Optics and Lasers in Engineering 107 (2018) 352–363

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

journal homepage: www.elsevier.com/locate/optlaseng

Optical information authentication using optical encryption and sparsity constraint

Junxin Chen [a,*], Nan Bao [a], Leo Yu Zhang [b], Zhi-liang Zhu [c,*]

[a] Sino-Dutch Biomedical and Information Engineering School, Northeastern University, Shenyang 110169, China
[b] School of Information Technology, Deakin University, Victoria 3216, Australia
[c] Software College, Northeastern University, Shenyang 110169, China

ARTICLE INFO

Keywords:
Optical security
Double random phase encoding
Information authentication
Sparsity constraint

ABSTRACT

Recent advances indicate that optical encryption can be used not only for signal secrecy but also for information authentication. By integrating optical encryption with a sparsity constraint, the recovered image of the decoder is always visually unrecognizable, whereas it can be authenticated by optical correlation means. Such a design can provide an additional security layer for conventional optical encryption techniques, since the authentication is carried out without information leakage of the primary signal. Advances of optical authentication are reviewed in this paper, theoretical principles as well as implementation examples are included to illustrate the performance of representative authentication systems. Contrastive analyses and future perspectives are also discussed, and it is expected that this review work can be beneficial to the development of optical security area.

1. Introduction

Benefiting from the inherent superiorities, such as parallel processing, high speed, and multi-dimensional characteristics [1], optical techniques have attracted significant interests for information security in the past decades. Double random phase encoding (DRPE) that was proposed by Refregier and Javidi to encrypt the primary image into stationary white noise [2] is the pioneering work, and has paved the way for subsequent booming of optical security research. It is revealed that DRPE is capable of converting any noise polluted to ciphertext into a wide-sense stationary white additive noise for the decrypted image [3], which can be subsequently filtered out to reduce the noise-caused degradation. It is also shown that this technique provides satisfactory robustness to the loss of encrypted data. Inspired by this successful optical encryption technique, much effort was developed to investigate new alternatives. However, originating from its intrinsic linearity as well as the dramatic progress of cryptanalysis, DRPE and its enhanced variants have shown vulnerabilities against various attacks when the secret keys are repeatedly used without being updated [4]. This prompts researchers to develop novel optical security systems.

Recent advances indicate that optical encryption can be used not only for secrecy but also for authentication of the user, data, or device in optical security systems [5]. In [6], it has been demonstrated that integration of DRPE with photon-counting imaging can be adopted to build secure information authentication system. The primary image is encrypted by DRPE as usual, while photon-counting imaging is subsequently employed to obtain a photon-limited version of the encrypted distribution. The sparse ciphertext leads to a recovered image that does not reveal any visual information of its plaintext, whereas it can be authenticated by nonlinear optical correlation (NOC) approach [7]. A distinct peak in the correlation plane indicates authenticity of the noisy decrypted image. Obviously, decisional criterion of this system is the appearance of correlation peak rather than visual recovery of the original image, and such a design can therefore provide an additional security layer for DRPE and make the authentication process more secure against various attacks [8]. Inspired by this pioneering achievement [6], some optical authentication systems have been proposed in recent years. The primary procedures of these authentication systems include: (1) optical encryption procedure to conceal the plaintext information; (2) a sparsity constraint process to make the decrypted signal unrecognizable; and (3) an authenticator to verify the decoded information. The objective of such systems is to authenticate the decoded information without any leakage of the plaintext, or in other says, it is possible to discriminate the decoded signal from other similar signals without precise recovery of involved plaintext. This technique is pretty useful in the scenarios where authentication should be performed without accessing (or cannot access) the plaintext information. For instance, it is particularly applicable for authentication of integrated circuits (ICs) in electronic industry [9]. It is also effective to distinct an unrecognizable retrieved object from a database, for example, one cannot obtain sufficient realizations in ghost imaging to reconstruct the object with high resolution [10].

* Corresponding authors.
E-mail addresses: chenjx@bmie.neu.edu.cn (J. Chen), zhuzhiliang.sc@gmail.com (Z.-l. Zhu).

https://doi.org/10.1016/j.optlaseng.2018.04.009
Received 11 January 2018; Received in revised form 29 March 2018; Accepted 10 April 2018

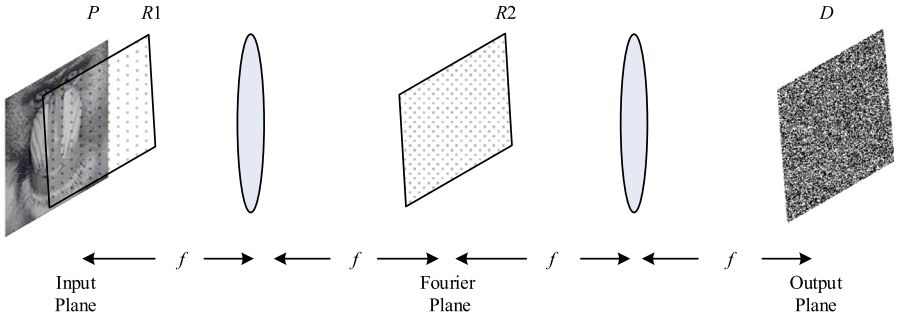

Fig. 1. The 4*f* setup of double random phase encoding.

This scenario may exist in military applications, where high-resolution imaging may be blocked by severe meteorology condition or dangerous battlefield situation.

In this paper, we will try our best efforts to review the recently proposed information authentication systems based on optical encryption and sparsity constraint. These schemes are categorized and discussed contrastively, with some representative proposals presented in more detail. Comprehensive reviews of relevant whereas different studies have been given in [11–13]. This work differs from [11,12], which focus on optical encryption means, in that we concentrate on advanced information authentication techniques. In the reviewed proposals, optical encryption is an important yet not the sole component, various sparsity strategies and kinds of authenticators also play critical roles in the authentication process. On the other hand, verifying whether the received information (such as the Quick Response (QR) code) had been counterfeited during its transmission, or in other says, whether the QR code was sent by a trusted party, is the primary concern of [13]. Specifically, QR code is proposed to be phase encoded with metal nanoparticles or thin films, while the verification decision is made based on whether the response of received QR code to certain optical measurements (speckle statistics, polarimetric signatures, etc.) delivers correct signal. To be concluded, the reviewed approaches in [13] prevent physical counterfeiting of the information container, rather than authentication of the information resides in this object, which is the primary concern of this paper.

The remainder of this paper is organized as follows. As the fundamental technique for many optical authentication systems, DRPE is first reviewed in Section 2. Authentication schemes integrating DRPE with sparsity constraint are described in Section 3, while Section 4 reviews the authentication systems using phase retrieval. The applications of QR code for optical authentication is given in Section 5, and a pioneering system which can simultaneously verify four factors is reviewed in Section 6. Section 7 reviews the authentication system using ghost imaging, and finally, conclusions and future perspectives are presented in Section 8.

2. Double random phase encoding

The so-called DRPE, i.e., double random phase encoding, is based on a 4*f* full-optical setup to convert the input image into stationary white noise with the help of two statistically independent random phase-only masks respectively placed in the input image plane and Fourier domain, as sketched in Fig. 1.

Following common cryptographic nomenclature, let us denote P the plain image, and $R1$, $R2$ the phase-only random masks. The primary image P is first amplitude-encoded using the first phase-only random distribution $R1$ to whitening the signal, and it is put in the input plane of the first lens. In the image focal plane of the first lens, Fourier transform of $P \cdot R1$ is therefore generated. This product is immediately point-to-point multiplied by another random phase mask $R2$ to further make it stationary while maintaining whiteness, and then the result will be converted to spatial domain by the second lens. The phase masks $R1$ and $R2$ are independently and randomly distributed in $[0, 2\pi]$, and serve as secret key of DRPE. Mathematically, DRPE can be summed up as Eqs. (1) and (2), in which $\cdot$ represents point-to-point multiplication, $\mathcal{F}$ is two-dimensional Fourier transform, and $\mathcal{F}^{-1}$ denotes inverse two-dimensional Fourier transform. Besides, the symbol $j = \sqrt{-1}$, while (x, y) and (μ, ν) refer to the coordinates of spatial plane and Fourier plane, respectively. As can be observed, output of DRPE, i.e., D in Eq. (1) is complex-valued, and a CCD camera is always adopted to record the intensity patterns.

$$D(x,y) = \mathcal{F}^{-1}\{exp[j \cdot R2(\mu,\nu)] \cdot \mathcal{F}(P(x,y) \cdot exp[j \cdot R1(x,y)])\}. \tag{1}$$

$$P(x,y) = \mathcal{F}^{-1}\{(\mathcal{F}[D(x,y)] \cdot exp[-j \cdot R2(\mu,\nu)]) \cdot exp[-j \cdot R1(x,y)]\}. \tag{2}$$

Investigation of optical techniques for information encryption and security had been lighted by DRPE, variants are subsequently reported. Some recent proposals with actual optical implementation are: series techniques for noise reduction of DRPE [14,15], 3D encryption with computer-generated holograms [16] and joint transform correlator [17], multiple data encryption by computational ghost imaging [18] and parallel encryption [19], Fresnel telescope [20] and integral imaging [21,22] means, as well as a digital holographic technique for packaging and encryption of multiple data [23].

3. Authentication using DRPE and sparsity constraint

In [6], Pérez-Cabré et al. first proposed their pioneering achievement to integrate photon-counting imaging (PhC) with DRPE and build a secure optical authentication system, that is the so-called PhC-DRPE. The schematic of PhC-DRPE is illustrated in Fig. 2, where a photon-counting imaging process is placed in DRPE. This architecture can be regarded as a basic structure for the optical authentication systems reviewed in this paper, and optical encryption, sparse procedure, authentication approach are the primary components of such systems.

In photon-counting imaging, the expected number of photons in $f_{ph}(x)$ is N_P, and the probability of counting $l(i)$ photons at pixel $f_{ph}(i)$ is shown to be Poisson distributed:

$$P_d[l(i);\lambda(i)] = \frac{\left[\lambda(i)^{l(i)}e^{-\lambda(i)}\right]}{l(i)!}, l(i) = 0, 1, 2, \ldots,$$

where $l(i)$ represents the number of detected photons and $\lambda(i)$ refers to Poisson parameter, i.e., the expected photons at $f_{ph}(i)$. Mathematically, $\lambda(i)$ can be calculated by $\lambda(i) = N_P f'(i)$, where $f'(i)$ is the normalized irradiance at $f_{ph}(i)$ such that $\sum_{i=1}^{M} f'(i) = 1$, under an assumption that M is the total pixel number in this scene. In PhC-DRPE, photon-counting imaging is implemented to the complex-valued ciphertext of DRPE, and sparse ciphertext is subsequently produced. As part of the ciphertext is available for decryption, only noisy signals where there is no meaningful visual perception can be obtained. Rather than precise visualization, the decrypted image is intended for information authentication by means of NOC. The nonlinear correlation of the decoded image with the original