Optics Letters

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 3 November 2021; revised 8 December 2021; accepted 12 December 2021; posted 15 December 2021; published 14 January 2022

In this Letter, we propose a physically enhanced ghost encoding scheme that is realized 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 a ghost encoding scheme, dramatically enlarging the key space and enhancing the security of optical ghost encoding schemes. To the best of our knowledge, this is the first time that dynamic scaling factors have been controlled in the optical path to realize physically enhanced ghost encoding. In addition to the 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 the feasibility and effectiveness of the proposed physically enhanced ghost encoding scheme. The proposed method could open up new research perspectives in optical ghost encoding.

https://doi.org/10.1364/OL.447620

Information transmission plays an important role in modern society, and information security is facing greater 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] were the first to propose double random phase encoding (DRPE) based on a $4f$ lens system in which two random phase masks are placed respectively in the object plane and the Fourier plane to transform object information into a noise-like pattern. Inspired by DRPE, much effort has been directed into the development of various optical cryptosystems [4–9]. DRPE-based techniques usually transform plaintext into a complex amplitude, and a reference wave is usually applied in optical experiments to store ciphertext in the form of intensity.

Unlike 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 to conventional optical encryption schemes, and has remarkable advantages in different wave-propagation environments (e.g., in scattering environments and at 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, a ghost encoding scheme may be attacked [12–14] as it is fundamentally linear, and the attacking methods provide insights that are useful for the cryptoanalysis of ghost encryption. It is desirable to achieve high security during ghost encoding to withstand the attacks. Physical layer security is one of the most promising security enhancement solutions owing to its unbreakable, provable, and quantifiable secrecy [15–18]. Existing ghost encoding schemes do not fully explore the channel characteristics of the optical process to conduct physical layer encryption. In the optical ghost encoding process, there are scaling factors that physically exist and can be used. However, scaling factors have been considered to be constant in previous works. Until now, as far as we are aware, there has been no research into the properties of dynamic scaling factors in optical encryption schemes. Therefore, it is believed to be important to explore the application of dynamic scaling factors in optical ghost encoding.

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

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, adjustment of the light source by a variable beam attenuator modulates the illumination pattern P, and then the optical wave propagating through the object O is further modulated by the modulation pattern P′, before single-pixel detection. The conventional optical ghost encoding scheme without the

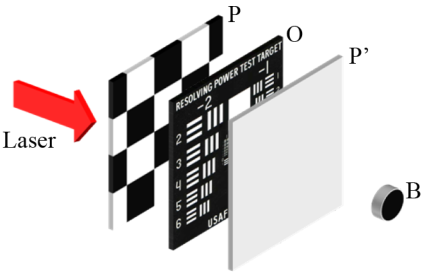

Fig. 1. Principle of the proposed method. P: illumination pattern; O: object; P′: modulation pattern; B: single-pixel (bucket) detector.

application of 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 of the optical path is considered constant, and has no any effect on the ghost encoding. In the proposed method, by flexible adjustment of the intensity of the light source and the usage of modulation patterns, it is feasible to physically and dynamically generate scaling factors during the optical ghost encoding process. For instance, when three different modulation strategies (i.e., different combinations of light-source intensity and modulation pattern) are separately applied, 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 it is described by

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

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

A schematic of the experimental setup used 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 the 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), an object (Edmund, negative 1951 USAF target) is sequentially illuminated by a series of illumination patterns through a 4f lens system. The optical wave propagating through the object illuminates a second amplitude-only SLM (Holoeye, LC-R720). The second SLM (SLM2) is applied to further modulate the intensity of the optical wave. The modulated optical wave is collected by a single-pixel (bucket) detector (Newport, 918D-UV-OD3R).

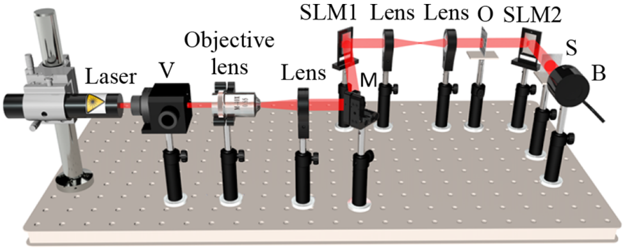

Fig. 2. A schematic of the experimental setup for the proposed physically enhanced ghost encoding scheme. V: variable beam attenuator; M: mirror; S: scattering medium (i.e., a diffuser).

The variable beam attenuator placed in the optical setup allows the power of the laser to be continuously adjusted by modifying its angle. As the angle increases, the intensity of the light source is less attenuated. The angle can be automatically rotated to a precision of 0.1°. SLM2 displays different 2D modulation patterns that are used to modulate the intensity of the optical wave. The modulation patterns can be designed and applied arbitrarily, and there is no need to align the modulation patterns with the illumination patterns embedded in SLM1. By using the variable beam attenuator and SLM2, flexible generation of dynamic scaling factors can be realized in the proposed physically enhanced ghost encoding scheme.

In optical experiments, different types of illumination patterns embedded into SLM1, e.g., random patterns [10], Hadamard patterns [19], and sinusoidal patterns [20], can be flexibly applied. Here, a series of Hadamard patterns with 128×128 pixels are used as typical illumination patterns to illustrate the proposed method. Three different types of modulation patterns, i.e., a white pattern, a random pattern, and a dark pattern, are designed and are used as typical examples. The size of each modulation pattern is 1280×768 pixels. All of the elements in the white pattern have a value of 1, while the elements in the random pattern are distributed randomly in the range from 0 to 1. In the dark pattern, most of the elements have small values, i.e., close to 0. These modulation patterns have the effect of adjusting the intensity of the 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 the modulation pattern P′ applied to modulate the intensity of the optical wave in the proposed scheme can be flexibly designed to be other patterns.

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 the effectiveness and robustness of the proposed method can be demonstrated. Other types of diffusers can also be flexibly applied in practice [21]. In free space without a scattering medium, the angle of the variable beam attenuator is tuned dynamically from 2° to 30° in optical experiments. In free space

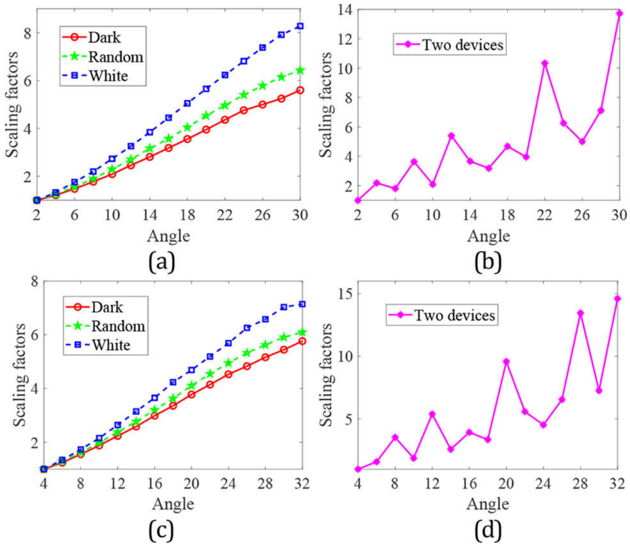

Fig. 3. (a) Linear and (b) nonlinear variation in scaling factors in free space without a scattering medium, and (c) linear and (d) nonlinear variation in scaling factors in free space with a scattering medium. Angle unit is degree.

with a scattering medium, the angle of the variable beam attenuator is tuned dynamically from 4° to 32°. In free space without a scattering medium, the reference is obtained by using an angle of 2° for the 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° for the variable beam attenuator and the dark modulation pattern. In these two free-space wave propagation environments, when the modulation pattern embedded in SLM2 remains unchanged, sequentially changing the angle of the variable beam attenuator leads to nearly linear variation of the scaling factors, as shown in Figs. 3(a) and 3(c). When the intensity of the light source and the modulation pattern embedded in SLM2 are dynamically changed at the same time, nonlinear variation of the scaling factors can be achieved, as shown in Figs. 3(b) and 3(d). In this case, the variation of the scaling factors is random and dynamic, and the range of variation in the 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 applied in a ghost encoding scheme. Figures 4(a)–4(d) show how dynamic scaling factors can be used 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. It is then 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 while the angle of the variable beam attenuator and the modulation pattern embedded in SLM2 remains unchanged. These measured Hadamard spectrum coefficients serve as a reference without any loss of generality. In the proposed method, these Hadamard spectrum coefficients are also measured when the proposed modulation strategies are applied. Comparisons between the encrypted Hadamard spectrum coefficients and the original Hadamard spectrum coefficients (i.e., the reference) are

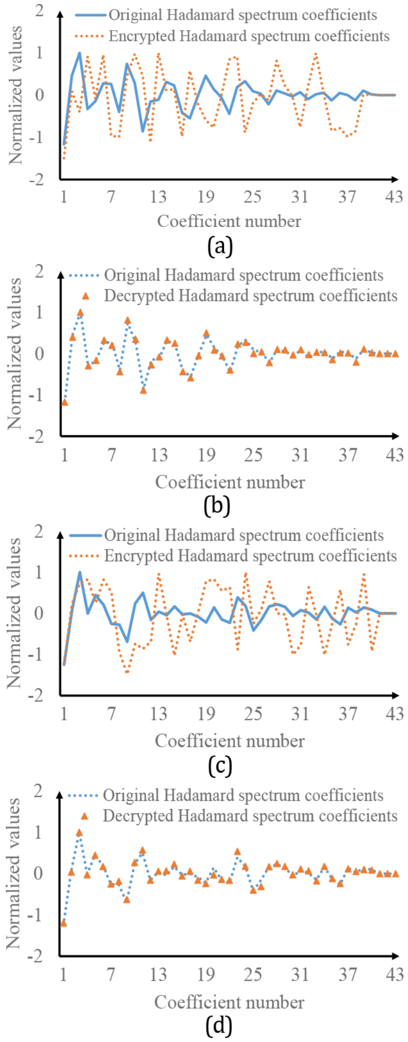

Fig. 4. Comparison between the encrypted Hadamard spectrum coefficients and original Hadamard spectrum coefficients in (a) free space without a scattering medium and (c) free space with a scattering medium. Comparison between the decrypted Hadamard spectrum coefficients and original Hadamard spectrum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

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 of the 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 shown in Figs. 4(a)–4(d) demonstrate that the physically and dynamically generated scaling factors can also serve as keys in ghost encoding schemes.

Based on the optical experimental results shown in Fig. 4, it is feasible to conduct physically enhanced ghost encoding using the proposed method. Thus, the ghost encoding of two different images with 128×128 pixels is conducted and realized in free space without a scattering medium and in free space with a scattering medium, as shown in Figs. 5(a)–5(d). Only 10.0% of the Hadamard spectrum coefficients are measured and physically encoded by the generated dynamic scaling factors. The total

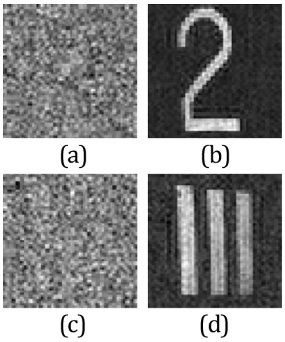

Fig. 5. Encrypted images obtained in (a) free space without a scattering medium and (c) free space with a scattering medium, and decrypted images obtained in (b) free space without a scattering medium and (d) free space with a scattering medium.

number of realizations is 3200 due to the use of differential measurement, and the SLM refresh rate is 1.25 Hz. As can be seen in Figs. 5(a) and 5(c), the original object information is fully encrypted using the proposed method. It is worth noting that the results shown in Figs. 5(a) and 5(c) are obtained when the inverse Hadamard transform is directly applied after collecting the light intensities. When the keys, i.e., the illumination patterns P and the dynamic scaling factors, are correctly applied, the decoded images are obtained, as shown in Figs. 5(b) and 5(d). This fully demonstrates that the proposed method is valid.

The performance of the proposed ghost encoding scheme based on physically and dynamically generated scaling factors is also analyzed. Figures 6(a) and 6(b) show the performance achieved using dynamic scaling factors in the decoding process in the two different free-space wave propagation environments. All illumination patterns P are assumed to be correctly applied. As shown in Figs. 6(a) and 6(b), when the eavesdropping percentage of the dynamic scaling factors decreases, the correlation coefficient [22] calculated to quantify the quality of the decoded image declines dramatically. When the eavesdropping percentage of the scaling factors is lower than 90.0%, the decoded image cannot provide any information about the plaintext, as shown by the insets of Figs. 6(a) and 6(b). This experiment verifies that physically and dynamically generated keys, i.e., dynamic scaling factors, can provide another security layer for ghost encoding, making the proposed optical ghost encoding scheme to be able to fully withstand methods of attack.

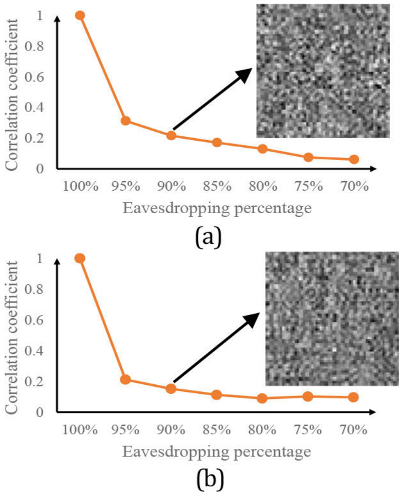

Fig. 6. Eavesdropping analysis of the scaling factors in (a) free space without a scattering medium and (b) free space with a scattering medium.

In conclusion, we have proposed a physically enhanced ghost encoding scheme that is achieved by physically and dynamically generating scaling factors in the optical ghost encoding process. The channel characteristics of the optical ghost encoding process have been fully explored. Nonlinear variation of scaling factors has been achieved using a variable beam attenuator and an amplitude-only SLM. It has been demonstrated that 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 was found to be achieved in ghost encoding schemes using the proposed method. The proposed physically enhanced ghost encoding scheme could open up new research perspectives in optical encryption.

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. Photonics **1**, 589 (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, 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. Photonics **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 (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 (2021).
19. Y. Xiao, L. Zhou, and W. Chen, IEEE Photonics Technol. 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 Photonics 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).