Securing 2D information carriers over dynamic and turbulent media in a free-space optical channel

YONGGUI CAO,[1] YIN XIAO,[1] AND WEN CHEN[1,2,*]

[1]*Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong, China*
[2]*Photonics Research Institute, The Hong Kong Polytechnic University, Hong Kong, China*
*owen.chen@polyu.edu.hk

In this Letter, a new scheme is proposed to realize high-fidelity secured free-space optical information transmission through dynamic and turbulent media by encoding 2D information carriers. The data is transformed into a series of 2D patterns as information carriers. A novel differential method is developed to suppress noise, and a series of random keys are also generated. A different number of absorptive filters are arbitrarily combined to be placed in the optical channel to generate ciphertext with high randomness. It is experimentally demonstrated that the plaintext can be retrieved only when correct security keys are applied. Experimental results demonstrate that the proposed method is feasible and effective. The proposed method could open an avenue for securing high-fidelity optical information transmission over dynamic and turbulent media in a free-space optical channel.

Ghost diffraction originated from quantum [1], and is promising for imaging. Object information can be retrieved with a correlation between 2D illumination patterns and a series of collected single-pixel intensities [1–4]. Recently, ghost diffraction is developed to realize optical data transmission in free space [5,6]. Security of free-space optical data transmission has also attracted much attention, since optical signals could be easily intercepted and monitored by unauthorized parties. To solve the problem, some methods were proposed to realize a secured transmission [7–11], e.g., transform-based [8] and chaos [10,11]. These methods can isolate the signal from potential eavesdropping, and possess remarkable advantages, e.g., provable and quantifiable secrecy. However, the methods could be complicated and difficult to be realized in free space through complex scattering media [12,13]. In recent years, ghost diffraction could provide a promising alternative to realize a secured free-space optical transmission. However, secured ghost transmission is implemented in free space through static media, and is not applicable in dynamic and turbulent media [2–4,14–16]. Real-time transmission errors are generated, when the environment keeps changing due to dynamic and turbulent media [17]. To realize the secured optical transmission in dynamic and turbulent scattering environments, transmission errors induced need to be temporally corrected and the received data needs to be decrypted at the same time. It is desirable to design an optical approach to realizing secured free-space optical data transmission through dynamic and turbulent media.

In this Letter, a new scheme is proposed by encoding 2D information carriers to realize high-fidelity secured free-space optical information transmission through dynamic and turbulent media. The transmitted data is transformed into a series of 2D patterns as information carriers. The noise is suppressed using a novel differential method, and a series of random keys are also generated. A different number of absorptive filters are arbitrarily combined to be placed in the optical channel to generate ciphertext with high randomness. The plaintext can be retrieved only when correct keys are used. Feasibility and effectiveness of the proposed method are verified by optical experiments. Practical implementation of the proposed scheme is simple and convenient, and no complex operations are used, e.g., system calibration or post-processing to eliminate noise. The proposed method realizes high-fidelity, high-reliability and high-security optical information transmission over dynamic and turbulent media in a free-space optical channel.

An algorithm is developed to first convert each pixel of an analog signal (i.e., plaintext) into a 2D pattern, and the proposed algorithm is as follows: i) A pixel value is enlarged with a given magnification factor M to be an intermediate value b. The integral part of b is denoted as c, and the fractional part of b is denoted as d. ii) A sequence T with a length of $2c$ is generated. Half of the values in T are randomly generated between 0 and 1, and the remaining half of T is computed by subtracting the corresponding value in the first half from 1. iii) A 2D pattern can be obtained by arbitrarily placing fractional part d and each value of the sequence T into a zero matrix.

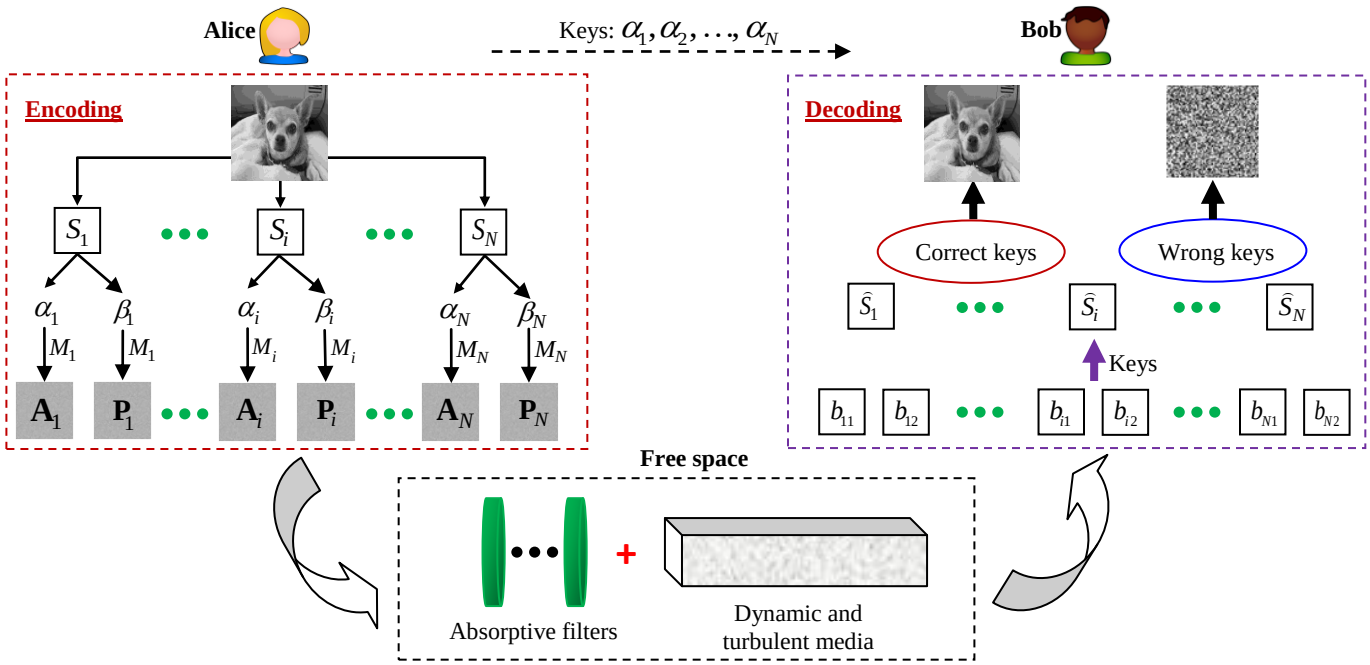

Fig. 1. A flow chart of the proposed secured optical transmission through dynamic and turbulent media in free space.

As shown in Fig. 1, Alice wants to optically transmit information (e.g., an image or an analog signal) to Bob in free space. Each pixel S_i (i=1,2,...,N) of the analog signal is first described by separate values α_i and β_i, i.e., $S_i = \alpha_i - \beta_i$. Then, each value α_i or β_i is transformed into a 2D pattern (i.e., $\mathbf{A}_i$ or $\mathbf{P}_i$) using the aforementioned algorithm. This differential method is developed to fully suppress noise, and a series of random security keys $(\alpha_i, i = 1,2,\ldots,N)$ are simultaneously generated. The generated 2D patterns, i.e., $\mathbf{A}_i$ and $\mathbf{P}_i$, are sequentially and alternately embedded into a spatial light modulator (SLM) to modulate the optical wave. The modulated wave propagates through dynamic and turbulent media in free space, and is collected by a single-pixel detector at the receiving end. A different number of absorptive filters are arbitrarily combined to be placed in the optical channel to modulate light intensities. The collected light intensity I_{out} could have a relationship with incident wave, i.e., denoted by a scaling factor k. When scaling factors linearly vary, the designed secured optical transmission system could be attacked. Here, a strategy is further developed to generate ciphertext with high randomness. A different number of absorptive filters (e.g., 1,2,...) are placed in the free-space optical channel at the transmitter, and then the scaling factors can possess dynamic and nonlinear properties. Moreover, scaling factors corresponding to two adjacent 2D patterns (i.e., $\mathbf{A}_i$ and $\mathbf{P}_i$) can be assumed to be the same in dynamic and turbulent environments. At the receiving end, collected light intensities b_{i1} and b_{i2} to serve as the ciphertext are respectively described by

$$b_{i1} \approx k_{i1} \iint \mathbf{A}_i(x,y)\,dxdy, \tag{1}$$

$$b_{i2} \approx k_{i2} \iint \mathbf{P}_i(x,y)\,dxdy, \tag{2}$$

where k_{i1} and k_{i2} respectively denote a scaling factor corresponding to 2D patterns $\mathbf{A}_i$ and $\mathbf{P}_i$, and $k_{i1} \approx k_{i2}$.

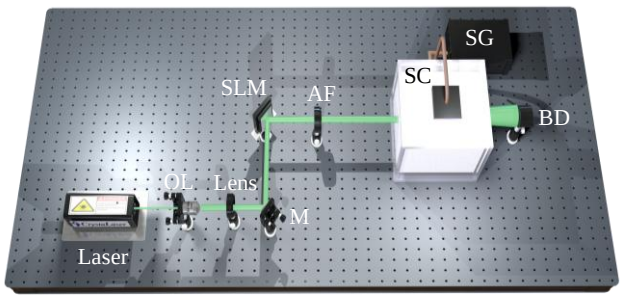

Fig. 2. A schematic experimental setup for the proposed secured free-space optical data transmission through dynamic and turbulent media. OL: Objective lens; M: Mirror; SLM: Amplitude-only spatial light modulator; AF: Absorptive filter(s); SC: Smoke chamber; SG: Smoke generator; BD: Single-pixel (bucket) detector.

After Bob receives the ciphertext b_{i1} and b_{i2}, he needs to use a series of random keys $(\alpha_i, i = 1,2,\ldots,N)$ to retrieve the plaintext. The decryption can be described by

$$\bar{S}_i = \alpha_i \left(1 - \frac{b_{i2}}{b_{i1}}\right). \tag{3}$$

Therefore, Bob can obtain ciphertext with high randomness and nonlinearity owing to the designed system, and random and nonlinear security keys can be provided by Alice. Only when correct keys α_i are used, the plaintext can be retrieved.

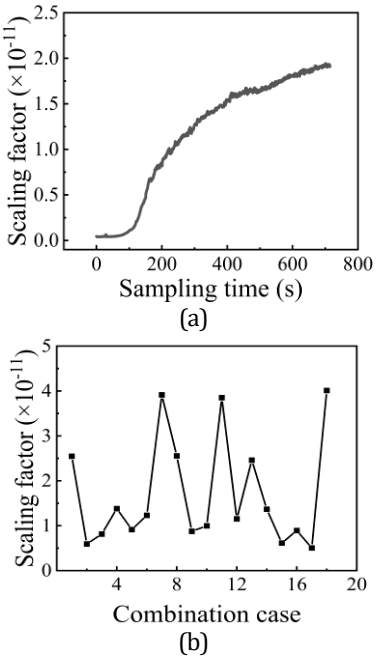

Fig. 3. (a) A variation of scaling factors corresponding to dynamic and turbulent media in free space, and (b) a nonlinear variation of scaling factors in dynamic and turbulent media. A combination case denotes a different number of absroptive filters to be placed in the free-space optical transmission channel.

A schematic experimental setup is shown in Fig. 2 to verify the proposed method. A green laser (CrystaLaser, CL532-025-S) is used as light source. Wavelength and power of the laser are 532.0 nm and 25.0 mW, respectively. The laser is expanded by an objective lens and collimated with a lens followed by the reflection with a mirror. The reflected wave is modulated by an amplitude-only SLM (Holoeye, LC-R720) and propagates through dynamic and turbulent media. The optical wave is modulated, when the series of 2D patterns is sequentially and alternately embedded into SLM. The free-space optical channel also consists of a different number of absorptive filters, a transparent acrylic smoke chamber [size of 30 (L) × 30 (W) × 40 (H) cm^3] and a single-pixel detector (Newport, 918D-UV-OD3R). The smoke is produced by a generator (HALFSun) with power of 3000W and pumping rate of 973.0cm^3/s. Smoke is pumped into the chamber with pumping time of 15 s. Axial distance between the SLM and absorptive filter is 10.0 cm, and axial distance between absorptive filter and front side of smoke chamber is 20.0 cm. The axial distance between back side of smoke chamber and single-pixel detector is 5.0 cm.

The dynamic property of turbulent media is shown in Fig. 3(a). The scaling factors increase with sampling time due to smoke liquefaction and sedimentation. When a different number of absorptive filters are arbitrarily combined (e.g., 1,2,3,...) to be placed in the free-space optical channel, a nonlinear and dynamic change of scaling factors can be obtained as shown in Fig. 3(b). Therefore, ciphertexts collected at the receiving end have high randomness and nonlinearity in the developed free-space optical data transmission system.

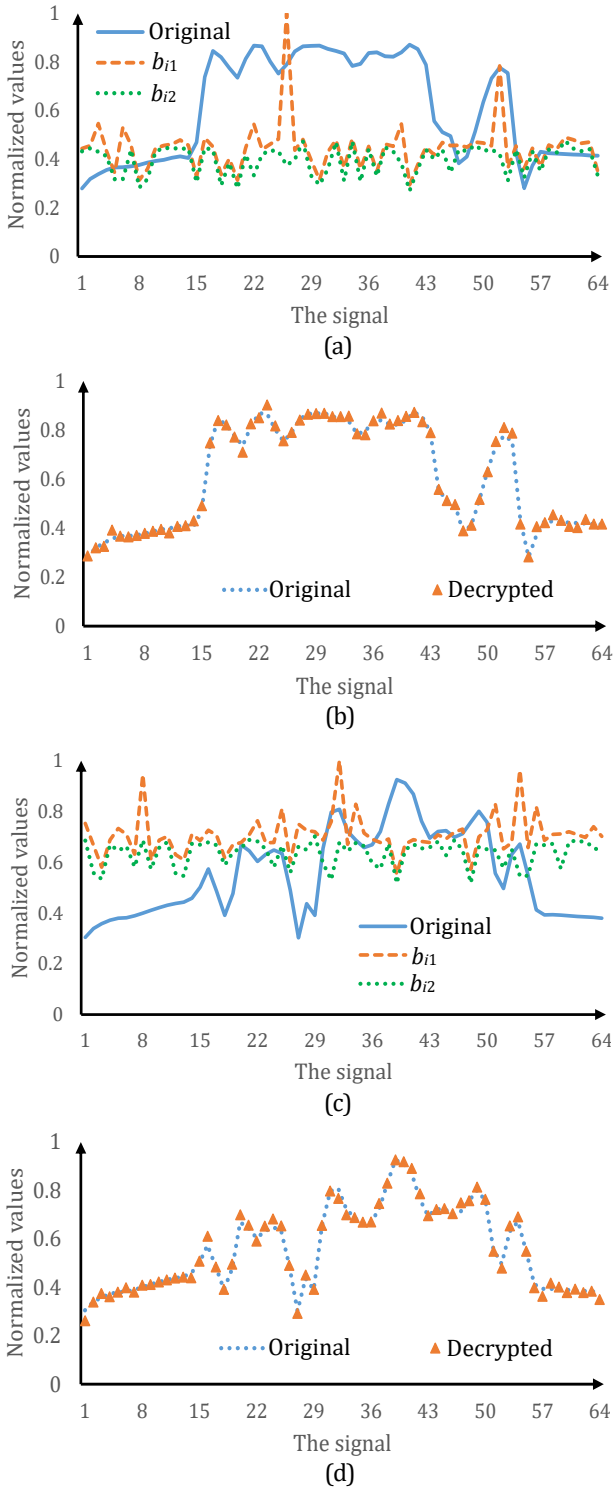

Fig. 4. (a) and (c) A comparison between original analog signal and the ciphertexts, and (b) and (d) the decrypted signals obtained when correct keys are used. MSE and PSNR values corresponding to b_{i1} and b_{i2} in (a) are 7.78×10^{-2}, 11.09 dB, 9.64×10^{-2} and 10.16 dB, respectively. MSE and PSNR values corresponding to b_{i1} and b_{i2} in (c) are 5.60×10^{-2}, 12.52 dB, 3.83×10^{-2} and 14.17 dB, respectively. MSE values corresponding to (b) and (d) are 2.14×10^{-4} and 2.83×10^{-4}, respectively. PSNR values corresponding to (b) and (d) are 36.71 dB and 35.48 dB, respectively.

Two irregular analog signals are experimentally tested as a typical example to show the proposed secured free-space optical transmission in dynamic and turbulent media. As shown in Figs. 4(a) and 4(c), original analog signals, i.e., plaintexts, are fully encrypted into random intensities at the receiving end. The analog signals can be precisely decrypted and obtained as shown in Figs. 4(b) and 4(d), when correct security keys are applied. Mean squared error (MSE) and peak signal-to-noise ratio (PSNR) are calculated to evaluate quality of the encrypted and decrypted signals, as given in Fig. 4.

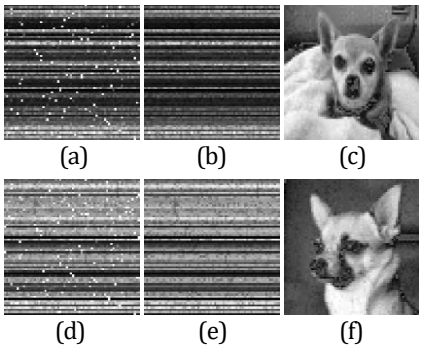

Fig. 5. (a) and (b) Ciphertexts (i.e., b_{i1} and b_{i2}) corresponding to a grayscale image experimentally encoded in the channel through dynamic and turbulent media, (d) and (e) ciphertexts (i.e., b_{i1} and b_{i2}) corresponding to another grayscale image experimentally encoded in the channel through dynamic and turbulent media, and (c) and (f) the decrypted images obtained when a series of correct keys are applied. MSE values corresponding to (a)–(f) are 0.15, 0.16, 4.05×10^{-4}, 0.10, 0.09 and 4.36×10^{-4}, respectively. PSNR values corresponding to (a)–(f) are 8.20 dB, 7.82 dB, 33.92 dB, 9.99 dB, 10.36 dB and 33.60 dB, respectively.

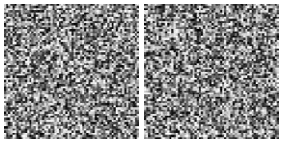

Fig. 6. (a) and (b) The decrypted images obtained when wrong security keys are used respectively corresponding to those in Figs. 5(c) and 5(f). MSE values corresponding to (a) and (b) are 1.33×10^{-2}, and 1.22×10^{-2}, respectively. PSNR values corresponding to (a) and (b) are 8.75 dB and 9.13 dB, respectively.

2D grayscale images are also tested, and are experimentally encrypted into random noise as shown in Figs. 5(a), 5(b), 5(d) and 5(e). When security keys are correctly applied, the retrieved images are shown in Figs. 5(c) and 5(f). It is demonstrated that the proposed method is feasible and effective to realize high-fidelity secured free-space optical data transmission through dynamic and turbulent media. Security of the proposed free-space optical transmission through dynamic and turbulent media is further analyzed. When security keys are wrong during the decryption, the plaintexts cannot be retrieved as shown in Figs. 6(a) and 6(b). Only noise-like images can be obtained. It is experimentally illustrated that the proposed method can realize high-security and high-fidelity free-space optical data transmission in dynamic and turbulent scattering environment. System security and the large key space are guaranteed to withstand the attacks [18], e.g., chosen-plaintext attacks, since a nonlinear and random mode is designed and applied here. Since different types of data (e.g., colour) can also be represented by analog or binary format, it is feasible to effectively apply the proposed method. It can be expected that the proposed scheme can be further used with other transmission methods in practice.

In conclusion, a new scheme has been proposed to realize high-fidelity secured free-space optical data transmission through dynamic and turbulent media by encoding information carriers. An encoding algorithm is designed to transform the data into a series of 2D patterns as information carriers. A novel differential method is developed to suppress noise, and a series of random security keys are also generated. The ciphertexts with high randomness are collected at the receiving end, when a different number of absorptive filters are arbitrarily applied in the free-space optical channel. Feasibility and effectiveness of the proposed method are fully verified by optical experiments. The proposed approach provides a promising way to realize high-fidelity secured optical data transmission over dynamic and turbulent media in a free-space optical channel.

Funding. Hong Kong Research Grants Council (C5011-19G, 15224921, 15223522); GuangDong Basic and Applied Basic Research Foundation (2022A1515011858); The Hong Kong Polytechnic University (1-W167, 1-W19E, 1-BD4Q).

Disclosures. The authors declare no conflicts of interest.

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.

REFERENCES

1. T. B. Pittman, Y. H. Shih, D. V. Strekalov, and A. V. Sergienko, Phys. Rev. A **52**, R3429 (1995).
2. P. Clemente, V. Durán, V. Torres-Company, E. Tajahuerce, and J. Lancis, Opt. Lett. **35**, 2391 (2010).
3. M. Tanha, R. Kheradmand, and S. Ahmadi-Kandjani, Appl. Phys. Lett. **101**, 101108 (2012).
4. P. Zheng, Q. Dai, Z. Li, Z. Ye, J. Xiong, H. C. Liu, G. Zheng, and S. Zhang, Sci. Adv. **7**, eabg0363 (2021).
5. Y. Cao, Y. Xiao, Z. Pan, L. Zhou, and W. Chen, Opt. Express **30**, 36464 (2022).
6. Z. Pan, Y. Xiao, Y. Cao, L. Zhou, and W. Chen, Opt. Express **30**, 43480 (2022).
7. C. Xue, N. Jiang, Y. Lv, G. Li, S. Lin, and K. Qiu, Opt. Lett. **41**, 3690 (2016).
8. A. Bouhous and K. Kemih, Opt. Laser Technol. **108**, 162 (2018).
9. F. Xu, M. Curty, B. Qi, and H. K. Lo, IEEE J. Sel. Top. Quantum Electron. **21**, 148 (2015).
10. N. Li, H. Susanto, B. Cemlyn, I. D. Henning, and M. J. Adams, Opt. Lett. **42**, 3494 (2017).
11. T. T. Hou, L. L. Yi, X. L. Yang, J. X. Ke, Y. Hu, Q. Yang, P. Zhou, and W. S. Hu, Opt. Express **24**, 23439 (2016).
12. E. Diamanti, H. K. Lo, B. Qi, and Z. Yuan, NPJ Quantum Inf. **2**, 1 (2016).
13. C. Xue, N. Jiang, Y. Lv, G. Li, S. Lin, and K. Qiu, Opt. Lett. **41**, 3690 (2016).
14. P. Réfrégier and B. Javidi, Opt. Lett. **20**, 767 (1995).
15. W. Chen, B. Javidi, and X. Chen, Adv. Opt. Photon. **6**, 120 (2014).
16. W. Chen, Light Sci. Appl. **11**, 11 (2022).
17. P. Lin, T. Wang, W. Ma, Q. Yang, and Z. Liu, Opt. Express **28**, 39216 (2020).
18. J. Feng, W. Huang, S. Jiao, and X. Wang, Opt. Express **29**, 43580 (2021).

FULL REFERENCES WITH TITLES

1. T. B. Pittman, Y. H. Shih, D. V. Strekalov, and A. V. Sergienko, "Optical imaging by means of two-photon quantum entanglement," Phys. Rev. A **52**(5), R3429–R3432 (1995).
2. P. Clemente, V. Durán, V. Torres-Company, E. Tajahuerce, and J. Lancis, "Optical encryption based on computational ghost imaging," Opt. Lett. **35**(14), 2391–2393 (2010).
3. 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).
4. P. Zheng, Q. Dai, Z. Li, Z. Ye, J. Xiong, H. C. Liu, G. Zheng, and S. Zhang, "Metasurface-based key for computational imaging encryption," Sci. Adv. **7**(21), eabg0363 (2021).
5. Y. Cao, Y. Xiao, Z. Pan, L. Zhou, and W. Chen, "High-fidelity temporally-corrected transmission through dynamic smoke via pixel-to-plane data encoding," Opt. Express **30**(20), 36464–36477 (2022).
6. Z. Pan, Y. Xiao, Y. Cao, L. Zhou, and W. Chen, "Optical data transmission through highly dynamic and turbid water using dynamic scaling factors and single-pixel detector," Opt. Express **30**(24), 43480–43490 (2022).
7. C. Xue, N. Jiang, Y. Lv, G. Li, S. Lin, and K. Qiu, "Security-enhanced chaos communication with time-delay signature suppression and phase encryption," Opt. Lett. **41**(16), 3690–3693 (2016).
8. A. Bouhous and K. Kemih, "Novel encryption method based on optical time-delay chaotic system and a wavelet for data transmission," Opt. Laser Technol. **108**, 162–169 (2018).
9. F. Xu, M. Curty, B. Qi, and H. K. Lo, "Measurement-device-independent quantum cryptography," IEEE J. Sel. Top. Quantum Electron. **21**(3), 148–158 (2015).
10. N. Li, H. Susanto, B. Cemlyn, I. D. Henning, and M. J. Adams, "Secure communication systems based on chaos in optically pumped spin-VCSELs," Opt. Lett. **42**(17), 3494–3497 (2017).
11. T. T. Hou, L. L. Yi, X. L. Yang, J. X. Ke, Y. Hu, Q. Yang, P. Zhou, and W. S. Hu, "Maximizing the security of chaotic optical communications," Opt. Express **24**(20), 23439–23449 (2016).
12. E. Diamanti, H. K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," NPJ Quantum Inf. **2**(1), 1–12 (2016).
13. C. Xue, N. Jiang, Y. Lv, G. Li, S. Lin, and K. Qiu, "Security-enhanced chaos communication with time-delay signature suppression and phase encryption," Opt. Lett. **41**(16), 3690–3693 (2016).
14. P. Réfrégier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**(7), 767–769 (1995).
15. W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," Adv. Opt. Photon. **6**(2), 120–155 (2014).
16. W. Chen, "Spatial nonlinear optics for securing information," Light Sci. Appl. **11**, 11 (2022).
17. P. Lin, T. Wang, W. Ma, Q. Yang, and Z. Liu, "Transmission characteristics of 1.55 and 2.04 μm laser carriers in a simulated smoke channel based on an actively mode-locked fiber laser," Opt. Express **28**(26), 39216–39226 (2020).
18. J. Feng, W. Huang, S. Jiao, and X. Wang, "Generalized forgery attack to optical encryption systems," Opt. Express **29**, 43580–43597 (2021).