Ciphertext-only attacks on the double random-phase encryption based on redundancy vulnerability

Xingzhi Wu

Suzhou University of Science and Technology

Haobo Chen

Suzhou University of Science and Technology

Liwei Zhang

Suzhou University of Science and Technology

Qiliang Ten

Suzhou University of Science and Technology

Wenqing Sun (✉ sunwenqing@mail.usts.edu.cn)

Suzhou University of Science and Technology <https://orcid.org/0000-0002-0861-0941>

Research

Keywords: Optical encryption, ciphertext-only attacks, phase retrieval, image analysis

Posted Date: December 17th, 2020

DOI: <https://doi.org/10.21203/rs.3.rs-128610/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 Optical Review on September 22nd, 2021.
See the published version at <https://doi.org/10.1007/s10043-021-00703-2>.

Abstract

Background: The double random phase encoding techniques have received considerable attention from researchers in recent years because of its advantages of parallel and high speed processing capability. Meanwhile, the security of cryptosystem is also one of the major concerns.

Methods : We experimentally demonstrated the ciphertext redundancy vulnerability of the coherent double random encryption system (DRPE). Based on the statistical ergodicity of speckles and the consistency of the power spectral density (ESD), we have proved that the most plaintext information can be retrieved from partial ciphertext alone.

Results: In this paper, the simulation and experiment result were performed to verify whether the algorithm is effectiveness. The ciphertext redundancy of the DRPE system is analyzed from the results of ciphertext occlusion test. There is a risk of plaintext leakage of this scheme, as long as the average ESD can be estimated from the sub-images. The results will help to open up deeper understanding of limitation of current optical security techniques.

Conclusions: The DRPE system has potential redundancy risk. Even one-time-pad manner is not secured in DRPE system. This vulnerability allows a cryptanalyst to estimate the plaintext information with only a half or less ciphertext.

Full Text

This preprint is available for [download as a PDF](#).

Figures

Figure 1

Dividing incomplete ciphertext with random startpoint.

Figure 2

The schematic flowchart of the proposed algorithm.

Figure 3

Simulation ciphertext and retrieved result. Scale bar: 100 pixels in a. Scale bars: 20 pixels in c to e. (a) ciphertext with occlusion; (b) input plaintext; (c) autocorrelation; (d) ESD; (e) retrieved plaintext.

Figure 4

Cryptanalysis experimental setup of the DRPE system.

Figure 5

Experimental ciphertext and retrieved result from complete ciphertext. Scale bar: 100 pixels in a. Scale bar: 20 pixels in c to e. (a) ciphertext; (b) input plaintext; (c) autocorrelation; (d) ESD; (e) retrieved plaintext.

Figure 6

Experimental ciphertext and retrieved result from incomplete ciphertext. Scale bar: 100 pixels in a. Scale bar: 20 pixels in c to e. (a) ciphertext with occlusion (The shaded area is invalid); (b) input plaintext; (c) autocorrelation; (d) ESD; (e) retrieved plaintext.

Figure 7

Retrieved plaintext with different percentage invalid data region in sub-images.

Figure 8

Retrieved plaintext from different the number of sub-images.