Optics Communications 417 (2018) 30–36

Contents lists available at ScienceDirect

Optics Communications

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

Optical image security using Stokes polarimetry of spatially variant polarized beam

Areeba Fatima, Naveen K. Nishchal *

Department of Physics, Indian Institute of Technology Patna, Bihta, Patna-801 106, Bihar, India

ARTICLE INFO

Keywords:
Optical security and encryption
Phase retrieval
Polarization
Fourier optics and signal processing

ABSTRACT

We propose a novel security scheme that uses vector beam characterized by the spatially variant polarization distribution. A vector beam is so generated that its helical components carry tailored phases corresponding to the image/images that is/are to be encrypted. The tailoring of phase has been done by employing the modified Gerchberg–Saxton algorithm for phase retrieval. Stokes parameters for the final vector beam is evaluated and is used to construct the ciphertext and one of the keys. The advantage of the proposed scheme is that it generates real ciphertext and keys which are easier to transmit and store than complex quantities. Moreover, the known plaintext attack is not applicable to this system. As a proof-of-concept, simulation results have been presented for securing single and double gray-scale images.

1. Introduction

Study of optical methods to secure information has found widespread interest among the researchers. The double random phase encoding (DRPE) scheme gave a convenient method to optically encrypt information to stationary white noise [1]. Since then, various other features of light have been explored for establishing a robust optical cryptosystem. Optical transformations such as the Fourier transform, gyrator transform, Fresnel transform, fractional Fourier transform etc. were used as tools to perform the encryption and decryption [2–4]. As vulnerabilities of the DRPE system to various attacks were established due to its inherent linearity [5–7], newer optical cryptosystems were introduced which were asymmetric systems. These asymmetric systems included phase truncation based Fourier transform (PTFT) techniques or the equal modulus decomposition techniques (EMD) [8–15]. Though these asymmetric cryptosystems provided resistance against the known-plaintext attack, yet it was soon found that they were vulnerable to the specific attack [16,17]. Hence, it is always an effort to find various schemes that gives a strong optical cryptosystem. Moreover, various studies have been reported that propose double image or multiple image encryption [18–22]. Apart from robustness, the research trends also show studies that try to find newer aspects of light that could be used in encoding information. In this regard, polarization is another aspect of light that has been extensively used to construct efficient cryptosystems and authentication schemes [23–28]. Studies using the Stokes formalism to encrypt information have been widely reported as it uses the intensity information and, therefore, it is easier to implement [23].

As compared to the mainstream polarization techniques, the use of spatially variant polarization (or vector beams) is a lesser studied tool for optical encryption [29–31]. A geometrical phase generated by space variant polarization condition due to a subwavelength grating has been employed to encrypt information [29]. In another work, Maluenda et al. developed a polarimetric measurement based encryption and verification scheme that used non uniform state of polarization (SOP) distribution [31]. The encryption setup was based on the Mach–Zehnder interferometer and it processed the transverse components of the beams in the two arms of the interferometer.

In general, vector beams are characterized by spatially varying SOP across the optical beam cross-section [32]. This property of vector beams has led to new features that enhance the range of performances of optical systems. For example, the vector beams can give tight focal spots which in turn have enabled high resolution imaging, optical trapping and plasmonic focusing. Vector beams have found applications in various other fields like atmospheric sensing and singular optics, to name a few [32]. Several methods have been proposed to generate different vector beams with non-uniform polarization. These methods involve interferometric arrangement or optical set-ups using liquid crystal displays [33–35]. In one of the works, a Mach–Zehnder interferometer set up was used to generate optical beam with non-uniform state of polarization [33]. Recently, a method to generate vector beams with tailored phase and polarization has been proposed [34,36]. The incident beam which would give the desired phase and polarization was determined using iterative Gerchberg–Saxton (GS) algorithm [37].

* Corresponding author.
E-mail address: nkn@iitp.ac.in (N.K. Nishchal).

https://doi.org/10.1016/j.optcom.2018.02.030
Received 26 December 2017; Received in revised form 22 January 2018; Accepted 12 February 2018

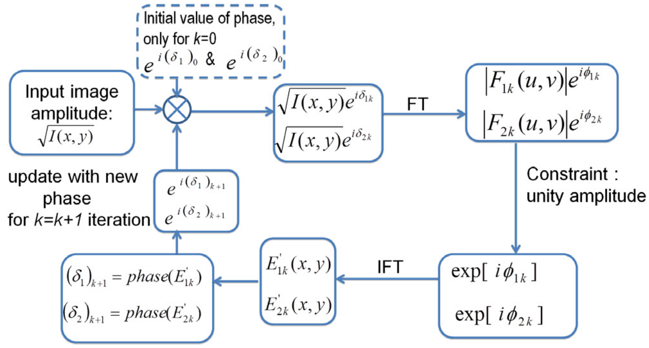

Fig. 1. Flowchart for modified GS Algorithm used to evaluate phase-only functions.

Refs. [29–31] show that space variant polarization distribution can be a source of encryption keys. In this work, we propose single and double optical image encryption scheme based on vector beams which have non-uniform arbitrary polarization distribution. The proposed scheme utilizes such a vector beam generator reported by Chen et al. [34]. Our motive is to study an optical system that generates vector beams carrying the encoded phase corresponding to the plaintexts. The phase of the vector beam carries the information of the plaintexts. Finally, the Stokes vector formalism for polarized light is used to generate the ciphertext and one of the keys. The encryption can be done optically, while the decryption can be done numerically.

The paper is organized as follows: in Section 2, we describe the encryption scheme for single image, elaborating the encryption as well as the decryption principle. In Section 3, the scheme is extended for double image encryption. The proposed method is validated by numerical simulations. Section 4 provides cryptanalysis of the encryption technique.

2. Optical security scheme for single image

2.1. Encryption principle

In this section, we discuss the principle of the proposed scheme for securing a gray-scale image. The scheme is based on obtaining a vector beam that can carry the plaintext information in its phase. The entire scheme consists of three major steps: (1) generation of two phase-only functions corresponding to the plaintext, (2) generation of vector beam carrying phase-only functions of step 1 as its phase, and (3) recording of Stokes parameters of the vector beam. These steps are described in detail in the following sub-sections.

2.1.1. Generation of phase-only functions

The first step involves the numerical evaluation of two different phase-only functions, namely, $\exp(i\phi_1)$ and $\exp(i\phi_2)$ corresponding to the plaintext. Phase-only functions corresponding to an intensity image $I(x,y)$ are complex quantities with amplitude as unity. When subjected to the inverse Fourier transform, they yield complex functions which have original intensity image $I(x, y)$ as their amplitude. To generate such functions, the iterative numerical method of modified GS algorithm (MGSA) [37] is used. Fig. 1 shows the flowchart depicting this iterative phase retrieval method. The steps shown in flowchart are discussed below. Here, k represents the iteration number.

Step 1: Two different random distribution functions $\delta_1(x,y)$ and $\delta_2(x,y)$, both lying in the interval $[0, 2\pi]$ are used to construct two different phases, $\exp[i\delta_1(x,y)]$ and $\exp[i\delta_2(x,y)]$, to initiate the iterative process (i.e. for the case $k = 0$). These phases are multiplied with the amplitude of the plaintext function $\sqrt{I(x,y)}$. For the kth iteration it can be written as

$$E_{1k}(x,y) = \sqrt{I(x,y)}\exp[i\delta_{1k}(x,y)] \tag{1}$$

$$E_{2k}(x,y) = \sqrt{I(x,y)}\exp[i\delta_{2k}(x,y)]. \tag{2}$$

Step 2: The above two quantities, Eqs. (1)–(2) are Fourier transformed.

$$F_{1k}(u,v) = \iint E_{1k}(x,y)\exp[-i2\pi(ux+vy)]dxdy = |F_{1k}(u,v)|\exp[i\phi_{1k}(u,v)] \tag{3}$$

$$F_{2k}(u,v) = \iint E_{2k}(x,y)\exp[-i2\pi(ux+vy)]dxdy = |F_{2k}(u,v)|\exp[i\phi_{2k}(u,v)]. \tag{4}$$

Step 3: Our objective is to obtain phase-only functions in the focal domain. Hence, the amplitudes of the quantities obtained in Eqs. (3)–(4) are replaced with unity:

$$F'_{1k}(u,v) = \exp[i\phi_{1k}(u,v)] \tag{5}$$

$$F'_{2k}(u,v) = \exp[i\phi_{2k}(u,v)]. \tag{6}$$

Step 4: The above quantities are inverse Fourier transformed (IFT).

$$E'_{1k}(x,y) = IFT\left\{F'_{1k}(u,v)\right\} \tag{7}$$

$$E'_{2k}(x,y) = IFT\left\{F'_{2k}(u,v)\right\}. \tag{8}$$

The phase of the obtained quantity is retained while the amplitude is substituted with the input image amplitude $\sqrt{I(x,y)}$, to evaluate the next iteration values:

$$(\delta_1)_{k+1} = phase\left(E'_{1k}\right) \tag{9a}$$

$$(\delta_2)_{k+1} = phase\left(E'_{2k}\right) \tag{9b}$$

$$[E_{1k}(x,y)]_{k+1} = \sqrt{I(x,y)}\exp[i(\delta_1(x,y))_{k+1}] \tag{10}$$

$$[E_{2k}(x,y)]_{k+1} = \sqrt{I(x,y)}\exp[i(\delta_2(x,y))_{k+1}]. \tag{11}$$

The iterations continue till the mean square error (MSE) between the absolute values of $E_1(x, y)$ of two consecutive iterations reach a predefined minima. This process is repeated for the absolute values of $E_2(x, y)$. At the end of the iterative process, we obtain phase-only functions, $\exp(i\phi_1)$ and $\exp(i\phi_2)$ which, though different valued, give the same input image intensity on being inverse Fourier transformed.

2.1.2. Generation of vector beam carrying phase-only functions as its phase

The aim of this second step is to generate a spatially variant polarization distribution beam which would carry the evaluated phase-only function $\exp(i\phi_1)$ and $\exp(i\phi_2)$ as its phase. This can be achieved by using a vector beam generator based on the use of two-dimensional (2D) holographic grating (HG) displayed on a spatial light modulator (SLM) [34]. Holograms prove to be a convenient means to incorporate a spatially dependent phase distribution. In this regard, a 2D HG can be understood as a combination of two one-dimensional gratings, aligned along the x- and the y-axes, respectively, each with their own phase distributions [38]. In the proposed scheme, these additional phase distributions of the HG is defined by ϕ_1 and ϕ_2 obtained from phase-only functions, $\exp(i\phi_1)$ and $\exp(i\phi_2)$ explained in Section 2.1.1. In this case then, the amplitude transmittance $t(x, y)$ of a 2D sinusoidal amplitude grating can be given as [34]:

$$t(x,y) = 0.5 + m\left[\cos(2\pi f_0 x + \phi_1(x,y)) + \cos(2\pi f_0 y + \phi_2(x,y))\right]/4. \tag{12}$$