The following publication Yin Xiao, Lina Zhou, Zilan Pan, Yonggui Cao, and Wen Chen, "Physically-enhanced ghost encoding," Opt. Lett. 47, 433-436 (2022) is available at https://dx.doi.org/10.1364/OL.447620.

Physically-enhanced ghost encoding

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
**Corresponding author: owen.chen@polyu.edu.hk*

Received XX Month XXXX; revised XX Month, XXXX; accepted XX Month XXXX; posted XX Month XXXX (Doc. ID XXXXX); published XX Month XXXX

In this Letter, we propose physically-enhanced ghost encoding by exploring optical channel characteristics, i.e., physically- and dynamically-generated scaling factors. It is found that scaling factors can be physically and dynamically generated to serve as security keys in ghost encoding scheme, which can dramatically enlarge the key space and enhance security of optical ghost encoding schemes. To the best of our knowledge, it is the first time to control dynamic scaling factors in the optical path to realize physically-enhanced ghost encoding. In addition to illumination patterns used in optical ghost encoding schemes, the proposed method applies a variable beam attenuator and an amplitude-only spatial light modulator (SLM) to physically generate dynamic scaling factors as keys. Nonlinear variation of scaling factors is achieved in different free-space wave propagation environments in the proposed method. A series of optical experiments are conducted to verify feasibility and effectiveness of the proposed physically-enhanced ghost encoding scheme. The proposed method could open up a new research perspective for optical ghost encoding.

Information transmission plays an important role in modern society, and information security is facing great challenges than ever before. Optical encryption has attracted increasing attention in recent years due to its inherent properties, i.e., parallel processing and multi-dimensional characteristics [1,2]. Réfrégier and Javidi [3] first proposed double random phase encoding (DRPE) based on a 4*f* lens system, in which two random phase masks are placed respectively in the object plane and Fourier plane to transform object information into a noise-like pattern. Inspired by the DRPE, much effort has been made to develop various optical cryptosystems [4–9]. The DRPE-based techniques usually transform a plaintext into complex amplitude, and a reference wave is usually applied in optical experiments to store ciphertext in the form of intensity.

Different from optical encryption schemes using pixelated sensor arrays [3–9], ghost encoding employs a single-pixel detector without spatial resolution to extract two-dimensional (2D) object information [10,11]. Ghost encoding provides a promising alternative for conventional optical encryption schemes, and has remarkable advantages in the different wave propagation environments (e.g., scattering environments and weak light levels). In conventional ghost encoding schemes, illumination patterns and the collected single-pixel intensity values usually serve as security keys and ciphertext, respectively. However, ghost encoding scheme may be attacked [12–14] due to its fundamentally linear property, and the attacking methods provide an insight for the cryptoanalysis of ghost encryption. It is desirable that high security can be achieved in ghost encoding to withstand the attacks. Physical layer security is one of the most promising solutions for security enhancement owing to the properties of unbreakable, provable and quantifiable secrecy [15–18]. The existing ghost encoding schemes do not fully explore channel characteristics in optical process to conduct physical layer encryption. In the optical ghost encoding process, scaling factors physically exist and can be used. However, scaling factors have been simply considered as a constant in previous works. Until now, no any research has been conducted to investigate the property of dynamic scaling factors in optical encryption schemes. It is believed that it is significant to explore the application of dynamic scaling factors in optical ghost encoding.

In this Letter, we propose physically-enhanced ghost encoding by exploring optical channel characteristics, i.e., physically- and dynamically-generated scaling factors in the optical encoding process. To the best of our knowledge, it is the first time to physically control dynamic scaling factors in optical encoding process to realize physically-enhanced ghost encoding. In the proposed method, in addition to illumination patterns, scaling factors are physically and dynamically generated in optical ghost encoding process to serve as keys. These dynamic scaling factors dramatically enlarge the key space and enhance security of optical ghost encoding schemes to withstand the attacks. A variable beam attenuator and an amplitude-only spatial light modulator (SLM) are applied to control intensity of the light source and the light intensity recorded at the receiving end. Our design using these two devices can dynamically generate scaling factors in ghost encoding process, and it is found that nonlinear variation of the scaling factors can be achieved in different free-space wave propagation environments. Principle of the proposed method is schematically shown in Fig. 1.

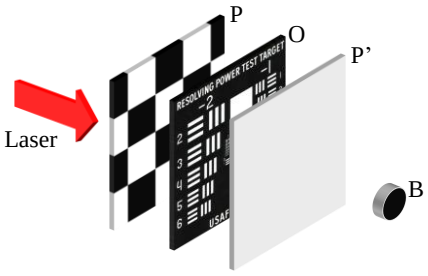

Fig. 1. Principle of the proposed method. P: Illumination pattern; O: Object; P': Modulation pattern; B: Single-pixel (bucket) detector.

In conventional optical ghost encoding schemes, a series of illumination patterns are used to sequentially illuminate an object, and then the optical wave is collected by a single-pixel detector. In the proposed method, as shown in Figs. 1 and 2, the light source adjusted by a variable beam attenuator modulates the illumination pattern P, and then the optical wave propagating through the object O is further modulated by using modulation patterns P' before single-pixel detection. Conventional optical ghost encoding scheme without a modulation pattern P' can be described by

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

where B denotes the intensity value collected by a single-pixel detector and k denotes a scaling factor. In conventional ghost encoding schemes, this scaling factor existing in the optical path is simply considered as a constant, which have no any effect on ghost encoding. In the proposed method, by flexible adjustment of intensity of the light source and the usage of modulation patterns, it is feasible to physically and dynamically generate scaling factors in the optical ghost encoding process. For instance, when three different modulation strategies (i.e., a combination of different intensities of light source and different modulation patterns) are individually used, the detected intensity values B_1, B_2 and B_3 are different and there are three different scaling factors (i.e., k_1, k_2 and k_3). A relationship can be obtained and described by

$$\mathrm{B}_1 : \mathrm{B}_2 : \mathrm{B}_3 \cdots = k_1 : k_2 : k_3 \cdots \rightarrow 1 : \frac{k_2}{k_1} : \frac{k_3}{k_1} \cdots, \tag{2}$$

where the first scaling factor k_1 is selected to serve as a reference without loss of generality. As can be seen in Eq. (2), when a reference is chosen and applied, other scaling factors can also be calculated. In the proposed optical ghost encoding scheme, the series of recorded single-pixel values is further physically encoded, when different modulation strategies (i.e., a combination of different intensities of light source and different modulation patterns) are applied. In conventional optical ghost encoding scheme, original object information can be correctly decoded, when illumination patterns and ciphertext (i.e., a series of single-pixel intensity values) are known. In the proposed method, it is impossible to obtain information of plaintext without further knowledge of the physically- and dynamically-generated scaling factors in optical ghost encoding process. Therefore, dynamic scaling factors generated in optical ghost encoding process also serve as keys to enhance security of ghost encoding. Here, a series of optical experiments have been conducted to verify feasibility and effectiveness of the proposed physically-enhanced ghost encoding.

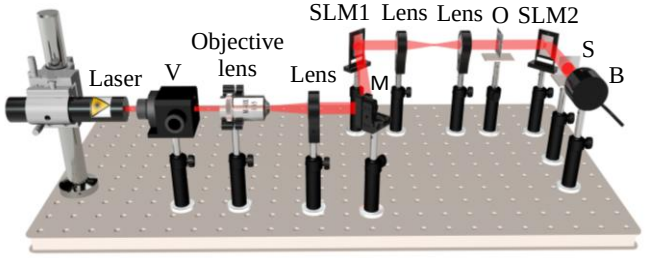

Fig. 2. A schematic experimental setup for the proposed physically-enhanced ghost encoding scheme. V: Variable beam attenuator; M: Mirror; S: Scattering medium (i.e., a diffuser).

A schematic experimental setup for the proposed physically-enhanced ghost encoding scheme is shown in Fig. 2. A He-Ne laser with power of 17.0 mW and wavelength of 633.0 nm propagates through a variable beam attenuator (Newport, VA-CB-633-CONEX). The variable beam attenuator is used to adjust intensity of the 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 the first amplitude-only SLM (Holoeye, LC-R720) with pixel size of 20 μm. In the first SLM (SLM1), a series of illumination patterns are used to sequentially illuminate an object (Edmund, negative 1951 USAF target) through a 4*f* lens system. The optical wave propagating through an object illuminates the second amplitude-only SLM (Holoeye, LC-R720). Here, the second SLM (SLM2) is applied to further modulate intensity of optical wave. The modulated optical wave is collected by a single-pixel (bucket) detector (Newport, 918D-UV-OD3R).

The variable beam attenuator placed in the optical setup can provide continuous power adjustment for the laser via a control of its angle values. As the angle value increases, intensity attenuation of light source is less. The angle can be automatically controlled to be rotated with a precision of 0.1 degree. The SLM2 placed in the optical setup displays different 2D modulation patterns which are used to modulate intensity of the optical wave. The modulation patterns can be arbitrarily designed and applied, and there is no need to align modulation patterns with the illumination patterns embedded in the SLM1. By using the variable beam attenuator and the SLM2, flexibly generating dynamic scaling factors is realized in the proposed physically-enhanced ghost encoding scheme.

In optical experiments, regarding illumination patterns embedded into the SLM1, different types of illumination patterns can be flexibly applied, e.g., random patterns [10], Hadamard patterns [19] and sinusoidal patterns [20]. Here, a series of Hadamard patterns with 128×128 pixels are used as illumination patterns, i.e., as a typical example, to illustrate the proposed method. Three different types of modulation patterns, i.e., white pattern, random pattern and dark pattern, are designed and used as a typical example. The size of modulation patterns is 1280×768 pixels. The white pattern means that the value of all elements is 1, and the random pattern means that the elements are distributed randomly in a range from 0 to 1. The dark pattern means that most elements have small values, i.e., close to 0. The modulation patterns have effect on adjusting intensity of optical wave collected by the single-pixel detector, and nonlinear variation of scaling factors can be achieved in the proposed optical ghost encoding scheme. It is worth noting that other types of modulation patterns P' can be flexibly designed and applied to modulate intensity of the optical wave in the proposed scheme.

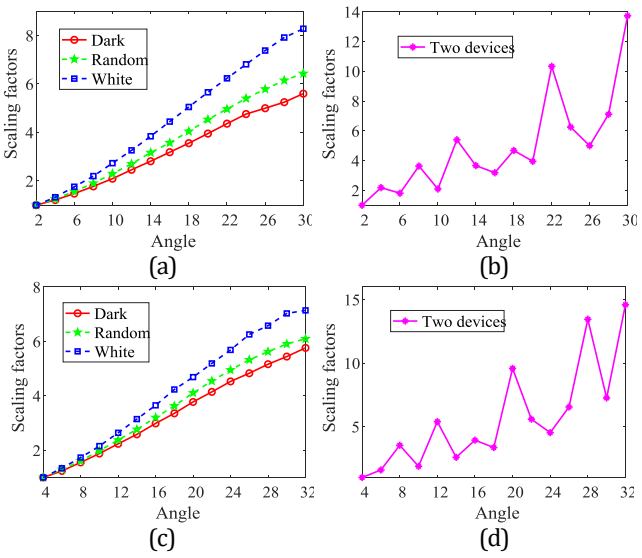

Fig. 3. (a) Linear and (b) nonlinear variation of scaling factors in free space without scattering media, and (c) linear and (d) nonlinear variation of scaling factors in free space with a scattering medium.

The proposed method is verified in two different environments, i.e., free space without scattering media and free space with a scattering medium (i.e., a diffuser, Thorlabs DG10-1500). The scattering medium is used to construct a complex environment, in which effectiveness and robustness of the proposed method are demonstrated. Other types of diffusers can also be flexibly applied in practice [21]. In free space without scattering media, angle of the variable beam attenuator is tuned dynamically from 2 to 30 degrees in optical experiments. In free space with a scattering medium, angle of the variable beam attenuator is tuned dynamically from 4 to 32 degrees. In free space without scattering media, the reference is obtained by using an angle of 2 degrees in variable beam attenuator and the dark modulation pattern. In free space with a scattering medium, the reference is obtained by using an angle of 4 degrees in variable beam attenuator and the dark modulation pattern. In these two free-space wave propagation environments, when the modulation pattern embedded in the SLM2 remains unchanged, sequentially changing the angle of variable beam attenuator leads to a nearly linear variation of scaling factors, as shown in Figs. 3(a) and 3(c). When intensity of the light source and the modulation pattern embedded in the SLM2 are dynamically changed at the same time, nonlinear variation of scaling factors can be achieved as shown in Figs. 3(b) and 3(d). In this case, the variation of scaling factors is random and dynamic, and the variation range of scaling factors is large as shown in Figs. 3(b) and 3(d).

Since scaling factors are physically and dynamically generated in our optical experiments, they can be further applied in ghost encoding scheme. Figures 4(a)–4(d) show how to use dynamic scaling factors as keys in the two different wave propagation environments. In optical experiments, a series of Hadamard patterns are sequentially applied to illuminate the target object, and the collected single-pixel values correspond to Hadamard spectrum coefficients. Then, it is demonstrated that dynamic scaling factors generated in the optical path further encode these Hadamard spectrum coefficients into random ones. For a comparison, 43 Hadamard spectrum coefficients are first measured, when the angle of variable beam attenuator and the modulation pattern embedded in the SLM2 remain unchanged. These measured Hadamard spectrum coefficients serve as a reference without loss of generality. In the proposed method, these Hadamard spectrum coefficients are also measured, when the proposed modulation strategies are applied. A comparison between the encrypted Hadamard spectrum coefficients and original Hadamard spectrum coefficients (i.e., the reference) are respectively shown in Figs. 4(a) and 4(c). As can be seen in Figs. 4(a) and 4(c), physically-generated dynamic scaling factors in the optical channel can further encode Hadamard spectrum coefficients into random ones. When all dynamic scaling factors (i.e., keys) are correctly applied, the decrypted Hadamard spectrum coefficients overlap with the reference, as shown in Figs. 4(b) and 4(d). The experimental results in Figs. 4(a)–4(d) demonstrate that the physically- and dynamically-generated scaling factors can also serve as keys in ghost encoding schemes.

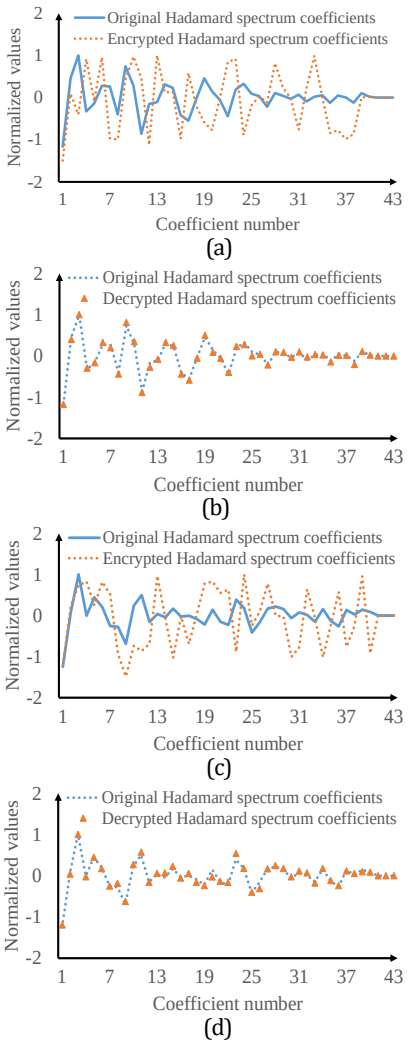

Fig. 4. A comparison between the encrypted Hadamard spectrum coefficients and original Hadamard spectrum coefficients in (a) free space without scaling media and (c) free space with a scattering medium. A comparison between the decrypted Hadamard spectrum coefficients and original Hadamard spectrum coefficients in (b) free space without scaling media and (d) free space with a scattering medium.

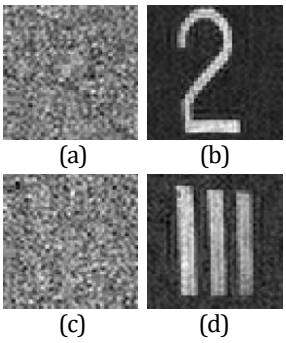

Fig. 5. The encrypted images obtained in (a) free space without scattering media and (c) free space with a scattering medium, and the decrypted images obtained in (b) free space without scattering media and (d) free space with a scattering medium.

Based on the optical experimental results in Fig. 4, it is feasible to conduct physically-enhanced ghost encoding by using the proposed method. Here, ghost encoding of two different images with 128×128 pixels is further conducted and realized respectively in free space without scattering media and in free space with a scattering medium, as shown in Figs. 5(a)–5(d). Only 10.0% Hadamard spectrum coefficients are measured and further physically encoded by the generated dynamic scaling factors. The total number of realizations is 3200 due to the use of differential measurement, and the refreshing rate of SLM is 1.25 Hz. As can be seen in Figs. 5(a) and 5(c), original object information is fully encrypted by using the proposed method. It is worth noting that the results in Figs. 5(a) and 5(c) are obtained when inverse Hadamard transform is directly applied after the light intensities are collected. When the keys, i.e., illumination patterns P and dynamic scaling factors, are correctly applied, decoded images are obtained as shown in Figs. 5(b) and 5(d). It is fully demonstrated that the proposed method is valid.

Performance of physically- and dynamically-generated scaling factors is further analyzed in the proposed ghost encoding scheme. Figures 6(a) and 6(b) show performance of the dynamic scaling factors in the decoding process in two different free-space wave propagation environments. Here, all the illumination patterns P are assumed to be correctly applied. As shown in Figs. 6(a) and 6(b), when the eavesdropping percentage of dynamic scaling factors decreases, correlation coefficients [22] calculated to quantify quality of the decoded images decline dramatically. When the eavesdropping percentage of scaling factors is lower than 90.0%, the decoded images cannot render any information about the plaintexts, as shown in the insets of Figs. 6(a) and 6(b). It is experimentally verified that physically- and dynamically-generated keys, i.e., dynamic scaling factors, can provide another security layer for ghost encoding, and make the proposed optical ghost encoding scheme to be able to fully withstand the attacking methods.

In conclusion, we have proposed physically-enhanced ghost encoding by physically- and dynamically-generating scaling factors in optical ghost encoding process. Channel characteristic in optical ghost encoding process has been fully explored. Nonlinear variation of scaling factors has been achieved by using a variable beam attenuator and an amplitude-only SLM. It is demonstrated that the dynamically- and physically-generated scaling factors can also serve as keys in the proposed ghost encoding scheme. The proposed method has been experimentally verified, and high security is achieved in ghost encoding schemes by using the proposed method. The proposed physically-enhanced ghost encoding scheme could open up a new research perspective for optical encryption.

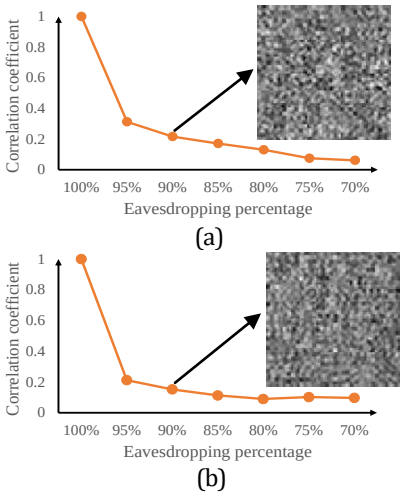

Fig. 6. Eavesdropping analysis of the scaling factors in (a) free space without scaling media and (b) free space with a scattering medium.

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

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. A. Alfalou and C. Brosseau, Adv. Opt. Photon. **1**, 589 (2009).
2. B. Javidi, A. Carnicer, M. Yamaguchi, et al., J. Opt. **18**, 083001 (2016).
3. P. Réfrégier and B. Javidi, Opt. Lett. **20**, 767 (1995).
4. W. Chen, X. D. Chen, and C. J. R. Sheppard, Opt. Lett. **35**, 3817 (2010).
5. O. Matoba and B. Javidi, Opt. Lett. **24**, 762 (1999).
6. G. Unnikrishnan, J. Joseph, and K. Singh, Opt. Lett. **25**, 887 (2000).
7. S. T. Liu, Q. L. Mi, and B. H. Zhu, Opt. Lett. **26**, 1242 (2001).
8. G. Situ and J. Zhang, Opt. Lett. **29**, 1584 (2004).
9. W. Chen, B. Javidi, and X.D. Chen, Adv. Opt. Photon. **6**, 120 (2014).
10. P. Clemente, V. Durán, V. Torres-Company, E. Tajahuerce, and J. Lancis, Opt. Lett. **35**, 2391 (2010).
11. Y. Xiao, L. Zhou, and W. Chen, Appl. Opt. **60**, B1 (2021).
12. A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, Opt. Lett. **30**, 1644 (2005).
13. C. Zhang, M. Liao, W. He, and X. Peng, Opt. Express **21**, 28523 (2013).
14. X. Peng, P. Zhang, H. Wei, and B. Yu, Opt. Lett. **31**, 1044 (2006).
15. L. Sun and Q. Du, Entropy **20**, 730 (2018).
16. N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, IEEE Commun. Mag. **53**, 20 (2015).
17. L. Liu, X. Tang, X. Jiang, Z. Xu, F. Li, Z. Li, H. Huang, P. Ni, L. Chen, L. Xi, and X. Zhang, Opt. Express **29**, 18976-18987 (2021).
18. Z. Wang, Y. Xiao, S. Wang, Y. Yan, B. Wang, Y. Chen, Z. Zhou, J. He, and L. Yang, Opt. Express **29**, 17890-17901 (2021).
19. Y. Xiao, L. Zhou, and W. Chen, IEEE Photon. Tech. Lett. **31**, 1975 (2019).
20. Z. Zhang, S. Jiao, M. Yao, X. Li, and J. Zhong, Opt. Express **26**, 14578 (2018).
21. Y. Xiao, L. Zhou, and W. Chen, IEEE Photon. Technol. Lett. **31**, 845 (2019).
22. W.H. Press, S. A. Teukolsky, W. T. Vetterling, and B. P. Flannery, *Numerical Recipes in C*, 2nd Ed., Cambridge University Press, 1992.

FULL REFERENCES WITH TITLES

1. A. Alfalou and C. Brosseau, "Optical image compression and encryption methods", Adv. Opt. Photon. **1**, 589-636 (2009).
2. B. Javidi, A. Carnicer, M. Yamaguchi, T. Nomura, E. Pérez-Cabré, M. S Millán, N. K Nishchal, R. Torroba, J. F. Barrera, W. He, X. Peng, A. Stern, Y. Rivenson, A Alfalou, C Brosseau, C. Guo, J. T Sheridan, G. Situ, M. Naruse, T. Matsumoto, I. Juvells, E. Tajahuerce, J. Lancis, W. Chen, X. Chen, P. W H Pinkse, A. P Mosk, and A. Markman, "Roadmap on optical security," J. Opt. **18**, 083001 (2016).
3. P. Réfrégier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**, 767-769 (1995).
4. W. Chen, X. D. Chen, and C. J. R. Sheppard, "Optical image encryption based on diffractive imaging," Opt. Lett. **35**, 3817-3819 (2010).
5. O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," Opt. Lett. **24**, 762-764 (1999).
6. G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," Opt. Lett. **25**, 887-889 (2000).
7. S. T. Liu, Q. L. Mi, and B. H. Zhu, "Optical image encryption with multistage and multichannel fractional Fourier-domain filtering," Opt. Lett. **26**, 1242-1244 (2001).
8. G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," Opt. Lett. **29**, 1584-1586 (2004).
9. W. Chen, B. Javidi, and X.D. Chen, "Advances in optical security systems," Adv. Opt. Photon. **6**, 120-155 (2014).
10. P. Clemente, V. Durán, V. Torres-Company, E. Tajahuerce, and J. Lancis, "Optical encryption based on computational ghost imaging," Opt. Lett. **35**, 2391-2393 (2010).
11. Y. Xiao, L. Zhou, and W. Chen, "Optical information authentication using phase-only patterns with single-pixel optical detection," Appl. Opt. **60**, B1-B7 (2021).
12. 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. **30**, 1644-1646 (2005).
13. C. Zhang, M. Liao, W. He, and X. Peng, "Ciphertext-only attack on a joint transform correlator encryption system," Opt. Express **21**, 28523-28530 (2013).
14. X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," Opt. Lett. **31**, 1044-1046 (2006).
15. L. Sun and Q. Du, "A Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions," Entropy **20**, 730-745 (2018).
16. 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**, 20-27 (2015).
17. L. Liu, X. Tang, X. Jiang, Z. Xu, F. Li, Z. Li, H. Huang, P. Ni, L. Chen, L. Xi, and X. Zhang, "Physical layer encryption scheme based on cellular automata and DNA encoding by hyper-chaos in a CO-OFDM system," Opt. Express 29, 18976-18987 (2021).
18. Z. Wang, Y. Xiao, S. Wang, Y. Yan, B. Wang, Y. Chen, Z. Zhou, J. He, and L. Yang, "Probabilistic shaping based constellation encryption for physical layer security in OFDM RoF system," Opt. Express 29, 17890-17901 (2021).
19. Y. Xiao, L. Zhou, and W. Chen, "Single-pixel imaging authentication using sparse Hadamard spectrum coefficients," IEEE Photon. Tech. Lett. **31**, 1975-1978 (2019).
20. Z. Zhang, S. Jiao, M. Yao, X. Li, and J. Zhong, "Secured single-pixel broadcast imaging," Opt. Express **26**, 14578-14591 (2018).
21. Y. Xiao, L. Zhou, and W. Chen, "Direct single-step measurement of Hadamard spectrum using single-pixel optical detection," IEEE Photon. Technol. Lett. **31**, 845-848 (2019).
22. W.H. Press, S. A. Teukolsky, W. T. Vetterling, and B. P. Flannery, *Numerical Recipes in C*, 2nd Ed., Cambridge University Press, 1992.