Optics Communications 419 (2018) 134–140

Contents lists available at ScienceDirect

Optics Communications

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

Security enhancement of optical encryption based on biometric array keys

Aimin Yan, Yang Wei *, Jingtao Zhang

College of Mathematics and Science, Shanghai Normal University, Shanghai 200234, China

ARTICLE INFO

Keywords:
Optical image encryption
Information security
Biometric keys

ABSTRACT

A novel optical image encryption method is proposed by using Dammann grating and biometric array keys. Dammann grating is utilized to create a 2D finite uniform-intensity spot array. In encryption, a fingerprint array is used as private encryption keys. An original image can be encrypted by a scanning Fresnel zone plate array. Encrypted signals are processed by an optical coherent heterodyne detection system. Biometric array keys and optical scanning cryptography are integrated with each other to enhance information security greatly. Numerical simulations are performed to demonstrate the feasibility and validity of this method. Analyses on key sensitivity and the resistance against to possible attacks are provided.

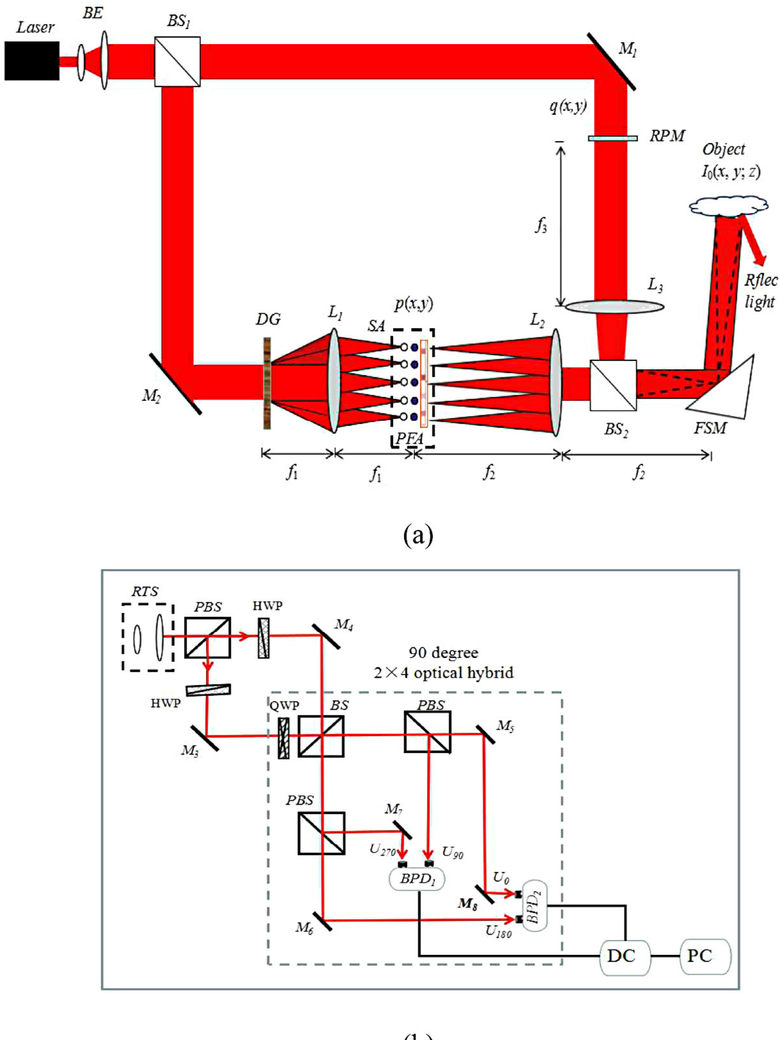
1. Introduction

Optical encryption techniques have been widely used in information security due to their multi-dimensional parameters, high speed and parallel processing capability [1]. Since Refregier and Javidi as pioneers proposed double random phase encoding (DRPE) in a well-known 4f system [2], DRPE has been developed in domains of fractional Fourier transform [3], Fresnel transform [4] and so on. However, numerical simulations as well as experimental results demonstrate that these methods based on DPRE appear to be vulnerable to several possible attacks such as known-plaintext attack (KPA) [5] and chosen-plaintext attack (CPA) [6]. The reason is that random phase masks (RPM) are the main keys introduced in the encryption system. In recent years, various optical image encryption schemes have been investigated such as compressive sensing [7], ghost imaging [8], photon-counting [9], nano- or micro-scale encryption [10], digital holography [11]. In Ref. [12], Mohammad et al. proposed a selective computational ghost imaging encryption (SCGI) method by using a different larger arbitrary element of the random matrix than others and results demonstrated its higher security. In 2017, J. Liu et al. [13] presented a parallel encryption system by encrypting multi-channel images simultaneously into a single cipher-text based on a JTC, which could be used to recover arbitrary original images with corresponding keys. Recently, B. Javidi et al. [14] discussed the recent advances, potentials, challenges of optical security and encryption methods using free space optics in detail. From the cryptography point of view, public keys and private keys play important roles in the optical encryption area. In data security, public keys are available to public and receivers have their private keys. In this way, keys can be associated with personal users' authentication. In 1976, Diffie and Hellman first proposed the historic idea of public key cryptography [15]. Subsequently, some research work has been focused on public key encryption. In 2015, T.Y. Zhao et al. [16] proposed a novel image encryption system with fingerprint used as secret key based on the phase retrieval algorithm and RSA public key algorithm. Fingerprints use as secret keys are used in both the encryption and decryption processes. In the next year, Y. Wang et al. [17] proposed a new asymmetric optical image encryption scheme based on an improved amplitude-phase retrieval algorithm. Two random phase masks are served as public encryption keys and one of private keys can be redesigned. The application of public keys and private keys greatly improve the security of optical encryption.

In order to further enhance the security of optical cryptosystem , biometric authentication has also become an important research field in optical security. Compared to passwords, biometric information such as fingerprints, faces and irises, possesses the specificity and immutability of one individual. Significantly, they are more difficult to be copied or shared with others when used as private keys. Therefore, biometric information can offer higher security and more convenience for personal verification. Since Tashima et al. [18] proposed the encryption method by using fingerprint keys in DPRE system for avoiding KPA, researchers have made an attempted to develop more novel encryption schemes by integrating biometric keys with cryptosystem. Murillo et al. [19] proposed a fingerprint image encryption scheme based on hyperchaotic Rossler map and presented better results in some aspects such as uniform distribution histograms, large key space, low pixels correlation and fast encryption. Yan et al. [20] developed an optical image encryption strategy to combine optical scanning cryptography with fingerprints

* Corresponding author.
E-mail address: 1000398608@smail.shnu.edu.cn (Y. Wei).

https://doi.org/10.1016/j.optcom.2018.03.002
Received 16 January 2018; Received in revised form 21 February 2018; Accepted 1 March 2018



(a)

(b)

Fig. 1. Proposed cryptography system: (a) encryption optical system; (b) optical coherent detection system.

to enhance security. But the scanned information is processed by an electronic lock-in amplifier. The processing speed of the electronic phase locked signal is slower than the all-optical processing speed.

In this paper, we propose a novel optical image encryption method by using Dammann grating (*DG*) and biometric array keys. Encrypted signals are processed by an optical coherent heterodyne detection system. During encryption process, a fingerprint array is used as private encryption keys. An original image can be encrypted by a scanning Fresnel zone plate array. Biometric array keys and all-optical coherent detection system are integrated with each other to enhance data security. Numerical simulations are performed to demonstrate the feasibility and validity of this method. Analyses on key sensitivity and the resistance against to possible attacks are provided.

The rest of this paper is organized as follows: In Section 2, general theory on proposed cryptosystem will be introduced in detail. In Section 3, numerical simulations and security analyses are presented to verify the validity and feasibility of this method. Finally, conclusions of this study are summarized in Section 4.

2. General theory on proposed cryptosystem

The schematic setup of the proposed cryptography system is shown in Fig. 1. A He–Ne laser beam is collimated and divided into two beams by a beam splitter. Two beam splitters (BS_1 and BS_2) and two mirrors (M_1 and M_2) form a Mach–Zehnder interferometer. Two pupils $p\ (x, y)$ and $q\ (x, y)$, located at the front focal plane of positive lenses L_2 and L_3 respectively, are illuminated by two collimated laser beams. $q\ (x, y)$ is a random phase mask (*RPM*) $exp\ [j\ 2\pi r\ (x, y)]$. $r\ (x, y)$ is a random function distributed in the interval $[0, 2\pi]$. $p\ (x, y)$ is a phased-fingerprint array (*PFA*), which illuminated by the spot array (*SA*). The spot array is generated by the *DG* located at the focal plane of the lens L_1. *DG* is a phase-only grating, which can form a finite uniform-intensity spot array [21,22]. Let $g_D(x_0, y_0)$ denotes the transmittance function of *DG*,

$$g_D\left(x_0, y_0\right) = \sum_{\text{k}} \sum_{l} \exp\left[j\Phi_D(x_0 - kt_x, y_0 - lt_y)\right] \tag{1}$$

where t_x and t_y represent *DG*' s periods. $\Phi_D(x, y)$ denotes the phase in one period.

At the back focal plane of the lens L_1, a $M \times N$ uniform-intensity spot array can be generated. It can be expressed as

$$G_D(u, v) = \sum_{m}^{M} \sum_{n}^{N} G_{mn}\left(u - mT_x, u - nT_y\right) \exp\left(j\phi_{mn}\right) \tag{2}$$

where G_{mn} and ϕ_{mn} represent the amplitude and phase of the Fourier spectrum. T_x and T_y represent periods of the spot array in x and y directions, which are the distance between the center of adjacent spots. So, the pupil $p\ (x, y)$ can be modified by

$$p\,(x, y) = \sum_{m}^{M} \sum_{n}^{N} G_{mn}\left(\frac{x}{\lambda f} - mT_x, \frac{y}{\lambda f} - nT_y\right) e^{j\phi_{mn}} e^{jF_{mn}} \tag{3}$$