Optics and Lasers in Engineering 112 (2019) 151–161

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Optical image authentication scheme using dual polarization decoding configuration

Qu Wang [a,b], Deping Xiong [a], Ayman Alfalou [b,*], Christian 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] Lab-STICC, Université de Brest, 6 avenue Le Gorgeu, CS 93837, 29238 Brest Cedex 3, France

ARTICLE INFO

Keywords:
Optical authentication
Polarization encoding
Sparse encoding

ABSTRACT

We report on an optical image authentication scheme using dual polarization decoding configuration. We examine a sparse encoding method based on image division to process the original image. Next, the sparse original image is separated into two noise-like structure images with random polarization parameters which are digitally encoded. During the decoding stage, the encoded images are sent into a dual polarization decoding configuration where a pixelated polarizer with sparse distribution of transmission angle is employed for image recovering. The proposed scheme avoids complicated recording of complex information and resolves the alignment problem of previous polarization encoding methods. Then we examine numerical simulations to show that the proposed scheme is well suited to recover the original image when decryption keys are correctly used. We find evidence that the verification system exhibits high robustness and flexibility against attacks and interference. We expect that these results might be useful for polarization-encoding based optical verification.

1. Introduction

Over the past two decades, the development of optical information security schemes has been an extremely active research area due to their remarkable advantages, such as built-in parallel processing, multidimensional capability and multiple parameters [1,2]. Much effort has been devoted to searching for new types of encryption methods that can be implemented with an optical setup, such as the phase retrieval iterative algorithm [3,4], diffraction imaging [5,6], interference-based methods [7–9] and digital holographic encoding [10,11]. These methods exhibit high security level and processing efficiency. However, many of these encryption schemes remain difficult to be optically implemented. For example, coherent illumination of these encryption systems often leads to high sensitivity to the misalignment and coherent artifact noise [12]. Additionally, several schemes involve complicated holographic recording and/or computational times for using these schemes are usually quite long. To circumvent these technical problems, several schemes using totally incoherent illumination have been reported [13–16], in which only intensity information is recorded and manipulated. In recent years, some researchers attempted to overcome these limitations by combining polarization encoding and incoherent illumination [17–21]. In a recent study, Alfalou and Brosseau developed a dual image encryption scheme based on Mueller polarization (real-valued) calculus of polarization states [17]. Compared with polarization encoding methods based on Jones's formalism and coherent optics [22], Alfalou and Brosseau scheme is more suitable for optical realization because Mueller formalism only needs to manipulate intensity distribution without any phase information to be examined. Moreover, using polarization parameters is helpful to strengthen the resistance against brute-force and video sequence attacks. An asymmetric modified scheme using phase-truncation technique has been proposed by Rajput and coworkers to improve the robustness against chosen-plaintext attack and known-plaintext attack [19]. In another study, Wang and coworkers examined a multiple image encryption by combing Mueller formalism and optical interference structure [20]. However, these schemes based on Mueller polarization calculus still encounter technical problem. For example, the main encoding instrument is a pixelated polarizer (or an array of micro-polarizers) with a random distribution of transmission angle. In practice, aligning high density micro-polarizers with precision is a technical challenge. Increasing the size of each micro-polarizer (or reducing the density of micro-polarizers in the array) can resolve the alignment problem, but it inevitably weakens security strength. In addition, above schemes based on Muller formalism are still confined in the field of conventional image encryption. By now, we cannot find any report on application of such schemes in image authentication yet.

To enhance the encoding efficiency and accelerate transmission of the encrypted information, some optical authentication schemes have been proposed [23–31]. Contrasting with conventional optical encryption systems, these schemes do not reveal any visual information as-

* Corresponding author.

https://doi.org/10.1016/j.optlaseng.2018.09.008
Received 9 July 2018; Received in revised form 29 August 2018; Accepted 10 September 2018
Available online 25 September 2018

sociated with the original image during the decryption period, which guarantees security against chosen plaintext and plaintext attacks. There is a variety of encryption techniques for realizing invisibility of original information in the decrypted image, such as photon-counting imaging (PCI) [23,24,26,27], amplitude field random sampling and phase-information multiplexing [29]. To evaluate whether the decryption is successfully performed, several optical correlation methods are employed to recognize secret information hidden in the noise fluctuation [32–34]. A prominent peak in the correlation plane suggests that decryption has been carried out with correct keys. In a recent work, Chen examined an authentication system where the information of ciphertext is compressed by binary phase rather than earlier sparse encoding method [31]. Recently, a 3D optical correlation method has also been developed by Chen for image authentication [35]. A multiple-image authentication method based on sparse phase encoding has also been proposed by Wang and coworkers in which a cascaded phase-only filtering structure, instead of correlation method, is used for final verification [30].

In this work, we apply an optical authentication algorithm using dual decryption configuration and sparse decoding of pixelated polarizer. Our approach involves two steps- the original image is first processed with a sparse encoding method based on random division of image, and then the sparse original image is digitally encoded into two noise-like encrypted images by using random decomposition operation and a random computer-generated distribution of polarization angle. During the decryption step, the encrypted images are sent into an optoelectronic hybrid platform using incoherent polarized light. This polarization optical system is similar to the dual encryption configuration described in Ref. [17], but in this study it serves as a decoding platform. Another innovation of this approach is that a pixelated polarizer with sparse distribution of transmission angle is introduced in the setup to perform the final decoding. This eventually ensures that secret information on specified positions is reserved. More importantly, the sparse distribution of transmission angle is also useful to relax the strict alignment constraint of pixelated polarizer. Finally, by connecting to a remote database, a nonlinear correlation algorithm is applied to authenticate decoded images without information disclosure. To the best of our knowledge, this is the first work where image authentication task is performed by a dual optical configuration using incoherent polarization light. Incoherent illumination avoids complicate recording of complex-valued information while polarization light introduces more random parameters to improve the security strength. Moreover, our work further enhances feasibility of Mueller-formalism-based polarization encoding schemes in practical application because of the relaxation of alignment problem.

The paper is organized as follows: after this introduction, Section 2 reviews the encoding principle. Section 3 discusses the decoding procedure of this algorithm, while Section 4 shows simulation results and performance analysis. Finally, Section 5 presents the conclusions of the work.

2. Encoding principle

Now, we review the encoding process. Let $f(x, y)$ denotes a normalized gray-scale image to be encoded. Firstly, the original image is processed with a sparse encoding algorithm based on image division strategy. We divide the image plane of $f(x, y)$ into a number of rectangular blocks with $M \times N$ pixels (e.g. 4×4 pixels, as shown in Fig. 1, $B_1, B_2, \cdots$). In each block, we select a single pixel position (x_i, y_i) where the gray-scale value $f(x_i, y_i)$ is closest to the median (or average) value of $f(x, y)$ within the block B_i. This selecting rule ensures that different distributions of the sparse coordinates can be produced for different original images. According to these assigned coordinates, a binary mask $M_b(x, y)$ and a random distribution $I_1(x, y)$ can be written as

$$M_b(x,y) = \begin{cases} 1 & (x,y) = (x_i, y_i) \\ 0 & (x,y) \neq (x_i, y_i) \end{cases}, \tag{1}$$

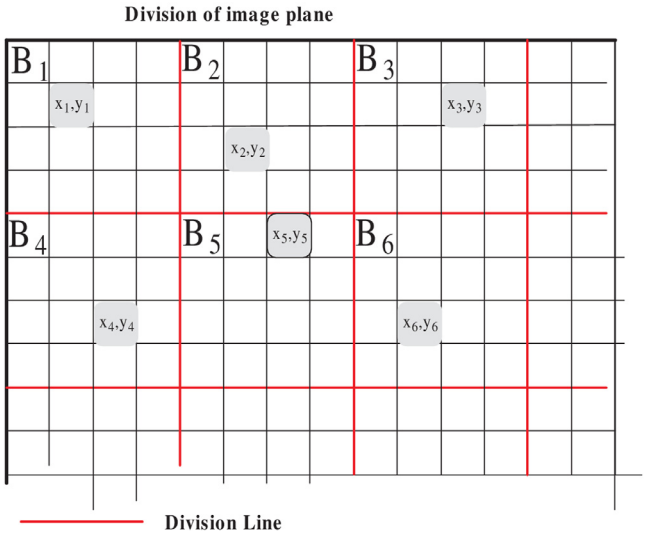

Fig. 1.. Image division and selection of sparse positions.

$$I_1(x,y) = \begin{cases} 0 & (x,y) = (x_i, y_i) \\ \text{random number within } [0,1] & (x,y) \neq (x_i, y_i) \end{cases}, \tag{2}$$

By performing the following computation, a sparse original image is then given by

$$f'(x,y) = f(x,y) M_b(x,y) + I_1(x,y), \tag{3}$$

which only retains the image information on the assigned positions (x_i, y_i) $(i = 1, 2, 3, \ldots)$ while for another region $((x, y) \neq (x_i, y_i))$ it is filled with noise interference. By adjusting the size and shape of division block, the distribution density of sparse positions in the image plane can be flexibly controlled. Division scheme of image plane and selecting rule of sparse coordinates can be considered as additional keys which will be used to fabricate a pixelated polarizer during the decryption stage. Let $S_{f'}(x, y) = |f'(x, y)|^2$ represents the light intensity distribution of the sparse original image when it is illuminated by an incoherent light source. The intensity distribution can be written as

$$E(x,y) = \frac{4 S_{f'}(x,y)}{1 + \cos\left[2\psi_{\text{rand}}(x,y)\right]}, \tag{4}$$

where $\psi_{\text{rand}}(x, y)$ is a computer-generated random angle distribution within the range of $[-\pi/4, \pi/4]$. Next, this distribution is decomposed into two noise-like distributions as

$$\begin{aligned} E_1(x,y) &= \tfrac{E(x,y)}{2}\left[1 + I_2(x,y)\right], \\ E_2(x,y) &= \tfrac{E(x,y)}{2}\left[1 - I_2(x,y)\right], \end{aligned} \tag{5}$$

where $I_2(x, y)$ denotes a random computer-generated distribution in the [0, 1] range. Each square root of these noisy distributions $\sqrt{E_1(x,y)}$ and $\sqrt{E_2(x,y)}$ will serve to encode the image. We note that the multiplication and additive random factors found in Eqs. (4) and (5) can further strengthen the randomness of the encoded images. For safety reason, the encoded images are sent to different authenticated users.

3. Decoding and authentication principles

Next we examine the hybrid optoelectronic setup used for recovering the original image (Fig. 2). Two independent incoherent light sources of the same type with equal optical power are used to illuminate the input planes where two spatial light modulator (SLMs) are placed to display the sparse encoded images $\sqrt{E_1(x,y)}$ and $\sqrt{E_2(x,y)}$, respectively. For simplicity, the input illumination beams are assumed to be non-polarized. In the Mueller-Stokes formalism, the polarized states of the light fields immediately after the SLMs can be described by the Stokes