Research Article Vol. 12, No. 8 / August 2025 / Optica 1261

OPTICA

Statistically stationary random light for high-security encryption

Shuqin Lin,[1] Xinlei Zhu,[1] Yijie Shen,[2,3] Fei Wang,[4] Xianfeng Chen,[1,5,7] Greg Gbur,[6,8] Yangjian Cai,[1,9] and Jiayi Yu[1,*]

[1]Shandong Provincial Engineering and Technical Center of Light Manipulation and Shandong Provincial Key Laboratory of Optics and Photonic Devices, School of Physics and Electronics, Shandong Normal University, Jinan 250358, China
[2]Centre for Disruptive Photonic Technologies, School of Physical and Mathematical Sciences and The Photonics Institute, Nanyang Technological University, Singapore 637371, Singapore
[3]School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798, Singapore
[4]School of Physical Science and Technology, Soochow University, Suzhou 215006, China
[5]State Key Laboratory of Advanced Optical Communication Systems and Networks, School of Physics and Astronomy, Shanghai Jiao Tong University, Shanghai 200240, China
[6]Department of Physics and Optical Science, University of North Carolina at Charlotte, Charlotte, North Carolina 28223, USA
[7]xfchen@sjtu.edu.cn
[8]gjgbur@uncc.edu
[9]yangjian_cai@163.com
*jiayiyu0528@163.com

Received 1 November 2024; revised 27 April 2025; accepted 1 July 2025; published 8 August 2025

In the modern landscape of the internet, the secure storage and transmission of information are key objectives. Optical encryption is a long-standing method for improving information security; however, existing optical encryption strategies are unable to reliably recover encrypted information following free-space transmission. We propose an encryption protocol that utilizes the statistical features of random light fields to overcome the limitations of existing approaches. This protocol entails continuously refreshing the white complex noise to generate a colored complex noise set that carries encrypted information. Users can recover information by determining the spatial coherence structure of the ciphertext at the receiving end. Furthermore, the proposed protocol exhibits resilience against external noise attacks within the transmission channel, and the protocol's unlimited key set makes it resistant to computer brute-force attacks. We hope that optical coherence engineering will extend the capabilities of existing optical encryption protocols, paving the way for future optical encryption technology.

https://doi.org/10.1364/OPTICA.546899

1. INTRODUCTION

With the rise in popularity of smart wearable devices, individuals now have the capability to access or share information from the Internet at any time and from any location. A significant portion of it, whether pertaining to personal matters, corporate interests, or even national security, requires strict confidentiality that is restricted solely to the sender and the recipient. Cryptography stands as the foundation for safeguarding confidential information [1]; however, in the swiftly evolving online landscape, the one-dimensional and serial processing characteristics of conventional digital passwords fall short of meeting the heightened security demands of rapid network data transmission [2]. Within this dynamic setting, optical encryption has arisen to address these challenges. By merging optical coding modulation technology with traditional encryption methods, optical encryption has great potential for data transmission applications involving multiple degrees of freedom (DoFs) [3,4], and exhibits significant promise within the realm of information security [5–8].

The inception of optical security systems traces back to the pioneering work of Refregier and Javidi with the development of double random phase encoding [3]. With the introduction of light having non-trivial structuring in its amplitude, phase, polarization, or coherence [9–11], the DoFs inherent in "structured light" have emerged as the preferred avenue for optical encryption [5–7]. For instance, recent innovations include optical encryption techniques leveraging phase structure modulation [12–14], orbital angular momentum [15,16], and polarization mode division multiplexing protocols [17–19]. However, the free-space diffraction of light beams, especially through turbulent media, poses a potential threat to the integrity of the encryption protocol. Present encryption protocols typically concentrate solely on the discussion of light sources, neglecting the crucial aspect of information recovery after free-space transmission. Consequently, the development of an optical encryption protocol optimized for free-space transmission, and ideally resilient to external attacks within the transmission channel, has emerged as a pressing challenge. On the other hand,

researchers are working on increasing the number of keys by manipulating various DoFs within the light fields to enhance the security of optical encryption systems [13]. However, the number of keys is often limited due to limitations in optical DoFs. Therefore, establishing a high-security optical encryption protocol that can flexibly customize the number of keys on demand, or even provide an unlimited key set, is another open problem.

Optical coherence, which characterizes the statistical properties of light, has been effectively manipulated to imbue light fields with various physical features while mitigating adverse effects during light–matter interactions [20]. In recent years, the swift advancement of coherence structure engineering theory [21,22] and corresponding experimental techniques [20,23] has broadened the usefulness of random light beams for numerous applications [20,24–28]. This paper introduces an encryption protocol founded on the spatial coherence structure (SCS) of statistically stationary random light fields. The ciphertext generated by this protocol is not only transportable through free space but also exhibits resilience against external attacks. Additionally, the protocol provides an unlimited key set to enhance the security of optical encryption systems.

2. RESULTS

A. Principle

A schematic diagram illustrating the principle of the proposed protocol is depicted in Fig. 1(a). Utilizing a Cartesian coordinate system, the encrypted information is represented as $I(\mathbf{v})$, where $\mathbf{v}$ is a two-dimensional variable, assumed to be a positive function. It undergoes Fourier transformation subsequent to the application of white complex noise $\aleph(\mathbf{v})$ (a random complex matrix) that satisfies the standard normal distribution, and then embeds the encryption key $K(\mathbf{r})$ to encrypt the information into colored complex noise $\Psi(\mathbf{r}) = \mathcal{F}[\sqrt{I(\mathbf{v})}\aleph(\mathbf{v})]K(\mathbf{r})$, where $\mathbf{r}$ is the spatial position, and $\mathcal{F}$ denotes the Fourier transform operators. Different from the traditional double random phase encryption [3], our protocol encrypts the information into a set of colored complex noise, $\{\Psi_m(\mathbf{r})\}_M$, by continually refreshing statistically independent white complex noise. The subscripts m and M denote an element of the sequence and the total number of set elements, respectively. In practice, the continuously refreshed, statistically independent white complex noise causes the illuminated encrypted information to become an incoherent light field. The Fourier transformation is considered the actual optical path response function, which converts the incoherent light field into a partially coherent field, serving as an encryption mechanism to embed both the encrypted information and the key into the statistical characteristics of random light fields [22]. Figures 1(b) and 1(c) visually depict white complex noise and colored complex noise, both of which conform to Gaussian statistics [29]. Crucially, it is noteworthy that the embedded encryption key can be represented as a key set $\{K_n(\mathbf{r})\}_N$, where n and N denote the sequence element and number of key elements. In principle, the elements within the key set can be infinite, consequently allowing for an unlimited number of keys within the proposed protocol. The security of an encryption protocol can undergo exponential enhancement through the augmentation of key numbers. We proceed to evaluate the security of this protocol below.

The above-colored complex noise set elements are randomly and cyclically applied to a deterministic electric field $E(\mathbf{r})$, resulting in a random electric field $U(\mathbf{r}) = E(\mathbf{r})\Psi(\mathbf{r})$ that fluctuates randomly with space and time [30]. The inclusion of colored complex noise introduces a new DoF in light fields, coherence, which is governed by the statistics of the field. In accordance with statistical optics [29] and optical coherence theory [21,22], the second-order statistics of the random electric field $U(\mathbf{r})$ can be characterized

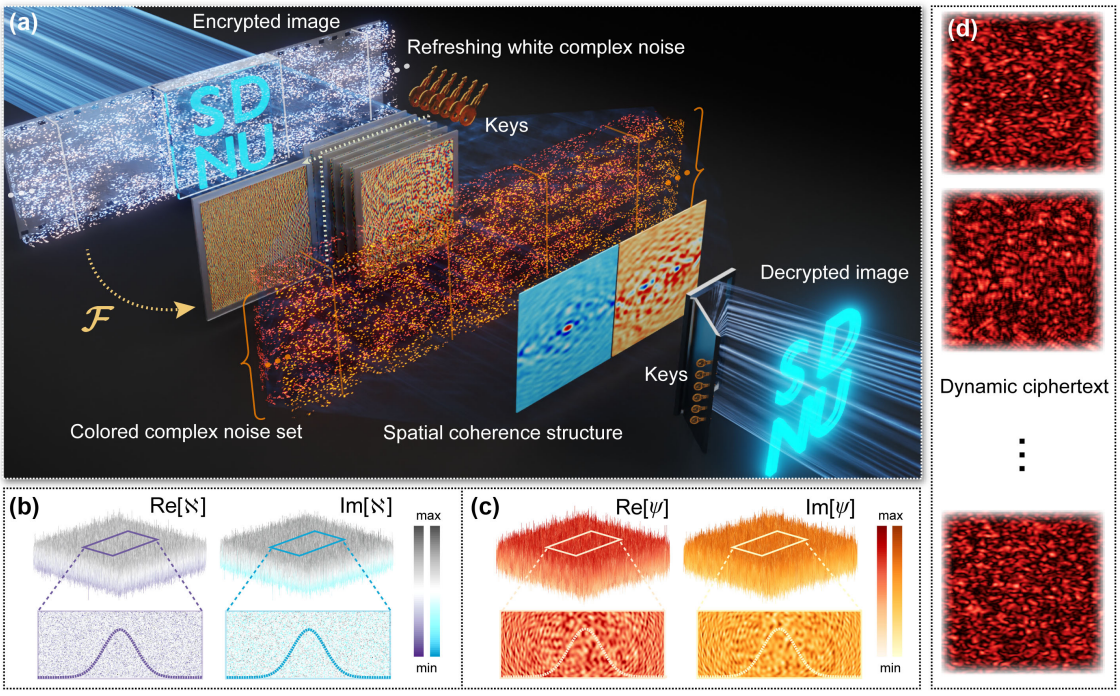

Fig. 1. Encryption principle of spatial coherence structure. (a) Schematic diagram of information encryption based on dynamic white complex noise and decryption based on a colored complex noise set. (b, c) Spatial distribution of real and imaginary components of white and colored complex noise with Gaussian statistics. (d) Intensity distribution of ciphertexts transmitted through free space.

by the function $\langle U(\mathbf{r}_1)U^*(\mathbf{r}_2)\rangle = E(\mathbf{r}_1)E^*(\mathbf{r}_2)\langle \Psi(\mathbf{r}_1)\Psi^*(\mathbf{r}_2)\rangle$, where the asterisk represents the complex conjugate. Because the colored complex noise $\Psi(\mathbf{r})$ conforms to Gaussian statistics, its first-order statistical average is zero, and the second-order statistical average is equal to the corresponding spatial coherence of the source [21], i.e., $\langle \Psi(\mathbf{r})\rangle = 0$ and $\langle \Psi(\mathbf{r}_1)\Psi^*(\mathbf{r}_2)\rangle = \mu(\mathbf{r}_1, \mathbf{r}_2)$, implying that the colored complex noise determines the spatial coherence characteristics of the random electric field. Therefore, the four-dimensional SCS can be described by the second-order statistics of the random electric field, $\mu(\mathbf{r}_1, \mathbf{r}_2) \propto \langle U(\mathbf{r}_1)U^*(\mathbf{r}_2)\rangle$, and encrypted information and keys are encoded into the SCS of random light fields. Previous research has shown that random light with prescribed SCS exhibits resilience to environmental disruptions. Therefore, leveraging the SCS as a carrier of encrypted information endows the proposed protocol with resistance against noise attacks. We proceed to analyze the performance of this protocol in resisting attacks below.

The set of random electric fields carrying encrypted information and keys is transmitted and focused by a lens. We conduct the analysis on an ensemble of random electric fields at the receiving end (focal plane/far field). It is important to note that our protocol is applicable to any propagation distance. Wolf proved that the second-order statistical average of light fields satisfy a pair of wave equations and the Helmholtz equation, respectively, and the statistical characteristics of light evolve in a well-defined manner during propagation [31]. The second-order statistics of the random electric fields endowed with colored complex noise at the receiving end can be derived using the generalized Collins integral formula [32]:

$$\begin{aligned}&\left\langle U(\boldsymbol{\rho}_1)U^*(\boldsymbol{\rho}_2)\right\rangle \\ &= \int \left\langle U(\mathbf{r}_1)U^*(\mathbf{r}_2)\right\rangle G(\mathbf{r}_1, \boldsymbol{\rho}_1)G^*(\mathbf{r}_2, \boldsymbol{\rho}_2)\mathrm{d}^2\mathbf{r}_1\mathrm{d}^2\mathbf{r}_2, \end{aligned} \quad (1)$$

where $G(\mathbf{r}, \boldsymbol{\rho})$ denotes the Green's function with $\mathbf{r}$ and $\boldsymbol{\rho}$ represent the spatial coordinate in source plane and receiving plane, respectively.

Through the above formula, we can get the second-order statistics of the set of electric fields with colored complex noise at the receiving end:

$$\left\langle U(\boldsymbol{\rho}_1)U^*(\boldsymbol{\rho}_2)\right\rangle = \mathcal{F}\left\{\mathcal{F}[I(\mathbf{v})]\{K_n(\mathbf{r}_1)\}_N\{K_n^*(\mathbf{r}_2)\}_N\right\}. \quad (2)$$

Leveraging the relationship between the SCS and the second-order statistics of the random electric field at the receiving end, $\mu(\boldsymbol{\rho}_1, \boldsymbol{\rho}_2) \propto \langle U(\boldsymbol{\rho}_1)U^*(\boldsymbol{\rho}_2)\rangle$, users can assess the SCS of the received random light beams and recover the encrypted information by inversely performing the encryption process and utilizing the key corresponding to the conjugate of the encryption key using the following formula:

$$I(\mathbf{v}) \propto \mathcal{F}^{-1}\left\{\mathcal{F}^{-1}\left[\mu\left(\boldsymbol{\rho}_1, \boldsymbol{\rho}_2\right)\right]\left\{K_n^*(\mathbf{r}_1)\right\}_N\{K_n(\mathbf{r}_2)\}_N\right\}. \quad (3)$$

A more detailed description of the theoretical framework of the protocol is given in Supplementary Note 1.

B. Security Analysis

As an illustrative example, according to our protocol, we choose the key set expression as $\{K_n(\mathbf{r})\}_N = \sum_n^N \exp(iq_n^{p_n}|\mathbf{r}|^{p_n}/10^{3p_n})$, where p_n is called the exponential key and q_n is called the coefficient key. In the following discussion, we set $N = 3$, i.e., utilizing six keys (three exponential keys and three coefficient keys) to encrypt the image "SDNU" (Shandong Normal University) into the colored complex noise set simultaneously. The detailed parameters of the customized keys for this case are provided in Supplementary Note 2. In Fig. 1(d), we present a selection of partial ciphertexts (random light speckles) transmitted through free space. In the ciphertext generation mechanism, the number of ciphertexts corresponds to the total number of elements in the colored noise set. Setting $M = 5000$, and leveraging the collected 5000 ciphertexts, we employ the phase-perturbation method [33] to measure the SCS of the light carrying encrypted information. Refer to Supplementary Note 3 for details regarding the measurement method. We present the numerical simulation results of the SCS after transmission in Fig. 2(a) and recover the image based on the SCS. Figure 2(b) displays the encrypted image and the decryption result. To quantitatively assess the decryption result quality, we compute the correlation coefficient (CC) between the original image and the decryption result [34]:

$$\mathrm{CC} = \frac{\sum_i \sum_j (I(i, j) - \bar{I})(I'(i, j) - \bar{I}')}{\sqrt{\sum_i \sum_j (I(i, j) - \bar{I})^2 \sum_i \sum_j \left(I'(i, j) - \bar{I}'\right)^2}}, \quad (4)$$

where $I(i, j)$ and $I'(i, j)$ represent the intensity values of the original image and the decrypted result, respectively, where i and j denote the pixel coordinates. $\bar{I}$ and $\bar{I}'$ are the intensity averages of the original image and the decrypted result, respectively. The relationship between the correlation strength of the decrypted result and the original image and the CC value is given in Supplementary Note 4. The value of CC below 0.4 indicates a weak correlation between the original and decrypted images. Therefore, CC = 0.4 is selected as the threshold for evaluating the decryption result. Our findings indicate that discernible information correlated with the original image is only evident when six keys are simultaneously correct, with CC = 0.91 between the decrypted result and the original. This high CC value signifies that the decryption is successful and the correlation strength is "very strong" [34]. In contrast, if the keys are not entirely correct, the decrypted output fails to reveal any discernible information linked to the original image, and all CC values fall below 0.4, indicating decryption failure. For examples of decryption failure result, refer to Supplementary Note 5. The rigorous one-to-one correspondence between encryption rules and decryption outcomes safeguards the security of the implemented protocol.

Additionally, evaluating the security of the encryption protocol necessitates computer brute-force attacks testing. To ascertain our protocol's resilience against brute-force attacks, we first perform a key tolerance test analysis. We define the error value between the incorrect and correct key as $\Delta\delta$. Figure 2(c) illustrates the decryption results for varying $\Delta\delta$. We observe that as $|\Delta\delta|$ decreases, the CC gradually increases. When $|\Delta\delta|$ reduces to 0.1, the CC of the incorrect decoding result approaches 0.4. When $|\Delta\delta| < 0.1$, the CC exceeds 0.4, even with an incorrect key. Consequently, the key tolerance value for this encryption protocol is established at $|\Delta\delta| = 0.1$.

In response to the threat of brute-force attacks on computers, we have analyzed the resilience of the proposed protocol against them using two common methods [35]. The first method involves the computer enumerating all possible keys and testing each sequentially. The second method entails the computer randomly selecting guessed keys for a more haphazard approach to the attack. For the former method, the attack time can be estimated by the formula:

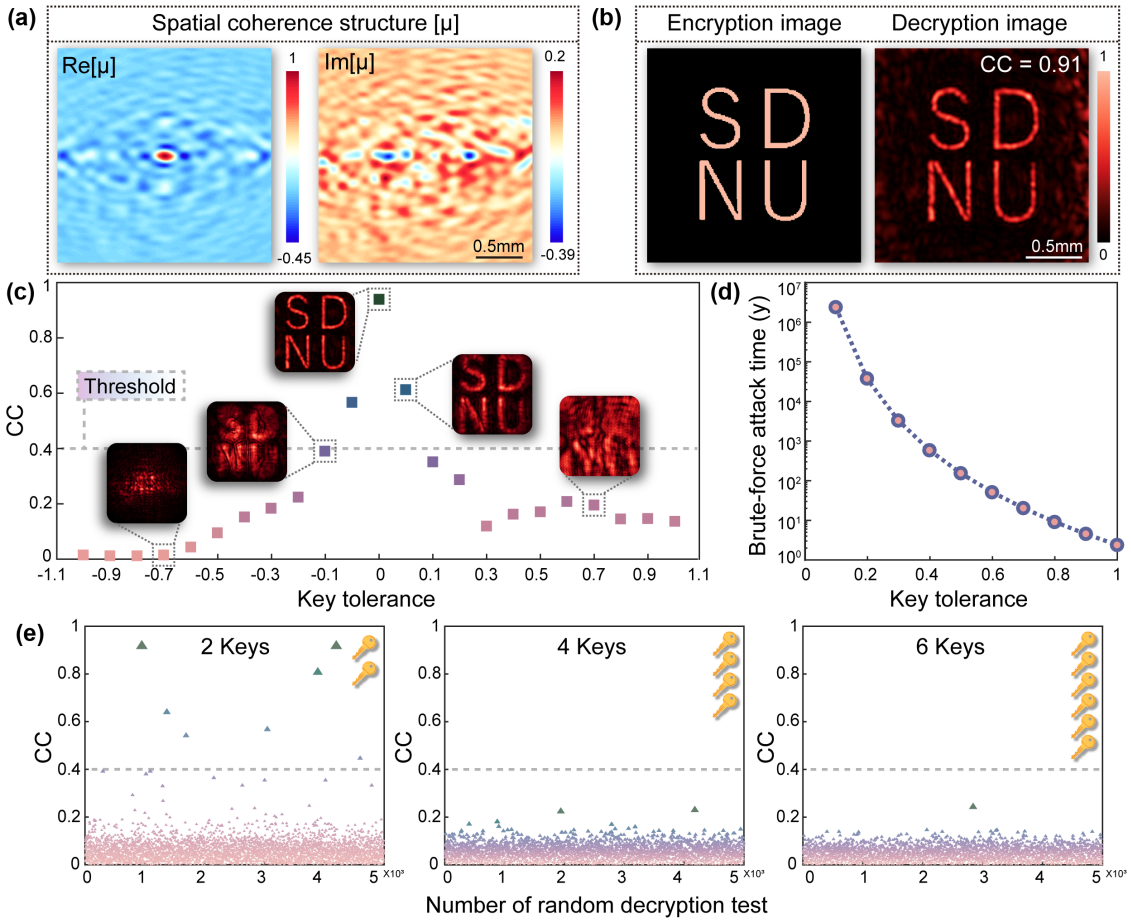

Fig. 2. Simulation results demonstration. (a) Spatial distribution of real and imaginary components of the spatial coherence structure of random light carrying encrypted image and key information. (b) Encrypted image "SDNU" and simulated decryption result with CC = 0.91. (c) Key tolerance analysis shows the decryption test results under different key error values. (d) The relationship between the time required for computer brute-force attacks and the key tolerance. (e) Test results of performance against random brute-force attacks under different numbers of keys.

$t = (Q/\alpha)^{N'} \Delta t$, where Q represents the range of possible key values, α is the step between guessed keys, Δt is the time required for each decryption attempt, and N' is the total number of keys involved. Assuming the range for the guessed key values in computer brute-force attack is set between $[-10, 10]$, with a step size of 0.1 (corresponding to the key tolerance), and each decryption attempt takes $\Delta t = 2$ s. It is important to note that, according to the correct key values listed in Supplementary Note 2, the range set for guessed key values is quite narrow. Despite this limitation, the computer would need to operate continuously for approximately 4.1 million years to complete the attack. This timeframe renders the task practically impossible. Figure 2(d) illustrates the computer brute-force attack times under varying levels of guessing accuracy, corresponding to different key tolerances. More crucially, our protocol allows for the expansion of the number of keys or an increase in the numerical difference between keys (i.e., increasing the key value range Q), which poses a significant challenge for brute-force attacks. We depict this challenge graphically as a function of the number of keys and the key value range in Supplementary Note 6. For the latter, we conducted a brute-force attack test using a computer. Figure 2(e) displays the brute-force attack resistance when setting 2, 4, and 6 keys, respectively, according to our protocol. In the above setup, we performed 5000 random decryption tests. Our test results indicate that even with only two keys, the protocol exhibits strong resistance against brute-force attacks. As the number of keys increases, so does the protocol's capability to resist against brute-force attacks. Specifically, using six keys, the average CC of 5000 decryption tests is only 0.04, and the variance is 7.65×10^{-4}, confirming the high security and stability of our protocol. Supplementary Note 7 presents the average and variance of CC for different numbers of keys. Thus, the outcomes of these brute-force attack tests demonstrate that without the correct keys, brute-force attack methods are ineffective against our protocol, emphasizing its high security.

C. Experiment

Figure 3(a) presents a schematic diagram of the experimental setup for the proposed protocol, which comprises an encryption system, a transmission area, and a decryption system. The encryption system employs a complex amplitude modulation encoding algorithm [36] to encode colored complex noise into a computer-generated holograms set on SLM1, as shown in the illustration in the encryption system. SLM1 is used to simulate the effects of the image, white noise, and key in a single operation. A more detailed description of the algorithm is given in Supplementary Note 8. These holograms are cyclically loaded onto a spatial light modulator (SLM) with a refresh rate of 60 Hz. Plane waves then illuminate the computational hologram on the SLM, and a $4f$

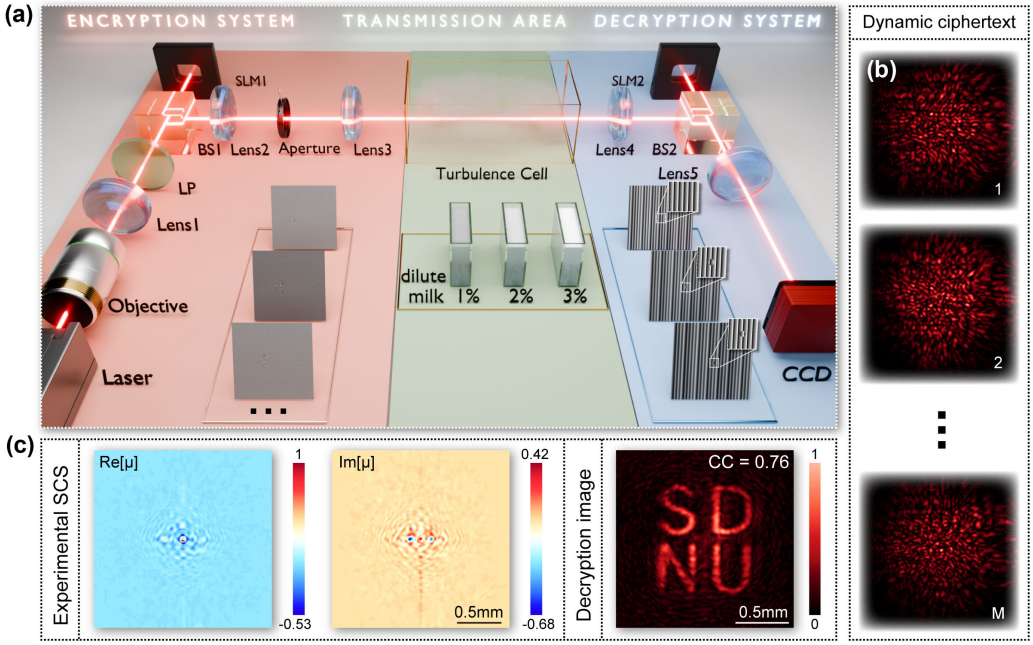

Fig. 3. Experimental demonstration of encryption and decryption. (a) The experimental setup contains the encryption system (pink), transmission area (green), and decryption system (blue). LP, linear polarizer; BS, beam splitter; SLM, spatial light modulator; CCD, charge-coupled device. The illustrations are the computational hologram, dilute milk medium with different concentrations, and phase perturbation screen. (b) Examples of dynamic ciphertext intensity distribution. (c) Spatial coherence structure distribution at the receiving end and experimental decryption result with CC = 0.76.

imaging system filters out the first-order diffracted beam from the grating to produce the dynamic ciphertext. It is worth noting that the SLM can be replaced with a high-speed modulator, such as a digital micromirror device, to accommodate applications requiring higher refresh rates [36]. Figure 3(b) illustrates examples of the dynamic ciphertext. They pass through the transmission area and are focused by a thin lens into the decryption system. Here, we use a phase-perturbation method to analyze the SCS of the dynamic ciphertext to achieve the extraction of encrypted information. Illustration in the decryption system shows three phase-perturbation screens loaded onto the SLM in the decryption system. It is important to note that external noise can be introduced into the ciphertext's transmission path to experimentally test the protocol's resilience against noise attacks. The experimental diagrams for static noise (dilute milk medium) and dynamic noise (simulating atmospheric turbulence) are displayed in the transmission area of Fig. 3(a). We will subsequently evaluate the protocol's performance against noise attacks.

Figure 3(c) displays the experimental results of the SCS distribution and the decryption result of the ciphertext at the receiving end following free-space transmission. We discovered that using the correct keys can recover encrypted information very effectively. The CC between the experimentally decrypted result and the original image is 0.76, indicating successful decryption with a strong correlation. Supplementary Note 9 presents the decryption outcomes using randomly incorrect keys. As anticipated, these incorrect keys failed to reveal any discernible information related to the original image, with all CC being less than 0.4. To further validate the reliability of the proposed encryption and decryption protocols, we include experimental results for two distinct sets of ciphertexts in Supplementary Note 10. Here we briefly summarize: both simulation and experimental findings confirm that the optical encryption protocol, which leverages the statistical features of statistically stationary random light, is both effective and resistant to computer brute-force attacks.

D. Noise Attack Resistance Test

Encryption protocols with attack resistance alone do not fully address the requirements of practical applications. It is also essential to ensure that the transmission of information can withstand environmental attacks. Specifically, the protocol must allow for the accurate extraction of information at the receiving end, even if the light field carrying the data is disrupted during transmission. To assess our protocol's resilience to external noise attacks, we conducted experimental attack resistance tests using a dilute milk medium to simulate static noise attacks and a controllable turbulence cell for dynamic noise attacks. Figure 4(a) (top) illustrates the results of experiments conducted with dilute milk media at concentrations of 1%, 2%, and 3% placed in the transmission path. We observed that, despite the intensity and phase distribution of the ciphertext being compromised by the dilute milk medium, the encrypted information could still be decrypted and recovered at the receiving end by analyzing its SCS. To quantitatively demonstrate the noise attack of the diluted milk medium, we measured the intensity transmittance of the light beam after passing through the medium at varying concentrations, which serves as an indicator of the medium's scattering capability. As depicted in Fig. 4(b), the intensity transmittance at concentrations of 1%, 2%, and 3% was 5.82%, 0.59%, and 0.08%, respectively. These results confirm that our protocol remains effective even under severe static noise conditions. Supplementary Note 11 includes actual photographs showing the different concentrations and container sizes used in the experiments, providing further insight into the experimental setup and conditions.

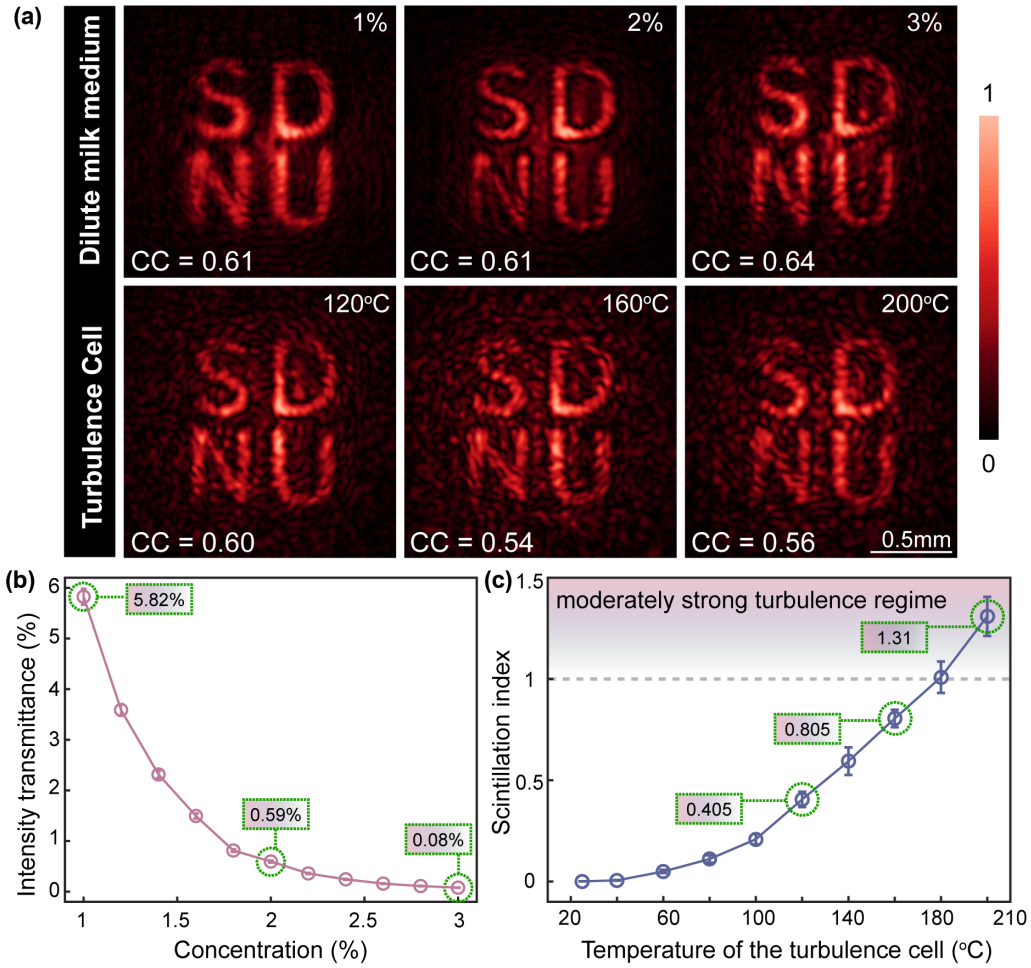

Fig. 4. Noise attack resistance experimental test results. (a) Experimental decryption results after experiencing different strong of static noise attacks (dilute milk medium) and dynamic noise (turbulence cell) attacks. (b) Measured light intensity transmittance of a Gaussian beam passing through a dilute milk medium as a function of medium concentration. (c) Measured scintillation index of a Gaussian beam propagating through the turbulence cell as a function of control temperature. Error bars represent the standard deviation of 10 independent measurements.

To confirm that the proposed protocol is also resilient to dynamic noise attacks, we began by measuring the turbulence strong after transmitting a Gaussian beam through the turbulence cell channel. Known to cause beam distortion and beam wander, moderate or strong turbulence can lead to significant fluctuations in ciphertext intensity and phase at the receiving plane. These fluctuations can be quantitatively evaluated using the scintillation index. Figure 4(c) displays the relationship between the measured scintillation index and the control temperature of the turbulence cell. The scintillation index ranges from 0 to 1.31, which indicates that the turbulence cell can provide up to moderately strong turbulence. In realistic urban environments, where the refractive index structure parameter C_n^2 typically is of the order of 10^{-13} to 10^{-15}. Our experimental data, based on the Kolmogorov turbulence model, indicate that the maximum scintillation index is 1.31, corresponding to an actual transmission distance of 2–20 km. Both beam distortion and beam wander contribute to the increase in the scintillation index, making it a standard measure of turbulence strong. Figure 4(a) (bottom) presents the experimental decryption results when the ciphertext is transmitted through a thermally turbulent medium. Remarkably, even when the turbulence cell temperature is set to 200°C, producing a scintillation index of 1.31, our protocol still successfully recovers the encrypted information. Thus, even under high-strong dynamic noise attacks, our protocol enables the correct decryption of encrypted information through the analysis of the SCS of the ciphertext at the receiving end. In summary, our noise attack resistance test results confirm that our protocol is able to effectively resist noise attacks, emphasizing its robustness under challenging environmental conditions.

3. CONCLUSION AND DISCUSSION

We proposed and experimentally verified a high-security optical encryption protocol based on the statistical features of statistically stationary random light that overcomes the limitations of existing optical encryption strategies in ensuring the transportability of encrypted information. The proposed protocol utilizes continuously refreshing white complex noise to dynamically hide image information and embed key information simultaneously. Subsequently, it generates a colored complex noise set that carries both image and key information. When illuminated by plane waves, dynamic ciphertext speckles, influenced by the colored complex noise, can be transmitted. Users can recover the original image by measuring the SCS of the received dynamic ciphertext speckles.

Compared with other existing optical encryption protocols, our protocol effectively addresses challenges in the contemporary optical encryption landscape and offers several key advantages. These include immunity of dynamic ciphertext speckles to free-space diffraction effects, ensuring the transmission of encrypted information, and robust resilience against external attacks; the introduction of an unlimited key set to accommodate customized key quantity requirements and significantly enhance encryption system security. It is worth emphasizing that the extended DoFs afforded by random light allow for seamless integration of statistical features with polarization and orbital angular momentum control, thereby establishing a wider information carrier space [36] and enabling high-capacity optical encryption with an unparalleled level of security. As a matter of fact, the SLM in our protocol can be substituted with a metasurface to strengthen the integration of the encryption system. Photonic platforms offer the advantages of ultra-high spatial resolution and ultra-wide bandwidth, and have found applications in optical encryption [12,16,19]. Recently, research on generating statistically stationary random light using photonic platforms has been reported [37,38], suggesting that the combination of photonic platforms and optical coherence engineering holds exciting potential in the realm of optical encryption. Our findings underscore that optical coherence engineering expands the functionality of existing optical encryption protocols, promoting the development of optical encryption systems for high-security storage and transfer of information, and inspiring the application of optical coherence engineering in high-security optical communications and quantum information.

APPENDIX A: METHODS

Information encryption. According to the generalized van Cittert–Zernike theorem, statistically stationary random lights can be generated through the transmission of spatially incoherent light sources. During the process, the SCS of the light is constructed due to the transmission of incoherent light, which is determined by the intensity distribution of the incoherent light and the response function of the optical system. In practical encryption scenarios, the incoherent light intensity distribution can be tailored to represent encrypted information, while the response function of the optical system can serve as the encryption key during the encryption process. This enables the encryption of both the information and the key into the SCS of the random light. Hence, when the SCS is measured, combining it with the key allows for the reconstruction of the original information based on the reciprocity relationship. The detailed theoretical derivation process is given in Supplementary Note 1.

Complex amplitude modulation encoding algorithm. In our experiment, we employed the complex amplitude modulation encoding algorithm to synthesize random light, facilitating information encryption based on SCS. We represent the cross-spectral density function of random light carrying encrypted image and key information as an incoherent sum of multiple complex random modes. These complex random modes are expressed through complex random transmittance functions associated with SCS. By standardizing the weights of all complex random modes, we could overlay a finite number of them to generate the random light containing encrypted image and key information. The complex amplitude modulation encoding algorithm utilized in our work offers a streamlined and adaptable method for modulating SCS. Detailed algorithm content is given in Supplementary Note 8.

Phase-perturbation method. Our experiment uses the phase-perturbation method to measure the SCS of a random light containing encrypted image and key information. We construct the cross-spectral density function of the random light on the target plane by recording the intensity of the random light on the Fourier plane after three different phase perturbations. By setting the position of the phase perturbation point as the position of the reference point, we perform a difference operation on the two phase-perturbed Fourier plane intensities and the third one and then perform the inverse Fourier transform. Subsequently, we multiply the coefficients related to the perturbation value respectively to obtain the cross-spectral density function related to the position of the perturbation point. For detailed measurement methods, see Supplementary Note 3.

Funding. National Key Research and Development Program of China (2022YFA1404800); National Natural Science Foundation of China (12374276, 12304326, 12192254); China Postdoctoral Science Foundation (2022M721992); Natural Science Foundation of Shandong Province (ZR2023QA081); Ministry of Education - Singapore (MOE) AcRF Tier 1 (RG157/23, RT11/23); Singapore Agency for Science, Technology and Research (A*STAR) MTC Individual Research Grants (M24N7c0080).

Disclosures. The authors declare no conflicts of interest.

Data availability. No data were generated or analyzed in the presented research.

Supplemental document. See Supplement 1 for supporting content.

REFERENCES

1. J. Buchmann, *Introduction to Cryptography* (Springer, 2004).
2. B. Javidi, *Optical and Digital Techniques for Information Security* (Springer, 2005).
3. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**, 767–769 (1995).
4. B. L. Volodin, B. Kippelen, K. Meerholz, *et al.*, "A polymeric optical pattern-recognition system for security verification," Nature **383**, 58–60 (1996).
5. W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," Adv. Opt. Photonics **6**, 120–155 (2014).
6. B. Javidi, A. Carnicer, M. Yamaguchi, *et al.*, "Roadmap on optical security," J. Opt. **18**, 083001 (2016).
7. N. K. Nishchal, *Optical Cryptosystems* (IOP Publishing, 2019).
8. Z. Wan, H. Wang, Q. Liu, *et al.*, "Ultra-degree-of-freedom structured light for ultracapacity information carriers," ACS Photonics **10**, 2149–2164 (2023).
9. A. Forbes, "Structured light from lasers," Laser Photonics Rev. **13**, 1900140 (2019).
10. A. Forbes, M. de Oliveira, and M. R. Dennis, "Structured light," Nat. Photonics **15**, 253–262 (2021).
11. C. He, Y. Shen, and A. Forbes, "Towards higher-dimensional structured light," Light **11**, 205 (2022).
12. G. Qu, W. Yang, Q. Song, *et al.*, "Reprogrammable meta-hologram for optical encryption," Nat. Commun. **11**, 5484 (2020).
13. K. T. Lim, H. Liu, Y. Liu, *et al.*, "Holographic colour prints for enhanced optical security by combined phase and amplitude control," Nat. Commun. **10**, 25 (2019).
14. H. Wang, X. Yang, Z. Liu, *et al.*, "Deep-learning-based recognition of multi-singularity structured light," Nanophotonics **11**, 779–786 (2022).
15. X. Fang, H. Ren, and M. Gu, "Orbital angular momentum holography for high-security encryption," Nat. Photonics **14**, 102–108 (2020).
16. H. Yang, P. He, K. Ou, *et al.*, "Angular momentum holography via a minimalist metasurface for optical nested encryption," Light **12**, 79 (2023).
17. X. Li, T. H. Lan, C. H. Tien, *et al.*, "Three-dimensional orientation-unlimited polarization encryption by a single optically configured vectorial beam," Nat. Commun. **3**, 998 (2012).

18. X. Zhan, Z. Zhou, W. Zhou, *et al.*, "Wavelength-tunable circularly polarized laser arrays for multidimensional information encryption," Adv. Opt. Mater. **11**, 2200872 (2023).
19. J. Ji, C. Chen, J. Sun, *et al.*, "High-dimensional Poincare beams generated through cascaded metasurfaces for high-security optical encryption," PhotoniX **5**, 13 (2024).
20. J. Yu, X. Zhu, F. Wang, *et al.*, "Research progress on manipulating spatial coherence structure of light beam and its applications," Prog. Quantum Electron. **91–92**, 100486 (2023).
21. L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics* (Cambridge University Press, 1995).
22. E. Wolf, *Introduction to the Theory of Coherence and Polarization of Light* (Cambridge University Press, 2007).
23. Y. Cai, Y. Chen, J. Yu, *et al.*, "Generation of partially coherent beams," Prog. Opt. **62**, 157–223 (2017).
24. J. Chen, Y. Wang, B. Jia, *et al.*, "Observation of the inverse Doppler effect in negative-index materials at optical frequencies," Nat. Photonics **5**, 239–242 (2011).
25. B. Redding, M. A. Choma, and H. Cao, "Speckle-free laser imaging using random laser illumination," Nat. Photonics **6**, 355–359 (2012).
26. D. Peng, Z. Huang, Y. Liu, *et al.*, "Optical coherence encryption with structured random light," PhotoniX **2**, 6 (2021).
27. X. Zhao, Z. Wang, X. Lu, *et al.*, "Ultrahigh precision angular velocity measurement using frequency shift of partially coherent beams," Laser Photonics Rev. **17**, 2300318 (2023).
28. Y. Liu, Z. Dong, Y. Zhu, *et al.*, "Three-channel robust optical encryption via engineering coherence Stokes vector of partially coherent light," PhotoniX **5**, 8 (2024).
29. J. W. Goodman, *Statistical Optics* (Wiley, 2015).
30. O. Korotkova, *Random Light Beams: Theory and Applications* (CRC Press, 2017).
31. E. Wolf, "Optics in terms of observable quantities," Il Nuovo. Cim. **12**, 884–888 (1954).
32. S. A. Collins, "Lens-system diffraction integral written in terms of matrix optics," J. Opt. Soc. Am. **60**, 1168–1177 (1970).
33. J. Zeng, X. Lu, L. Liu, *et al.*, "Simultaneous measurement of the radial and azimuthal mode indices of a higher-order partially coherent vortex beam based on phase detection," Opt. Lett. **44**, 3881–3884 (2019.
34. M. J. Campbell, *Statistics at Square One* (Wiley, 2021).
35. A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography* (CRC Press, 2018).
36. X. Zhu, J. Yu, Y. Chen, *et al.*, "Generation of stochastic structured light beams with controllable beam parameters," ACS Photonics **10**, 2272–2279 (2022).
37. L. Liu, W. Liu, F. Wang, *et al.*, "Spatial coherence manipulation on the disorder-engineered statistical photonic platform," Nano Lett. **22**, 6342–6349 (2022).
38. L. Liu, W. Liu, F. Wang, *et al.*, "Ultra-robust informational metasurfaces based on spatial coherence structures engineering," Light **13**, 131 (2024).