Research Article Vol. 30, No. 5 / 28 Feb 2022 / Optics Express 8186
Optics EXPRESS

Physically-secured high-fidelity free-space optical data transmission through scattering media using dynamic scaling factors

YIN XIAO, LINA ZHOU, ZILAN PAN, YONGGUI CAO, AND WEN CHEN*

Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong, China
*owen.chen@polyu.edu.hk

Abstract: In this paper, we propose a method of physically-secured high-fidelity free-space optical data transmission through scattering media using physically- and dynamically-generated scaling factors. Optical channel characteristics are explored, and scaling factors are physically and dynamically generated to serve as security keys in the developed free-space optical data transmission system. The generated dynamic scaling factors provide a security layer for free-space optical data transmission. To the best of our knowledge, it is the first time to physically and dynamically generate scaling factors in free-space optical data transmission system to realize data encryption. The scaling factors existing in free-space optical data transmission channel are physically and dynamically controlled by using two optical devices, i.e., variable beam attenuator (VBA) and amplitude-only spatial light modulator (SLM). Nonlinear and dynamic variation of scaling factors is realized in different free-space wave propagation environments. It is experimentally demonstrated that high security can be guaranteed in the developed physically-secured high-fidelity free-space optical data transmission system, since one random scaling factor is physically and dynamically generated for the transmission of each signal pixel value. In addition, the proposed physically-secured free-space optical data transmission scheme is robust to noise and scattering, and high-fidelity signals are retrieved at the receiving end. The proposed method could open up a new research perspective for the secured free-space optical data transmission.

1. Introduction

Free-space optical communication has attracted much attention, since it offers remarkable advantages (e.g., low power consumption, high transmission capacity and being free from electromagnetic interference [1–5]) in many applications. However, it has been found that there are some significant challenges in free-space optical data transmission. One of the challenges is low-fidelity optical data transmission through scattering media. When optical wave propagates through scattering media, it is always difficult to describe wave propagation process [6–8] and information loss could be unavoidable [9,10]. In addition, noise existing in free-space optical data transmission channel has severe effect on the quality of the retrieved signals at the receiving end, which is also a significant challenge to be overcome.

Recently, it has been studied that each signal pixel value to be transmitted can be transformed into 2D amplitude-only patterns [11–13]. Then, the generated 2D amplitude-only patterns serving as optical information carriers are illuminated to propagate through scattering media, and high-fidelity signals can be retrieved at the receiving end. However, data security in free-space optical transmission has not been investigated. The most commonly-used security measure is to apply an encryption algorithm to encode data before optical transmission. However, putting security on top of an unsecure optical channel is not a sensible decision [14]. Quantum optical theory

#448943 https://doi.org/10.1364/OE.448943
Journal © 2022 Received 17 Nov 2021; revised 15 Jan 2022; accepted 17 Jan 2022; published 25 Feb 2022

Optics EXPRESS

provides an absolutely secure communication method [15] for data transmission. However, the required quantum entanglement state is difficult to achieve in free-space optical communication. Chaotic optical communication could provide a high level of privacy in data transmission by encoding data into chaotic optical carriers [16–18]. However, it is required to establish chaotic synchronization, and parameters of the receiver should match those of the transmitter. This is difficult to achieve in practice [19]. Secured free-space communication using polarization multiplexing has also been reported [20]. The polarization and modal multiplexing used to encode data are essentially based on diffractive optics [21–25] which could be strongly affected by interference effect, and the data transmission system could become unstable during light-matter interactions. A striking technique called physical layer security has also been demonstrated, which possesses several remarkable advantages, e.g., unbreakable, provable, and quantifiable secrecy [26,27]. In free-space optical transmission channel, scaling factors physically exist between the transmitter and the receiver. However, the previous studies do not explore optical channel characteristics, i.e., scaling factors, for securing free-space optical data transmission. It is highly desirable to investigate the property of dynamic scaling factors in order to realize physically-secured free-space optical data transmission through scattering media.

In this paper, we propose physically-secured high-fidelity free-space optical data transmission through scattering media using physically- and dynamically-generated scaling factors. Free-space optical channel characteristics, i.e., scaling factors, are explored. The scaling factors existing in optical channel are physically and dynamically generated to serve as security keys for free-space optical data transmission. The generated dynamic scaling factors provide a security layer for the developed free-space optical data transmission system. To the best of our knowledge, it is the first time to physically- and dynamically-generate scaling factors in free-space optical data transmission to realize data encryption. The scaling factors are physically and dynamically controlled by using two optical devices, i.e., variable beam attenuator (VBA) and amplitude-only spatial light modulator (SLM). The VBA is used to adjust optical intensity of light source via a control of its angle values, and various modulation patterns can be arbitrarily designed to be embedded into the SLM. The VBA and SLM are used to create dynamic conditions at the transmitter in the developed free-space optical data transmission system. Nonlinear and dynamic variation of scaling factors is realized in different free-space wave propagation environments. It is experimentally demonstrated that high security can be guaranteed for the developed physically-secured free-space optical data transmission system, since one random scaling factor is physically and dynamically generated for the transmission of each signal pixel value. In addition, the proposed physically-secured free-space optical data transmission scheme is robust to noise and scattering, and high-fidelity signals can be retrieved at the receiving end. Compared to previous studies, the proposed physically-secured high-fidelity free-space optical data transmission scheme has significant advantages as follows: 1) Security keys, i.e., scaling factors, are physically and dynamically controlled at the transmitter for the first time. 2) Nonlinear and dynamic variation of scaling factors is realized which can fully guarantee the security of the developed free-space optical data transmission system. 3) The proposed physically-secured free-space optical data transmission scheme is also able to retrieve high-fidelity signals at the receiving end, and is robust against noise and scattering.

The remainder of this paper is organized as follows. Section 2 describes principle of the proposed method and an experimental setup of the proposed physically-secured high-fidelity free-space optical data transmission scheme. In Section 3, experimental results are presented and discussed to illustrate feasibility and effectiveness of the proposed method in two different wave propagation environments, i.e., free space without scattering media and free space with a scattering medium. A conclusion is drawn in Section 4.

Optics EXPRESS

2. Principle

Principle of the proposed physically-secured high-fidelity free-space optical data transmission scheme is shown in Figs. 1 and 2. A laser modulated by a VBA illuminates the first SLM (SLM_1) which sequentially displays a series of 2D signal patterns. Here, the 2D signal patterns are generated by using the following procedure to encode the transmitted signal: (i) apply Fourier transform to an initialized random pattern to get its Fourier spectrum; (ii) use one pixel value of the transmitted signal to replace zero-frequency component of the generated Fourier spectrum in Step (i) and then a new Fourier spectrum is obtained; (iii) apply inverse Fourier transform to the new Fourier spectrum in order to generate a 2D signal pattern corresponding to that pixel value of the transmitted signal in Step (ii). Therefore, all signal pixels can be sequentially encoded into 2D signal patterns, and point-to-plane transformation is realized. The generated 2D signal patterns, i.e., a series of 2D random amplitude-only patterns, serve as optical information carriers, and a differential protocol [11–13] is applied to suppress noise for the retrieval of high-fidelity signals at the receiving end. Subsequently, optical wave is further modulated by another SLM (SLM_2) which sequentially displays modulation patterns. Without power adjustment of the light source and the modulation patterns, single-pixel detection in conventional methods can be described by

$$\mathrm{B} = k \sum \mathrm{S}, \tag{1}$$

where B denotes an intensity value collected by a single-pixel detector, k denotes a scaling factor, and S denotes a 2D signal pattern embedded into the SLM_1. As can be seen in Eq. (1), each collected single-pixel intensity value B is proportional to a transmitted signal pixel value. This scaling factor is considered as a constant in previous studies, and has no any effect on signal retrieval at the receiving end. In the proposed method, by the adjustment of intensity of light source and the usage of modulation patterns at the transmitter, it is feasible to physically and dynamically control scaling factors in free-space optical data transmission. When different combinations (i.e., different intensities of light source and different modulation patterns) are used, a series of dynamic scaling factors are randomly generated as security keys in optical data transmission channel.

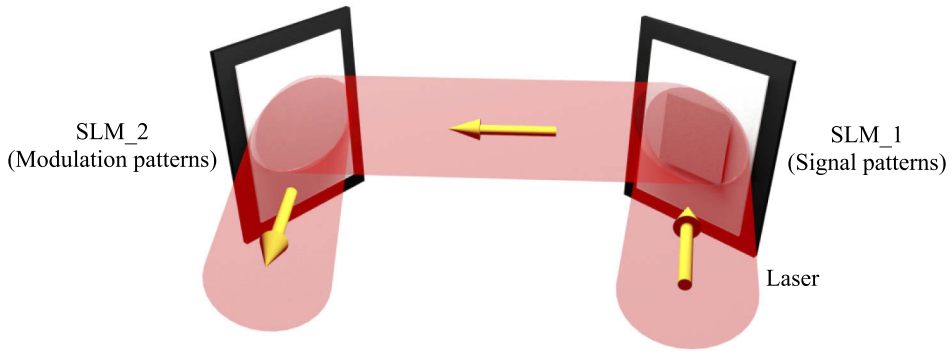

Fig. 1. Principle of the proposed physically-secured free-space optical data transmission scheme.

In the developed free-space optical data transmission system, after a series of single-pixel intensity values are collected by the single-pixel detector, signal retrieval at the receiving end can be conducted by using a normalization operation. However, it is impossible to further retrieve correct signal information without knowledge of the physically- and dynamically-generated scaling factors. A series of optical experiments are conducted to verify feasibility and effectiveness of the proposed physically-secured high-fidelity free-space optical data transmission scheme.

Optics EXPRESS

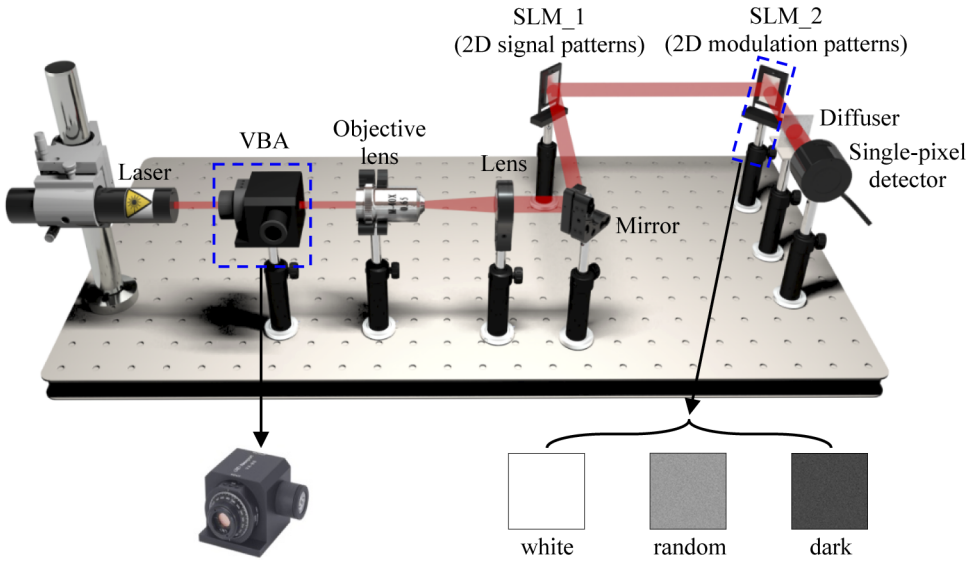

Fig. 2. A schematic experimental setup for the proposed physically-secured high-fidelity free-space optical data transmission through scattering media. Here, a diffuser (Thorlabs, DG10-1500) is used as the scattering medium. VBA: Variable beam attenuator.

A schematic experimental setup is shown in Fig. 2. A He-Ne laser with power of 17.0 mW and wavelength of 633.0 nm propagates through a VBA (Newport, VA-CB-633-CONEX). The VBA is used to adjust intensity of light source. Then, the laser is expanded by an objective lens and collimated by a lens with a focal length of 100.0 mm. The collimated laser illuminates amplitude-only SLM_1 (Holoeye, LC-R720) with pixel size of 20.0 μm. A series of 2D signal patterns with 512×512 pixels are sequentially embedded into the SLM_1, and amplitude-only SLM_2 (Holoeye, LC-R720) displays modulation patterns. At the receiving end, a single-pixel (bucket) detector (Newport, 918D-UV-OD3R) is used to record single-pixel intensity values.

The VBA placed in the optical setup provides power adjustment of the laser via a control of its angle values. The rotation angle can be automatically controlled with a precision of 0.1 degree. The SLM_2 displays 2D modulation patterns to be used to further modulate the propagating wave. The 2D modulation patterns can be arbitrarily designed and applied, and there is no need to align these modulation patterns with the generated 2D signal patterns displayed by the SLM_1. Here, three different 2D modulation patterns are used as a typical example to verify the proposed method, i.e., white pattern, random pattern and dark pattern, as shown in Fig. 2. The size of modulation patterns is 1280×768 pixels. In the white pattern, the value of all its elements is 1. In the random pattern, all its elements are distributed randomly in a range from 0 to 1. In the dark pattern, most of its elements have small positive values, i.e., close to 0. Other 2D modulation patterns can also be designed and applied to modulate the optical wave. By using the VBA and the SLM_2, flexibly generating dynamic scaling factors as security keys can be easily realized in the developed physically-secured high-fidelity free-space optical data transmission system.

In the proposed physically-secured high-fidelity free-space optical data transmission scheme, before optical signal transmission, a calibration about security keys (i.e., scaling factors) can be conducted in optical transmission channel. A 2D signal pattern corresponding to a known value (i.e., to be transmitted) is generated and embedded into the SLM_1, and remains unchanged. Then, by applying different combinations (i.e., different intensities of light source and different modulation patterns displayed by the SLM_2), a series of single-pixel intensity values are correspondingly collected by single-pixel detector. The ratio between the series of collected

Optics EXPRESS

single-pixel intensity values and the known value is sequentially calculated to obtain security keys as a lookup table. Since the VBA angle adjustment step can be set to be small and various modulation patterns can be arbitrarily applied, there are a large number of combinations which fully guarantee the key space.

3. Experimental results and discussion

3.1. Free space without scattering media

In Fig. 2, angle of the VBA is tuned dynamically from 4 to 28 degrees in optical experiments for free-space optical data transmission without scattering media. When the modulation pattern embedded into the SLM_2 remains unchanged, sequentially adjusting the angle of VBA could lead to a nearly linear variation of scaling factors, as shown in Fig. 3(a). When the VBA angle is randomly adjusted rather than just in a sequence, the variance of scaling factors could become nonlinear. When intensity of light source and the modulation pattern embedded into the SLM_2 are dynamically adjusted at the same time, nonlinear variation of scaling factors can be easily realized as shown in Fig. 3(b). It is demonstrated that nonlinear and dynamic variation of scaling factors can be easily realized by simultaneously applying the VBA and the modulation patterns.

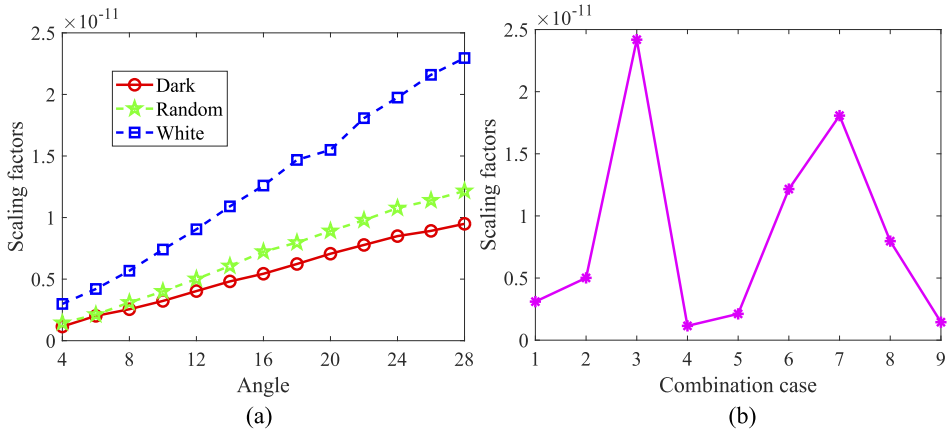

Fig. 3. Experimental results obtained in free-space optical data transmission without scattering media: (a) linear variation of scaling factors by just sequentially adjusting the angle of VBA, and (b) nonlinear variation of scaling factors. Combination case means that arbitrarily adjusting the VBA and the modulation patterns has been conducted at the same time.

Experimental results in Figs. 3(a) and 3(b) demonstrate that simultaneously adjusting intensities of the light source and the modulation patterns can easily make the variation of scaling factors nonlinear and dynamic, and security keys for free-space optical data transmission are correspondingly generated.

Since scaling factors are physically and dynamically controlled at the transmitter, the proposed method can be applied for optically securing the transmitted data. Figure 4 shows that the physically- and dynamically-generated scaling factors can be used to encode one signal pixel value (i.e., 0.4615) into different and random values. After a 2D signal pattern corresponding to the signal pixel value to be transmitted is generated and embedded into the SLM_1, the recorded intensity values can be random and dynamic by simultaneously adjusting the VBA and the 2D modulation patterns. The experimental results in Fig. 4 demonstrate that each signal pixel value to be transmitted can be fully encoded by dynamically generating scaling factors in free-space optical data transmission channel, and a random value can be correspondingly retrieved at the

Optics EXPRESS

receiving end. Therefore, it is impossible to obtain correct information of the transmitted signal without further knowledge of the physically- and dynamically-generated scaling factors (i.e., security keys). The proposed method can fully guarantee the security of free-space optical data transmission, since one random scaling factor is physically and dynamically generated for the transmission of each signal pixel value.

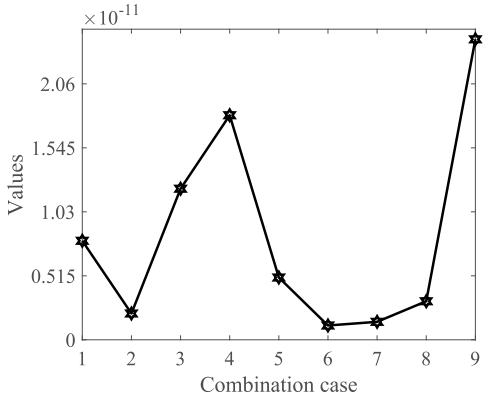

Fig. 4. One signal pixel value (i.e., 0.4615) experimentally encoded into any random values in free-space optical data transmission without scattering media as a typical example to verify the proposed method. Combination case means that simultaneously adjusting the VBA and the modulation patterns has been conducted.

Based on experimental verifications in Figs. 3 and 4, it is straightforward to conduct physically-secured optical data transmission in free space without scattering media. Here, three 1D signals are transmitted in free space without scattering media, and for simplicity each signal with 6 pixels is tested and presented. As shown in Figs. 5(a), 5(c) and 5(e), original signal is fully encoded, and the encrypted signals obtained at the receiving end cannot directly render originally transmitted information. When security keys (i.e., dynamic scaling factors) are correctly applied, the decoded signals are further obtained which overlap with original signals as shown in Figs. 5(b), 5(d) and 5(f). To quantitatively evaluate experimental results, signal-to-noise ratio (SNR) and mean squared error (MSE) are calculated. In Figs. 5(a) and 5(b), SNR values for the encrypted signal and the decoded signal are 2.18 dB and 30.36 dB, respectively. The MSE values are 0.33 and 4.98×10^{-4}, respectively. In Figs. 5(c) and 5(d), SNR values are 0.20 dB and 34.26 dB, respectively. The MSE values are 0.40 and 1.59×10^{-4}, respectively. In Figs. 5(e) and 5(f), SNR values are 1.59 dB and 34.27 dB, respectively. The MSE values are 0.40 and 2.17×10^{-4}, respectively. Table 1 shows SNR and MSE values of the encrypted signals and decoded signals in Fig. 5. The signals to be transmitted are effectively encrypted by the physically- and dynamically-generated scaling factors, and the decoded signals are of high quality when correct security keys are further used. Experimental results in Figs. 5(a)–5(f) demonstrate that the proposed physically-secured high-fidelity optical data transmission in free space without scattering media is valid.

3.2. *Free space with scattering media*

Optical experiments are also conducted to verify the proposed physically-secured high-fidelity free-space optical data transmission through scattering media. In free space through scattering media (i.e., a diffuser, Thorlabs DG10-1500), angle of the VBA is tuned dynamically from 10 to 34 degrees. When a modulation pattern embedded in the SLM_2 remains unchanged, sequentially adjusting the angle of VBA could lead to a nearly linear variation of scaling factors, as shown in Fig. 6(a). When the VBA angle is randomly adjusted rather than just in a sequence, the variance of scaling factors could become nonlinear. When intensity of the light source and

Optics EXPRESS

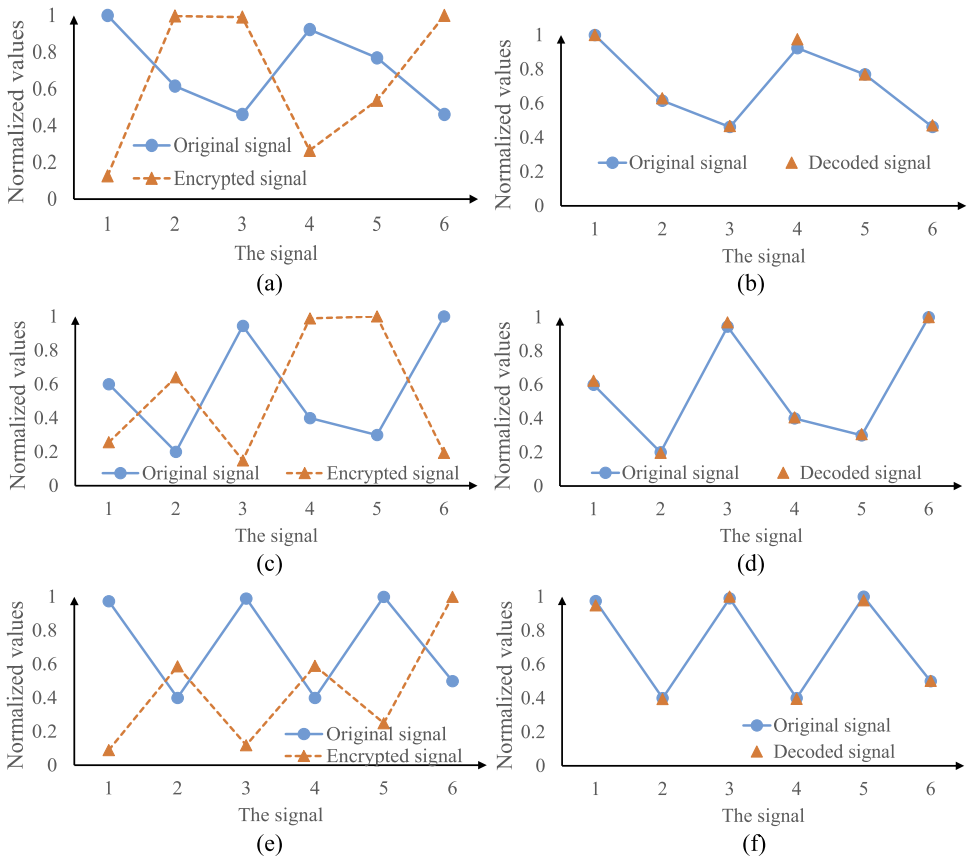

Fig. 5. Experimental results obtained in free-space optical data transmission without scattering media: (a), (c) and (e) comparisons between the encrypted signal and original signal, and (b), (d) and (f) comparisons between the decoded signal and original signal.

Table 1. SNR and MSE values of the encrypted signals and decoded signals

Signal	SNR (dB)	MSE
The encrypted signal in Fig. 5(a)	2.18	0.33
The decoded signal in Fig. 5(b)	30.36	4.98×10^{-4}
The encrypted signal in Fig. 5(c)	0.20	0.40
The decoded signal in Fig. 5(d)	34.26	1.59×10^{-4}
The encrypted signal in Fig. 5(e)	1.59	0.40
The decoded signal in Fig. 5(f)	34.27	2.17×10^{-4}

the 2D modulation patterns are dynamically adjusted at the same time, nonlinear and dynamic variation of scaling factors can be easily realized as shown in Fig. 6(b).

Experimental results in Figs. 6(a) and 6(b) demonstrate that simultaneously adjusting intensities of the light source and the modulation patterns can easily make the variation of scaling factors nonlinear and dynamic in free-space optical transmission through scattering media. Figure 7 shows the experimental result, when physically- and dynamically-generated scaling factors are used to encode one signal pixel value (i.e., 0.5508) into different and random values. Therefore, it is impossible to retrieve correct signal without further knowledge of the physically- and

Optics EXPRESS

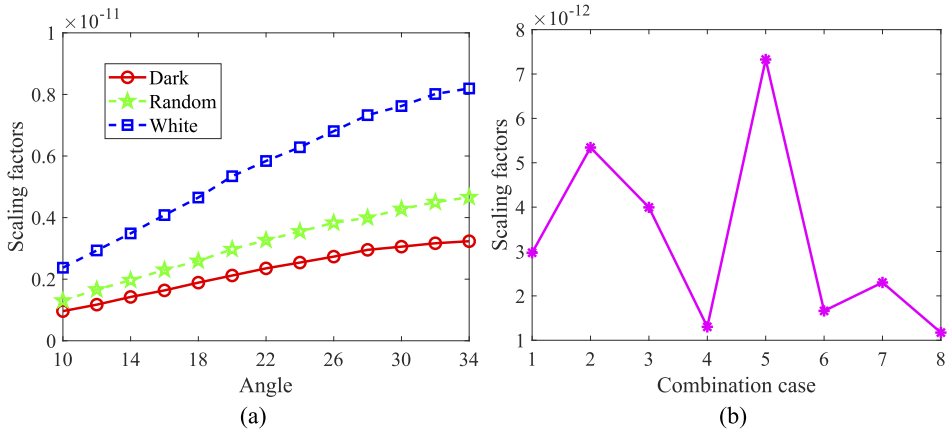

Fig. 6. Experimental results obtained in free-space optical data transmission through scattering media: (a) linear variation of scaling factors by just sequentially adjusting the angle of VBA, and (b) nonlinear variation of scaling factors. Combination case means that simultaneously adjusting the VBA and the modulation patterns has been conducted.

dynamically-generated scaling factors (i.e., security keys) at the receiving end. Since one random scaling factor is physically and dynamically generated for the transmission of each signal pixel value, the security of free-space optical transmission system is fully guaranteed.

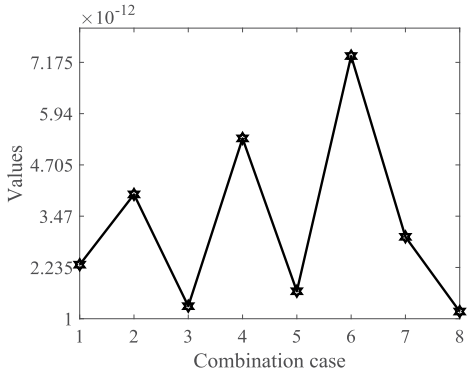

Fig. 7. One signal pixel value (i.e., 0.5508) experimentally encoded into any different and random values in free-space optical data transmission through scattering media as a typical example to verify the proposed method. Combination case means that simultaneously adjusting the VBA and the modulation patterns has been conducted.

Here, three 1D signals are tested and transmitted in free space through scattering media, and for simplicity each signal with 6 pixels is tested. It is demonstrated in Figs. 8(a), 8(c) and 8(e) that original signal can be fully encoded into random values, and the encrypted signals obtained at the receiving end cannot render originally transmitted information. When dynamic scaling factors are correctly applied, the decoded signals are further obtained which overlap with original signals as shown in Figs. 8(b), 8(d) and 8(f). Quantitative evaluation of the encrypted signals and decoded signals is also conducted. In Figs. 8(a) and 8(b), SNR values for the encrypted signal and the decoded signal are 7.41 dB and 28.93 dB, respectively. The MSE values are 0.11 and 7.54×10^{-4}, respectively. In Figs. 8(c) and 8(d), SNR values for the encrypted signal and the decoded signal are 4.00 dB and 28.36 dB, respectively. The MSE values are 0.18 and 6.67×10^{-4},

Optics EXPRESS

respectively. In Figs. 8(e) and 8(f), SNR values for the encrypted signal and the decoded signal are 5.99 dB and 32.80 dB, respectively. The MSE values are 0.18 and 3.71×10^{-4}, respectively. The SNR and MSE values of the encrypted signals and decoded signals in Fig. 8 are further listed in Table 2. The signals to be transmitted are encrypted in free space through scattering media by the physically- and dynamically-generated scaling factors, and the decoded signals obtained by using correct security keys are of high quality. Based on the experimental results in Figs. 5 and 8, it is demonstrated that the proposed method is robust against scattering, and scattering media show no impact on the performance of the proposed method.

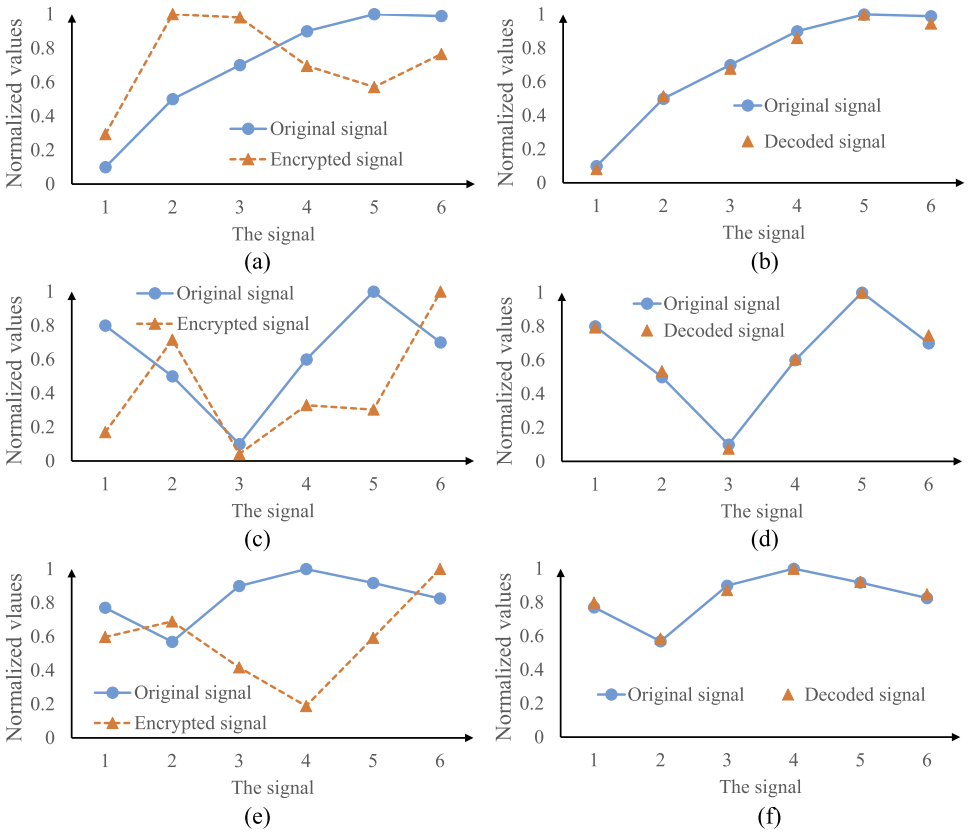

Fig. 8. Experimental results obtained in free-space optical data transmission through scattering media: (a), (c) and (e) comparisons between the encrypted signal and original signal, and (b), (d) and (f) comparisons between the decoded signal and original signal.

Table 2. SNR and MSE values for the encrypted signals and decoded signals

Signal	SNR (dB)	MSE
The encrypted signal in Fig. 8(a)	7.41	0.11
The decoded signal in Fig. 8(b)	28.93	7.54×10^{-4}
The encrypted signal in Fig. 8(c)	4.00	0.18
The decoded signal in Fig. 8(d)	28.36	6.67×10^{-4}
The encrypted signal in Fig. 8(e)	5.99	0.18
The decoded signal in Fig. 8(f)	32.80	3.71×10^{-4}

Optics EXPRESS

To fully illustrate the proposed method, signals with more pixels are further tested. Here, two irregular signals are used for verifying the proposed physically-secured high-fidelity optical data transmission through scattering media, and each signal has 64 pixels. Experimental results are shown in Figs. 9(a)–9(d). As can be seen in Figs. 9(a) and 9(c), since optical encryption is integrated into free-space optical data transmission, the encrypted signals retrieved at the receiving end are totally different from original signals. When correct keys (i.e., dynamic scaling factors) are further used for the decoding, high-quality decoded signals are obtained which overlap with original signals as shown in Figs. 9(b) and 9(d). In Figs. 9(a) and 9(b), SNR values for the encrypted signal and the decoded signal are 3.05 dB and 33.41 dB, respectively. The MSE values are 0.20 and 1.84×10^{-4}, respectively. In Figs. 9(c) and 9(d), SNR values for the encrypted signal and the decoded signal are 4.66 dB and 34.44 dB, respectively. The MSE values are 0.11 and 1.12×10^{-4}, respectively. Experimental results in Figs. 9(a)–9(d) demonstrate that the proposed physically-secured high-fidelity free-space optical data transmission through scattering media is feasible and effective.

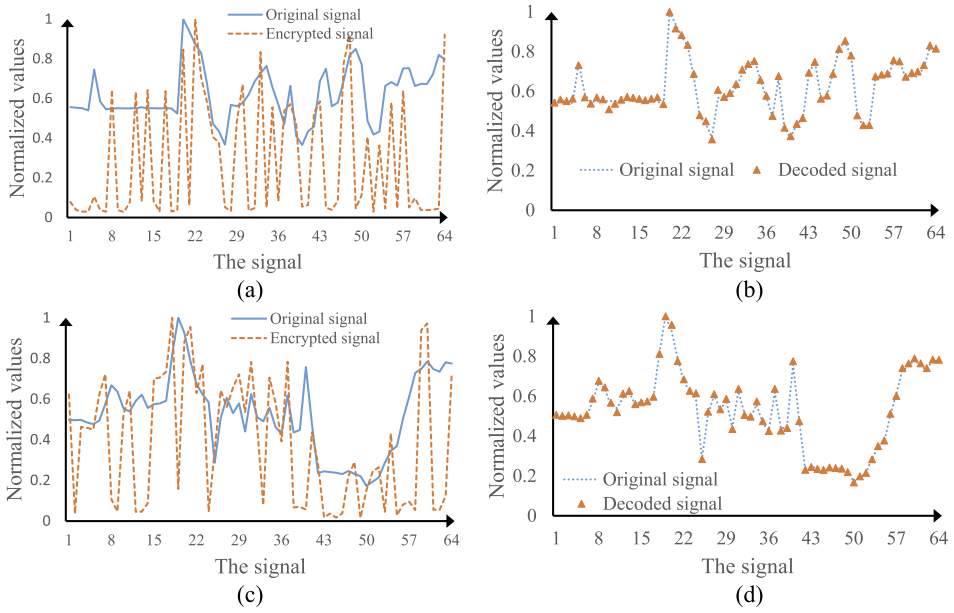

Fig. 9. Experimental results obtained in free-space optical data transmission through scattering media: (a) the encrypted signal retrieved at the receiving end and (b) a decoded signal; (c) the encrypted signal retrieved at the receiving end and (d) a decoded signal. (a) and (b): one signal; (c) and (d): another signal.

To enhance optical encryption efficiency for free-space optical data transmission, a group modulation strategy is further developed. One physically-generated scaling factor can be used to modulate a group of signal pixels, e.g., 4 pixels. Experimental results are shown in Figs. 10(a)–10(d). In Figs. 10(a) and 10(b), successive 4 pixels are considered as one group where the same security key, i.e., a scaling factor, is employed. The encrypted signal retrieved at the receiving end, as shown in Fig. 10(a), is different from original signal. When correct security keys are applied for the decoding, a decoded signal in Fig. 10(b) overlaps with original signal. In Figs. 10(a) and 10(b), SNR values for the encrypted signal and the decoded signal are 3.33 dB and 32.39 dB, respectively. The MSE values are 0.14 and 1.79×10^{-4}, respectively. In Figs. 10(c) and 10(d), successive 8 pixels are considered as a group where the same security key, i.e., a scaling factor, is employed. The SNR values for the encrypted signal in Fig. 10(c) and the decoded signal

Optics EXPRESS

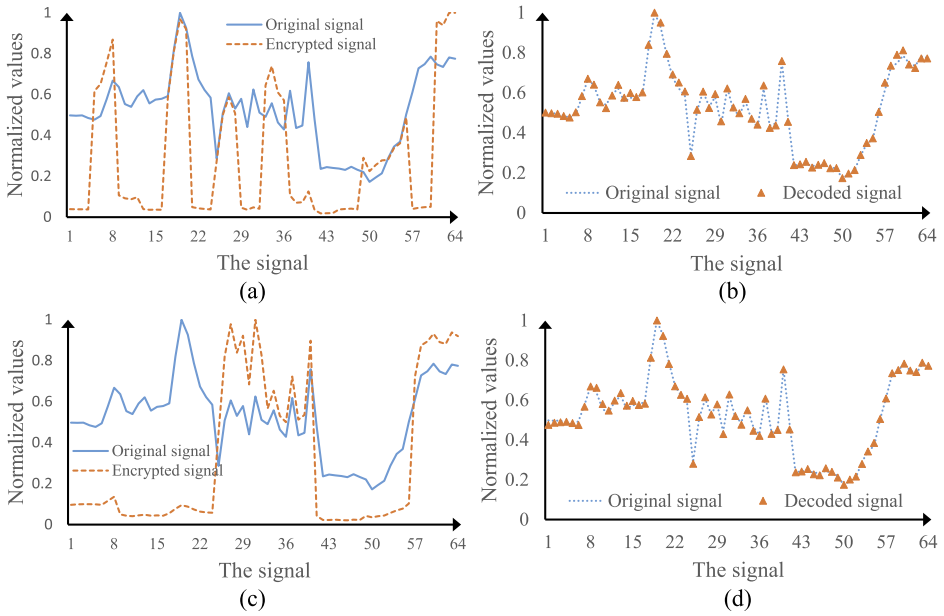

Fig. 10. Experimental results obtained when a group modulation strategy is used: (a) the encrypted signal retrieved at the receiving end and (b) a decoded signal when successive 4 pixels are considered as a group; (c) the encrypted signal retrieved at the receiving end and (d) a decoded signal when successive 8 pixels are considered as a group.

in Fig. 10(d) are 3.17 dB and 34.29 dB, respectively. The MSE values in Figs. 10(c) and 10(d) are 0.15 and 1.15×10^{-4}, respectively. Experimental results in Figs. 10(a)–10(d) demonstrate that the developed group modulation strategy can enhance optical encryption efficiency of the proposed physically-secured high-fidelity free-space optical data transmission scheme. However, each group should not contain many pixels (e.g., 8 pixels compared to the total 64 pixels in the transmitted signal), since there could be a risk of information leakage.

To further illustrate the proposed method, another optical experiment is conducted to verify the proposed physically-secured high-fidelity free-space optical data transmission through two cascaded diffusers (Thorlabs, DG10-1500). Typical experimental results are shown in Figs. 11(a) and 11(b). In Figs. 11(a) and 11(b), SNR values for the encrypted signal and the decoded signal

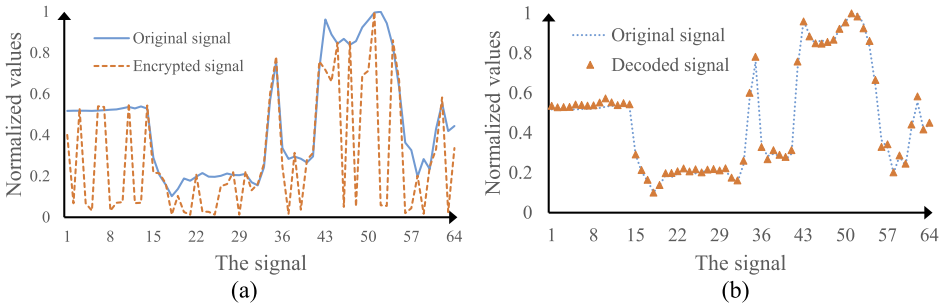

Fig. 11. Experimental results obtained in the proposed free-space optical data transmission through two cascaded diffusers: (a) the encrypted signal retrieved at the receiving end, and (b) a decoded signal.

Optics EXPRESS

are 4.98 dB and 30.03 dB, respectively. The MSE values are 0.09 and 2.82×10^{-4}, respectively. Experimental results in Figs. 11(a) and 11(b) demonstrate that the proposed physically-secured high-fidelity free-space optical data transmission through two cascaded diffusers is also feasible and effective.

4. Conclusion

We have proposed physically-secured high-fidelity free-space optical data transmission through scattering media using physically- and dynamically-generated scaling factors. Channel characteristics in free-space optical data transmission have been explored. Nonlinear and dynamic variation of scaling factors has been realized by using a VBA and an amplitude-only SLM. It is experimentally demonstrated that the dynamically- and physically-generated scaling factors can serve as security keys in the free-space optical data transmission system, and physical layer security has been successfully integrated. The proposed method has been experimentally verified to be feasible and effective. High security is achieved in free-space optical data transmission through scattering media, since one random scaling factor is physically and dynamically generated for the transmission of each signal pixel value. The proposed physically-secured high-fidelity optical data transmission scheme could open up a new research perspective for free-space optical communication.

Funding. Hong Kong Research Grants Council (15224921, C5011-19G); The Hong Kong Polytechnic University (1-W167, 1-W19E, 4-R006, G-R006).

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. M. A. Esmail, A. Ragheb, H. Fathallah, and M. S. Alouini, "Investigation and demonstration of high speed full-optical hybrid FSO/fiber communication system under light sand storm condition," IEEE Photonics J. **9**(1), 1–12 (2017).
2. H. H. Lu, C. Y. Li, C. M. Ho, M. T. Cheng, X. Y. Lin, Z. Y. Yang, and H. W. Chen, "64 Gb/s PAM4 VCSEL-based FSO link," Opt. Express **25**(5), 5749–5757 (2017).
3. C. W. Liu, S. Q. Zhai, J. C. Zhang, Y. H. Zhou, Z. W. Jia, F. Q. Liu, and Z. G. Wang, "Free-space communication based on quantum cascade laser," J. Semicond. **36**(9), 094009 (2015).
4. L. C. Andrews, R. L. Phillips, and C. Y. Hopen, *Laser Beam Scintillation with Applications* (SPIE, 2001), Chap. 7.
5. A. K. Majumder and J. C. Ricklin, *Free-Space Laser Communications: Principles and Advances* (Springer, 2008), Chap.1.
6. X. D. Chen, *Computational Methods for Electromagnetic Inverse Scattering* (Wiley-IEEE, 2018).
7. P. Peng, *Introduction to Wave Scattering, Localization and Mesocopic Phenomena* (Academic, 1995).
8. D. S. Wiersma, "Disordered photonics," Nat. Photonics **7**(3), 188–196 (2013).
9. J. W. Goodman, "Some fundamental properties of speckle," J. Opt. Soc. Am. **66**(11), 1145–1150 (1976).
10. C. W. J. Beenakker, "Random-matrix theory of quantum transport," Rev. Mod. Phys. **69**(3), 731–808 (1997).
11. Y. Xiao, L. Zhou, and W. Chen, "High-fidelity ghost diffraction and transmission in free space through scattering media," Appl. Phys. Lett. **118**(10), 104001 (2021).
12. Y. Xiao and W. Chen, "High-fidelity optical transmission around the corner," IEEE Photon. Technol. Lett. **33**(1), 3–6 (2021).
13. Y. Xiao, L. Zhou, and W. Chen, "Wavefront control through multi-layer scattering media using single-pixel detector for high-PSNR optical transmission," Opt. Lasers Eng. **139**, 106453 (2021).
14. M. P. Fok, Z. X. Wang, Y. H. Deng, and P. R. Prucnal, "Optical layer security in fiber-optic networks," IEEE Trans. Inf. Foren. Sec. **6**(3), 725–736 (2011).
15. H. G. Song and C. B. Xie, "Analysis and discussion on practical quantum communication," China Basic Science **13**(3), 21–25 (2011).
16. A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. García-Ojalvo, C. R. Mirasso, L. Pesquera, and K. A. Shore, "Chaos-based communications at high bit rates using commercial fibre-optic links," Nature **438**(7066), 343–346 (2005).
17. A. Argyris, E. Grivas, M. Hamacher, A. Bogris, and D. Syvridis, "Chaos-on-a-chip secures data transmission in optical fiber links," Opt. Express **18**(5), 5188–5198 (2010).
18. Q. C. Zhao and H. X. Yin, "Performance analysis of dense wavelength division multiplexing secure communications with multiple chaotic optical channels," Opt. Commun. **285**(5), 693–698 (2012).

Optics EXPRESS

19. Q. Huang, D. Liu, Y. Chen, Y. Wang, J. Tan, W. Chen, J. Liu, and N. Zhu, "Secure free-space optical communication system based on data fragmentation multipath transmission technology," Opt. Express **26**(10), 13536–13542 (2018).
20. C. H. Yeh, Y. J. Chang, C. W. Chow, and W. P. Lin, "Utilizing polarization-multiplexing for free space optical communication transmission with security operation," Opt. Fiber Technol. **52**, 101992 (2019).
21. S. N. Khonina, D. A. Savelyev, and N. L. Kazanskiy, "Vortex phase elements as detectors of polarization state," Opt. Express **23**(14), 17845–17859 (2015).
22. C. Rosales-Guzmán, N. Bhebhe, and A. Forbes, "Simultaneous generation of multiple vector beams on a single SLM," Opt. Express **25**(21), 25697–25706 (2017).
23. S. N. Khonina, S. V. Karpeev, and V. D. Paranin, "A technique for simultaneous detection of individual vortex states of Laguerre-Gaussian beams transmitted through an aqueous suspension of microparticles," Opt. Lasers Eng. **105**, 68–74 (2018).
24. S. N. Khonina, A. P. Porfirev, and S. V. Karpeev, "Recognition of polarization and phase states of light based on the interaction of nonuniformly polarized laser beams with singular phase structures," Opt. Express **27**(13), 18484–18492 (2019).
25. Z. Wang, N. Zhang, and X. C. Yuan, "High-volume optical vortex multiplexing and de-multiplexing for free-space optical communication," Opt. Express **19**(2), 482–492 (2011).
26. L. Sun and Q. Du, "A review of physical layer security techniques for internet of things: challenges and solutions," Entropy **20**(10), 730–745 (2018).
27. N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," IEEE Commun. Mag. **53**(4), 20–27 (2015).