Optik 124 (2013) 2363–2367

Contents lists available at SciVerse ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Phase mask generation for DRPE method using chaos theory and hash function

Motahareh Taheri, Saeed Mozaffari*

Electrical and Computer Engineering Department, Semnan University, Semnan, Iran

ARTICLE INFO

Article history:
Received 12 March 2012
Accepted 2 July 2012

Keywords:
Double random phase encoding (DRPE)
Hash function
SHA-512 algorithm
Chaos theory
Two-dimensional coupled logistic map,
phase mask generation

ABSTRACT

The aim of this paper is to increase security of double random phase encoding (DRPE) method using chaos theory and hash function for phase mask generation. DRPE encodes the input image by the use of two keys which are random phase masks. Having these keys, the original image can be easily obtained with the reverse process, called decoding. To enhance the system's security, instead of sending random phase masks, initial conditions and parameter of two dimensional coupled logistic map and SHA-512 algorithm are transferred to the authorized user through a secure channel. The proposed method not only obviates the need for sending large phase masks, but it considerably increases DRPE security. Experimental results and computer simulation demonstrate promising results of the proposed technique.

1. Introduction

With the prevalence of internet, individuals can easily share their resources such as documents, videos, voices, and images on the web. However, this torrent of information should be sheltered from malicious activities. Data encryption has emerged as a practical technique for data protection. Among different methods, optical techniques play a vital role in image security systems [1–4]. This is mainly due to their high security level and fast encryption process. Double random phase encoding (DRPE) is one the most common optical-based methods which encodes the input image with two random phase masks (PM1 and PM2), located in the input and in the spatial frequency planes within 4f optical system [1].

Fig. 1 shows the DRPE encoding process. First, the input image, $f(x,y)$,is modulated by a random phase mask, $\theta(x,y)$, obtained by Eq. (1).

$$\theta(x, y) = \exp\ [i2\pi\theta_0(x, y)] \tag{1}$$

After passing the first lens, Fourier transform of the modulated image is obtained. Then, the result image is modulated by the second random phase mask, expresed by:

$$\varphi(x, y) = \exp\ [i2\pi\varphi_0(u, v)] \tag{2}$$

In Eqs. (1) and (2), $\theta_0(x,y)$ and $\varphi_0(x,y)$ are the two phase-functions inserted in the input plane and Fourier plane, respectively their values are randomly distributed over interval $[0,2\pi]$. The second lens performs the inverse Fourier transform and the encoded image, $g(x,y)$, is resulted.

$$g(x, y) = \mathrm{FT}^{-1}\{\mathrm{FT}\{f(x, y) \cdot \theta(x, y)\} \cdot \varphi(u, v)\} \tag{3}$$

To reconstruct the input image, the following process should be performed.

$$f(x, y) = \mathrm{FT}^{-1}\{\mathrm{FT}\{g(x, y) \cdot \exp\ [-i2\pi\varphi_0(u, v)]\} \cdot \exp\ [-i2\pi\theta_0(x, y)] \tag{4}$$

The decryption procedure is similar to the encryption but in the reversed order. DRPE needs the random phase masks, called private keys, to retrieve the original image. Most of the previous efforts focused on phase mask generation [5,6], efficient inserting phase masks in a cover image [7–11], and making encryption system more secure [12–15].

Sending large phase masks (the same size as the input image), not only need huge cover image but considerably reduces DRPE's security. To get around this problem, several methods have been proposed. In the first attempt, a cascaded iterative Fourier transform (CIFT) algorithm is presented [5]. Two phase masks are concurrently generated from the input image through an iterative method. This method does not need encoded image transmission and instead, the two encoding keys are inserted into the host image. In the receiver, the two keys are extracted from the host image and the input image is reconstructed. In the second method, two masks are generated by an affine transformation operation through a pseudo-random pattern generated from a source image. The masks depend on the affine transformation parameters and the iteration number that control theirs randomness. Affine transformation is implemented by using reflection, translation,

* Corresponding author.
E-mail addresses: taheri@semnan.ac.ir (M. Taheri), mozaffari@semnan.ac.ir (S. Mozaffari).

0030-4026/$ – see front matter © 2012 Published by Elsevier GmbH.
http://dx.doi.org/10.1016/j.ijleo.2012.07.050

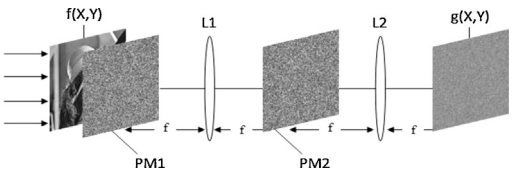

Fig. 1. Double random phase encoding process.

rotation, shearing and scaling operations. Rather than sending the encrypting mask, source image and 18 parameters which indicate the affine transforms are sent through a secure channel [6].

In this paper, a new technique based on chaos theory and hash function has been proposed to generate the phase masks and enhance the security of the conventional DRPE system. Instead of sending the phase masks to the authorizer user, the set of key elements that generated phase masks are transmitted through a secure channel. Without having these keys, it is almost impossible for an unauthorized person to reconstruct the original image.

The paper is organized as follows. The proposed algorithm is presented in Section 2. Experimental results are given in Section 3. Finally, some conclusions are presented in Section 4.

2. Propose method

As mentioned before, DRPE algorithm needs two random phase masks located at input plane (PM1) and Fourier plane (PM2). In this paper, these two random phase masks are generated by chaos method and Hash function to increase the system's security. Rather than sending the phase masks to the authorizer user, the set of passwords and parameters that leads to construction of the phase masks are transmitted. Compared to previous methods, parameters which are needed for phase generation are much less. Fig. 2 shows overview of the proposed phase mask generation approach. With the help of an arbitrary password, Hash algorithm produces a semi-random image which is used as PM1. The obtained phase mask is then utilized by the second stage, chaos block, and the second phase mask, PM2, is generated.

2.1. Hash function

Hash algorithms can be classified into following subsets: SHA-1, SHA-256, SHA-384, and SHA-512 [16]. All of them are iterative and one-way that process a message to produce a condensed representation, called message digest. Any change to the message results in a different message digest. Hash algorithm needs preprocessing and hash computation steps. Preprocessing involves padding a message, parsing the padded message into m-bit blocks, and setting initialization values to be used in the hash computation. The hash computation generates a message schedule from the padded message and uses it, along with functions, constants, and word operations to iteratively generate a series of hash values. The final hash value generated by the hash computation is used to determine the message digest.

The above algorithms differ in the security level and number of bits that are provided for the data being hashed. The algorithm

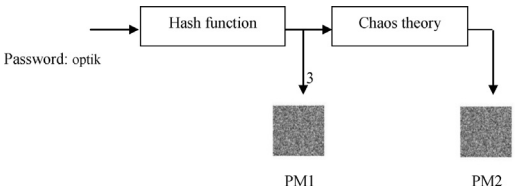

Fig. 2. Overview of the proposed phase masks generation.

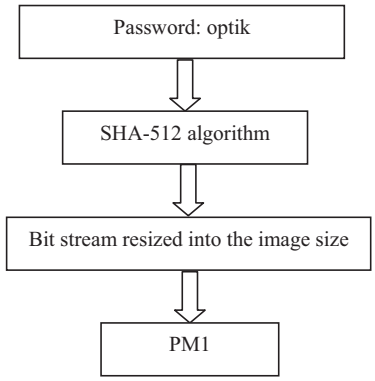

Fig. 3. The process of first mask generation.

uses the strength of a 1D hash function algorithm, namely SHA-2, and makes a 2D mask for DRPE image encryption. A hash function (h) converts an arbitrary large domain (x) into an output in a fixed small range [17]. Hash function should satisfy three features:

(1) Is not reversible.
(2) Input information can not be extracted from out put information.
(3) Hard to find collisions.

According to property 1, using hash functions provides high security. Property 2 and 3 ensure input sensitivity. The SHA-2 standard surrogates the existing SHA-1 with adding three new hash functions, SHA-2(256), SHA- 2(384), and SHA-2(512), for computing a message digest [17], security of these algorithms are different. Among them, SHA-512 has the highest security. In this paper, the hash string is converted into a matrix form with the size of input image and used as the PM1 (Fig. 3).

2.2. Chaos function

Chaos functions have been used mainly to develop the mathematical models of non-linear systems. Several interesting properties have been reported for chaos function. Being sensitive to the initial conditions makes chaos function proper for authentication applications. Two-dimensional coupled logistic map [18] has been used in this paper to generate second phase mask needed for DRPE. Two-dimensional coupled logistic map is described as follows [18]:

$$x_{n+1} = \mu_1 x_n[1 - x_n] + \gamma_1 y_n^2 \tag{5}$$

$$y_{n+1} = \mu_2 y_n[1 - y_n] + \gamma_{2(1)x_n^2 + x_n y_n} \tag{6}$$

$$n = 0, 1, 2, 3, \ldots, N \times N, \quad 0.15 < \gamma_1 < 0.21$$

$$0.13 < \gamma_2 < 0.15, 2.75 < \mu_1 < 3.14$$

$$2.75 < \mu_2 < 3.45$$

where $N \times N$ is size of the input image.

The initial values of x_0, y_0 and the parameters μ_1, μ_2 are used as the keys in this research. Chaos function needs two stages: diffusion and substitution. In the diffusion stage, the pixel values are modified sequentially so that a small variation in one pixel scattered to almost all pixels in the whole image. In substitution stage, interleaving algorithm is employed and image pixels are permuted secretly, without any changes in their values.

Details of random image generation by chaos function are described as follows: