The following publication Y. Cao, Y. Xiao, Z. Pan, L. Zhou and W. Chen, "Physically-Secured Ghost Diffraction and Transmission," in IEEE Photonics Technology Letters, vol. 34, no. 22, pp. 1238-1241, 15 Nov.15, 2022 is available at https://doi.org/10.1109/LPT.2022.3210026.

Physically-Secured Ghost Diffraction and Transmission

Yonggui Cao, Yin Xiao, Zilan Pan, Lina Zhou, and Wen Chen

***Abstract*—A new approach to realizing physically-secured ghost diffraction and transmission is proposed in this letter. A series of random 2D arrays of numbers are used as optical information carriers to transmit original data, e.g., analog signals or images as ghosts. Computer-generated magnification factors are applied for optical data encoding, and physically-generated scaling factors are generated with absorptive filters in free-space optical data transmission. The series of computer-generated magnification factors and physically-generated scaling factors serves as security keys, and is explored to realize high-fidelity and high-security free-space optical data (ghost) transmission. It is experimentally demonstrated that the proposed method is feasible and effective in different environments, i.e., without or with scattering media. The proposed physically-secured ghost diffraction scheme offers a new research perspective on secured optical information (e.g., analog signal) transmission in free space.**

***Index Terms*—Optical encoding, physical-layer security, scattering media, optical analog-signal transmission, free space.**

I. Introduction

CLASSICAL ghost diffraction [1] originates from quantum, which was explored to be applied in different areas, e.g., data transmission and imaging. In ghost diffraction, a single-pixel detector is utilized to collect light intensities, and correlation algorithms using 2D illumination patterns and the collected light intensities are developed to reconstruct image of the object. Data encryption has been recognized to be important in ghost diffraction. However, the ghost diffraction process was directly treated as an encryption approach in previous studies [2],[3], and its security was not high. Recently, free-space optical data transmission with high fidelity was further developed by using ghost diffraction [4]. However, high-fidelity secured optical data (ghost) transmission in scattering environment is also challenging, since the propagation of waves through scattering media poses inherent limitations in enabling optical data (ghost) transmission. Research has not been fully conducted on the data security of ghost diffraction and transmission through scattering media. It is desirable and important to explore secured ghost diffraction and transmission through scattering media. In terms of encryption, security keys are often numerically designed [5],[6], and the methods may be vulnerable to the attacking algorithms [7] with sufficiently computational capability. Physical-layer security can provide unbreakable, provable and quantifiable secrecy, and can be one of promising solutions [8]–[15]. Therefore, in ghost diffraction and transmission through scattering media, a promising strategy is to combine computer-generated keys with physically-generated keys in order to realize high-security and high-fidelity data transmission.

In this letter, ghost diffraction and transmission with high fidelity and high security are reported. A series of 2D arrays of random numbers are used to encode each pixel value of data to be transmitted, e.g., analog signals or images as ghosts, and a random magnification factor is distributed to process each pixel value. Dynamic scaling factors are generated physically in free-space optical transmission. Nonlinear variation of scaling factors is physically produced by using absorptive filters. Experimental results demonstrate that the proposed method realizes ghost diffraction and transmission with high fidelity and high security. The proposed method provides a large key space and guarantees the security of free-space optical data (ghosts) transmissions, since security keys are generated by using computer-generated magnification factors and physically-generated dynamic scaling factors.

II. Principle

A 2D array of random numbers is first generated as follows to encode each pixel value S of the signal or image (as ghosts): (i) Value T is obtained by a multiplication of original pixel value S and a magnification factor M. The integer part of T is represented as m, and n represents the decimal part of T. (ii) A random sequence Y is generated, length of which is $2m$. Half of sequence Y is random values between 0 and 1, and the other half is obtained by using the difference between 1 and each value of the first half. (iii) A 2D array of random numbers is generated by arbitrarily assigning the decimal value n and the sequence Y to $(2m+1)$ positions in a predesigned zero matrix. The sequence Y is used in the final step of the proposed algorithm to generate 2D arrays of random numbers P.

Pixel values (i.e., S_i, i=1,2,3,…,N) of the ghost (e.g., an image) are sequentially encoded into a series of 2D arrays of random numbers (i.e., P_i, i=1,2,3,…,N). To encode each pixel, a

This work was supported by GuangDong Basic and Applied Basic Research Foundation (2022A1515011858), Hong Kong Research Grants Council (C5011-19G, 15224921), and The Hong Kong Polytechnic University (1-W19E, 1-BD4Q). *(Corresponding author: Wen Chen)*

Yonggui Cao, Yin Xiao, Zilan Pan, and Lina Zhou are with the Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong, China.

Wen Chen is with the Department of Electronic and Information Engineering & Photonics Research Institute, The Hong Kong Polytechnic University, Hong Kong, China (e-mail: owen.chen@polyu.edu.hk).

random magnification factor (i.e., M_i, i=1,2,3,…,N) is correspondingly used. The magnification factors are used to also make the encoded neighboring pixels have a big difference (i.e., several orders of magnitude). A differential method is used to generate two 2D arrays of random numbers (i.e., D_{i1} and D_{i2}, i=1,2,3,…,N) corresponding to each generated 2D array of random numbers during optical data transmission to further eliminate environmental noise, where D_{i1}=B+P_i, D_{i2}=B-P_i, and B denotes a real and non-negative value. A spatial light modulator (SLM) modulates the optical field information in free space by sequentially embedding the generated 2D arrays of random numbers as information carriers. The collected light intensity I_{out} at the receiving end and incident optical field E_{in} have a proportional relationship [16], i.e., $I_{out} \approx f|E_{in}|^2$ where f represents a scaling factor. In conventional methods [4], scaling factors are always considered to be a constant. Here, time-dependent scaling factors are present in optical data transmission channels. A random scaling factor, i.e., f_{i1} or f_{i2} (i=1, 2, 3,…,N), is generated and applied to each 2D array of random numbers (i.e., D_{i1} or D_{i2}, i=1,2,3,…,N), when different absorptive filters are used in Figs. 1 and 2. Therefore, a series of magnification factors and physically-generated dynamic scaling factors can serve as security keys, and single-pixel light intensities collected at the receiving end are used as ciphertexts. When correct keys (i.e., magnification factors and scaling factors) are not used, the transmitted data cannot be correctly retrieved at the receiving end. By conducting a series of optical experiments, the proposed method is capable of implementing high-fidelity and high-security ghost diffraction and transmission. As a clear illustration of the proposed method, a flow chart of the proposed physically-secured ghost diffraction and transmission scheme is shown Fig.1.

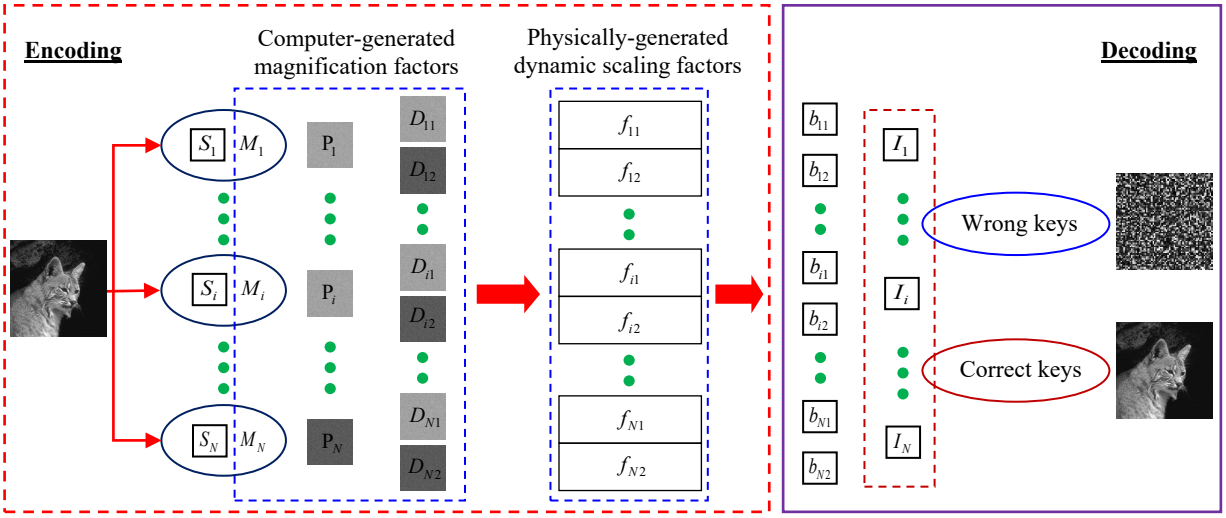

Fig. 1. A flow chart of the proposed physically-secured ghost diffraction and transmission scheme.

Figure 2 shows an experimental setup for the proposed physically-secured ghost diffraction scheme. Control of the laser diode current is performed with a laser driver (Thorlabs, LDC205C) in a range of 0 to 500 mA. An electronic controller (Thorlabs, TED200C) stabilizes the laser at room temperature. A laser diode with wavelength of 690.0 nm is utilized in optical experiments and inserted into a laser diode mount (Thorlabs, LDM56/M). The laser beam is reflected by a mirror, and illuminates the SLM (Holoeye, LC-R720) with a pixel size of 20.0 μm. Then, the modulated wave propagates through an absorptive filter and scattering media in free space. Here, a typical example of scattering media, i.e., two cascaded diffusers (Thorlabs, DG10-1500), is used to verify the proposed method. A single-pixel bucket detector (Newport, 918D-UV-OD3R) is placed at the receiving end to collect light intensities. Axial distance between the SLM and absorptive filter is 100.0 mm, and axial distance between absorptive filter and the first diffuser is 75.0 mm. Axial

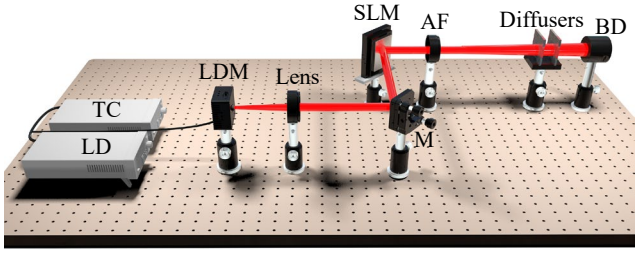

Fig. 2. A schematic experimental setup for the proposed physically-secured ghost diffraction and transmission scheme. TC: Temperature controller; LD: Laser driver; LDM: Laser diode mount; M: Mirror; SLM: Amplitude-only spatial light modulator; AF: Absorptive filter(s); BD: Single-pixel (bucket) detector. Two cascaded diffusers are employed as a typical example of scattering media in this study.

distance between the two diffusers is 10.0 mm, and axial distance between the second diffuser and single-pixel bucket detector is 75.0 mm. The SLM modulates the input light wave when the series of generated 2D arrays of random numbers is sequentially embedded into the SLM, and then the modulated light wave propagates through absorptive filter. The optical transmission channel can be used to generate dynamic scaling

factors. The ghost signals or images can be effectively retrieved, only when correct security keys, i.e., magnification factors and scaling factors, are applied.

III. EXPERIMENTAL RESULTS AND DISCUSSION

Optical transmission environments without and with scattering media (i.e., two cascaded diffusers, Thorlabs DG10-1500) in free space are used to verify the proposed physically-secured ghost diffraction. The proposed method can also be applied in other types of scattering environment [17], [18] to evaluate its effectiveness and robustness. Figures 3(a) and 3(b) show typical nonlinear variations of scaling factors in free space without and with scattering media, respectively. In Figs. 3(a) and 3(b), each combination case is defined by how the absorptive filters are arbitrarily selected and combined (e.g., 1, 2 or more) to be used in optical experiment. Nonlinear variation of scaling factors can be easily obtained with different combinations of the filters, and a large key space of physical security keys is established. To encrypt different pixels, absorptive filters can be continuously changed during data transmission. As shown in Figs. 3(a) and 3(b), nonlinear variation of scaling factors is always realized in free space without and with scattering media, when different absorptive filters are used at the transmitter in the optical transmission channel.

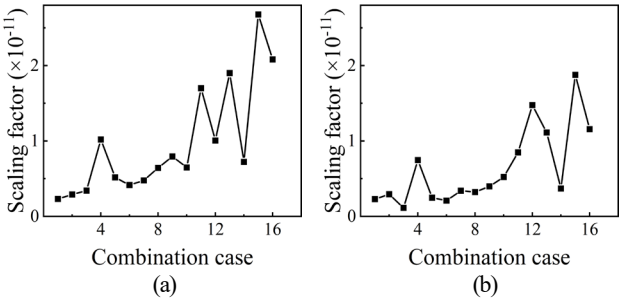

Fig. 3. (a) Nonlinear variation of scaling factors in free space without scattering media, and (b) nonlinear variation of scaling factors in free space with scattering media.

Then, a series of physically-secured ghost diffraction experiments are conducted. Two irregular analog signals are used as a typical example, and each signal has 64 pixels to be encoded into 128 2D arrays of random numbers which are sequentially displayed by the SLM. Experimental results obtained in these optical transmission environments are shown in Fig. 4. As can be seen in Figs. 4(a) and 4(c), it is impossible to reconstruct original ghost signals from the signals obtained at the receiving end, since original ghost signals are encoded into random values. Decoded signals overlap with original signals, when correct security keys are applied as shown in Figs. 4(b) and 4(d). Quantitative evaluation of ghost retrieval is realized by calculating peak signal-to-noise ratio (PSNR) and mean square error (MSE). The MSE and PSNR values are given in Fig. 4. It is experimentally demonstrated that high-fidelity and high-security ghost diffraction and transmission can be effectively realized in the proposed method.

Optical experiments to test the transmission of two grayscale images of 64×64 pixels are also conducted to verify the proposed method. As can be seen in Figs. 5(a) and 5(c), original ghost images are effectively encoded into noise-like patterns at the receiving end. When correct security keys are applied, ghost images can be retrieved with high fidelity as shown in Figs. 5(b) and 5(d). It is demonstrated by the given high PSNR values and low MSE values that the proposed high-fidelity and high-security ghost diffraction scheme is feasible and effective.

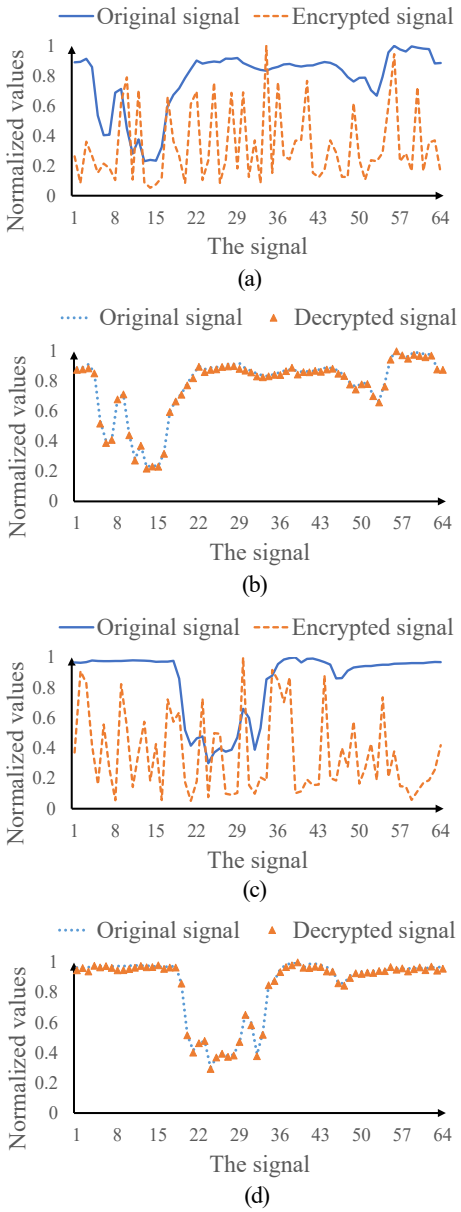

Fig. 4. (a) and (c) A comparison between the experimentally encoded signal and original ghost, and (b) and (d) a comparison between the decoded signal and original ghost: (a) and (b) Experimental results obtained in free space without scattering media; (c) and (d) experimental results obtained in free space with scattering media. The MSE values corresponding to (a)-(d) are 0.28, 1.86×10^{-4}, 0.33 and 1.78×10^{-4}, respectively. The PSNR values corresponding to (a)-(d) are 5.53 dB, 37.31 dB, 4.79 dB and 37.49 dB, respectively.

Performance of security keys is further analyzed in the proposed physically-secured ghost diffraction scheme. Figures 6(a)–6(d) show the decoded ghost images using different keys

to evaluate the security. As can be seen in Figs. 6(a) and 6(c), when correct magnification factors and wrong physically-generated scaling factors are used, no information about the plaintexts can be obtained from the decoded ghost images. As can be seen in Figs. 6(b) and 6(d), when wrong magnification factors and correct physically-generated scaling factors are used, it is also impossible to obtain any information about the plaintexts from the decoded ghost images. It is experimentally verified that the series of computer-generated magnification factors and physically-generated dynamic scaling factors can provide a large key space compared with conventional methods [5],[6], and the proposed physically-secured ghost diffraction scheme possesses high security. Since the key space is large, the proposed method possesses high resistance against brute force attack.

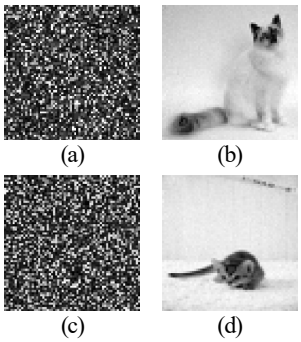

Fig. 5. The experimentally encoded ghost images in (a) free space without scattering media and (c) free space with scattering media, and the decoded ghost images obtained in free space (b) without scattering media and (d) with scattering media when correct security keys are applied. The MSE values for (a)-(d) are 0.32, 2.40×10^{-4}, 0.37 and 1.71×10^{-4}, respectively. The PSNR values for (a)-(d) are 4.92 dB, 36.20 dB, 4.34 dB and 37.67 dB, respectively.

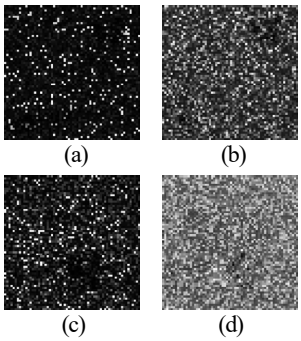

Fig. 6. (a) and (c) The decoded ghost images obtained by using correct magnification factors and wrong physically-generated scaling factors; and (b) and (d) the decoded ghost images obtained by using wrong magnification factors and correct physically-generated scaling factors: (a) and (b) Free space without scattering media; (c) and (d) free space with scattering media. The MSE values corresponding to (a)-(d) are 0.59, 0.30, 0.58 and 0.10, respectively. The PSNR values corresponding to (a)-(d) are 2.31 dB, 5.27 dB, 2.33 dB and 9.95 dB, respectively.

IV. Conclusion

In this letter, a new approach has been proposed to realize high-fidelity and high-security ghost diffraction and transmission. A flexible combination of computer-generated magnification factors and physically-generated scaling factors are utilized as security keys to achieve high-security free-space optical transmission. Absorptive filters are used to generate nonlinear scaling factors. Feasibility and effectiveness of the proposed method have been demonstrated experimentally. A novel research perspective for secured optical analog-signal transmission through scattering media in free space could be opened up by the proposed physically-secured ghost diffraction.

References

[1] R. S. Bennink, S. J. Bentley, and R. W. Boyd, ""Two-photon" coincidence imaging with a classical source," *Phys. Rev. Lett.,* vol. 89, no. 11, pp. 113601, Sep 9, 2002.

[2] Z. Pan, and L. Zhang, "Optical cryptography-based temporal ghost imaging with chaotic laser," *IEEE Photon. Technol. Lett.,* vol. 29, no. 16, pp. 1289-1292, Aug 15, 2017.

[3] W. Chen, "Correlated-photon secured imaging by iterative phase retrieval using axially-varying distances," *IEEE Photon. Technol. Lett.,* vol. 28, no. 18, pp. 1932-1935, Sep 15, 2016.

[4] Y. Xiao, L. Zhou, and W. Chen, "High-fidelity ghost diffraction and transmission in free space through scattering media," *Appl. Phys. Lett.,* vol. 118, no. 10, pp. 104001, Mar 8, 2021.

[5] P. Réfrégier, and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.,* vol. 20, no. 7, pp. 767-769, Apr 1, 1995.

[6] W. Chen, X. Chen, and C. J. R. Sheppard, "Optical image encryption based on diffractive imaging," *Opt. Lett.,* vol. 35, no. 22, pp. 3817-3819, Nov 15, 2010.

[7] A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," *Opt. Lett.,* vol. 30, no. 13, pp. 1644-1646, Jul 1, 2005.

[8] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.,* vol. 53, no. 4, pp. 20-27, Apr, 2015.

[9] Y. Xiao, L. Zhou, Z. Pan, Y. Cao, and W. Chen, "Physically-enhanced ghost encoding," *Opt. Lett.,* vol. 47, no. 2, pp. 433-436, 2022.

[10] Y. Xiao, L. Zhou, Z. Pan, Y. Cao, and W. Chen, "Physically-secured high-fidelity free-space optical data transmission through scattering media using dynamic scaling factors," *Opt. Express,* vol. 30, no. 5, pp. 8186-8198, Feb 28, 2022.

[11] J. Zhao, B. Liu, Y. Mao, J. Ren, X. Xu, X. Wu, L. Jiang, S. Han, and J. Zhang, "High-security physical layer in CAP-PON system based on floating probability disturbance," *IEEE Photon. Technol. Lett.,* vol. 32, no. 7, pp. 367-370, Apr 1, 2020.

[12] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *NPJ Quantum Inf.,* vol. 2, no. 1, pp. 1-12, Nov 8, 2016.

[13] F. Xu, M. Curty, B. Qi, and H. K. Lo, "Measurement-device-independent quantum cryptography," *IEEE J Sel. Top. Quantum Electron.,* vol. 21, no. 3, pp. 148-158, 2015.

[14] N. Li, H. Susanto, B. Cemlyn, I. Henning, and M. Adams, "Secure communication systems based on chaos in optically pumped spin-VCSELs," *Opt. Lett.,* vol. 42, no. 17, pp. 3494-3497, Sep 1, 2017.

[15] A. Bogris, A. Argyris, and D. Syvridis, "Encryption efficiency analysis of chaotic communication systems based on photonic integrated chaotic circuits," *IEEE J Quantum Electron.,* vol. 46, no. 10, pp. 1421-1429, Oct, 2010.

[16] E. Tajahuerce, V. Durán, P. Clemente, E. Irles, F. Soldevila, P. Andrés, and J. Lancis, "Image transmission through dynamic scattering media by single-pixel photodetection," *Opt. Express,* vol. 22, no. 14, pp. 16945-16955, Jul 14, 2014.

[17] Y. Xiao, L. Zhou, and W. Chen, "Direct single-step measurement of Hadamard spectrum using single-pixel optical detection," *IEEE Photon. Technol. Lett.,* vol. 31, no. 11, pp. 845-848, Jun 1, 2019.

[18] W. Chen, "Spatial nonlinear optics for securing information," *Light Sci. Appl.,* vol. 11, no. 1, pp. 1-2, Feb 7, 2022.