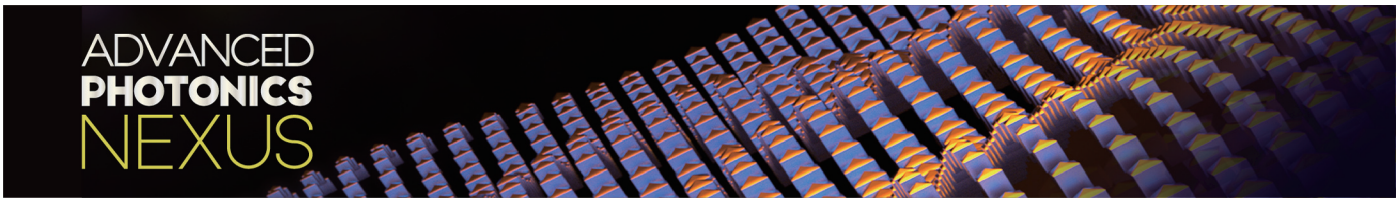
Research Article



Multiuser computational imaging encryption and authentication with OFDM-assisted key management

Hongran Zeng,[a,†] Ping Lu,[a,†] Xiaowei Li,[a,†,*] Lingling Huang,[b] Chaoyun Song,[c] Dahai Li,[a] In-kwon Lee,[d] Seok-Tae Kim,[e] Qiong-Hua Wang,[f,*] and Yiguang Liu[g,*]

[a]Sichuan University, School of Electronics and Information Engineering, Chengdu, China
[b]Beijing Institute of Technology, School of Optics and Photonics, Beijing Engineering Research Center of Mixed Reality and Advanced Display, Beijing, China
[c]King's College London, Department of Engineering, London, United Kingdom
[d]Yonsei University, Department of Computer Science, Seoul, Republic of Korea
[e]Pukyong National University, Department of Information and Communications, Busan, Republic of Korea
[f]Beihang University, School of Instrumentation and Optoelectronic Engineering, Beijing, China
[g]Sichuan University, College of Computer Science, Chengdu, China

Abstract. Single-pixel imaging (SPI) enables an invisible target to be imaged onto a photosensitive surface without a lens, emerging as a promising way for indirect optical encryption. However, due to its linear and broadcast imaging principles, SPI encryption has been confined to a single-user framework for the long term. We propose a multi-image SPI encryption method and combine it with orthogonal frequency division multiplexing-assisted key management, to achieve a multiuser SPI encryption and authentication framework. Multiple images are first encrypted as a composite intensity sequence containing the plaintexts and authentication information, simultaneously generating different sets of keys for users. Then, the SPI keys for encryption and authentication are asymmetrically isolated into independent frequency carriers and encapsulated into a Malus metasurface, so as to establish an individually private and content-independent channel for each user. Users can receive different plaintexts privately and verify the authenticity, eliminating the broadcast transparency of SPI encryption. The improved linear security is also verified by simulating attacks. By the combination of direct key management and indirect image encryption, our work achieves the encryption and authentication functionality under a multiuser computational imaging framework, facilitating its application in optical communication, imaging, and security.

Keywords: computational imaging; optical encryption; optical authentication; key management.

Received Jun. 1, 2024; revised manuscript received Jul. 16, 2024; accepted for publication Aug. 1, 2024; published online Aug. 27, 2024.

[DOI: 10.1117/1.APN.3.5.056016]

1 Introduction

With the increasing demand for personal privacy and the growing scarcity of communication resources, multiuser encryption has become an important trend for the future development of optical cryptography. Among the optical cryptography methods, single-pixel imaging (SPI), as a typical type of indirect computational imaging technique, has revealed significant potential due to the non-visual and encryption-like imaging principle.[1–4] Instead of depending on the direct encrypting quality, SPI encryption approaches rather are based on the correlation of a series of modulated patterns and an invisible target. The corresponding imaging principle can be described as

*Address all correspondence to Xiaowei Li, xwli@scu.edu.cn; Qiong-Hua Wang, qionghua@buaa.edu.cn; Yiguang Liu, liuyg@scu.edu.cn

†These authors contributed equally to this work.

$$Y_k = \sum_x \sum_y \mathbf{M}^{(x,y)} \times \mathbf{P}_k^{(x,y)}, \tag{1}$$

where Y_k denotes the intensity value in the k'th detection, and $\mathbf{M}^{(x,y)}$ and $\mathbf{P}_k^{(x,y)}$ denote the spatial distribution of the plaintext and the k'th pattern projected, respectively. Since the series of patterns can be used to encrypt object specifics over non-line-of-sight range,[5–7] various SPI encryption schemes have been developed to enhance the security, including spatial-multiplexed SPI encryption[8] and algorithm-dependent image hiding.[9] SPI encryption is also combined with other technologies, such as holography,[10] visual encryption,[11] and computer vision technologies,[12] to expand the application schemes. By alternatively applying a photosensitive surface without a lens, human poses can be securely recovered in a sequence of modulated intensity.[12] Also, by the combination of steganography and a Malus metasurface, the huge burden of transmitting patterns of SPI encryption can also be decreased.[13] However, due to the linear imaging principle in Eq. (1) and broadcast behavior, the multiuser SPI framework has not been investigated well. Specifically, obvious linearity in the SPI ciphertext is caused by the convolutional process, therefore triggering the security vulnerability. Besides, receivers in different locations can only receive the same intensity sequence at one time.[5,6] Thus, only the same plaintext can be recovered by users, limiting the channel transmitting capacity. It can be hard for the direct design on plaintext SPI encryption algorithms to solve these two issues based on Eq. (1).

Fortunately, key management, playing as the upstream layer of plaintext encryption responsible for all the tasks of related keys,[14–17] can remarkably promote the security of multiuser services.[18–22] To protect the privacy in the internet of vehicles, certificateless-group-assisted,[23] quantum-key-based,[24] and artificial-intelligence-enabled[18] key management methods are proposed. Encryption-based key management methods are also applied in other multiuser scenarios, such as elliptic-curve-cryptography-based key management in multi-sensor networks[25] and Chebyshev chaotic map key management in blockchain authentication.[26] Different from digital key management, optical key management requires an entity to carry keys, while the metasurface providing the information at the submillimeter level[27–30] and efficiency for multiplexing degrees of freedom of light[31–33] can decrease the exposure risk during physical key transmission. At the same time, orthogonal frequency division multiplexing (OFDM) is able to transmit parallel data streams on independent subcarriers while overlapping the sequential characteristic of signals,[34] being viable for accommodating multiple cryptographical keys.

Thus, in this paper, we provide a complete solution to multiuser SPI cryptography and authentication framework combined with OFDM-assisted key management. Within the framework, regional and global encryptions are first conducted to form a composite intensity sequence to be transmitted to different individuals, simultaneously generating the corresponding keys specially used by users. Then, keys are isolated into independent frequency points and asymmetrically encapsulated into a Malus metasurface by OFDM-assisted key management. By the key distribution of the metasurface in a polarized manner, users can eventually recover their designated SPI images and verify their authenticity. To verify the security of the multiuser SPI framework, five pioneering SPI encrypting works relying on direct plaintext encryption and our scheme are compared. The results show that the multiuser scheme can resist multiple types of attacks and can verify the authenticity even when one of the users is compromised to Eve. Our work facilitates the development of indirect computational imaging security into the multiuser framework, enhancing its application in secure optical communication, anticounterfeiting, and security.

2 Principle and Methodology

2.1 Multiuser SPI Encryption and Authentication Framework

Figure 1 shows the procedure of N users. N plaintexts with an authentication image are first encrypted and transmitted by the Fourier SPI encryption. While in key space, a pair of private key sets $\mathbf{\Psi}$ and $\mathbf{\Phi}$ dedicated to decryption and authentication, respectively, and a commonly used key set $\mathbf{\Omega}$ for all users are generated. Enabled by OFDM-like and RSA asymmetric coding, $\mathbf{\Psi}$ and $\mathbf{\Phi}$ are multiplexed and cross-encapsulated as $\mathbf{\Lambda}$, sealed with $\mathbf{\Omega}$ into the light envelope of a Malus metasurface. In the receiving end, two polarized channels of the metasurface are inversely extended into $2N + 1$ keys (i.e., three types of key sets) for N users. Receiving the bucket signal, users can retrieve plaintexts privately using their own keys and further collaboratively verify the authenticity of the decrypted images. In the following sections, we will quantify this process, taking $N = 8$ as a case study, to demonstrate the detailed mechanism of our method.

2.2 Composite Fourier SPI Encryption

As shown in Fig. 2, the Fourier SPI encryption is composed of regional encryption, containing whitening and permutation, basically providing internal privacy among users, and global encryption, including diffusion and Fourier SPI, of all users for authentication and countering malicious attacks from Eve. In order to conduct the encryption, whitening, permutation, and diffusion keys $\{\mathbf{W}_k^{m\times n}\}$, $\{\mathbf{P}_k^{u\times v}\}$, and $\{\mathbf{D}_q^{3m\times 3n}\}$ are generated in terms of chaos and will be further processed in terms of key management.

For regional encryption, as shown in Fig. 3(a), plaintexts $\mathbf{I}_k$, $k = 1,2,\ldots,9$, with the identical dimension of $m \times n$ pixels (i.e., here 96×96) are planarly concatenated into a triplex-grid image $\mathbf{I}_{\text{concate}}$, in which $\mathbf{I}_1 \sim \mathbf{I}_8$ are the private plaintexts for each user whereas the common $\mathbf{I}_9$ is attached in case of counterfeiting for authentication of all users. Because the direct super-pixel permutation of plaintexts without any alteration of image pixel values can still reveal the content information and are affected by ciphertext analysis, as shown in Fig. 3(b), the integrated image $\mathbf{I}_{\text{concate}}$ should be whitened pixel-by-pixel in advance to cover the basic texture.

Therefore, for each $\mathbf{I}_k$, we define nine chaotic masks $\mathbf{W}_k^{m\times n}$, $k = 1,2,\ldots,9$, independently corresponding to different initial conditions of chaos, including the type index of generation functions ζ_k^{whiten}, the starting values of chaotic sequence α_k^{whiten}, the sequence size $\varepsilon^{\text{whiten}} = m$, and the initial number to start count β_k^{whiten}. The generation of the whitening masks by the four chaos conditions is shown in Fig. 4. The type of generation functions is independently chosen among the Bernoulli map, piecewise linear chaotic map (PWLCM), and Lorenz map. Then, we integrate the following generated masks $\mathbf{W}_k^{m\times n}$ into triplex-grid form and XOR it with $\mathbf{I}_{\text{concate}}$: $\mathbf{I}_{\text{whiten}}^{3m\times 3n} = \mathbf{I}_{\text{concate}} \oplus \mathbf{W}_{\text{concate}}^{3m\times 3n}$.

Subsequently, the adjacent $i \times j$ (i.e., here 12×12) regular pixels in $\mathbf{I}_k$ form a super-pixel, and $3u \times 3v$ super-pixels

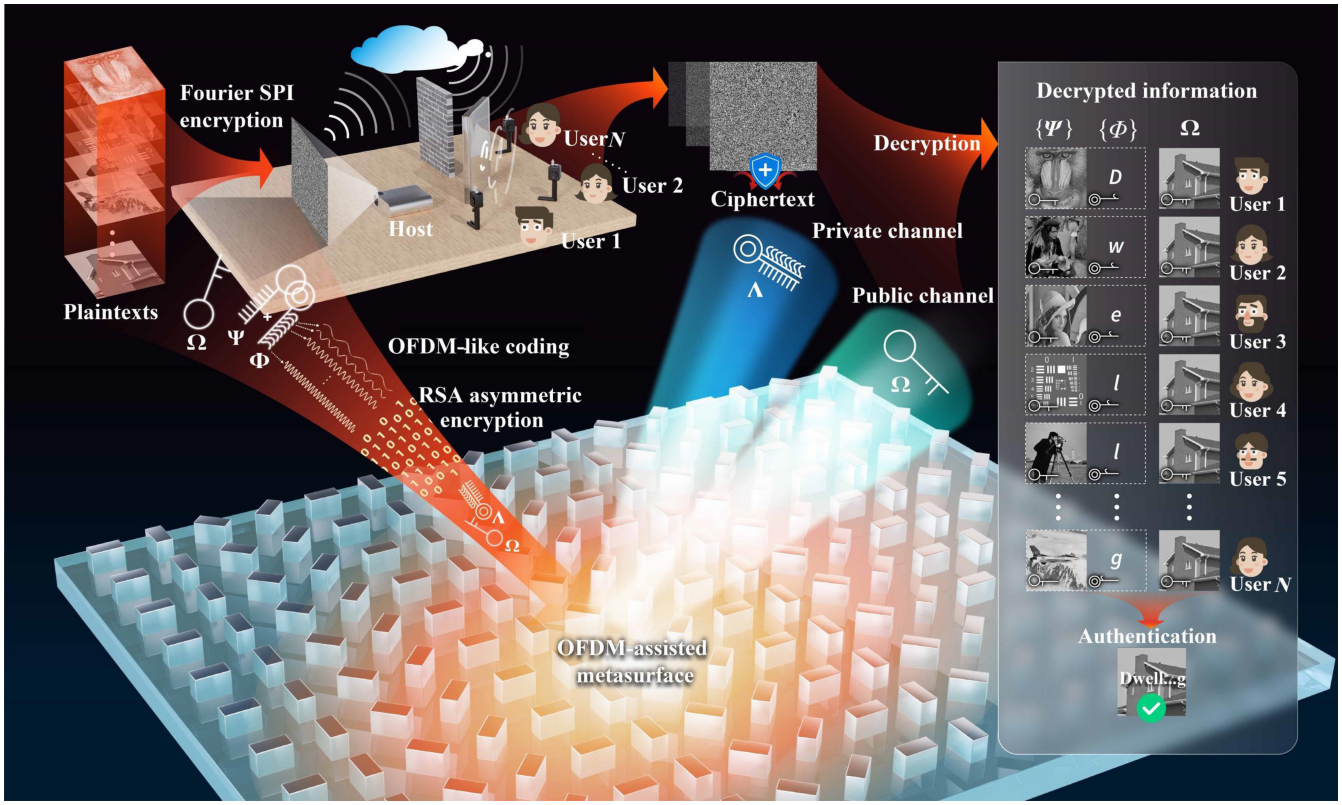


Fig. 1 Concept of the multiuser SPI security framework. *N* plaintexts are compositely encrypted and transparently transmitted to all users by the composite SPI Fourier encryption. Simultaneously, three types of key sets $\mathbf{\Psi}$, $\mathbf{\Phi}$, and $\mathbf{\Omega}$ are encapsulated into the metasurface for key distribution. After receiving the bucket signal, users access the metasurface to acquire their own secret keys to decrypt different plaintexts. The private $\{\mathbf{\Psi}\}$ and $\{\mathbf{\Phi}\}$ sets represent the $2N$ decomposed keys from $\mathbf{\Lambda}$, a pair of which corresponds to the plaintext and authenticating information for each user. $\mathbf{\Omega}$ denotes a common key set for authentication.

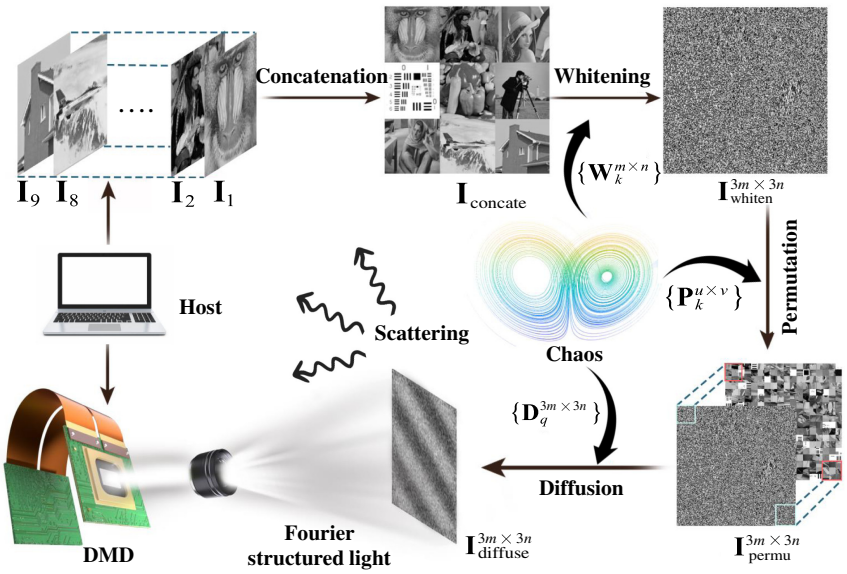


Fig. 2 Schematic of the Fourier SPI encryption. The host digitally processes $\mathbf{I}_1 \sim \mathbf{I}_9$ and configures a Fourier SPI optical path, where a digital micromirror device (DMD) and Fourier structured light are presented. To improve the efficiency of the following key processing, the initial conditions of chaos instead of the generated masks are encapsulated.

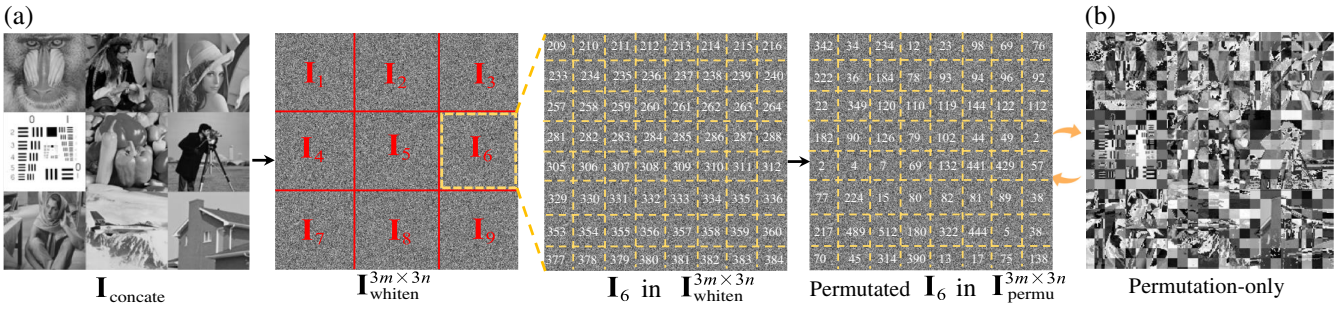


Fig. 3 Schematic of regional encryption. (a) Texture information and spacing distribution of pixels can be scrambled by whitening and permutation, whereas (b) permutation-only encryption still can reveal the content information.

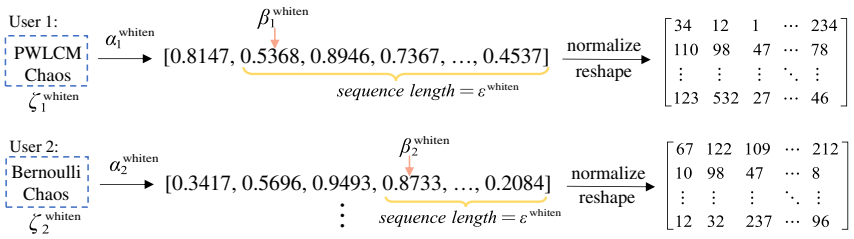


Fig. 4 Flowchart for generating different whitening masks $\mathbf{W}_k^{m\times n}$ by chaos.

integrate the whole $\mathbf{I}_{\text{whiten}}^{3m\times 3n}$, with the coordinate index ranging from 0 to 575. Note that $u = m/i$ and $v = n/j$. Afterward, we re-utilize the PWLCM chaos to generate the corresponding permutation matrix $\mathbf{P}_{\text{concate}}^{3u\times 3v}$ to scramble the index 0 to 575, equivalent to switching the position of each super-pixel within the entire $\mathbf{I}_{\text{whiten}}^{3m\times 3n}$: $\mathbf{I}_{\text{permu}}^{3m\times 3n} = \pi(\mathbf{P}_{\text{concate}}^{3u\times 3v}, \mathbf{I}_{\text{whiten}}^{3m\times 3n})$. For the $\mathbf{I}_k$ of each user, the permutation key is noted as $\mathbf{P}_k^{u\times v}$ and $\{\mathbf{P}_k^{u\times v}\}$, $k = 1,2,\ldots,9$, constituting the whole $\mathbf{P}_{\text{concate}}^{3u\times 3v}$.

For global encryption, a series of masks $\{\mathbf{D}_q^{3m\times 3n}\}$, $q = 1,2,\ldots,Q$, are sequentially generated in terms of the initial chaos conditions $\{\alpha_q^{\text{diffuse}}, \zeta_q^{\text{diffuse}}, \varepsilon_q^{\text{diffuse}}, \beta_q^{\text{diffuse}}\}$. The rows and columns of $\{\mathbf{D}_q^{3m\times 3n}\}$ are applied as the basic unit to finish Q rounds of diffusion specific to $\mathbf{I}_{\text{permu}}^{3m\times 3n}$. In general, $Q \geqslant 2$ should be satisfied to achieve an effective avalanche effect against cryptanalysis, particularly differential analysis. Thus, two-round diffusion is used in our design, and an instance flowchart of diffusion is shown in Fig. 5. XOR is used in the first diffusion, and MOD calculation is used in the second round so that only one mask $\mathbf{D}_1^{3m\times 3n}$ can be used to realize the effective diffusing performance, declining the workload of further key processing.

Eventually, the diffused image $\mathbf{I}_{\text{diffuse}}^{3m\times 3n}$ is illuminated by Fourier structured light to be broadcasted to users. For the generation of structured light, four-step phase shifting is applied in SPI encryption. Four Fourier patterns are designed to be $\mathbf{J}_\phi = a + b\cos(2\pi f_x x + 2\pi f_y y + \phi)$, $\phi = [0, \pi/2, \pi, 3\pi/2]$, where (x, y) and f_x, f_y denote the two-dimensional (2D) Cartesian coordinates in the scene and spatial frequency distribution of images, respectively, while a and b denote the average image intensity and image contrast, respectively. After the illumination of each set of four-step phase shifted patterns, four intensities O_ϕ can be acquired by each user. Following this process, a corresponding Fourier coefficient of the target can be further obtained by $C(f_x, f_y) = [O_0(f_x, f_y) - O_\pi(f_x, f_y)] + j \cdot [O_{\pi/2}(f_x, f_y) - O_{3\pi/2}(f_x, f_y)]$.[35] Finally, after collecting all the Fourier coefficients, users only have to operate inverse fast

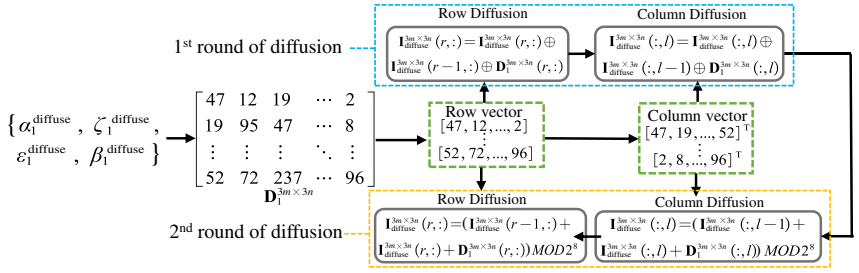


Fig. 5 Schematic of diffusion encryption.

Fourier transform (IFFT) to recover the image without correlating with any pattern. The complete code demonstration of composite Fourier encryption can be found in Sec. S1 in the Supplementary Material.

Different encrypting steps generate keys with different functions. According to the functions, we divide the keys as two groups for separate management. Regional encryption is privately used for each user to independently protect their own plaintext. Thus, $\{\mathbf{W}_k^{m\times n}, \mathbf{P}_k^{u\times v}\}$, $k = 1,2,\ldots,8$, form Ψ_k and $\mathbf{\Psi} = [\Psi_1, \Psi_2, \ldots, \Psi_8]^{\mathrm{T}}$, is treated as the access of the metasurface to $\mathbf{I}_1 \sim \mathbf{I}_8$. Global encryption is commonly used for all users countering external attacks from Eve. Thus, $\{\mathbf{W}_9^{m\times n}, \mathbf{P}_9^{u\times v}\}$ and $\{\mathbf{D}_q^{3m\times 3n}\}$ are grouped as $\mathbf{\Omega}$, also publicly used to retrieve the authentication image $\mathbf{I}_9$. Simultaneously, to verify the authentication image, we also generate a synonym (i.e., dwelling) from $\mathbf{I}_9$ as an authentication key, namely token, for parallel OFDM-like modulation.

2.3 OFDM-Assisted Key Management

As shown in Fig. 6(a), after SPI encryption, key management is used to isolate and distribute corresponding keys to different users, addressing the contradiction between multiuser privacy and SPI broadcast transparency. Figure 6(b) shows the encapsulating flowchart of key management. The authenticating token generated from $\mathbf{I}_9$ is first divided into eight parallel components, which are further isolated onto separate OFDM carriers, producing $\mathbf{\Phi}$ as the eight private keys for synergic authentication and a multiplexed ciphertext $\mathbf{S}$. Then, $\mathbf{\Psi}$ and $\mathbf{\Phi}$ are further cross-encapsulated by RSA to terminate the progressive dependency of key generation. Consequently, each user can use the asymmetric RSA pair to decrypt their keys coded in the OFDM sequence. Finally, nanobricks are used to modulate the polarization state of the cross-encapsulated keys pixel-by-pixel, forming a discrete and stable structure for key service.

For OFDM-like coding, the complex Fourier bases in traditional OFDM algorithms are first replaced by trigonometric bases. Other modulating bases, such as Chebyshev polynomial and Hadamard sequences, are also considered as one of the encoding options (see Sec. S1 in the Supplementary Material) to enlarge the key space. In addition, to demodulate the coded sequence without distortion in user ends, the adjacent subcarriers are designed to secretly differ by one complete period in an OFDM symbol duration with a sampling rate $N_s = 32$. The symbol rate is regarded as $R_{\mathrm{symbol}} = 1$ symbol/s, equivalent to the bit rate. Moreover, to ensure separability when decrypting plaintexts, frequency interval Δf among subcarriers should be greater than the R_{symbol}, whereas to handle more users, Δf is derived as unit 1 to be as less as possible. The modulating process of the token is shown in Fig. 7(a) and Fig. S1 in the Supplementary Material. The token is first compartmentalized into single letters as sub-tokens. Each sub-token (e.g., the initial "D" corresponding to user 1) is then transferred into an ACSII character as we regulate the metasurface to be monochrome in view of the error tolerance of keys and possible errors triggered by manual recognition of grayscale pixels, noted as a binary vector $\mathbf{s}_t = [s_{t,1}, s_{t,2}, \ldots, s_{t,8}]^{\mathrm{T}}$, $t = 1,2,\ldots,8$, (e.g., "D" $\rightarrow$ "01000100"). Then, eight frequency indices denoted as $\mathbf{\Phi} = [\Phi_1, \Phi_2, \ldots, \Phi_8]^{\mathrm{T}}$ are randomly initialized and assigned to eight users as the first-level keys. The subcarrier of t'th user is written as $\mathbf{y}_{\Phi_t} = [y_{\Phi_t,1}, y_{\Phi_t,2}, \ldots, y_{\Phi_t,N_S}]$, and the orthogonality is expressed as Eq. (2), where $t \neq z$ and $n = 1,2,\ldots,N_s$:

$$\langle \mathbf{y}_{\Phi_t} \cdot \mathbf{y}_{\Phi_z} \rangle = \langle \mathcal{R}e[e^{j2\pi(f_I+\Phi_t\Delta f)n}] \cdot \mathcal{R}e[e^{j2\pi(f_I+\Phi_z\Delta f)n}] \rangle = 0. \tag{2}$$

Note that f_I denotes the randomly chosen initial frequency. Based on this principle, each symbol of $\mathbf{s}_t$ is separately modulated by the assigned subcarrier in terms of Eq. (3):

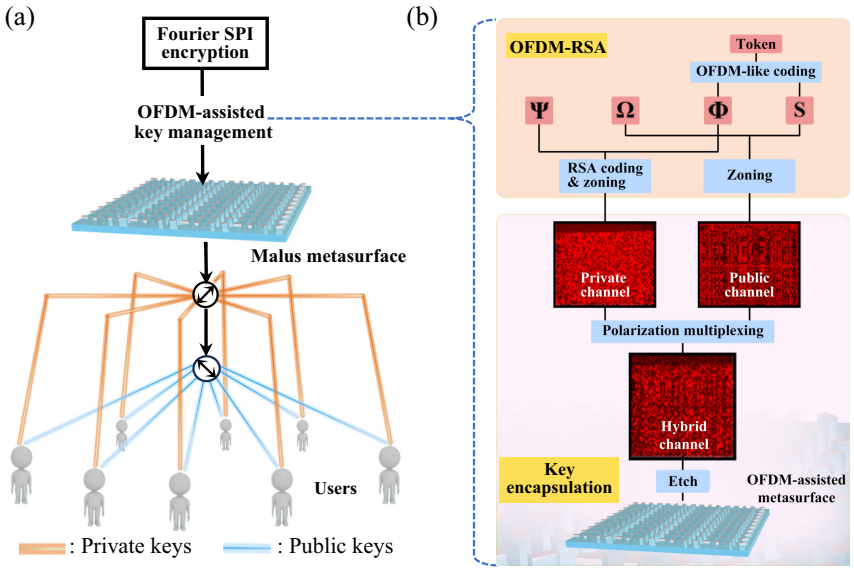


Fig. 6 Design concept of OFDM-assisted key management. (a) Connecting role of key management between SPI encryption and multiple users. (b) Keys are separately processed by OFDM-like coding and RSA, zoned as the private channel and public channel, which are further physically confused by polarization and etched into the metasurface.

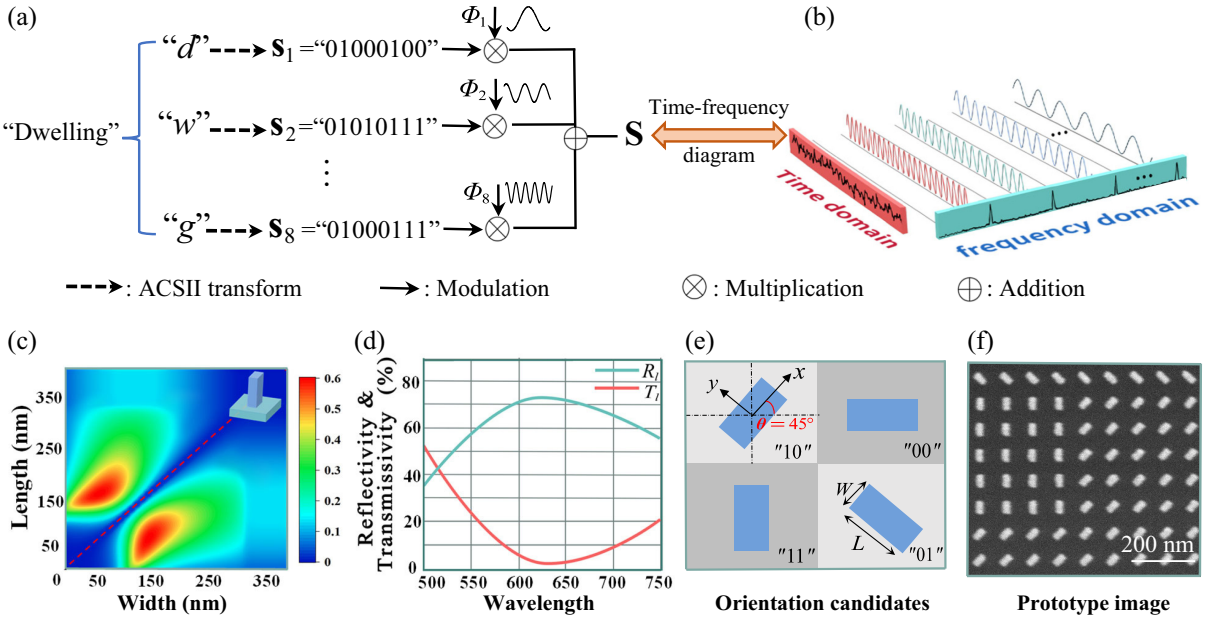


Fig. 7 Design principle of the OFDM-assisted key management. (a) Flowchart of OFDM-like coding. (b) Time-frequency diagram of **S**. (c) 2D parameter optimization of nanobricks, in which the upper region of the red dashed line represents the RPRE of long-polarized light and the lower region indicates that of the short-polarized light. (d) Simulated R_l and T_l. The Malus metasurface is designed to operate in the reflective mode. (e) Four states of the unit cell, where "1" and "0" denote the positive and negative states of the private (public) channel of the metasurface, respectively. (f) Top view of the prototype captured by a scanning electron microscopy with scale bar of 200 nm.

$$\mathbf{S} = \sum_{t=1}^{8} \mathbf{s}_t \cdot \mathbf{y}_{\Phi_t}, \tag{3}$$

where $\mathbf{S}$ is an $8 \times N_s$ matrix. $\mathbf{s}_t$ and $\mathbf{y}_{\Phi_t}$ are vectors in size 8×1 and $1 \times N_s$, respectively. From $\mathbf{S}$, the p'th row represents the sum of the p'th character of each user modulated by their corresponding carrier: $\mathbf{S}(p,:) = s_{1,p} \cdot \mathbf{y}_{\Phi_1} + s_{2,p} \cdot \mathbf{y}_{\Phi_2} + \ldots + s_{8,p} \cdot \mathbf{y}_{\Phi_8}$. Thus, it can be seen that sub-tokens for all users are mixed into a unified temporal signal, characterized by extensive overlapping that precludes the disclosure of the individual key component, as shown in Fig. 7(b). However, in the frequency domain, $\mathbf{S}$ allows for distinct separation of each user's keys. Finally, the continuous matrix $\mathbf{S}$ is reshaped into a one-dimensional (1D) sequence and transformed into the discrete binary form in terms of IEEE Standard 754 to be recorded in the metasurface.

Symmetric encryption, such as OFDM-like coding, can trigger an extension of the trust chain, continuously requiring another cryptography to protect the keys in turn produced by the one before. Thereby, as a root of trust, OFDM-like coding needs to be further integrated with RSA asymmetric coding to terminate the progressive dependency. Through the process, t'th user produces a unique pair of keys, in which the public $(n,e)_t$ is broadcasted and the private $(n,d)_t$ is preserved. Receiving $(n,e)_t$ for each user, the host connects the private key set Ψ_t and Φ_t in serial and encapsulates them as a whole plaintext to acquire the binary ciphertext Λ_t. As a result, $\mathbf{\Lambda} = [\Lambda_1, \Lambda_2, \ldots, \Lambda_8]^{\mathrm{T}}$, which contains all information about $\mathbf{\Psi}$ and $\mathbf{\Phi}$ recorded in the private channel, whereas $\mathbf{S}$ and $\mathbf{\Omega}$ are publicly used for members generally with a lower security requirement, is arranged serially to form the public channel expression of the metasurface, as shown in Fig. S2 in the Supplementary Material (see S3 in the Supplementary Material).

Finally, a Malus metasurface is used to record the processed keys to provide information entities, integrating the 17 subchannels of keys into a whole as well. A rectangular aluminous nanobrick is designed to be etched on a top of glass substrate, forming a unit nanobrick cell, where $L = 180$ nm, $W = 100$ nm, $H = 50$ nm, and CS $= 360$ nm. The size of the unit cell is optimized according to the relative polarized reflection efficiency (RPRE), as shown in Fig. 7(c), and the corresponding operating wavelength is set as $\lambda = 625$ nm. Simultaneously, the simulated reflectivity R_l and transmissivity T_l of the incident light polarized along the long-axis (l) are shown in Fig. 7(d) (for more optimization details, see Sec. S3 in the Supplementary Material). According to the Jones derivation, the orientation angle is selected among the four: 0, 45, 90, and 135 deg, as shown in Fig. 7(e). Specifically, the private channel of $\mathbf{\Lambda}$ and public channel of $\mathbf{S}$ and $\mathbf{\Omega}$ are set as $\alpha_1 = 45$ deg, $\alpha_2 = 90$ deg and $\alpha_1 = 135$ deg, $\alpha_2 = -90$ deg, respectively, where α_1 and α_2 denote the rotating angle of a polarizer and an analyzer, respectively. Note that as long as the metasurface can clearly display key information to achieve the security function of keys, the parameters of the nanobricks, including material or shape, are not strictly confined. Finally, the metasurface of 172.8 μm $\times$ 172.8 μm with the size of 96 pixel $\times$ 96 pixel is fabricated, as shown in Fig. 7(f). Each pixel is composed of a 5×5 nanobrick array.

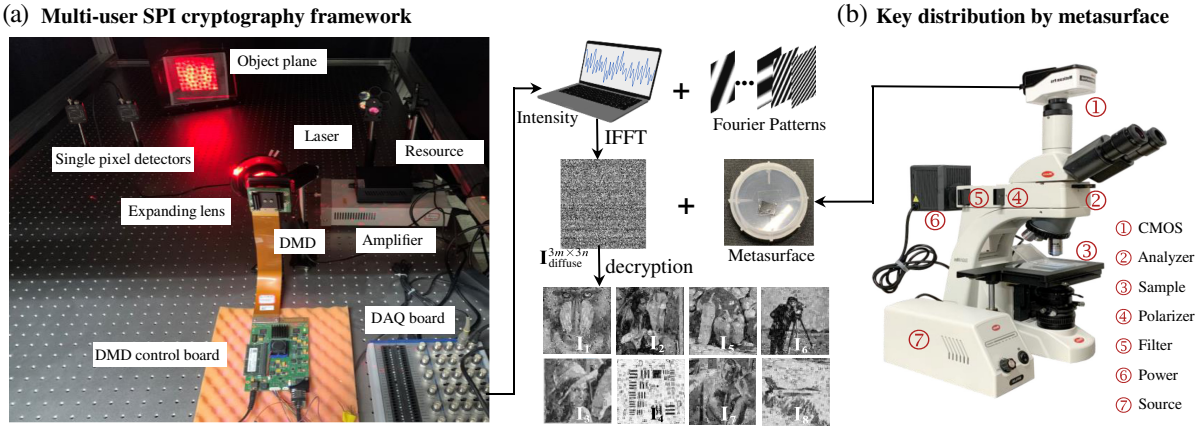


Fig. 8 Optical setup of the proposed scheme. (a) Setup of the multiuser SPI encryption framework and decryption mechanism. (b) Configuration of key distribution.

3 Results

3.1 Experimental Decryption and Authentication

The optical experimental configurations of the multiuser SPI encryption and authentication framework with the metasurface are shown in Fig. 8. The setup of the multiuser SPI encryption framework and decryption mechanism is shown in Fig. 8(a). The laser beam is emitted by a light source operating at the wavelength of 625 nm. Then, the laser beam is reflected by a DMD (Amphenol V-7001 VIS), and the modulated patterns are expanded by an expanding lens. Subsequently, the patterns are projected onto the object plane and gathered by a bucket detector (Thorlabs DET100A2 320 to 1100 nm) equipped with a photodiode amplifier (Thorlabs PDA200C) and a data acquisition (DAQ) board (NI USB-6343). During the experiment, since two bucket detectors are owned only, four repeated experiments were conducted, where the two intensity detectors were separately positioned in different locations in each experiment to imitate the original eight users.

For decryption and receiving the bucket signals, eight users first need to operate the IFFT to acquire $\mathbf{I}_{\text{diffuse}}^{3m\times 3n}$. Then, each user accesses the metasurface to decode their keys. The experimental setup of acquiring keys by the metasurface is based on a BA310MET-T microscope, as shown in Fig. 8(b). First, they access the public channel of the metasurface and extract $\mathbf{D}_1^{3m\times 3n}$ from $\mathbf{\Omega}$ for global decryption. Sequentially, for RSA decryption, the t'th user accesses the private channel to decode Λ_t by $(\Phi_3, \Psi_3) = \Lambda_3^{d_3}\ MOD\ n_3$, obtaining the Ψ_t for regional decryption and Φ_t for OFDM demodulation. Note that when the t'th user accesses the private channel, all the Λ_t actually have been exposed to him. However, because the t'th user only owns the unpublished $(n, d)_t$, only the ciphertext Λ_k can be decoded, whereas the other $\Lambda_z, t \neq z$ are still under protection of RSA. After acquiring Ψ_t and Φ_t, the user eventually can recover $\mathbf{I}_t$ of his own privately, as shown in Fig. 8(a), during which the decryption is symmetrically inverse to the regional encryption of the composite Fourier SPI encryption.

For authentication, $\mathbf{\Omega}$ is first reconstructed in the public channel to retrieve the common $\mathbf{I}_9$. Implementing the decrypted $\mathbf{\Phi}$ by RSA decryption, users recover subcarriers afterward to demodulate $\mathbf{S}$, acquiring their secret sub-token by $\mathbf{s}_t = \mathbf{S} \cdot \mathbf{y}_{\Phi_t}^{\mathrm{T}}$. During the calculation, the p'th symbol in $\mathbf{s}_t$ corresponding to the t'th user can be represented by the inner product of the p'th row in $\mathbf{S}$ and carrier $\mathbf{y}_{\Phi_t}$: $s_{t,p} = \langle \mathbf{S}(p, :), \mathbf{y}_{\Phi_t} \rangle = \langle (s_{1,p} \cdot \mathbf{y}_{\Phi_1} + \ldots + s_{8,p} \cdot \mathbf{y}_{\Phi_8}), \mathbf{y}_{\Phi_t} \rangle$. After ACSII-to-character transforms, the eight letters are consociated in sequence, and it is evaluated whether the combined word matches $\mathbf{I}_9$, as shown in Fig. 9. The synergetic scheme is specially established for the multiuser scenario since a single letter can convey a multitude of implications, such as "*D*" revealing "document," "paddle," and "wood." Unless a sufficient number of users cooperate with others, the splitting letter can reveal little information. Therefore, the authenticating credibility (i.e., house element in $\mathbf{I}_9$) can still be maintained even if one of the users is compromised to Eve.

3.2 Security Assessment by Confrontation and Numerical Analysis

3.2.1 Deep differential attack

The essence of an encrypting scheme consists of confrontation. Thus, we develop a cracking model of SPI encryption, namely a deep differential attack (technical details are supplied in S5 in the Supplementary Material), to intuitively demonstrate the security and capacity of the proposed multiuser scheme. The security and capacity are assessed in terms of the external and internal attack, respectively (see Sec. S5.1 in the Supplementary Material). Five current works without key management, including single-user SPI-metasurface encryption,[13] single-user SPI encryption,[8,11,36] and multiuser SPI encryption,[6] are also attacked for comparison. The numbers of encrypting steps are 3, 2, 1, 4, and 2, indicating different levels of attacking difficulty. Also, we carry on the confrontation on three different datasets including MINIST, USC-SIPI, and University-1652 to verify the security generalization of the multiuser SPI encryption framework.

As shown in Fig. 10, the ciphertexts of the five current SPI encrypting schemes are approximately cracked. Intuitively, the sensitive profiles, particularly letters or foreground objects, can be roughly recognized though the recovered ones differ from the ground truths and legally decrypted versions. This inconsistency occurs mainly due to the different methods and depths of encryption, which means that the errors can gradually accumulate as the cryptanalysis progresses step by step. But for our method, the external attack turns out to be ineffective in seeking

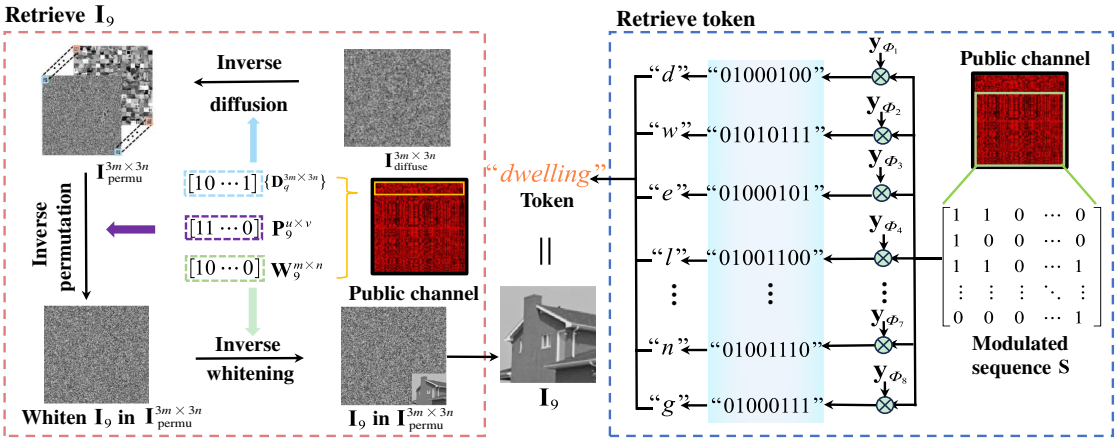


Fig. 9 Synergetic authentication mechanism. The red dashed box shows the retrieving process of $\mathbf{I}_9$, whereas the blue dashed box displays the retrieving process of the token by the OFDM-assisted key management.

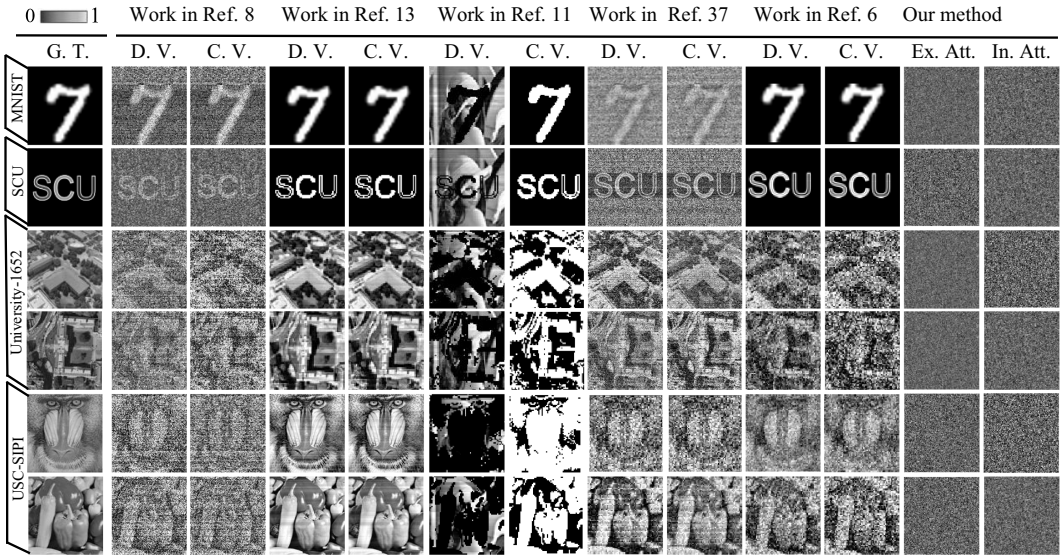


Fig. 10 Attacking results from a deep differential attack. G. T., D. V., and C. V. denote ground truth, the legal decrypted version, and cracked version, respectively. Ex. Att. and In. Att. mean the external and internal attacking results from Eve and internal user, respectively. The attack mode is only directed toward the pertinent stages of SPI encryption. The measures unrelated to encryption, such as steganography and holography, are assumed to be prior-known by default. SCU is the abbreviation of Sichuan University and is used with the permission of Sichuan University.

correlation between the SPI optical paths and key management, showing the effective security of the multiuser SPI cryptography framework. In addition, the imperceptible outcomes suggest that internal users also are unable to decipher the plaintexts of others. Thus, the independent encrypted transmission of each user and, consequently, the SPI encryption capacity under the multiuser scheme are available. Provided that the security and capacity of multiple users are satisfied, the multi-user SPI encryption and authentication framework is achieved.

3.2.2 Brute force attack

Further, a brute force attack is conducted for the SPI image encryption and key management. Technically, the brute force attack against OFDM-assisted key management refers to the attack against the authentication key $\mathbf{S}$ and ciphertext key $\mathbf{\Lambda}$ presented in the two meta-channels separately, whereas the attack against Fourier SPI encryption refers to the bucket signal $\mathbf{o}$.

For the attack against OFDM-assisted key management, authentication key $\mathbf{S}$ should be first considered. During the process, a set of candidates of OFDM modulation should be first determined, which is also the merit compared to the optical encryption inspired by code division multiplexing (CDM).[5,37] Specifically, only one type of parameter (i.e., the index of orthogonal codes) pertains in CDM to encrypt plaintexts, whereas the type of the modulation bases, symbol modulating categories, N_s, f_1, and Δf in OFDM, can supply more complex

Table 1 Key space of Fourier SPI image encryption and key management.

Objective	Key category	Key space	$>2^{100}$
Key management on the metasurface	7	$\approx 10^{400}$	Pass
SPI Fourier encryption for images	4	$\approx 10^{80}$	Pass

key space. For $\mathbf{\Lambda}$, a 1024-bit key is needed for RSA encryption, and thus the key space is roughly on the order of 2^{1024}.

For the brute force attack against SPI Fourier image encryption, the key length of chaos conditions $\{\alpha_k^{\text{whiten}}, \zeta_k^{\text{whiten}}, \varepsilon^{\text{whiten}}, \beta_k^{\text{whiten}}\}$ of whitening mask $\{\mathbf{W}_k^{m\times n}\}$ refers to 64-8-8-8-bit. The generating conditions of $\mathbf{P}_k^{u\times v}$ and $\mathbf{\Omega}$ are presented in bits in the same way. Thus, in total, the key space of the key management algorithm and image encryption is shown in Table 1. The results show that both the key spaces are larger than the minimal requirement 2^{100},[38] showing the ability to resist the brute force attack.

3.2.3 Tampering attack

Encryption attacks not only involve the illegal acquirement of plaintexts, such as the deep differential attack and brute force attack, but also include the destruction of ciphertexts, such as tampering, forgery, and noise disturbance. Hence, we study the resilience to errors of the OFDM-like encoded sequence $\mathbf{S}$ within the metasurface, in scenarios where tampering or defective pixels occur due to partial detachment of nanostructures or oxidation. White dots are assumed to be wrongly recognized with the error ratios from 0% to 25%, as shown in Fig. 11(a). To evaluate the general applicability of the error tolerance, we randomly select pixels to introduce errors.

In Fig. 11(a), it is observed that the token can be completely recovered within the error ratio equaling to 10%. Besides, as the error ratio increases to 20%, the recovered "dwelling" begins to experience misspelling but still remains within the range of single letter error. When one-fourth of the metasurface is tampered with or rendered unrecognizable, errors in the spelling of the letters "*e*" and "*l*" in the token begin to appear. More intuitively, Fig. 11(b) compares the corresponding bit error rate (BER) performance of $\mathbf{S}$ and the direct recognition of string $\mathbf{s}_t$ without OFDM correction. The results show that our OFDM BER always remains lower than the BER of direct recognition. This is because, by the modulation of each sub-token, the effective authentication information is dispersed across the orthogonal carriers, thereby mitigating the sharp recognition offset of the sub-token, indicating our OFDM-metasurface is robust against tampering attacks.

3.2.4 Numerical assessment

Except for direct confrontation, we also conducted numerical analysis on the SPI ciphertext, including the light intensity sequence $\mathbf{o}$ and $\mathbf{I}_{\text{diffuse}}^{3m\times 3n}$. Figures 12(a) and 12(b) show an intensity sequence and three-dimensional randomness view of three local sequences sampled from the sequence. It is observed that the broadcasted $\mathbf{o}$ does not reveal any obvious characteristic and the kurtosis of $\mathbf{o}$ sequence equals 4.4×10^{-7}, showing that there is no obvious intensity outlier for Eve to analyze.

Figure 12(c) presents the histogram of $\mathbf{I}_{\text{diffuse}}^{3m\times 3n}$. From the results, the pixel distribution of $\mathbf{I}_1 \sim \mathbf{I}_9$ has been eliminated, and no statistical information is leaked. Simultaneously, the variance, chi-square, and flatness are adopted to quantitatively analyze the histogram. The variance of $\mathbf{I}_{\text{diffuse}}^{3m\times 3n}$ is 339.61, and flatness equals 0.0031, indicating the uniform alteration of pixels in the ciphertext. Also, the chi-square is calculated as 268.49 lower than the threshold $\chi^2_{0.05} = 293.25$, where the significant level is set as 0.05. Figure 12(d) shows the weak correlation of pixels in horizontal, vertical, and diagonal directions, and the quantitative correlation in the three directions are 0.00526, 0.00217, and 0.00283, respectively. The global entropy is calculated as 7.9977. Except for the global entropy, we also calculate the local Shannon entropy to test the indeterminacy of the regional area in $\mathbf{I}_{\text{diffuse}}^{3m\times 3n}$. Thirty blocks are randomly divided in $\mathbf{I}_{\text{diffuse}}^{3m\times 3n}$, and the size of each segmented block should be set as 44×44.[39] Subsequently, the local Shannon entropy is derived as 7.9028, satisfying the effective interval ranging from $h_{\text{left}}^{l\times\alpha} = 7.9015$ to $h_{\text{right}}^{l\times\alpha} = 7.9034$.

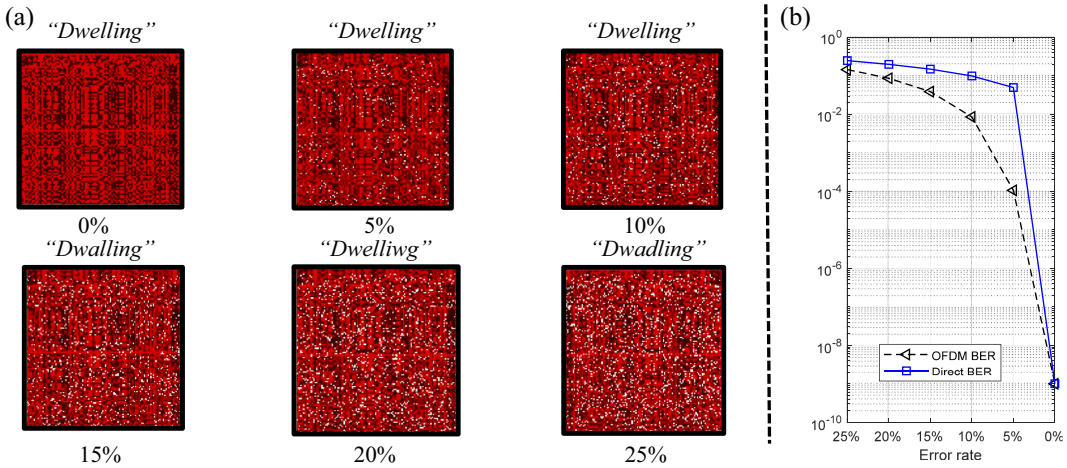


Fig. 11 Error tolerance analysis. (a) Recovered token display under the recognition errors occurring with different ratios. (b) BER performance of OFDM-like coding and the raw token.

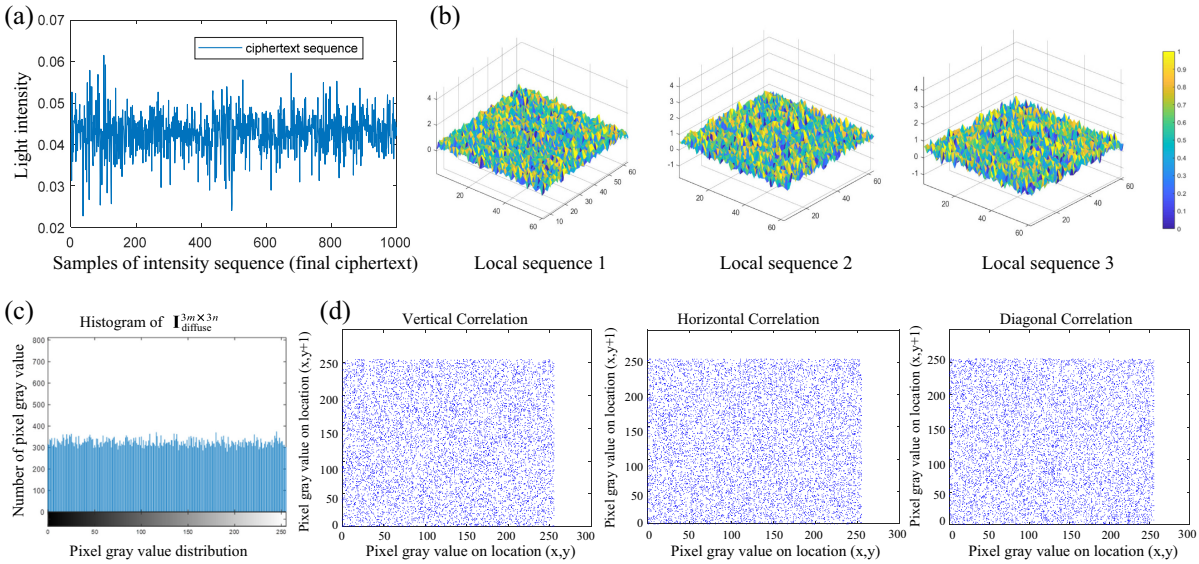


Fig. 12 Numerical assessment of bucket signal $\mathbf{o}$ and $\mathbf{I}_{\text{diffuse}}^{3m\times 3n}$ of SPI encryption. (a) Intensity sequence. (b) Visual randomness assessment of the sampled intensity sequence. (c) Histogram of $\mathbf{I}_{\text{diffuse}}^{3m\times 3n}$. (d) Correlation test of $\mathbf{I}_{\text{diffuse}}^{3m\times 3n}$.

Finally, the NPCR and UACI are calculated as 99.63% and 33.16%, respectively, approximating the ideal performance of 99.6094% and 33.4635%[40] and thus indicating the desirable sensitivity. (The parameter comparison of ciphertext $\mathbf{I}_{\text{diffuse}}^{3m\times 3n}$ and other three plaintexts is shown in Table S1 in the Supplementary Material).

4 Discussion and Conclusion

For a cryptography, security and capacity are the most important concerns to be developed into multiuser framework. The limited two have been the inherent issues for SPI encryption due to the pattern-projection-depended principle in Eq. (1).[1–11,36] It is worth noting that metasurfaces with (non-)orthogonal polarization pairs are first applied to enhance the overall security of an SPI cryptosystem and reduce the exposing risk of SPI patterns.[13,41] However, the alternative patterns still need to be projected, so the vulnerability and limited capacity still exist. In contrast to our method, the capacity of the multiuser is expanded by eightfold. In fact, the number of users N is not limited to eight. The proposed framework theoretically supports an arbitrary number of clients as long as the individual keys can be coded in advance. For security, a deep differential attack is developed based on the most threatening cryptanalysis mode, a chosen plaintext attack (CPA). If the proposed framework can resist CPA, the other three cryptanalysis modes, including a cipher-only attack, known plaintext attack, and chosen cipher attack, can also be resisted.[42,43]

To summarize, we have developed a multiuser SPI cryptography and authentication framework combined with OFDM-assisted key management. This approach allows multiple users to privately reconstruct different plaintexts, concurrently resisting multiple kinds of attacks and realizing authentication. The framework consists of four components, including a composite Fourier SPI encrypting method, key management, experimental decryption and authentication, and security assessment, recording the whole life of keys from generation to application. The realization of the proposed multiuser SPI framework, including security and capacity, is verified by simulation and numerical experiments. By the combination of direct key management and indirect image encryption, our work realizes the multiuser computational imaging encryption and authentication framework, facilitating its development toward more complicated application scenes.

5 Appendix: Fabrication and Attack

The main notations of this paper are listed as follows. The lowercase, uppercase, boldface lowercase, and boldface uppercase letter t, T, $\mathbf{t}$, and $\mathbf{T}$ denote a scalar variable, constant, vector, and matrix, respectively. $\mathcal{R}e\{\cdot\}$ denotes the real-part operation, $\mathbf{T}^{\mathrm{T}}$ denotes the transpose of matrix $\mathbf{T}$, $\pi(\cdot)$ denotes position exchange, $\|\mathbf{t}\|$ denotes the norm of vector $\mathbf{t}$, and $\langle\cdot\rangle$ denotes the inner product.

5.1 Sample Fabrication

The metasurface was fabricated by electron beam lithography (EBL). A layer of photoresist was spin-coated on a clean JGS1 substrate, followed by the sample bake. After the process above repeated once, the conductive adhesive AR-PC 5090.02 was spin-coated, and then the baked sample was exposed in LC-40 EBL mode with 140 pA beam current. The AR 600-55 developer and subsequent IPA fixer were used. A 50-nm-thick layer of aluminum was then deposited by electron beam evaporation, and the sample was soaked in acetone to peel off the metal layer.

5.2 Deep Differential Attack

Equation (4) demonstrates the instance process of a typical sort of SPI cryptography, which is likely to encrypt patterns as keys and then scramble (i.e., or by other process) the intensity.[6,13,36] $\mathbf{m} = [m_1, m_2, \ldots, m_{N^2}]^{\mathrm{T}}$ denotes the $N \times N$ plaintext. $\mathbf{P}$ denotes the original pattern set, and $\mathbf{P}^* = [\mathbf{p}_1^*; \mathbf{p}_2^*; \ldots; \mathbf{p}_{N^2}^*]$ denotes the patterns encrypted by key $\mathbf{v}$, where $\mathbf{p}_n^* = [p_{n,1}^*, p_{n,2}^*, \ldots, p_{n,N^2}^*]$

represents each encrypted one. $\mathbf{n}$ denotes noise, and $\{\mathbf{u}_i\}$, $i = 1,2,\ldots,I$ represents scrambling masks:

$$\begin{aligned}\mathbf{c} &= [(\mathbf{P}^*\mathbf{m}+\mathbf{n})\oplus\mathbf{u}_1]\ldots\oplus\mathbf{u}_I = \mathcal{H}[\mathcal{F}(\mathbf{m}|\mathbf{P},\mathbf{v})|\{\mathbf{u}_i\}.] \\ &= \mathcal{H}_{\{\mathbf{u}\}}\circ\mathcal{F}_{\mathbf{v}}(\mathbf{m}).\end{aligned} \tag{4}$$

For differential analysis, the equivalent mask $\mathbf{u}_1\oplus\mathbf{u}_2\oplus\ldots\mathbf{u}_I$ is first derived by reflexivity: $\mathbf{u}_{\text{equiv}} = \mathcal{H}_{\{\mathbf{u}\}}\circ\mathcal{F}_{\mathbf{v}}(\mathbf{z})$, where $\mathbf{z}$ denotes an all-zero matrix. Then, we artificially differentiate each pixel of $\mathbf{m}$ to observe the degree of change in $\mathbf{c}$, representing the binary value of a pattern at the corresponding position. Mathematically, $\hat{\mathbf{P}}^*$ (i.e., Jacobian matrix) can be acquired:

$$\hat{\mathbf{P}}^* = \nabla_{\mathbf{m}}\mathbf{c} = \frac{\partial\mathbf{c}}{\partial\mathbf{m}}. \tag{5}$$

Regardless of how complicated the cryptographer operates on patterns, we are only concerned with the $\mathbf{P}^*$ containing all the information of both $\mathbf{v}$ and $\mathbf{P}$. As long as $\hat{\mathbf{P}}^*$ and intensity $\mathcal{H}^{-1}_{\mathbf{u}_{\text{equi}}}(\mathbf{c})$ are obtained, the plaintext can be retrieved by the classic SPI correlation.

When encryption algorithms are so complex that $\hat{\mathbf{P}}^*$ greatly deviates from $\mathbf{P}^*$ (i.e., recovering keys by analyzing encrypting steps is not viable), deep learning is required to further mitigate the distortion by directly analyzing the key set (i.e., OFDM-assisted key management), shown in Fig. S7 in the Supplementary Material. For encryptions without a key-management platform, correct key sets are directly employed as labels to train the network for key compensation. Here, the network $\mathcal{R}_\zeta$ defined by a set of weights and biases Θ with $\mathcal{L}_1$ regularization is applied:

$$\begin{cases}\hat{\zeta} = \arg\min_{\zeta\in\Theta}\|\mathcal{R}_\zeta(\hat{\mathbf{P}}^*|\eta>0) - \mathbf{P}^*\|^2 + \mathcal{L}_1 \\ \tilde{\mathbf{P}}^* = \mathcal{R}_{\hat{\zeta}}(\hat{\mathbf{P}}^*)\end{cases}, \tag{6}$$

where η represents the correlation among pixels and $\tilde{\mathbf{P}}^*$ implies the optimized pattern. Note that we cannot directly obtain the key set (i.e., always in confidential state by oracle) or improve pseudorandom $\hat{\mathbf{P}}^*$ where $\eta \approx 0$ is highly ill-posed. Thus, as shown in Fig. S6 in the Supplementary Material, a training method based on signal width expansion is studied. $\hat{\mathbf{P}}^*$ patterns are transformed into 1D pulse signals with the extended width being an on–off keying signal, which enables the network to be trained offline (i.e., polluted key sets can be simulated aforehand by Eve) and realize desired performance.

Disclosures

The authors declare no conflicts of interest.

Code and Data Availability

All data needed to evaluate the conclusions in the paper are present in the paper and/or the Supplementary Materials. Additional data related to this paper are available from the corresponding author upon reasonable request.

Acknowledgments

The work was supported by the National Key R&D Program of China (Grant No. 2021YFB3900300), National Natural Science Foundation of China (Grant Nos. 61860206007, 62275177, and 62371321), Ministry of Education Science and Technology Chunhui Project (Grant No. HZKY20220559), International S and T Cooperation Program of Sichuan Province (Grant No. 2023YFH0030), Sichuan Science and Technology Innovation Seeding Project (Grant No. 23-YCG034), Sichuan Science and Technology Program (Grant No. 2023YFG0334), and Chengdu Science and Technology Program (Grant No. 2022-GH02-00001-HZ).

References

1. M. P. Edgar, G. M. Gibson, and M. J. Padgett, "Principles and prospects for single-pixel imaging," *Nat. Photonics* **13**(1), 13–20 (2019).
2. A.-X. Zhang et al., "Tabletop X-ray ghost imaging with ultra-low radiation," *Optica* **5**(4), 374–377 (2018).
3. B. Sun et al., "3D computational imaging with single-pixel detectors," *Science* **340**(6134), 844–847 (2013).
4. G.-Y. Wang et al., "A tri-channel liquid crystal device for single-pixel-imaging encryption," *Appl. Phys. Lett.* **123**(9), 091102 (2023).
5. Y. Kang et al., "One-to-many optical information encryption transmission method based on temporal ghost imaging and code division multiple access," *Photonics Res.* **7**(12), 1370–1380 (2019).
6. Z. Zhang et al., "Secured single-pixel broadcast imaging," *Opt. Express* **26**(11), 14578–14591 (2018).
7. M. Tanha, R. Kheradmand, and S. Ahmadi-Kandjani, "Gray-scale and color optical encryption based on computational ghost imaging," *Appl. Phys. Lett.* **101**(10), 101108 (2012).
8. S. Jiang et al., "Information security scheme based on computational temporal ghost imaging," *Sci. Rep.* **7**(1), 7676 (2017).
9. J. Xiong et al., "Algorithm-dependent computational ghost encryption and imaging," *Phys. Rev. Appl.* **18**(3), 034023 (2022).
10. Y. Xiao, L. Zhou, and W. Chen, "Secured single-pixel ghost holography," *Opt. Lasers Eng.* **128**, 106045 (2020).
11. S. Jiao et al., "Visual cryptography in single-pixel imaging," *Opt. Express* **28**(5), 7301–7313 (2020).
12. A. Tsoy et al., "Image-free single-pixel keypoint detection for privacy preserving human pose estimation," *Opt. Lett.* **49**(3), 546–549 (2024).
13. P. Zheng et al., "Metasurface-based key for computational imaging encryption," *Sci. Adv.* **7**(21), eabg0363 (2021).
14. W. Zhang, et al., "A device-independent quantum key distribution system for distant users," *Nature* **607**(7920), 687–691 (2022).
15. Z. Qi et al., "A 15-user quantum secure direct communication network," *Light: Sci. Appl.* **10**(1), 183 (2021).
16. P. Bagga et al., "On the design of mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system," *IEEE Trans. Veh. Technol.* **70**(2), 1736–1751 (2021).
17. J.-P. Chen et al., "Quantum key distribution over 658 km fiber with distributed vibration sensing," *Phys. Rev. Lett.* **128**(18), 180502 (2022).
18. S. S. Chaeikar, A. Jolfaei, and N. Mohammad, "Ai-enabled cryptographic key management model for secure communications in the internet of vehicles," *IEEE Trans. Intell. Transp. Syst.* **24**(4), 4589–4598 (2022).
19. V. Scarani et al., "The security of practical quantum key distribution," *Rev. Mod. Phys.* **81**(3), 1301 (2009).
20. M. Wazid et al., "AKM-IoV: authenticated key management protocol in fog computing-based internet of vehicles deployment," *IEEE Internet Things J.* **6**(5), 8804–8817 (2019).
21. X. Zheng et al., "Heterogeneously integrated, superconducting silicon-photonic platform for measurement-device-independent quantum key distribution," *Adv. Photonics* **3**(5), 055002 (2021).

22. J. Wang et al., "Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure," *IEEE Trans. Ind. Inf.* **16**(3), 1984–1992 (2019).
23. H. Tan, W. Zheng, and P. Vijayakumar, "Secure and efficient authenticated key management scheme for UAV-assisted infrastructure-less IoVs," *IEEE Trans. Intell. Transp. Syst.* **24**(6), 6389–6400 (2023).
24. Q. Shi et al., "QKBAKA: a quantum-key-based authentication and key agreement scheme for internet of vehicles," *IEEE Internet Things J.* **11**(7), 12292–12306 (2024).
25. X. Du et al., "Transactions papers a routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks," *IEEE Trans. Wireless Commun.* **8**(3), 1223–1229 (2009).
26. Y. Long et al., "Blockchain-based anonymous authentication and key management for internet of things with Chebyshev chaotic maps," *IEEE Trans. Ind. Inf.* **20**(5), 7883–7893 (2024).
27. M. Jeong et al., "Printable light-emitting metasurfaces with enhanced directional photoluminescence," *Nano Lett.* **24**(19), 5783–5790 (2024).
28. X. Ding et al., "Metasurface holographic image projection based on mathematical properties of Fourier transform," *PhotoniX* **3**, 16 (2020).
29. X. Guo et al., "Stokes meta-hologram toward optical cryptography," *Nat. Commun.* **13**(1), 6687 (2022).
30. Z. Wang et al., "3D intelligent cloaked vehicle equipped with thousand-level reconfigurable full-polarization metasurfaces," *Adv. Mater.* **36**, 2400797 (2024).
31. Y. Cao et al., "Four-channel display and encryption by near-field reflection on nanoprinting metasurface," *Nanophotonics* **11**(14), 3365–3374 (2022).
32. X. Yin et al., "Photonic spin hall effect at metasurfaces," *Science* **339**(6126), 1405–1407 (2013).
33. E. Choi et al., "360° structured light with learned metasurfaces," *Nat. Photonics* **18**, 848–855 (2024).
34. G. L. Stuber et al., "Broadband MIMO-OFDM wireless communications," *Proc. IEEE* **92**(2), 271–294 (2004).
35. Z. Zhang, X. Ma, and J. Zhong, "Single-pixel imaging by means of Fourier spectrum acquisition," *Nat. Commun.* **6**(1), 6225 (2015).
36. S. Lin et al., "Steganographic optical image encryption based on single-pixel imaging and an untrained neural network," *Opt. Express* **30**(20), 36144–36154 (2022).
37. X. Li et al., "Code division multiplexing inspired dynamic metasurface holography," *Adv. Funct. Mater.* **31**(35), 2103326 (2021).
38. Z. Gu et al., "IEPSBP: a cost-efficient image encryption algorithm based on parallel chaotic system for green IoT," *IEEE Trans. Green Commun. Networking* **6**(1), 89–106 (2021).
39. Y. Wu et al., "Local Shannon entropy measure with statistical tests for image randomness," *Inf. Sci.* **222**, 323–342 (2013).
40. Y. Wu et al., "NPCR and UACI randomness tests for image encryption," *Cyber J.: Multidiscipl. J. Sci. Technol., J. Sel. Areas Telecommun.* **3**(2), 31–38 (2011).
41. H.-C. Liu et al., "Single-pixel computational ghost imaging with helicity-dependent metasurface hologram," *Sci. Adv.* **3**(9), e1701477 (2017).
42. X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Process.* **92**(4), 1101–1108 (2012).
43. S. Qi et al., "A principled design of image representation: towards forensic tasks," *IEEE Trans. Pattern Anal. Mach. Intell.* **45**(5), 5337–5354 (2022).

Xiaowei Li received his MS and PhD degrees in information and communications engineering from Pukyong National University, Busan, South Korea, in 2011 and 2014, respectively. From 2014 to 2015, he was a researcher at the College of Computer Engineering, Yonsei University, Seoul, South Korea. He is currently a professor at the School of Electronics and Information Engineering, Sichuan University, Chengdu, China. He authored or co-authored approximately 80 papers cited by Science Citation Index (SCI). As first author, he has published approximately 50 SCI papers, and the impact factor of half of the papers is greater than 3. His research interests include three-dimensional integral imaging, holography, optical encryption, and image watermarking.

Qiong-Hua Wang is a professor of optical engineering at the School of Instrumentation and Optoelectronic Engineering, Beihang University, Beijing, China. She was a professor at Sichuan University from 2004 to 2018. She was a post-doctoral research fellow at the School of Optics/CREOL, University of Central Florida, from 2001 to 2004. She worked at the University of Electronic Science and Technology of China (UESTC) from 1995 to 2001. She received BS, MS, and PhD degrees from UESTC in 1992, 1995, and 2001, respectively. She has published more than 300 papers cited by SCI and authored three books. She holds 5 U.S. patents and more than 150 Chinese patents. She is a fellow of the Society for Information Display and an associate editor of the *Journal of the Society for Information Display*, *Journal of Information Display*, and *PhotoniX*. Her research interests include display and imaging technologies.

Yiguang Liu was a research fellow, visiting professor, and senior research scholar at the National University of Singapore, Singapore; Imperial College London, London, UK; and Michigan State University, East Lansing, Michigan, USA, respectively. He was chosen into the MOE program New Century Excellent Talents in 2008 and chosen as a scientific and technical leader in Sichuan Province in 2010. He is currently the director of the Vision and Image Processing Laboratory and a professor at the School of Computer Science, Sichuan University, Chengdu, China, and a reviewer for the *Mathematical Reviews* of the American Mathematical Society. He has co-authored more than 100 international journal and conference papers and a chapter of the book entitled *Computational Intelligence and Its Applications* (Imperial College Press, 2011). His research interests include computer vision and image processing, computational imaging, and computational intelligence.

Biographies of the other authors are not available.