

NEWS & VIEWS

Open Access

Spatial nonlinear optics for securing information

Wen Chen¹✉

Abstract

The high degrees of freedom of light, various optical structures and optical materials can be explored and applied to develop optical encryption for securing information. An exciting optical image encryption approach has been proposed based on spatial nonlinear optics.

With a rapid development of modern technologies, it has been well recognized that information security plays an important role in many applications, e.g., secured data storage and communication. Securing information with optical means has attracted much current attention, since double random phase encoding¹ was proposed. The remarkable characteristics of optical encryption^{2–9}, e.g., parallel processing and multi-dimensional capabilities, have been continuously explored. For instance, parallel processing can be realized by using optical devices, and multiple-dimensional and multiple-parameter capabilities of the light are explored and applied in optical image encryption systems.

Various transform domains, optical materials and optical imaging methods^{2–9} have been studied for optical encryption, e.g., digital holography, computer-generated hologram, diffractive imaging, and ghost imaging. These designs, infrastructures and algorithms have greatly enriched optical image encryption field, and make optical encryption to be feasible and effective in practical applications. However, it has also been demonstrated and verified that linearly optical image encryption systems may be attacked, and security vulnerability could be detected by using some properly-designed algorithms^{10,11}, e.g., chosen-ciphertext attack and known-plaintext attack. Therefore, the breakthroughs need to be continuously made in the field of optical encryption to achieve high security and high applicability.

To overcome the challenges, Hou and Situ¹² proposed to apply spatial nonlinear optics for securing information. Nonlinear characteristic is obtained for optical image encryption in an optical setup using $\text{Sr}_{0.61}\text{Ba}_{0.39}\text{Nb}_2\text{O}_6$ (SBN:61) crystal¹² as schematically shown in Fig. 1. To encode an image, two statistically-independent random phase patterns are embedded into phase-only spatial light modulators, and the nonlinearity is generated by using photorefractive crystal in the designed optical encoding setup. The nonlinear Schrödinger transform has been defined and applied in the proposed optical encryption approach¹².

Regarding misalignment toleration, robustness against noise and effect of nonlinearity strength, the analysis has been conducted in detail to show good performance of the proposed nonlinear encryption approach¹². It is also demonstrated that owing to self-phase modulation effect of photorefractive crystal, the proposed approach is robust against known-plaintext attack. In addition, the proposed nonlinear encryption approach can withstand deep learning-based attacks, since plaintext-dependent strategy is integrated into the designed optical encryption system. The work in Ref. ¹² sheds light on optical information security based on spatial nonlinear optics.

In optical encryption, there are still some significant challenges that deserve more attention and effort to overcome, and high encoding capacity, high applicability and high security are desired. Various optical parameters, optical structures and optical materials, e.g., metasurface, can be continuously designed and applied to realize high-capacity and high-security nonlinearly optical encryption. With the development of optical

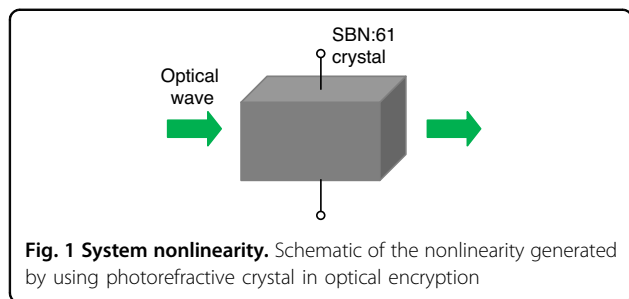
Correspondence: Wen Chen (owen.chen@polyu.edu.hk)

¹Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong, China

© The Author(s) 2022



Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>.



instruments and nanomaterials, it can be expected that high-speed data decoding using an optical way could also be feasible. The continuously-developed new concepts can create a new era of optical encryption.

Conflict of interest

The author declares no competing interests.

Published online: 07 February 2022

References

1. Refregier, P. & Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **20**, 767–769 (1995).
2. Matoba, O., Nomura, T., Cabré, E. P., Millán, M. S. & Javidi, B. Optical techniques for information security. *Proc. IEEE* **97**, 1128–1148 (2009).
3. Chen, W., Javidi, B. & Chen, X. D. Advances in optical security systems. *Adv. Opt. Photon.* **6**, 120–155 (2014).
4. Clemente, P., Durán, V., Torres-Company, V., Tajahuerce, E. & Lancis, J. Optical encryption based on computational ghost imaging. *Opt. Lett.* **35**, 2391–2393 (2010).
5. Zhou, L., Xiao, Y. & Chen, W. Learning complex scattering media for optical encryption. *Opt. Lett.* **45**, 5279–5282 (2020).
6. Fang, X., Ren, H. & Gu, M. Orbital angular momentum holography for high-security encryption. *Nat. Photonics* **14**, 102–108 (2020).
7. Qu, G. Y. et al. Reprogrammable meta-hologram for optical encryption. *Nat. Commun.* **11**, 5484 (2020).
8. Georgi, P. et al. Optical secret sharing with cascaded metasurface holography. *Sci. Adv.* **7**, eabf9718 (2021).
9. Javidi, B. et al. Roadmap on digital holography [Invited]. *Opt. Express* **29**, 35078–35118 (2021).
10. Carnicer, A., Montes-Usategui, M., Arcos, S. & Juvells, I. Vulnerability to chosen-ciphertext attacks of optical encryption schemes based on double random phase keys. *Opt. Lett.* **30**, 1644–1646 (2005).
11. Peng, X., Zhang, P., Wei, H. & Yu, B. Known-plaintext attack on optical encryption based on double random phase keys. *Opt. Lett.* **31**, 1044–1046 (2006).
12. Hou, J. F. & Situ, G. H. Image encryption using spatial nonlinear optics. *eLight* **1**, 10, <https://doi.org/10.1186/s43593-021-00010-y> (2022).