



ELSEVIER

Contents lists available at ScienceDirect

Optics Communications

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

Optical encryption for large-sized images

Takuho Sanpei, Tomoyoshi Shimobaba*, Takashi Kakue, Yutaka Endo, Ryuji Hirayama, Daisuke Hiyama, Satoki Hasegawa, Yuki Nagahama, Marie Sano, Minoru Oikawa, Takashige Sugie, Tomoyoshi Ito

Chiba University, Graduate School of Engineering, 1–33 Yayoi-cho, Inage-ku, Chiba 263–8522, Japan

ARTICLE INFO

Article history:

Received 8 September 2015

Received in revised form

22 November 2015

Accepted 23 November 2015

Keywords:

Computer-generated hologram

Electroholography

Hologram

Holography

Holographic projection

Kinoform

Phase-only hologram

ABSTRACT

We propose an optical encryption framework that can encrypt and decrypt large-sized images beyond the size of the encrypted image using our two methods: random phase-free method and scaled diffraction. In order to record the entire image information on the encrypted image, the large-sized images require the random phase to widely diffuse the object light over the encrypted image; however, the random phase gives rise to the speckle noise on the decrypted images, and it may be difficult to recognize the decrypted images. In order to reduce the speckle noise, we apply our random phase-free method to the framework. In addition, we employ scaled diffraction that calculates light propagation between planes with different sizes by changing the sampling rates.

© 2015 Elsevier B.V. All rights reserved.

1. Introduction

Optical encryption methods [1,2] are promising technology because they have unique properties of parallel processing ability and multiple keys, which are random phase, wavelength, polarization and propagation distance. Double random phase encoding (DRPE) [3] is pioneering work, in which an original image is encrypted by using two random phase planes and then recorded as a hologram. Subsequently to this pioneering work, in order to reinforce the decoding resistance, a large number of optical encryption schemes have been proposed: for example, the extension to Fresnel domain [4], binary key code [5], fractional Fourier transform-based [6], gyrator transform-based [7], M-sequence [8], and ghost imaging-based schemes [9]. Optical encryption is also suitable for optical memory because of writing and reading data from the optical memory as encrypting and decrypting the data [10].

In the decryption process in optical encryption, the speckle noise in decrypted images is often a problem and it hinders the recognition of the decrypted information. Recently, optical encryption methods using Quick Response (QR) code tolerant to the speckle noise [11,12] have been proposed. In these methods, the original information is first converted to QR code and then the QR code is encrypted. Even if the decrypted QR code is contaminated

by noise, the information can be retrieved due to the property of the QR code.

If we want to encrypt large-sized images beyond the size of the encrypted image, we need to apply random phase, which is one of the causes of the speckle noise, to the images because it is necessary to widely diffuse the light of the images. In order to avoid degradation of the decrypted images, we can use the QR code schemes; unfortunately, the QR code does not contain a large amount of information.

In this paper, we propose an optical encryption framework that can encrypt and decrypt large-sized images beyond the size of the encrypted image using two methods: random phase-free method [13] and scaled diffraction [14,15]. Recently, we proposed a random phase-free method and it can record and reconstruct large-sized images without using the random phase. This method can dramatically reduce the speckle noise. Scaled diffraction calculates the light propagation between planes with different sizes by changing the sampling rates on the original and encrypted images. Section 2 describes our optical encryption framework for large-sized images, Section 3 shows the simulation results of the proposed method and Section 4 concludes this work.

2. Optical encryption framework for large-sized images

Fig. 1 shows the optical encryption framework for large-sized images. The framework consists of “Input scheme” for large-sized

* Corresponding author. Fax: +81 43 290 3361.

E-mail address: shimobaba@faculty.chiba-u.jp (T. Shimobaba).

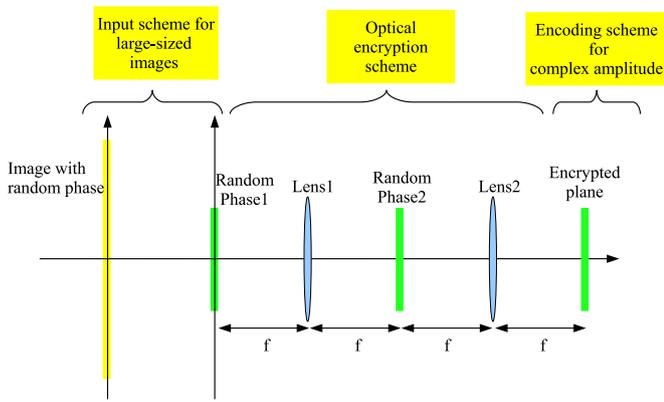


Fig. 1. Optical encryption framework for large-sized images with random phase.

images, “Optical encryption scheme” and “Encoding scheme” for complex amplitude. The input scheme plays the role of inputting the light from large-sized images to the encryption scheme with as little degradation as possible. The encryption scheme encrypts the light from the input scheme, e.g. we can use DRPE, Fresnel-based DRPE, fractional Fourier transform-based and gyrator transform-based optical encryption. The last part, the encoding scheme, encodes the complex amplitude from the output of the encryption scheme to a hologram, e.g. we can use digital holography [16,17]. Fig. 1 shows a conventional method for encrypting large-sized images. In this conventional method, we apply the random phase to the input image in the input scheme, and we use DRPE as the optical encryption scheme.

Most images in general contain many low frequency components, and thus cannot spread light widely because the spread angle is proportional to $\sin^{-1}(\lambda\nu)$ where λ and ν are the wavelength and the spatial frequency of the image, respectively [13]. In the case without the random phase on the large-sized images, the low frequency parts on the images cannot reach the first random phase in DRPE; therefore, the parts cannot be encrypted. The random phase on the images is required for widely spreading the light.

Fig. 2 shows the simulation results of decrypted images with and without the random phase on the input image. These results were obtained by conventional DRPE with planar wave illumination. The parameters of the simulation are the wavelength of 532 nm, the distance between the images and the first random phase in DRPE of 1.5 m, the resolution of the input image and the

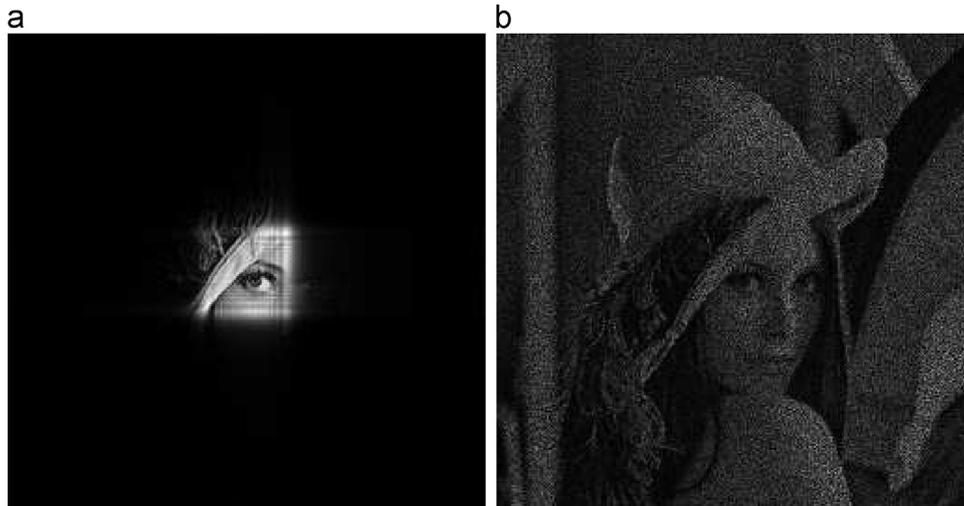


Fig. 2. Simulation results of decrypted images: (a) without the random phase on the input image and (b) with the random phase on the input image.

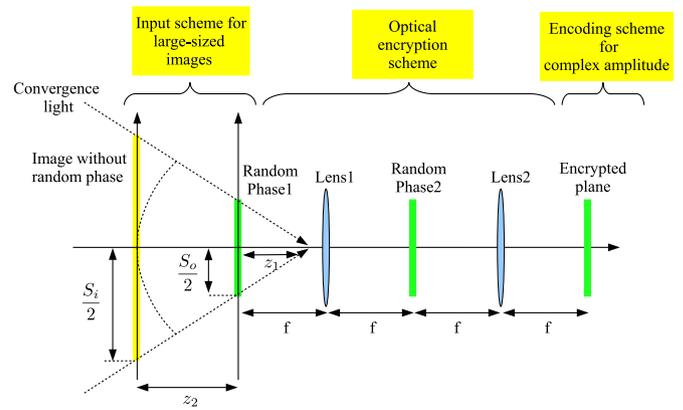


Fig. 3. Optical encryption framework for large-sized images with the proposed method.

encrypted image of $N \times N = 2048 \times 2048$ pixels, and the pixel pitches on the input image and the others (Random phases 1, 2 and the encrypted plane) of $p_i = 20 \mu\text{m}$ and $p_o = 4 \mu\text{m}$, respectively. Fig. 2(a) shows the decrypted image without the random phase on the input image. As we can see, only part of the image is decrypted, whereas the decrypted image in Fig. 2(b) can decrypt the entire image; unfortunately, the decrypted image is contaminated by speckle noise.

Fig. 3 shows optical encryption framework for large-sized images using the random phase-free method [13], which can encrypt large-sized images without applying random phase to the images, thus we expect that the reconstructed image is not contaminated by speckle noise. The only difference between Figs. 1 and 3 is the use of spherical convergence light, instead of random phase on the input image. The areas of the input image and the others are $S_i \times S_i$ ($S_i = N \times p_i$) and $S_o \times S_o$ ($S_o = N \times p_o$), respectively. In the proposed method, we multiply the input image $u_i(x_i, y_i)$ by the convergence given by $w(x_i, y_i)$. $w(x_i, y_i)$ is expressed as a convergence spherical light $w(x_i, y_i) = \exp(-i\pi(x_o^2 + y_o^2)/\lambda f_i)$ where $f_i = z_1 + z_2$ is the focal length. The distance between the focus point of the convergence light and the first random phase in DPPE is denoted by z_1 , and is set to the distance at which Random phase 1 just fits to the cone of the convergence light. The distance between the input image and the first random phase (this is the decryption distance) is denoted by z_2 . Subsequently, we calculate the complex amplitude on Random phase 1 using $u_h(x_h, y_h) = \text{Prop}_{z_2}\{u_o(x_o, y_o)w(x_o, y_o)\}$ where

Download English Version:

<https://daneshyari.com/en/article/1533811>

Download Persian Version:

<https://daneshyari.com/article/1533811>

[Daneshyari.com](https://daneshyari.com)