Optics and Lasers in Engineering ■ (■■■■) ■■■–■■■

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Single-random-phase holographic encryption of images

P.W.M. Tsang

Department of Electronic Engineering, City University of Hong Kong, Hong Kong

ARTICLE INFO

Article history:
Received 11 November 2015
Received in revised form
4 January 2016
Accepted 18 January 2016

Keywords:
Holographic encryption
Double-random-phase encryption
Bi-directional error diffusion
Single-random-phase encryption

ABSTRACT

In this paper, a method is proposed for encrypting an optical image onto a phase-only hologram, utilizing a single random phase mask as the private encryption key. The encryption process can be divided into 3 stages. First the source image to be encrypted is scaled in size, and pasted onto an arbitrary position in a larger global image. The remaining areas of the global image that are not occupied by the source image could be filled with randomly generated contents. As such, the global image as a whole is very different from the source image, but at the same time the visual quality of the source image is preserved. Second, a digital Fresnel hologram is generated from the new image, and converted into a phase-only hologram based on bi-directional error diffusion. In the final stage, a fixed random phase mask is added to the phase-only hologram as the private encryption key. In the decryption process, the global image together with the source image it contained, can be reconstructed from the phase-only hologram if it is overlaid with the correct decryption key. The proposed method is highly resistant to different forms of Plain-Text-Attacks, which are commonly used to deduce the encryption key in existing holographic encryption process. In addition, both the encryption and the decryption processes are simple and easy to implement.

1. Introduction

Image encryption has been an area of immense interest for many decades, as it protects pictorial contents that are dedicated to a targeted community of illegitimate viewers. The technology has found numerous important applications in the consumer, industrial, commercial, communication, and military sectors. Amongst different methods, a simple way of encrypting an image is through private key encryption as shown in Fig. 1.

In the encoder, a source image is converted into a new form (generally referred to as the ciphertext) with the incorporation of a secret encryption key *K*. In the decoder, the ciphertext would be reverted to the source image if the correct secret key is input. Failure of an image encryption can lead to serious monetary loss and security breach. Research on developing sophisticated image encryption methods has been conducted vigorously for many years.

The emergence of optics and digital holography has instigated a new direction in image encryption known as holographic or optical encryption. Briefly, a source image is converted into a hologram and encrypted into a cipertext. A hologram image comprises of high frequency fringe patterns which bears little clue on the image it represents, and it is often more difficult to be attacked than the encryption of the source image directly.

The most effective holographic encryption techniques developed to date, are mostly based on the double-random-phase encryption (DRPE) framework initiated from the pioneering work in [1]. Subsequently, quite a number of enhancement on the parent method (for example using QR Code [2]) had been developed as in [3–6]. However, as pointed out in [7,7–11], the DRPE method is inherently susceptible to plaintext attacks, if the cryptanalyst can access the encoder and generate the ciphertext image of selected source images. Attempts to decrease the vulnerability of the DRPE framework have been conducted as reported in [12–16].

The effectiveness of the DRPE frameworks developed to date is unquestionable. However, to enhance the robustness of these methods, the complexity of the optical setups and the computation involved also increase. The objective of this paper is to explore the feasibility of a low complexity random phase encryption method.

2. The proposed single-random-phase-encryption (SRPE) method

This paper reports a holographic encryption method which is referred as single-random-phase encryption (SRPE). The proposed

E-mail address: eewmtsan@cityu.edu.hk

http://dx.doi.org/10.1016/j.optlaseng.2016.01.017
0143-8166/

method is inspired by the DRPE technique. Essentially, the research involves simplifying the architectures of the encryption and the decryption processes by adopting a single random phase mask as the encryption key. The simplification is achieved without jeopardizing the security of the encryption process, but by distorting the source image in a way that is perceptually acceptable in practice. Due to the distortion of the source image, the cryptanalyst will have no knowledge on what is being encrypted, and hence cannot identify the relationship between the ciphertext hologram and the source image. It also increases the difficulty in deducing the encryption key through large scale chosen plaintext attack. The proposed method can be divided into 3 stages as illustrated in Fig. 2, and explained as follows.

2.1. Stage 1: converting the source image into a global image

For better illustration of the proposed method, we assuming that the source is a two dimensional planar image $I(x,y)$ that is parallel to the hologram, where x is the horizontal, and y is the vertical discrete co-ordinate axis. A larger image $G(x,y)$ (hereafter referred as the global image), with a size that is larger than the source image is generated and will be taken as the input to the encoder. To start with, the length and width of the source image are resized by scaling factors s_x and s_y, respectively, and translated to a random position on $G(x,y)$. The area not being occupied by the source image will be filled with random contents (e.g. text characters, shapes, other images). It is mandatory that the larger image $G(x,y)$ must be composed inside the encoder, so that the operator of the encoder will have absolutely no knowledge on what is actually being encrypted. Mathematically, $G(x,y)$ is given by

$$G(x,y) = I(s_x x + T_x, s_y y + T_y) \cup P, \tag{1}$$

where T_x and T_y are the translation along the T_x and the T_y directions respectively, and P represents the added random content. As an example, the source image in Fig. 3(a) is converted to a larger image in Fig. 3(b). It can be envisaged that the source image will be subject to translation and scaling, as well as insertion of additional content in the conversion process. Such kind of simple geometric changes on images are seldom regarded as distortion, as they are commonly imposed by the display monitors and the viewing position of the observer. The inserted contents enrich the scene with extra information, but they do not contaminate the source image. For example, it is rather common that sub-titles, identity icons of the source or the content provider, or advertisement banners are posted onto web pages and video contents. However, incorporating the above changes to the source image will result in a global image that is significantly different from the source image in both spatial and spectral domains.

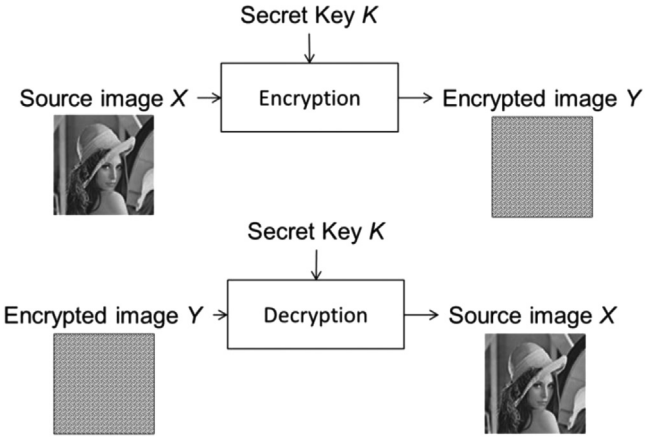


Fig. 1. Concept of encryption and decryption.

2.2. Stage 2: generation of the global phase-only hologram

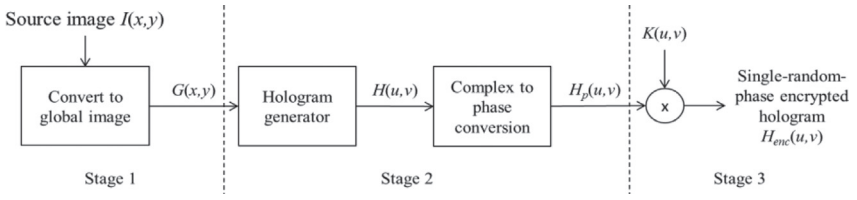
The global image is first converted into a complex Fresnel hologram $H(u,v)$, which is referred to as the global hologram, as given by [17]

$$H(u,v) = \sum_{x=-X/2}^{X/2-1} \sum_{y=-Y/2}^{Y/2-1} G(x,y) \exp\left[\frac{i2\pi}{\lambda} r_{x;y;u;v}\right], \tag{2}$$

where λ is the wavelength of the optical beam. $r_{x;y;u;v}$ is the distance from a point at (x,y) on the global image, to a point (u,v) on the hologram. The number of columns and rows of the image (assumed to be identical to the hologram) are given by X and Y, respectively. Suppose the axial distance between the global image and the global hologram is denoted by z, and δ is the sampling interval which is assumed to be identical along the horizontal and the vertical directions, represented as:

$$r_{x;y;u;v} = \sqrt{(x-u)^2\delta^2 + (y-v)^2\delta^2 + z^2} \tag{3}$$

Next, the complex global hologram is converted into a phase-only global hologram $H_p(u,v)$ based on the bi-directional error method reported in [18]. As the detail has been provided in the article, only a brief outline of the method is described as follows. The hologram is processed from the bottom to the top row. Along the even and the odd rows, pixels are scanned from left-to-right, and right-to-left directions. The magnitude of each scanned pixel is set to unity (transparent), while its phase remains intact, as



Stage 1: Convert the source image $I(x,y)$ into a global image $G(x,y)$.
Stage 2: Convert the global image into a global phase-only hologram $H_p(u,v)$.
Stage 3: Adding a random phase mask $K(u,v)$ to obtain the single-random-phase encrypted hologram $H_{enc}(u,v)$.

Fig. 2. Concept of the proposed method.