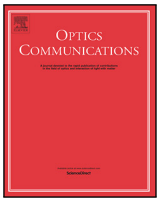
Optics Communications 415 (2018) 56–63

Contents lists available at ScienceDirect

Optics Communications

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



Optical image encryption method based on incoherent imaging and polarized light encoding

Q. Wang [a,b], D. Xiong [a], A. Alfalou [b,*], C. Brosseau [c]

[a] School of Physics and Optoelectronic Engineering, Guangdong University of Technology, Guangzhou, 510006, China
[b] Vision Lab. ISEN Brest L@bISEN, 20 rue Cuirassé Bretagne, CS 42807, 29228 Brest Cedex 2, France
[c] Université de Brest, Lab-STICC, 6 avenue Le Gorgeu, CS 93837, 29238 Brest Cedex 3, France

ARTICLE INFO

Keywords:
Optical information processing
Optical image encryption
DRP
Polarization

ABSTRACT

We propose an incoherent encoding system for image encryption based on a polarized encoding method combined with an incoherent imaging. Incoherent imaging is the core component of this proposal, in which the incoherent point-spread function (PSF) of the imaging system serves as the main key to encode the input intensity distribution thanks to a convolution operation. An array of retarders and polarizers is placed on the input plane of the imaging structure to encrypt the polarized state of light based on Mueller polarization calculus. The proposal makes full use of randomness of polarization parameters and incoherent PSF so that a multidimensional key space is generated to deal with illegal attacks. Mueller polarization calculus and incoherent illumination of imaging structure ensure that only intensity information is manipulated. Another key advantage is that complicated processing and recording related to a complex-valued signal are avoided. The encoded information is just an intensity distribution, which is advantageous for data storage and transition because information expansion accompanying conventional encryption methods is also avoided. The decryption procedure can be performed digitally or using optoelectronic devices. Numerical simulation tests demonstrate the validity of the proposed scheme.

1. Introduction

Over the past two decades, optical image encryption technology has become an extremely active research area, of great importance owing to its inherent ability to make use of multiple parameters and parallel operation [1]. Since the double random phase encryption (DRPE) technique was proposed by Refregier and Javidi [2], much effort has been devoted to searching for new types of encryption methods that can be realized using optical platforms, such as the phase retrieval iterative algorithm [3,4], diffraction imaging [5,6], interference-based methods [7–9] and digital holographic encoding [10–12]. These methods have also been extended to the Fresnel transform [13,14], fractional Fourier [15,16] and gyrator transform domains [17]. However, despite their efficiency and high security level, many of these schemes are sensitive to misalignment and coherent artifact noise because they use coherent illumination [18]. Moreover, some of these mentioned systems involve recording and transition of complex-valued images (ciphertexts and masks) which increase the complexity of the optical implementation. Several earlier attempts based on incoherent illumination have been made to avoid these limitations. For example, Rosen et al. reported a specific design of fluorescent microscope in which Fresnel incoherent holography was used for 3D imaging [19,20]. A scheme based on incoherent digital holography was also proposed to compensate for and measure aberrations [21]. An image encryption system using totally incoherent illumination was suggested by Tajahuerce and coworkers [18]. Recently, Zang et al. presented a simple image encryption system with a spatially illumination light source [22]. This encryption scheme can be regarded as an imaging system where the incoherent point spread function (PSF) serves as decryption key. The PSF is determined by a random phase-only mask (RPM) and geometry of the imaging system. Optical experiments have been conducted to verify the feasibility of this encryption system.

Since Dollfus and coworkers reported their pioneering study of polarization imaging [23], the relationship between polarization and encryption has aroused the interest of researchers because polarization parameters can provide additional degree of freedom to the key design of an encryption system. For example, Mogensen and Gluckstad

---

[*] Corresponding author.
E-mail address: ayman.al-falou@isen-bretagne.fr (A. Alfalou).

https://doi.org/10.1016/j.optcom.2018.01.018
Received 30 September 2017; Received in revised form 28 December 2017; Accepted 10 January 2018
0030-4018/

devised a phase-based encryption system using polarization-sensitive elements [24]. A two-dimensional polarization encoding system using a phase-only spatial light modulator (SLM) was also presented by Davis et al. [25]. Javidi and coworkers developed polarization-encoding input images based on Jones's polarization (complex-valued) calculus and a nonlinear joint transform correlator (JTC) was employed for validation [26]. In another study, a dual image encryption scheme based on the Mueller polarization (real-valued) calculus was developed by Alfalou and Brosseau [27,28]. Compared with Jones's polarization formalism, Mueller formalism of polarization is more advantageous for optical implementation because it involves processing intensity information only. This scheme was also found to be resistant to brute force attacks and video sequence attacks because of the large number of possible key combinations. By applying a phase-truncation technique Rajput et al. presented a modified scheme which can resist known- and chosen-plaintext attacks [29]. Recently, a multiple-image encryption scheme based on the Mueller formalism was also devised by Wang et al. [30]. In spite of this recent progress, polarization encoding methods based on Mueller polarization calculus still encounter many critical issues in practical implementation. For example, in order to introduce randomness in encoding, these schemes need to use an array of micro-polarizers with random distribution of transmission angles. Although a polarizer array significantly contributes to encoding randomness, it can lead to serious technical issues such as alignment and increase of the implementation cost. Increasing the size of each micro-polarizer can alleviate the alignment problem and may be cost-effective, but to the detriment of the security level.

In this study, we present an image encryption system using spatially incoherent polarized light. In this scheme, an incoherent imaging system is integrated with polarization instrumentation to realize an image encryption with high security strength. Polarization encoding and a conventional method based on phase-manipulation are combined to secure information. The incoherent imaging system serves as the core structure of this scheme, in which an RPM and an imaging lens are used to control the PSF key. Due to the spatially incoherent illumination, the imaging system can be considered as a convolution operation between PSF and input intensity, in which complicated manipulation and recording of a complex-valued signal are avoided. In the input and output planes of this imaging system, retarder and polarizer arrays are employed to encode the intensity information of the polarized light. In contrast to the earlier Mueller-calculus based encryption methods [27–30] which use only a single polarizer array, the introduction of the linear retarder array can further strengthen the safety of system. Likewise, a linear retarder characterized by phase shift and fast-axis orientation angle enables us to encode the polarization state with additional polarization parameters. The final recorded ciphertext of this scheme is just a noisy intensity distribution without any requirement for phase information, which is not only helpful to reduce the complexity of recording but also advantageous to ciphertext storage and transition. As is well known, many coherent-optics based encryption methods of real-positive image often result in the increase of the amount of information due to the generation of complex-valued ciphertext [31,32]. Incoherent PSF and the arrays constituted by the micro-polarization instruments provide a rich variety of encoding parameters to increase the key space that protects the secret image from illegal attacks. The ciphertext intensity can be decoded digitally or thanks to an algorithm which is compatible with optoelectronic decryption. By combining incoherent imaging with polarization encoding instruments, we found that the alignment issue of polarization arrays can be alleviated to a certain extent. Numerical simulation tests have been conducted to verify the effectiveness and feasibility of this scheme.

In Section 2, the main procedures of encryption and decryption are described. The validity and performance of the proposed method are checked by numerical simulations in Section 3. Finally, a brief conclusion is presented in Section 4.

2. Basic principle

2.1. Encryption procedures

In this section, we first introduce the encryption procedures using spatially incoherent polarization light in the dual encryption setup shown in Fig. 1. In this setup, two independent narrowband light sources (i.e. LED arrays) with the same peak wavelength λ are employed to generate the two incident light beams L_1 and L_2. Two rotation diffusers are placed immediately after the light sources to ensure that the incident beams are spatially incoherent. Before reaching the input planes, two linear polarizers (Pol_1 and Pol_2) with horizontal transmission orientation are inserted in the light paths to polarize the incident beams. In the input planes of L_1 and L_2, two spatial light modulators, SLM_1 and SLM_2, are placed to display a gray-scale secret image $f(x,y)$ and a random gray-scale key image $k(x,y)$, respectively. The SLMs work in the amplitude modulation mode. The key image will be used as additional key to cover the secret information in the subsequent procedures. To quantitatively describe the polarization encoding, the secret and key images are parameterized into Stokes vectors using the Stokes–Mueller formalism. Because the incident light beams are horizontally polarized, the Stokes vectors of the secret image and the key image can be written as

$$S_f^{(x,y)} = \left[I_f(x,y), I_f(x,y), 0, 0\right]^T \tag{1a}$$

$$S_k^{(x,y)} = \left[I_k(x,y), I_k(x,y), 0, 0\right]^T \tag{1b}$$

where T stands for matrix transpose. The four components of Stokes vector can be measured as $S_0 = I_0 + I_{\pi/2}$, $S_1 = I_0 - I_{\pi/2}$, $S_2 = 2I_{\pi/4} - \left(I_0 - I_{\pi/2}\right)$ and $S_3 = 2I_{\lambda/4,\pi/4} - \left(I_0 - I_{\pi/2}\right)$ where I_0, $I_{\pi/4}, I_{\pi/2}$ denote the measured intensity along the angles, 0, $\pi/4$ and $\pi/2$, respectively. $I_{\lambda/4,\pi/4}$ represents the measured intensity obtained from a polarizer with $\pi/4$ transmission orientation angle and a quarter-wave plate. In our case, $S_{f0} = S_{f1} = I_f(x,y) = |f(x,y)|^2$ and $S_{k0} = S_{k1} = I_k(x,y) = |k(x,y)|^2$ carry the information related to the secret and random key images, respectively. For a horizontally polarized light field, the other Stokes components are zero, i.e. $S_{f2} = S_{f3} = S_{k2} = S_{k3} = 0$. Then, by using a beam splitter (BS), the two polarized beams are combined together based on the incoherent superposition

$$S_1^{(x,y)} = \left[I_f(x,y) + I_k(x,y), I_f(x,y) + I_k(x,y), 0, 0\right]^T. \tag{2}$$

From the above expressions, one finds that the intensity information of the secret image is hidden by the counterpart of the key image. In order to realize the coverage without information exposing, the total energy of key image should be at least 5–6 times higher than the energy of the secret image. After the BS, an array of linear retarders is used to convert the combined signal to new polarization states. The phase shift ϕ and fast axis orientation angle θ of each micro-retarder are randomly selected within the range of $[-\pi, \pi]$. According to the Mueller calculus, the real elements of the Mueller matrix characterize the interaction of the light with the polarization element [33]. The Mueller matrix of the retarder array reads as Eq. (3) given in Box I.

In the interaction plane, the cross section of light field is evenly divided into many sub-zones, i.e. 2 × 2-pixels region. Each sub-zone of the light beam acts as a retarder with random polarization parameters. The interaction can be described as

$$\begin{aligned} S_2^{(x,y)} &= M_{\mathrm{ret}}^{(x,y)} S_1^{(x,y)} = \left[I_f(x,y) + I_k(x,y)\right] \\ &\times \begin{pmatrix} 1 \\ \cos^2\left(2\theta^{(x,y)}\right) + \cos\phi^{(x,y)} \sin^2\left(2\theta^{(x,y)}\right) \\ \frac{1}{2}\sin\left(4\theta^{(x,y)}\right) - \frac{1}{2}\sin\left(4\theta^{(x,y)}\right)\cos\phi^{(x,y)} \\ \sin\left(2\theta^{(x,y)}\right)\sin\phi^{(x,y)} \end{pmatrix}, \end{aligned} \tag{4}$$