Research Article

ADVANCED PHOTONICS NEXUS

Neuromorphic encryption: combining speckle correlography and event data for enhanced security

Shuo Zhu,[a,b] **Chutian Wang**,[a] **Jianqing Huang**,[a,c] **Pei Zhang**,[a] **Jing Han**,[b,*] **and Edmund Y. Lam**[a,*]

[a]The University of Hong Kong, Department of Electrical and Electronic Engineering, Hong Kong, China

[b]Nanjing University of Science and Technology, School of Electronic and Optical Engineering, Nanjing, China

[c]Shanghai Jiao Tong University, School of Mechanical Engineering, Key Lab of Education Ministry for Power Machinery and Engineering, Shanghai, China

Abstract. Leveraging an optical system for image encryption is a promising approach to information security since one can enjoy parallel, high-speed transmission, and low-power consumption encryption features. However, most existing optical encryption systems involve a critical issue that the dimension of the ciphertexts is the same as the plaintexts, which may result in a cracking process with identical plaintext-ciphertext forms. Inspired by recent advances in computational neuromorphic imaging (CNI) and speckle correlography, a neuromorphic encryption technique is proposed and demonstrated through proof-of-principle experiments. The original images can be optically encrypted into event-stream ciphertext with a high-level information conversion form. To the best of our knowledge, the proposed method is the first implementation for event-driven optical image encryption. Due to the high level of encryption data with the CNI paradigm and the simple optical setup with a complex inverse scattering process, our solution has great potential for practical security applications. This method gives impetus to the image encryption of the visual information and paves the way for the CNI-informed applications of speckle correlography.

Keywords: optical encryption; computational neuromorphic imaging; speckle correlography; deep learning.

Received Mar. 27, 2024; revised manuscript received May 19, 2024; accepted for publication Jun. 20, 2024; published online Jul. 17, 2024.

[DOI: 10.1117/1.APN.3.5.056002]

1 Introduction

Optical techniques have been widely investigated and implemented in the field of information security, encryption, and authentication.[1,2] Information security is a crucial challenge to modern society,[3] for example, data encryption for the critical databases of private and commercial information. Much impressive progress with optical techniques has been investigated and demonstrated in information encryption and authentication. The main purpose of utilizing optical techniques for information security is that data waveforms possess multiple dimensions, including phase, amplitude, spectrum, polarization, orbital angular momentum, etc. These dimensions can be combined in various approaches to enhance encryption security and make it more resistant to attacks. After the first proposal of double random phase encryption,[4] many optical encryption schemes with optoelectronic setups have been developed. The classical encryption system based on holography,[5,6] interference,[7,8] ptychography,[9,10] single-pixel imaging[11,12] and scattering imaging[13,14] are proposed, which are a further expansion of the application with the traditional optical system. Recently, to upgrade the security level and fully exploit the abundant degrees of freedom of encryption systems, more advanced optical systems have been designed and demonstrated, for example, nonlinear encryption engine,[15] meta-optics cryptography system,[16,17] and angular-momentum holography nested encryption.[18]

Utilizing a random scattering media as a coding mask is a simple yet effective way for image encryption.[3] Speckle correlography is a cutting-edge technique that enables the

*Address all correspondence to Edmund Y. Lam, elam@eee.hku.hk; Jing Han, eohj@njust.edu.cn

construction of high-resolution images of laser-illuminated objects.[19,20] Briefly, the backscattered laser speckle intensity patterns are collected and then used to create a detailed visual representation of the diffuse object with computational approaches. The imaging approach is grounded on the principle that the average energy spectrum of laser-illuminated objects can be ascertained through the autocorrelation of speckle patterns in the Fourier domain. In the context of speckle correlography, an iterative phase retrieval (PR) algorithm is employed to reconstruct images from the estimated Fourier modulus of the diffuse object. Therefore, speckle correlography can be employed as a random phase encoding approach for optical encryption applications.[21] Despite coherent scattering-based encryption schemes, the incoherent scattering method based on speckle correlation is also proposed for image encryption.[13,22] The physics-informed method for a ciphertext-only attack hinges on utilizing speckle correlography, which establishes that the autocorrelation of the ciphertext is fundamentally indistinguishable from that of the speckle.[23]

Recent advances in optical encryption methods mainly focus on the complexity of experimental setups, which are based on advanced optoelectronic devices. The photorefractive crystal or metasurface device encodes information with light signals and the plaintext-ciphertext form is consistent with a frame-based camera. The same data form would lead to a high risk of the system being cracked. Meanwhile, traditional intensity images are redundant and temporally sparse. Therefore, a different data dimension between encryption and decryption might be a promising approach to facing information security.[24]

Event cameras are representative neuromorphic devices that are inspired by the architecture of the human brain and have the potential to revolutionize computing by providing a more efficient and effective way to process information.[25] Compared to conventional frame-based cameras, the event camera with bionic circuit units has microsecond-level responsiveness and higher dynamic range, hence showing greater feasibility for optical encryption under high-speed recordings and poor illumination conditions. Event cameras offer trade-offs in terms of power consumption and frame rate, in exchange for sparsely sampling visual scenes and still achieving remarkable performance on computational imaging tasks. Equipped with neuromorphic devices and computational algorithms, computational neuromorphic imaging (CNI) is anticipated to emerge as a promising and rapidly advancing field in optical imaging.[26] CNI-informed computing modality achieves superior efficiency with low power consumption and low latency for certain algorithms,[27,28] and information security would greatly benefit from focusing on well-defined optical encryption.

An event camera is utilized in the neuromorphic encryption system to capture per-pixel intensity changes in an asynchronous manner, generating event streams that encode information on the time, pixel position, and polarity. Consequently, when the object undergoes motion, the speckle patterns are moved correspondingly, and speckle events are generated and recorded by an event camera. These speckle events arise due to light scattering, which produces a distinctive, unpredictable pattern of intensity fluctuations that can be employed to form a process-prior-empowered key. Therefore, a neuromorphic encryption system with different data forms processing can be developed using an event camera.

In this work, a neuromorphic encryption technique is proposed using event-stream speckles, which has a different data form of the ciphertext and high encrypted efficiency. The proposed encryption scheme has been demonstrated with simulated analysis and experimental verification. The inherent randomness and unpredictability of speckle events make it extremely difficult for attackers to replicate the same pattern of events and produce the correct key. Furthermore, the neuromorphic encryption method has the potential for high-speed encryption and decryption processing, which makes it suitable for practical applications. For image decryption, we propose a physical key based on a physics-informed neural network, which is trained with a simulated forward model. In addition, the proposed encryption method has remarkable noise immunity, showing impressive robustness in practical noisy scenarios.

2 Principle and Method

2.1 Optical Cryptosystem with Speckle Correlography

Speckle correlography is mainly the coherent scattering process in that we can use the statistical correlation between speckle patterns to encrypt information. As shown in Fig. 1, the encryption process is realized by the speckle correlography modulation and events recorded with the neuromorphic sensors. The detailed forward processes are depicted in the blue dashed box. That is, the origin information modulated with a coherent scattering process and the generation of corresponding event-stream ciphertext are synchronously realized via the neuromorphic encryption system.

The generation of the encrypted speckles can be illustrated based on the imaging correlography.[19] The plaintext object is illuminated with a coherent light source, and the non-imaged speckle patterns then can be collected by a frame-based camera. The encrypted object exhibits optical roughness, and its micro-scale surface height variations are random and comparable in

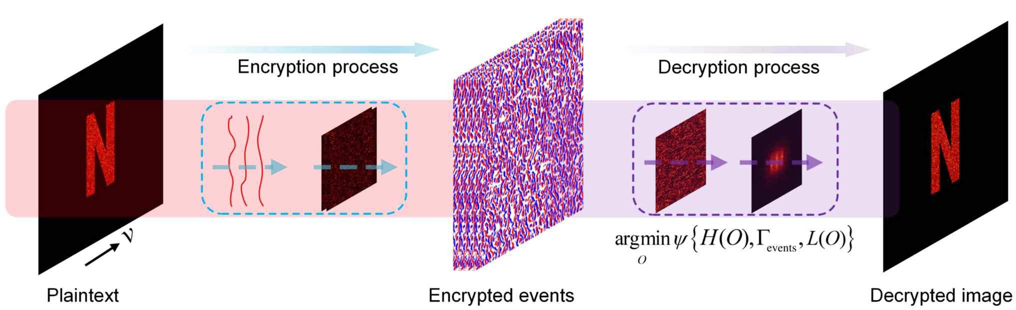

Fig. 1 Schematic illustration of the neuromorphic encryption and decryption processes.

size to the light's wavelength. As a result, the reflected beam undergoes random and coherent dephasing, resulting in the detector in the image plane recording the intensity pattern of speckle grains.[19,29] The fully developed speckles $I(u)$ can be described as the squared modulus of the Fourier transform of the object field:

$$I(u) = |F[f_n(v)]|^2, \tag{1}$$

where F denotes a Fourier transform, u denotes a 2D coordinate in the observation plane, and v is a 2D spatial coordinate vector in object space. $f_n(v) = |f_0(v)e^{i\phi_n(v)}|$ stands for the optical field coded by the diffuse object, $f_0(v)$ is the field amplitude of the encrypted object, and $\phi_n(v)$ denotes the stochastic phase of the nth instance of the encrypted object field that is related with the height profile of the diffuse object. Therefore, the autocovariance of the collected speckles can be estimated as

$$\hat{C}_I(\Delta u, N) = \int_{-\infty}^{\infty} P(u+\Delta u)\left\{\frac{1}{N}\sum_{n=1}^{N}[I_n(u+\Delta u)-\bar{I}][I_n(u)-\bar{I}]\right\}\mathrm{d}u, \tag{2}$$

where Δu is a vector separation in the image plane, $\bar{I}$ is the average intensity of the speckle grains, and $P(u)$ is the circular pupil function can be defined as

$$P(u) = \begin{cases} 1, & u \in P \\ 0, & u \notin P \end{cases}. \tag{3}$$

While an infinite number of speckle grains is used for estimating statistical autocovariance[19]

$$\begin{aligned} C_I(\Delta u, N) &= \lim_{N\to+\infty} \hat{C}_I(\Delta u, N) = \mathcal{H}(\Delta u)\cdot|\Gamma(\Delta u)|^2 \\ &= [P(u)\star P(u)]\cdot|\Gamma(\Delta u)|^2, \end{aligned} \tag{4}$$

where $\mathcal{H}$ is the transfer function of the optical system, $\Gamma(\Delta u) = |F[f_0(v)]|^2$ is the 2D Fourier transform amplitude of the object's field.[30] For plaintext image encryption, the power spectrum can be employed in iterative PR algorithms,[31] which is the same process for image decryption.

2.2 Neuromorphic Model for Speckle Events

If the object and image planes are laterally displaced or if the object rotates slightly, it is possible for independent realizations of the collected speckle intensity to occur. Event cameras have gained significant attention due to their bio-inspired properties, which mimic the functioning of neurons to process the information on changes in intensity, only respond to per-pixel logarithmic intensity changes in an asynchronous fashion.[25,26,32] The speckle grains move with the moving diffuse object, resulting in the events generated and recorded by neuromorphic sensors.

The speckle patterns shift as the object moves, and an event $e_k \triangleq (\mathbf{r}_k, t_k, p_k)$, triggered at a pixel $\mathbf{r}_k = (x_k, y_k)$ at time t_k once the intensity changes reach the threshold,[33,34] is encoded as a result as follows:

$$\Delta L(\mathbf{r}_k, t_k) \triangleq L(\mathbf{r}_{k+1}, t_{k+1}) - L(\mathbf{r}_k, t_k) = p_k T, \tag{5}$$

where $L(\mathbf{r}_k, t_k)$ is the log intensity, p_k is the event polarity that represents the sign of the changing, and T denotes the temporal contrast threshold. Therefore, a 2D intensity pattern can be synthesized by accumulating events within a certain time period Δt and can be expressed as[35]

$$I_{\text{events}} = \sum_{t_k\in\Delta t} p_k T\delta(x-x_k, y-y_k), \tag{6}$$

where δ is a Kronecker delta function. Therefore, the event-stream data can be processed by traditional optical methods, for example, Fourier transforms, image enhancement, and PR algorithms. The encrypted images can be further reconstructed with the 2D energy spectrum of speckle autocorrelation,[20,31] and the mathematical operations autocorrelation of accumulated events can be expressed as

$$\Gamma_{\text{events}} = F(I_{\text{events}}). \tag{7}$$

2.3 Inverse Decryption Approach

The optical encryption process with a speckle correlography system can be simplified as a linear system[19] and the distribution of accumulated patterns is strongly related to the original intensity distribution of the coherent laser speckles. The existing PR algorithms are not up to the task of properly solving the ill-posed problem associated with low-SNR speckle correlography of accumulated events. Deep neural networks (DNN) with skip or residual connections excel at learning identity-like mappings.[36] Learning PR algorithms have demonstrated the effectiveness of the inverse correlography,[37] which is more accurate than traditional retrieval methods.[20,38] Therefore, a DNN is employed for image reconstruction of event-stream data decryption.

To improve the generalization capability without characterizing the specific scattering process, related physics-priors of the invariant elements can be used to reduce the errors in the deconvolution of the different modulations.[39,40] As shown in Fig. 1, the decryption process with event-stream data contains several steps for the ciphertext recovery. For the optimization model with DNN, the final accumulated autocorrelation preprocess based on the forward physics model is selected as the network input. Therefore, the decryption strategy with a learning PR method can be written as[41,42]

$$\hat{O} = \arg\min_{O} \psi\{H(O), \Gamma_{\text{events}}, L(O)\}, \tag{8}$$

where O is the encrypted object, $\hat{O}$ is the decrypted object, $H(\cdot)$ is the forward operator of the optical system, ψ is the functional to minimize, and $L(\cdot)$ is the regularizer acting on O, that is, putting constraints on the solution. In a traditional optimization process, the regularizer would be arbitrarily selected.

In this work, a physics-informed DNN is chosen to determine a regularization built for the specific categories of objects. Benefiting from the forward process of speckle event generation, the physical model was used as a pre-processor for the generator that generates a training set.[43] Although plaintexts are degraded and formulated as speckle events, learning from a simulation scheme is a feasible and powerful tool to fill the gap of information loss. The well-known U-net architecture is employed as the PR learning model, which has been applied successfully to various inverse problems.[44] We select the negative Pearson correlation coefficient (NPCC) as the loss function to optimize the DNN in the training process. NPCC is an index used to evaluate the similarity between two variables and has been extensively used for inverse problem optimization.[42,45]

2.4 Experimental Setup and Datasets Preparation

The neuromorphic encryption system is schematically illustrated in Fig. 2, which includes an illumination laser (Thorlabs, HNL100LB, central wavelength: 632.8 nm) and a corresponding beam expander (Thorlabs, BE10M-A). A diffuse reflective object is selected as the plaintext and is mounted on a motorized translation stage (Winner Optics, WN262TA20). An event camera (iniVation, DAVIS 346) and a 40× objective lens (Nikon) are employed to collect the speckle events. Despite the encryption process involving a complex transformation, the hardware implementation is relatively simpler than conventional methods.[3] The object is a 10 mm × 10 mm letter with a reflective diffuse metal surface and the distance between the object and the event camera is about 300 mm. The movement speed of the translation stage is 0.2 mm/s in the horizontal direction.

In order to reduce the cost of data collection, a synthetic framework is proposed to generate the simulated data for DNN training. The training data are synthesized with the forward physical model of the speckle correlography[19] and the v2e process for event generation.[46] Here, the light source is assumed as a collimated coherent laser beam with a wavelength of 632.8 nm. The object is modulated by a random mask as the diffuse object and is numerically propagated over a far-field distance. The far-field distance d is also set to 300 mm, resulting in a speckle pattern $I(x,y)$. v2e toolbox that can generate realistic synthetic events from conventional frames, which is employed to simulate and make the training data of speckle events. The speckle field was shifted with two pixels with three consecutive grounds, which is used to generate the degraded speckle events. Then, the same set of speckle patterns of 32×32 in size is used for accumulated autocorrelation preprocess in both the simulation and experiment, and 256 pixel × 256 pixel is selected for autocorrelation calculation.

3 Results

For the neuromorphic encryption system, image encryption with physical modulation and data form transform are simultaneously conducted. In the simulated experiments, the detailed encryption process is analyzed in the method part and the intrinsic data are also presented for a better understanding of the forward encrypted process.

First, the characteristics of event-stream data with different scattering conditions are analyzed. As shown in Fig. 3, the accumulated speckle and corresponding retrieved autocorrelation are presented. The statistical characteristics can be obviously distinguished from the normalized intensity of the white dashed line. We can draw a similar conclusion with scalable imaging through unknown scattering media.[39] Therefore, the preprocessing step with the retrieved autocorrelation is essential for the physics-informed learning model, which is suitable for practical-synthetic environments and can reduce the differences in the data characteristics. By training on the autocorrelations of simulated event-stream data and their associated ground truth images, the proposed PR model reduces the potential for model mismatch and improves image reconstruction efficiency.

To demonstrate the effectiveness of the neuromorphic encryption method, detailed experiments are presented and analyzed. If we use conventional cameras, the frame-based cyphertext can be recorded as the intensity speckles, which is presented as the virtual cyphertext. The encrypted event-stream data can be further synthesized by the moving virtual speckles. Numerical simulations have been carried out to illustrate the effectiveness of the neuromorphic encryption method. In the simulated experiments, the size of all the images is set as 256 pixel × 256 pixel. A total of nine groups of speckle events are generated, which have distinct degraded processes with different scattering transport modes.[47,48] One group of data was used for test verification of the encryption, and the remaining eight sets of data were used for training the decryption algorithm

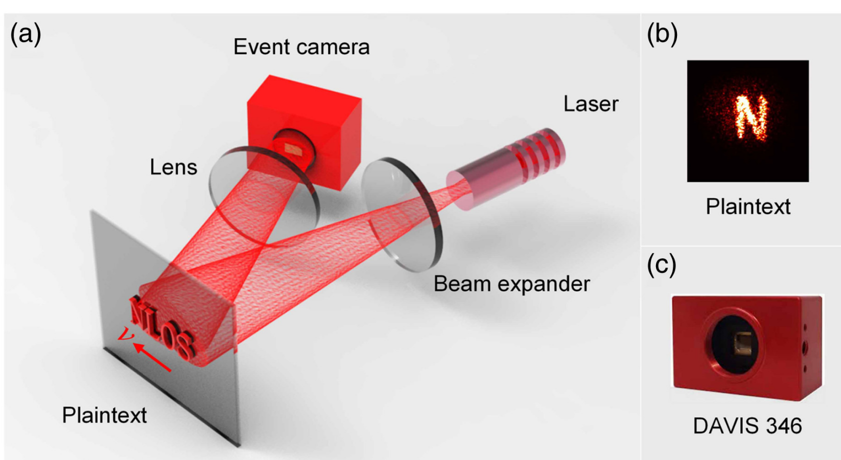

Fig. 2 Neuromorphic encryption system. (a) The optical configuration. (b) An encrypted letter "N" is made with a diffuse metal surface, captured with frame-mode and a focusing lens. (c) An event camera is employed as the neuromorphic sensor to collect the encrypted data.

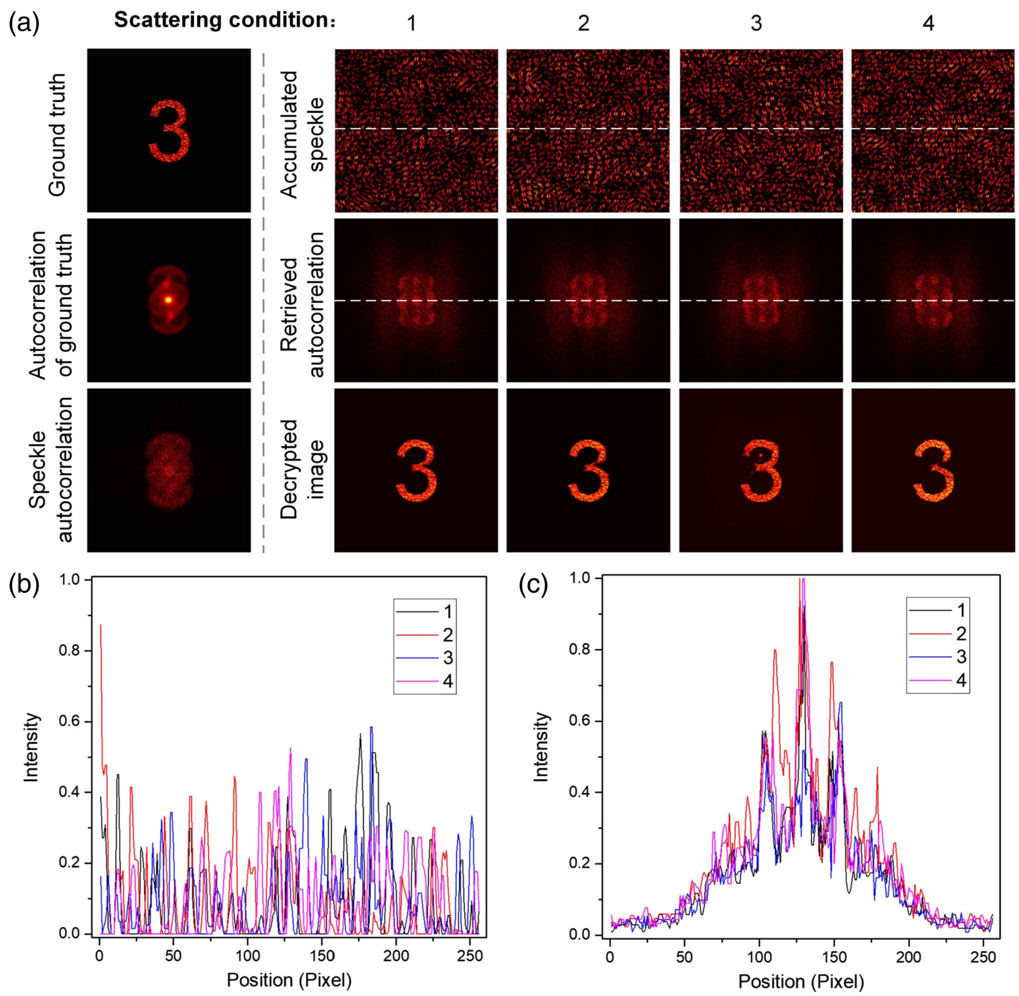

Fig. 3 Analysis of encryption-related data. (a) The accumulated speckle and corresponding retrieved autocorrelation and the final decrypted results in different scattering conditions are presented. (b) The normalized intensity of the dashed line in the accumulated speckle. (c) The normalized intensity of the dashed line in the retrieved autocorrelation.

model. According to the simulation results in Fig. 4, the final encrypted results are event-stream data. Therefore, the optical encryption scheme based on the CNI paradigm can encrypt images with different data forms. The original image recovery of the encrypted event is performed by the proposed physical key. Using the physics-informed PR algorithm for the encrypted event-stream data, the autocorrelation is first retrieved and employed for decrypted image reconstruction. From the final retrieved results, the decrypted image has been initially validated based on numerical simulations. Therefore, the effectiveness of the information security and high dimensional resistance to ciphertext attacks of the proposed method can be seen from the encrypted time data and decryption results.

In addition, we investigate the robustness of the proposed neuromorphic encryption scheme against cropping and noise. For practical information transport, the original information might be lost which results in part of the damaged event-stream data. Therefore, the capability to reconstruct useful information with damaged data is crucial for image decryption. The results are respectively presented in Figs. 5 and 6. The four images on the left side of Fig. 5 show the cropped ciphertexts with cropping ratios of 1/16, 1/8, 1/4, and 1/2, respectively. The autocorrelation of plaintext can be retrieved from the cropped ciphertext. According to the decryption results, we can see that the proposed method has resistance to the different cropping ratios. The two images on the left of Fig. 6 present the ciphertexts added zero-mean, Gaussian white noise with variance of 0.01 and 0.02; the two images on the right side of Fig. 6 present the ciphertexts added salt and pepper noise with 0.01 and 0.02 noise density. The retrieved autocorrelations of the corrupted ciphertexts and the reconstructed plaintext images are also presented together. From the final decryption results, the proposed method has the robustness capability against noise with different levels and types. Therefore, these results indicate that the neuromorphic encryption approach has superior robustness against data cropping and noise disturbance.

Further experimental validation is carried out for the effectiveness and practicality of the neuromorphic encryption scheme. We implement the practical CNI system as illustrated in Fig. 2 and verify it by the proposed algorithm. As shown in Fig. 7, the encrypted events, intermediate images, and corresponding decrypted results of the letters targets (i.e., "N" and "L") and

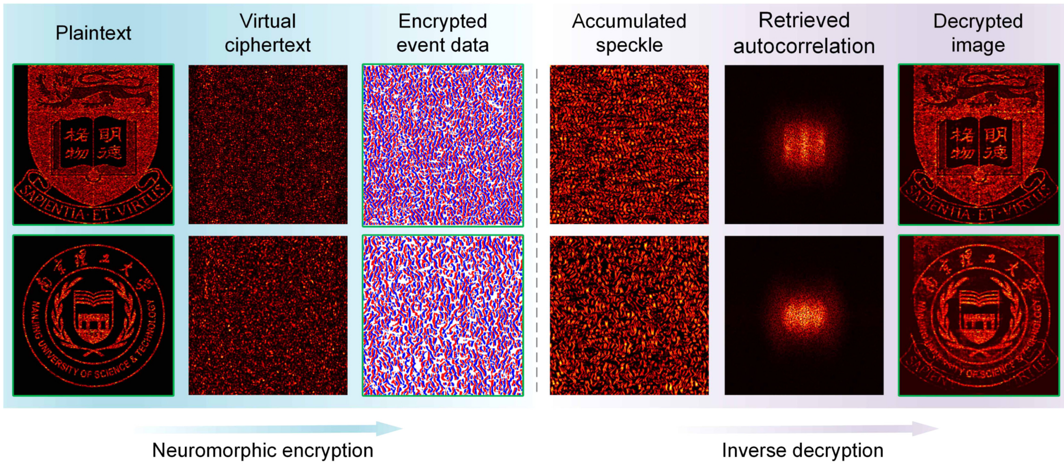

Fig. 4 Simulation results. The virtual cyphertext of speckle patterns from intermediate processes is used for event-stream data generation. The accumulated speckles with encrypted events and decrypted images with the learning PR algorithm.

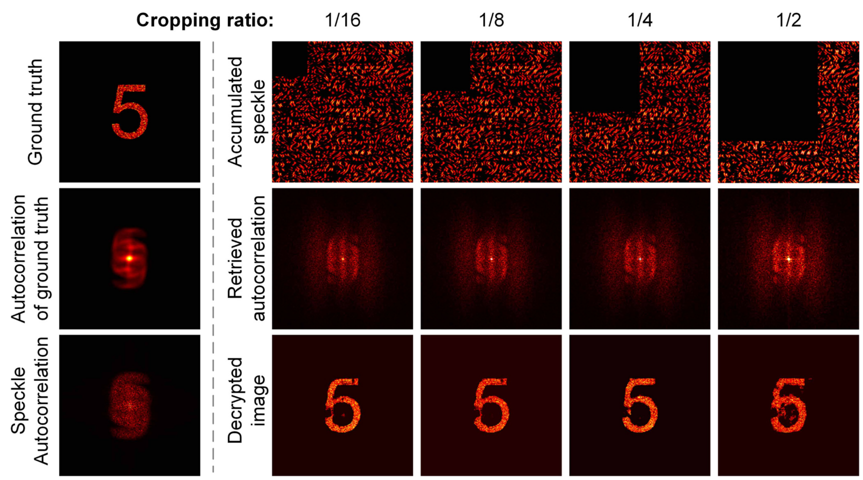

Fig. 5 Robustness test against cropping. Ciphertext with different cropping ratios are 1/16, 1/8, 1/4, and 1/2, respectively.

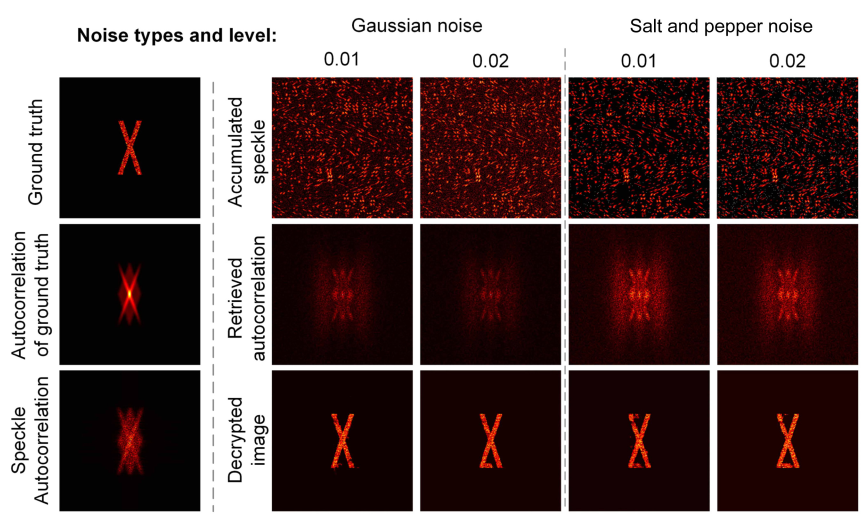

Fig. 6 Robustness test against noise. Ciphertext added zero-mean Gaussian white noise with variances of 0.01 and 0.02 and added salt and pepper noise with 0.01 and 0.02 noise densities.

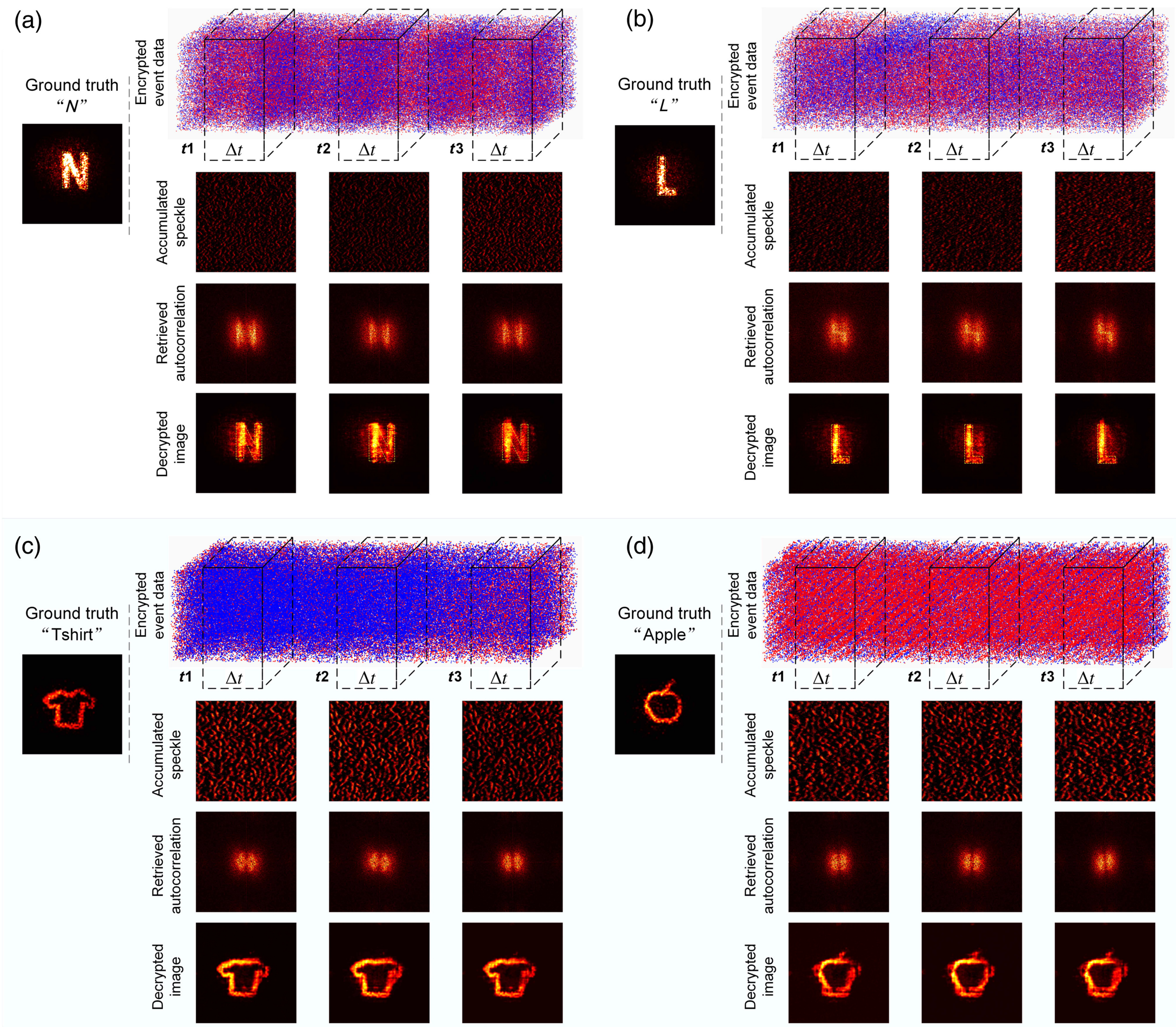

Fig. 7 Experimental results. (a) Letter target "N." (b) Letter target "L." (c) Quick draw target "Tshirt." (d) Quick draw target "Apple." For each subfigure: the first column from the left is the ground truth plaintext; the first row is the collected encrypted events that have the same time period and different time periods; the second and third rows are the accumulated speckle and corresponding autocorrelation; the last row is the decrypted result via the learning PR algorithm.

quick draw targets (i.e., "Tshirt" and "Apple") are presented.[49] The event-stream data are selected and preprocessed with accumulation and autocorrelation. From the experimental results, the accumulated speckle images with different time periods differ significantly. However, the corresponding autocorrelations have similar main structural information, and the final decrypted images are nearly identical to each other, which demonstrates the proposed method is robust to variable scattering processes. The known degraded physical process is the key element for the information decryption. Therefore, neuromorphic encryption is an innovative bio-inspired method for information security with a data-form transformation process.

4 Analysis

Since event cameras only capture motion, they predominantly record high-frequency information about moving targets, while low-frequency information with smooth grey-scale changes can be easily lost. Conventional phase recovery algorithms struggle to accurately reconstruct power spectra and inverse series with such incomplete information. By understanding the target's encryption process, we can generate corresponding degradation simulation data and employ learning methods to recover some lost information during the encryption process. As illustrated in Fig. 8, we compare the traditional hybrid input-output (HIO) PR algorithm to our learning method for event data decryption.[19,31]

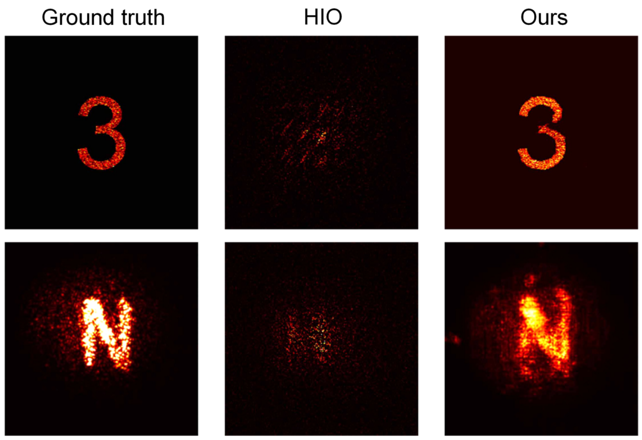

Fig. 8 Comparison results of the traditional HIO PR algorithm with our learning method for event data decryption.

For both simulated and experimental data, the HIO algorithm fails to produce reliable results, whereas our proposed learning PR algorithm effectively compensates for information loss in a simulated dataset containing a final forward encryption model.

In Eq. (6), the length of the time duration Δt is a predefined parameter for accumulated images with speckle events. By selecting different periods within a single continuous event stream, the accumulated images and the corresponding autocorrelation are calculated with the same starting point in time. As shown in Fig. 9, the short time duration (i.e., $0.1\Delta t$ and $0.2\Delta t$) can lead to sparse accumulated speckles, whereas the long one (i.e., $5\Delta t$ and $10\Delta t$) can result in the speckles being overlapped and blurred. As a result, the wrong time duration selection will produce the incorrectly retrieved autocorrelation and can not obtain the proper decrypted images. Therefore, an appropriate time duration with prior knowledge of the events process is crucial for accurate decryption. In specific extreme scenarios, accumulating adequate event information for signal parsing might be essential. This process can be further improved by employing warp or refocusing techniques for event stream data washout, which is one of our upcoming research topics.

5 Discussion

According to the experimental results and analysis, several highlights are pointed out as follows:

1. The neuromorphic encryption with speckle correlography exhibits a high level of encryption complexity, despite the fast encrypted process and relatively simple optical setup. A learning PR algorithm using a physics-informed model is proposed for decrypting ciphertexts, which has the generalization capability for different scenes. Due to the model being trained with a synthetic dataset based on the physical model and responses of bio-inspired sensors, the proposed method has a better physical key for unknown encrypted plaintext.
2. Since event-stream data are only produced by speckle motion in an otherwise static scene, the output data contain minimal redundant information about components. The event-stream data have the advantage of the random scattering process in that the plaintext information is fully coded into the events. Even if part of the event-stream data are lost, useful information can also be retrieved for image decryption. Meanwhile, the data are susceptible to noise in the dark field, which demonstrates the proposed method is robustly tested against noise.
3. Neuromorphic encryption using speckle events is in the nascent stage of development, and there are multiple challenges that must be addressed before it can be widely adopted. The information is lost during the conversion process from intensity to events. Furthermore, the reliability of speckle events in different environments needs to be thoroughly tested to ensure that they can be used in a variety of settings. As the technology continues to evolve, it is expected to see an increase in practical applications, and it may even become a preferred strategy of encryption for sensitive data.

6 Conclusion

In summary, we present a bio-inspired encryption system for optical information security, which is the first cryptography scheme using the CNI technique, to the best of our knowledge. The proposed methodology enhances speckle correlation through event-stream data, which provides a new paradigm for optical image encryption. CNI technique and speckle

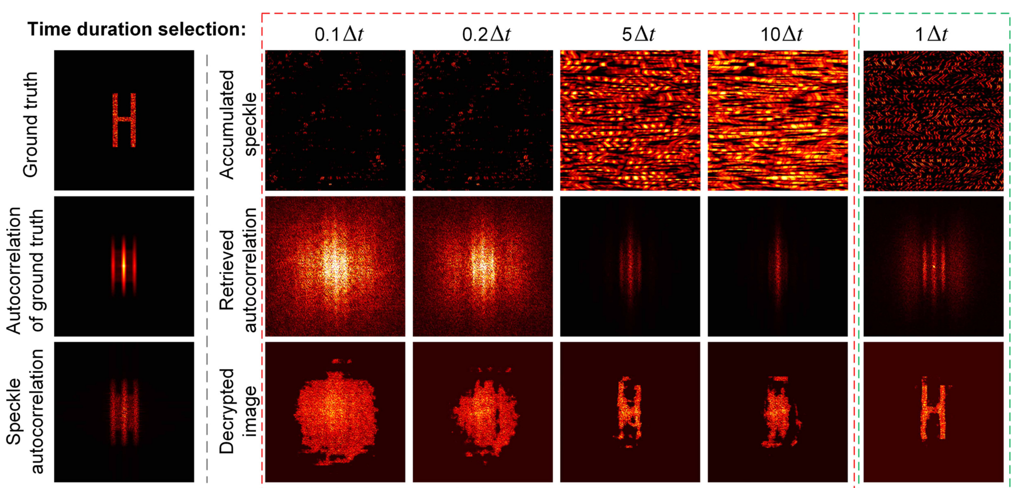

Fig. 9 Cracking resistance test with wrong time duration selection (in the red dash box). The correct process with a proper time duration selection is also presented in the green dash box.

correlography are combined to improve the security and efficiency of optical encryption, which shows the proposed methodology surpasses traditional methods in terms of security and encryption level. The potential benefits of neuromorphic encryption using event-stream data make it a promising research area that could transform the field of information security, which paves the way to CNI applications and provides a reference for complex scenarios computing with bio-inspired sensors.

Disclosures

The authors declare no conflicts of interest.

Code and Data Availability

Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

Acknowledgments

This work was supported by the Research Grants Council of Hong Kong (GRF 17201620), ACCESS—AI Chip Center for Emerging Smart Systems, sponsored by InnoHK funding, Hong Kong, China, the National Natural Science Foundation of China (Grant Nos. 62031018 and 61971227), and Hong Kong Scholars Program (Grant No. XJ2022032). We thank Wenjun Zhang, Zhou Ge, and Haosen Liu for their technical support and useful discussions.

References

1. A. Carnicer and B. Javidi, "Optical security and authentication using nanoscale and thin-film structures," *Adv. Opt. Photonics* **9**(2), 218–256 (2017).
2. S. Liu, C. Guo, and J. T. Sheridan, "A review of optical image encryption techniques," *Opt. Laser Technol.* **57**, 327–342 (2014).
3. B. Javidi et al., "Roadmap on optical security," *J. Opt.* **18**(8), 083001 (2016).
4. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.* **20**(7), 767–769 (1995).
5. B. Javidi and T. Nomura, "Securing information by use of digital holography," *Opt. Lett.* **25**(1), 28–30 (2000).
6. J. Guo et al., "Spatially structured-mode multiplexing holography for high-capacity security encryption," *ACS Photonics* **10**(3), 757–763 (2023).
7. Y. Zhang and B. Wang, "Optical image encryption based on interference," *Opt. Lett.* **33**, 2443–2445 (2008).
8. Y. Xiong, J. Du, and C. Quan, "Cryptoanalysis on the image encryption scheme based on interference and an amplitude mask," *Opt. Commun.* **517**, 128272 (2022).
9. Y. Shi et al., "Optical image encryption via ptychography," *Opt. Lett.* **38**(9), 1425–1427 (2013).
10. Y. Su, W. Xu, and J. Zhao, "Optical image encryption based on chaotic fingerprint phase mask and pattern-illuminated Fourier ptychography," *Opt. Lasers Eng.* **128**, 106042 (2020).
11. P. Clemente et al., "Optical encryption based on computational ghost imaging," *Opt. Lett.* **35**(14), 2391–2393 (2010).
12. 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).
13. M. Liao et al., "Ciphertext-only attack on optical cryptosystem with spatially incoherent illumination: from the view of imaging through scattering medium," *Sci. Rep.* **7**(1), 41789 (2017).
14. L. Zhou, Y. Xiao, and W. Chen, "Learning complex scattering media for optical encryption," *Opt. Lett.* **45**(18), 5279–5282 (2020).
15. J. Hou and G. Situ, "Image encryption using spatial nonlinear optics," *eLight* **2**(1), 3 (2022).
16. H. Zhou et al., "Correlated triple hybrid amplitude and phase holographic encryption based on a metasurface," *Photonics Res.* **10**(3), 678–686 (2022).
17. F. Zhang et al., "Meta-optics empowered vector visual cryptography for high security and rapid decryption," *Nat. Commun.* **14**(1), 1946 (2023).
18. H. Yang et al., "Angular momentum holography via a minimalist metasurface for optical nested encryption," *Light Sci. Appl.* **12**(1), 79 (2023).
19. J. R. Fienup and P. S. Idell, "Imaging correlography with sparse arrays of detectors," *Opt. Eng.* **27**(9), 778 (1988).
20. C. A. Metzler et al., "Deep-inverse correlography: towards real-time high-resolution non-line-of-sight imaging," *Optica* **7**(1), 63–71 (2020).
21. X. Bai et al., "Coherent imaging of objects through thin-layer highly scattering medium based on optical encryption," *Opt. Commun.* **506**, 127558 (2022).
22. Y. Shi et al., "Multiple-image double-encryption via 2D rotations of a random phase mask with spatially incoherent illumination," *Opt. Express* **27**(18), 26050–26059 (2019).
23. H. Wu et al., "Cryptographic analysis on an optical random-phase-encoding cryptosystem for complex targets based on physics-informed learning," *Opt. Express* **29**(21), 33558–33571 (2021).
24. B. Du et al., "Event encryption for neuromorphic vision sensors: framework, algorithm, and evaluation," *Sensors* **21**(13), 4320 (2021).
25. G. Gallego et al., "Event-based vision: a survey," *IEEE Trans. Pattern Anal. Mach. Intell.* **44**(1), 154–180 (2020).
26. S. Zhu et al., "Computational neuromorphic imaging: principles and applications," *Proc. SPIE* **12857**, 1285703 (2024).
27. M. Davies et al., "Advancing neuromorphic computing with loihi: a survey of results and outlook," *Proc. IEEE* **109**(5), 911–934 (2021).
28. G. Giamougiannis et al., "Neuromorphic silicon photonics with 50 GHz tiled matrix multiplication for deep-learning applications," *Adv. Photonics* **5**(1), 016004 (2023).
29. T. Mavroidis, J. Dainty, and M. Northcott, "Imaging of coherently illuminated objects through turbulence: plane-wave illumination," *J. Opt. Soc. Am. A* **7**(3), 348–355 (1990).
30. J. Cederquist et al., "Phase retrieval from experimental far-field speckle data," *Opt. Lett.* **13**(8), 619–621 (1988).
31. J. R. Fienup, "Phase retrieval algorithms: a comparison," *Appl. Opt.* **21**(15), 2758–2769 (1982).
32. C. Wang et al., "Tracking the shack-hartmann spots using neuromorphic motion compensation," in *Comput. Opt. Sens. and Imaging*, Optica Publishing Group, p. CTu2B–5 (2023).
33. D. Gehrig et al., "EKLT: asynchronous photometric feature tracking using events and frames," *Int. J. Comput. Vis.* **128**(3), 601–618 (2020).
34. S. Zhu et al., "Removing wall redundancy in non-line-of-sight object-tracking using neuromorphic imaging," in *Comput. Opt. Sens. and Imaging*, Optica Publishing Group, p. CTu2B–6 (2023).
35. Z. Ge et al., "Event-based laser speckle correlation for micro motion estimation," *Opt. Lett.* **46**(16), 3885–3888 (2021).
36. C. Metzler et al., "prDeep: robust phase retrieval with a flexible deep network," in *Int. Conf. Mach. Learn.*, PMLR, pp. 3501–3510 (2018).
37. M. Lyu et al., "Learning-based lensless imaging through optically thick scattering media," *Adv. Photonics* **1**(3), 036002 (2019).
38. F. Wang et al., "Phase imaging with an untrained neural network," *Light Sci. Appl.* **9**(1), 77 (2020).
39. S. Zhu et al., "Imaging through unknown scattering media based on physics-informed learning," *Photonics Res.* **9**(5), B210–B219 (2021).
40. A. Saba et al., "Physics-informed neural networks for diffraction tomography," *Adv. Photonics* **4**(6), 066001 (2022).

41. A. Goy et al., "Low photon count phase retrieval using deep learning," *Phys. Rev. Lett.* **121**(24), 243902 (2018).
42. S. Li et al., "Imaging through glass diffusers using densely connected convolutional networks," *Optica* **5**(7), 803–813 (2018).
43. F. Wang et al., "Learning from simulation: an end-to-end deep-learning approach for computational ghost imaging," *Opt. Express* **27**(18), 25560–25572 (2019).
44. S. Zhu et al., "Efficient color imaging through unknown opaque scattering layers via physics-aware learning," *Opt. Express* **29**(24), 40024–40037 (2021).
45. S. Zhu et al., "Displacement-sensible imaging through unknown scattering media via physics-aware learning," *Opt. Lasers Eng.* **160**, 107292 (2023).
46. Y. Hu, S.-C. Liu, and T. Delbruck, "v2e: from video frames to realistic DVS events," in *Proc. IEEE/CVF Conf. Comput. Vis. and Pattern Recognit.*, pp. 1312–1321 (2021).
47. X. Zhang et al., "Different channels to transmit information in scattering media," *PhotoniX* **4**(1), 1–13 (2023).
48. X. Zhang et al., "Physical origin and boundary of scalable imaging through scattering media: a deep learning-based exploration," *Photonics Res.* **11**(6), 1038–1046 (2023).
49. D. Ha and D. Eck, "A neural representation of sketch drawings," arXiv:1704.03477 (2017).

Shuo Zhu received his BS degree from Changchun University of Science and Technology in 2016, his MS degree from University of Shanghai for Science and Technology in 2019, and his PhD in optical engineering from Nanjing University of Science and Technology in 2023. He is now a postdoctoral fellow at the University of Hong Kong. His research interest is computational neuromorphic imaging and its optical applications.

Chutian Wang received his BS degree in Huang Kun Elite Class from the University of Science and Technology Beijing in 2020, and his MS degree in the major of optics and photonics from Imperial College London in 2021. He was a research assistant at Zhejiang University until 2022. He is currently working towards his PhD in the Department of Electrical and Electronic Engineering, University of Hong Kong. His research interests include computational optics and wavefront sensing.

Jianqing Huang received his BS degree from Harbin Institute of Technology in 2017, and his PhD in power engineering from Shanghai Jiao Tong University in 2022. He was a visiting researcher at Lund University, Sweden, from 2019 to 2021. He is now a postdoctoral fellow at the University of Hong Kong. His current research interests include deep learning, computational imaging, combustion diagnostics, and microplastics assessment.

Pei Zhang received his BS degree from Beijing University of Posts and Telecommunications, Beijing, China, and Queen Mary University of London, London, UK, in 2019, and his MS degree from University College London, London, in 2020. He is currently working toward his PhD in the Department of Electrical and Electronic Engineering, The University of Hong Kong, Hong Kong, China. His research interests include event-based vision and machine learning.

Jing Han received her BS and PhD degrees from Nanjing University of Science and Technology, China, in 2009 and 2015, respectively. She is currently a professor at Nanjing University of Science and Technology. Her research interests include computer vision, computational imaging, and deep learning in scattering imaging.

Edmund Y. Lam received his BS, MS, and PhD degrees in electrical engineering from Stanford University, Stanford, CA, USA. He was a visiting associate professor in the Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA, USA. He is currently a professor of electrical and electronic engineering at the University of Hong Kong. He is also a computer engineering program director and a research program coordinator at the AI Chip Center for Emerging Smart Systems. His research interests focus on computational imaging algorithms, systems, and applications. He is a fellow of SPIE, Optica, IEEE, IOP, IS&T, and HKIE and a founding member of Hong Kong Young Academy of Sciences.