 H_2SO_4/H_2O_2 cleaning to complete the metasurface fabrication.

■ ASSOCIATED CONTENT

Supporting Information

The Supporting Information is available free of charge at https://pubs.acs.org/doi/10.1021/acsphotonics.5c00770.

Note S1: The encoding process of the (2, 2) VC scheme for secret image. Note S2: Study on asymmetric off-axis illumination for decryption. Note S3: Analysis of capacity enhancement in off-axis holographic imaging. Note S4: Dual-beam coherent superposition analysis. Note S5: Advanced off-axis encryption scheme for high-precision information security. Note S6: Three-beam off-axis holographic encryption based on high-order VC (PDF)

■ AUTHOR INFORMATION

Corresponding Authors

Kun Song − *MOE Key Laboratory of Materials Physics and Chemistry Under Extraordinary Conditions, and Shaanxi Basic Discipline (Liquid Physics) Research Center, School of Physical Science and Technology, Northwestern Polytechnical University, Xi'an 710129, China*; Email: songkun@nwpu.edu.cn

Guangzhou Geng − *Beijing National Laboratory for Condensed Matter Physics, Institute of Physics, Chinese Academy of Sciences, Beijing 100190, China*; Email: genggz@iphy.ac.cn

Authors

Zhenfei Li − *MOE Key Laboratory of Materials Physics and Chemistry Under Extraordinary Conditions, and Shaanxi Basic Discipline (Liquid Physics) Research Center, School of Physical Science and Technology, Northwestern Polytechnical University, Xi'an 710129, China*; orcid.org/0009-0001-6322-8833

Yuhang Zhang − *MOE Key Laboratory of Materials Physics and Chemistry Under Extraordinary Conditions, and Shaanxi Basic Discipline (Liquid Physics) Research Center, School of Physical Science and Technology, Northwestern Polytechnical University, Xi'an 710129, China*

Shaojie Liu − *MOE Key Laboratory of Materials Physics and Chemistry Under Extraordinary Conditions, and Shaanxi Basic Discipline (Liquid Physics) Research Center, School of Physical Science and Technology, Northwestern Polytechnical University, Xi'an 710129, China*

Jiaru Lin − *MOE Key Laboratory of Materials Physics and Chemistry Under Extraordinary Conditions, and Shaanxi Basic Discipline (Liquid Physics) Research Center, School of Physical Science and Technology, Northwestern Polytechnical University, Xi'an 710129, China*

Xianfeng Wu − *MOE Key Laboratory of Materials Physics and Chemistry Under Extraordinary Conditions, and Shaanxi Basic Discipline (Liquid Physics) Research Center, School of Physical Science and Technology, Northwestern Polytechnical University, Xi'an 710129, China*; orcid.org/0000-0002-4739-3994

Shuo Du − *BOE Technology Group Co., Ltd., Beijing 100176, China; Beijing National Laboratory for Condensed Matter Physics, Institute of Physics, Chinese Academy of Sciences, Beijing 100190, China*

Xudong Bai − *College of Microelectronics, Northwestern Polytechnical University, Xi'an 710129, China*; orcid.org/0000-0001-6503-1922

Yahong Liu − *MOE Key Laboratory of Materials Physics and Chemistry Under Extraordinary Conditions, and Shaanxi Basic Discipline (Liquid Physics) Research Center, School of Physical Science and Technology, Northwestern Polytechnical University, Xi'an 710129, China*

Ruonan Ji − *State Key Laboratory of Infrared Physics, Shanghai Institute of Technical Physics, Chinese Academy of Sciences, Shanghai 200083, China*

Weiren Zhu − *Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, China*; orcid.org/0000-0002-6568-738X

Xiaopeng Zhao − *MOE Key Laboratory of Materials Physics and Chemistry Under Extraordinary Conditions, and Shaanxi Basic Discipline (Liquid Physics) Research Center, School of Physical Science and Technology, Northwestern Polytechnical University, Xi'an 710129, China*; orcid.org/0000-0002-0557-8579

Complete contact information is available at: https://pubs.acs.org/10.1021/acsphotonics.5c00770

Author Contributions

Z. L. conceived the idea, performed the numerical simulations and optical measurements. S. D., and G. G. performed theoretical analysis and sample fabrication. Y. Z, S. L., J. L, X. W., and X. B. performed visualization and data analysis. K. S. and Y. L. prepared the manuscript and supervised the whole project. R. J., W. Z., and X. Z. performed critical revision and editing. All authors discussed the results and participated in the drafting of the manuscript.

Funding

This work was supported by National Natural Science Foundation of China (NSFC) (62401474, 12374296, 62471399); Natural Science Basic Research Plan in Shaanxi Province of China (2024JC-YBMS-554); Fundamental Research Funds for the Central Universities (D5000230353, D5000230165); Gusu Leading Talents of Innovation and Entrepreneurship under Grant (ZXL2024332); CAS Pioneer Hundred Talents Program.

Notes

The authors declare no competing financial interest.

■ REFERENCES

(1) Liu, S.; Guo, C.; Sheridan, J. T. A review of optical image encryption techniques. *Opt. Laser Technol.* **2014**, *57*, 327−342.

(2) Matoba, O.; Nomura, T.; Perez-Cabre, E.; Millan, M. S.; Javidi, B. Optical Techniques for Information Security. *Proc. IEEE* **2009**, *97*, 1128−1148.

(3) Javidi, B. Optical information processing for encryption and security systems. In *Photonic Processing Technology and Applications*; SPIE, 1997; pp 122−128.

(4) Wang, L.; Kruk, S.; Tang, H.; Li, T.; Kravchenko, I.; Neshev, D. N.; Kivshar, Y. S. Grayscale transparent metasurface holograms. *Optica* **2016**, *3*, 1504.
(5) Zheng, G.; Mühlenbernd, H.; Kenney, M.; Li, G.; Zentgraf, T.; Zhang, S. Metasurface holograms reaching 80% efficiency. *Nat. Nanotechnol.* **2015**, *10*, 308−312.
(6) Huang, L.; Chen, X.; Mühlenbernd, H.; Zhang, H.; Chen, S.; Bai, B.; Tan, Q.; Jin, G.; Cheah, K.-W.; Qiu, C.-W.; Li, J.; Zentgraf, T.; Zhang, S. Three-dimensional optical holography using a plasmonic metasurface. *Nat. Commun.* **2013**, *4*, 2808.
(7) Li, L.; Jun Cui, T.; Ji, W.; Liu, S.; Ding, J.; Wan, X.; Bo Li, Y.; Jiang, M.; Qiu, C. W.; Zhang, S. Electromagnetic reprogrammable coding-metasurface holograms. *Nat. Commun.* **2017**, *8*, 197.
(8) Wang, B.; Dong, F.; Li, Q.-T.; Yang, D.; Sun, C.; Chen, J.; Song, Z.; Xu, L.; Chu, W.; Xiao, Y.-F.; Gong, Q.; Li, Y. Visible-Frequency Dielectric Metasurfaces for Multiwavelength Achromatic and Highly Dispersive Holograms. *Nano Lett.* **2016**, *16*, 5235−5240.
(9) Jin, L.; Dong, Z.; Mei, S.; Yu, Y. F.; Wei, Z.; Pan, Z.; Rezaei, S. D.; Li, X.; Kuznetsov, A. I.; Kivshar, Y. S.; Yang, J. K. W.; Qiu, C.-W. Noninterleaved Metasurface for (2^6-1) Spin- and Wavelength-Encoded Holograms. *Nano Lett.* **2018**, *18*, 8016−8024.
(10) Deng, Z.-L.; et al. Diatomic Metasurface for Vectorial Holography. *Nano Lett.* **2018**, *18*, 2885−2892.
(11) Deng, J.; Yang, Y.; Tao, J.; Deng, L.; Liu, D.; Guan, Z.; Li, G.; Li, Z.; Yu, S.; Zheng, G.; Li, Z.; Zhang, S. Spatial Frequency Multiplexed Meta-Holography and Meta-Nanoprinting. *ACS Nano* **2019**, *13*, 9237−9246.
(12) Hu, Y.; Li, L.; Wang, Y.; Meng, M.; Jin, L.; Luo, X.; Chen, Y.; Li, X.; Xiao, S.; Wang, H.; Luo, Y.; Qiu, C.-W.; Duan, H. Trichromatic and Tripolarization-Channel Holography with Noninterleaved Dielectric Metasurface. *Nano Lett.* **2020**, *20*, 994−1002.
(13) Fang, X.; Ren, H.; Gu, M. Orbital angular momentum holography for high-security encryption. *Nat. Photonics* **2020**, *14*, 102−108.
(14) Yuan, H.; Zhong, Z.; Zhang, Y.; Zhang, B. Multi-Channel Image Encryption Based on an All-Dielectric Metasurface Incorporating Near-Field Nanoprinting and Far-Field Holography. *Adv. Opt. Mater.* **2023**, *11*, 2300352.
(15) Gao, F.; Zhou, X.; Tao Lu, L.; Deng, J.; Yan, B. Seven-channel nanoprinting and meta-holography based on metasurface-space and angular multiplexing. *Results Phys.* **2023**, *52*, 106925.
(16) Li, Z.; Rukhlenko, I. D.; Zhu, W. Microwave metasurface hologram for holographic imaging and its data encryption applications. *J. Opt.* **2022**, *24*, 113001.
(17) Li, Z.; Premaratne, M.; Zhu, W. Advanced encryption method realized by secret shared phase encoding scheme using a multi-wavelength metasurface. *Nanophotonics* **2020**, *9*, 3687−3696.
(18) Georgi, P.; Wei, Q.; Sain, B.; Schlickriede, C.; Wang, Y.; Huang, L.; Zentgraf, T. Optical secret sharing with cascaded metasurface holography. *Sci. Adv.* **2021**, *7*, No. eabf9718.
(19) Li, Z.; Kong, X.; Zhang, J.; Shao, L.; Zhang, D.; Liu, J.; Wang, X.; Zhu, W.; Qiu, C.-W. Cryptography Metasurface for One-Time-Pad Encryption and Massive Data Storage. *Laser Photonics Rev.* **2022**, *16*, 2200113.
(20) Li, Z.; Du, S.; Wu, X.; Zhang, J.; Zhang, Y.; Song, K.; Liu, Y.; Geng, G.; Zhu, W.; Zhao, X.; Gu, C. One-Time Pad Incoherent Encryption with Optical Meta-Ciphertext and Dynamic Visual Keys. *ACS Photonics* **2024**, *11*, 4434−4443.
(21) Zheng, P.; Li, J.; Li, Z.; Ge, M.; Zhang, S.; Zheng, G.; Liu, H.-C. Compressive Imaging Encryption with Secret Sharing Metasurfaces. *Adv. Opt. Mater.* **2022**, *10*, 2200257.
(22) Yan, J.; Wei, Q.; Liu, Y.; Geng, G.; Li, J.; Li, X.; Li, X.; Wang, Y.; Huang, L. Single Pixel Imaging Key for Holographic Encryption Based on Spatial Multiplexing Metasurface. *Small* **2022**, *18*, 2203197.
(23) Guo, X.; Li, P.; Zhong, J.; Wen, D.; Wei, B.; Liu, S.; Qi, S.; Zhao, J. Stokes meta-hologram toward optical cryptography. *Nat. Commun.* **2022**, *13*, 6687.
(24) Zhang, F.; Guo, Y.; Pu, M.; Chen, L.; Xu, M.; Liao, M.; Li, L.; Li, X.; Ma, X.; Luo, X. Meta-optics empowered vector visual cryptography for high security and rapid decryption. *Nat. Commun.* **2023**, *14*, 1946.
(25) Meng, W.; Fröch, J. E.; Cheng, K.; Pi, D.; Li, B.; Majumdar, A.; Maier, S. A.; Ren, H.; Gu, M.; Fang, X. Ultranarrow-linewidth wavelength-vortex metasurface holography. *Sci. Adv.* **2025**, *11*, No. eadt9159.
(26) Matsushima, K. Shifted angular spectrum method for off-axis numerical propagation. *Opt. Express* **2010**, *18*, 18453−18463.
(27) Li, X.; Chen, L.; Li, Y.; Zhang, X.; Pu, M.; Zhao, Z.; Ma, X.; Wang, Y.; Hong, M.; Luo, X. Multicolor 3D meta-holography by broadband plasmonic modulation. *Sci. Adv.* **2016**, *2*, No. e1601102.
(28) Goodman, J. W.; Cox, M. E. Introduction to Fourier Optics. *Phys. Today* **1969**, *22*, 97−101.
(29) Naor, M.; Shamir, A. Visual cryptography. In *Advances in Cryptology EUROCRYPT'94*; Springer: Berlin, Heidelberg, 1995; pp 1−12.
(30) Shyu, S. J.; Huang, S. Y.; Lee, Y. K.; Wang, R. Z.; Chen, K. Sharing multiple secrets in visual cryptography. *Pattern Recogn.* **2007**, *40*, 3633−3651.
(31) Ateniese, G.; Blundo, C.; Santis, A. D.; Stinson, D. R. Extended capabilities for visual cryptography. *Theor. Comput. Sci.* **2001**, *250*, 143−161.
(32) Zhou, Z.; Arce, G. R.; Crescenzo, G. D. Halftone visual cryptography. *IEEE Trans. Image Process.* **2006**, *15*, 2441−2453.
(33) Ateniese, G.; Blundo, C.; De Santis, A.; Stinson, D. R. Visual Cryptography for General Access Structures. *Inf. Comput.* **1996**, *129*, 86−106.
(34) Gerchberg, R. W. A practical algorithm for the determination of phase from image and diffraction plane pictures. *Optik* **1972**, *35*, 237−246.
(35) Fienup, J. R. Phase retrieval algorithms: a comparison. *Appl. Opt.* **1982**, *21*, 2758−2769.
(36) Zalevsky, Z.; Mendlovic, D.; Dorsch, R. G. Gerchberg−Saxton algorithm applied in the fractional Fourier or the Fresnel domain. *Opt. Lett.* **1996**, *21*, 842−844.
(37) Kang, M.; Feng, T.; Wang, H.-T.; Li, J. Wave front engineering from an array of thin aperture antennas. *Opt. Express* **2012**, *20*, 15882−15890.
(38) Gutiérrez-Vega, J. C. Pancharatnam−Berry phase of optical systems. *Opt. Lett.* **2011**, *36*, 1143−1145.
(39) Situ, G.; Zhang, J. Multiple-image encryption by wavelength multiplexing. *Opt. Lett.* **2005**, *30*, 1306−1308.
(40) Wei, Q.; Huang, L.; Li, X.; Liu, J.; Wang, Y. Broadband Multiplane Holography Based on Plasmonic Metasurface. *Adv. Opt. Mater.* **2017**, *5*, 1700434.

https://doi.org/10.1021/acsphotonics.5c00770
ACS Photonics XXXX, XXX, XXX−XXX