Optical Coherence Encryption with Structured Random Light

Demin Peng

Soochow University

Zhaofeng Huang

Soochow University

Yonglei Liu

Shandong Normal University

Yahong Chen

Soochow University

Fei Wang

Soochow University

Sergey A. Ponomarenko

Dalhousie University

Yangjian Cai (✉ yangjiancai@suda.edu.cn)

Shandong Normal University & Soochow University

Research Article

Keywords: structured random light, spatial coherence, optical encryption, atmospheric turbulence

Posted Date: February 10th, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-205624/v1>

License: This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Version of Record: A version of this preprint was published at PhotoniX on April 20th, 2021. See the published version at <https://doi.org/10.1186/s43074-021-00027-z>.

Abstract

Information encryption with optical technologies has become increasingly important due to remarkable multidimensional capabilities of light fields. However, the optical encryption protocols proposed to date have been primarily based on the first-order field characteristics, such as the optical field amplitude and phase as well as its polarization. As the said first-order characteristics of light fields are strongly affected by interference effects, the conventional encoding protocols become quite unstable during light propagation and interaction with the matter. Here, we introduce an alternative optical encryption protocol whereby the information is encoded into the spatial coherence distribution of a structured random light beam via a generalized van Cittert–Zernike theorem. We show that the proposed approach has two key advantages over its conventional counterparts. First, the complexity of measuring the spatial coherence distribution of light enhances the encryption protocol security. Second, the relative insensitivity of the second-order statistical characteristics of light to environmental noise makes the protocol robust against the environmental fluctuations, e.g, the atmospheric turbulence. We carry out experiments to demonstrate the feasibility of the coherence-based encryption method with the aid of a fractional Fourier transform. Our results open up a promising avenue for further research into optical encryption in complex environments.

Full Text

Due to technical limitations, full-text HTML conversion of this manuscript could not be completed. However, the latest manuscript can be downloaded and [accessed as a PDF](#).

Figures

Figure 1

Principle of optical coherence-based encryption. (a) Encoding of an optical image with a transmission function $t(\mathbf{v})$ (plaintext) into the spatial coherence structure $W(\mathbf{r}_1, \mathbf{r}_2)$ (ciphertext) of a random light beam through a generalized van Cittert–Zernike theorem formed by a dynamic diffuser and an encoding system with the encryption keys embedded inside. (b) The generalized Hanbury–Brown Twiss experiment setup for measuring the complex spatial coherence structure. The phase difference between the reference fields is controlled by the phase retarders. (c) Decoding of the plaintext from the measured spatial coherence structure $W_R(\mathbf{r}_1, \mathbf{r}_2)$ and the encryption keys via an inverse transfer function of the encoding system.

Figure 2

Schematics of an experimental setup for optical image encryption into the spatial coherence structure of a random light beam and a setup for measuring the corresponding cross-spectral density function. The green arrows stand for the polarization directions of the light beams.

Figure 3

Experimental results for the real (a) and imaginary (b) parts of the recovered cross spectral density $W_R(\Delta \mathbf{r})$ for the case $p_R = p_E = 0.6$. (c) The measured intensity distribution of the encrypted image on the RGGD. (d) The reconstructed image from the Fourier transform of the measured cross-spectral density function in (a) and (b).

Figure 4

(a) through (e). Experimental results for the real (left panels) and imaginary (middle panels) parts of the recovered cross-spectral density $W_R(\Delta \mathbf{r})$ for $p_R = 0.5$ (top) and $p_R = 0.7$ (bottom), respectively. (c) and (f) Reconstructed images from a Fourier transform of the measured cross-spectral density functions.

Figure 5

Experimental results for the reconstructed images for p_R varying from 0.5 to 0.72 with the step size of 0.02. The scale bar is shown in panel (l).

Figure 6

Encryption of a moving object with the modulation of the cross-spectral density function. (a)–(d) Experimental results for the real part of the measured cross-spectral density of the beam illuminating a moving object located at different instantaneous positions. (e)–(h) Experimental results for the imaginary part of the corresponding measured cross-spectral density functions. (i)–(l) Experimental results for the reconstructed images at different locations.

Figure 7

Encryption of a moving object with the modulation of the cross-spectral density function. (a)–(d) Experimental results for the real part of the measured cross-spectral density of the beam illuminating a moving object located at different instantaneous positions. (e)–(h) Experimental results for the imaginary part of the corresponding measured cross-spectral density functions. (i)–(l) Experimental results for the reconstructed images at different locations.