Optik 125 (2014) 3043–3050

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Attack on double-random-phase-encoding-based image hiding method

Hongsheng Xu [a], Nong Sang [a,*], Bing Zhang [b], Jun Sang [b]

[a] Science and Technology on Multi-spectral Information Processing Laboratory, School of Automation, Huazhong University of Science and Technology, Wuhan 430074, Hubei, China
[b] School of Software Engineering, Chongqing University, Chongqing 401331, China

ARTICLE INFO

Article history:
Received 19 June 2013
Accepted 6 December 2013

Keywords:
Double-random phase encoding
Image hiding
Recover secret image
Attack technique

ABSTRACT

The double-random phase-encoding (DRPE) technique is a typical optical image encryption technique, which can also be used for image hiding. Usually, the secret image is encrypted with the DRPE technique and the encoded image is hidden into the host image via superimposition to obtain the stego-image. The attack technique on the DRPE-based image hiding method was proposed in this paper. Firstly, a randomly selected superimposition coefficient was used to approximate the original superimposition coefficient to extract the hidden encoded images from the stego-images approximately. Then, the chosen-plaintext attack technique on the DRPE-based optical image encryption technique was applied to recover the random phase masks used in the DRPE technique. The theoretical analysis indicated that, without considering the computational error, the recovered secret image via the proposed attack technique is identical to the original one. Even considering the computational error, it is identical to the secret image recovered with the original DRPE-based image hiding method, which demonstrates that the attack on the DRPE-based image hiding method is successfully achieved. The numerical simulation results demonstrated the correctness of the theoretical analysis.

1. Introduction

The double-random phase-encoding (DRPE) technique is a typical optical image encryption technique [1], which has been widely used for image encryption [2–17] and can also been used for image hiding [18–21].

For the typical DRPE-based image hiding methods [19,20], the secret image is encrypted with the DRPE technique to obtain the encoded image, and then the encoded image is hidden into the host image via superimposition to obtain the stego-image. Two security ways are employed in the DRPE-based image hiding method: one is the DRPE-based image encryption using two random phase masks as the secret key; another one is the superimposition-based image hiding using the superimposition coefficient as the secret key. If the superimposition coefficient and the random phase masks are known, the hidden encoded image can be extracted from the stego-image and the secret image can be recovered with the extracted encoded image via the DRPE technique.

Corresponding to the above two security ways, the attack technique on the DRPE-based image hiding method was proposed in this paper. A randomly selected superimposition coefficient was used to approximate the original superimposition coefficient to extract the encoded image from the stego-image approximately. Then, the chosen-plaintext attack on the DRPE-based optical image encryption technique [22] was applied to recover the random phase masks used for the DRPE-based image encryption. The theoretical analysis indicated that, without considering the computational error, using the approximate superimposition coefficient and the recovered random phase masks, the proposed attack technique can extract and recover the secret image identical to the original secret image. Even considering the computational error, the recovered secret image via the proposed attack technique is identical to the recovered secret image via the original DRPE-based image hiding method, which demonstrates that, with the proposed attack technique, the attack on the DRPE-based image hiding method is successfully achieved. The numerical simulation results demonstrated the correctness of the theoretical analysis.

The rest of this paper is organized as follows: in Section 2, the typical DRPE-based image hiding method and the existing chosen-plaintext attack technique on the DRPE-based optical image encryption technique were briefly introduced. The attack technique on the DRPE-based

* Corresponding author.
E-mail address: nsang@hust.edu.cn (N. Sang).

0030-4026/$ – see front matter © 2014 Elsevier GmbH. All rights reserved.
http://dx.doi.org/10.1016/j.ijleo.2013.12.012

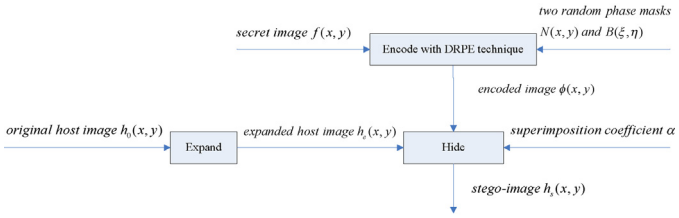

Fig. 1. Encoding and hiding procedure of the DRPE-based image hiding method.

image hiding method was proposed and the theoretical analysis was given in Section 3. In Section 4, the numerical simulations were given and the results were discussed. Section 5 presented the final conclusions.

2. Introduction on the DRPE-based image hiding method and the chosen-plaintext attack on the DRPE-based optical image encryption technique

2.1. DRPE-based image hiding method

2.1.1. Encrypt and hide the secret image

For the typical DRPE-based image hiding methods [19,20], the encoding and hiding procedure is shown in Fig. 1, which involves the following steps.

Step 1. Encode the secret image with the DRPE technique

The secret image $f(x, y)$ with the size of $M \times N$ is encrypted with the DRPE technique to obtain the encoded image $\phi(x, y)$ following Eq. (1).

$$\phi(x, y) = \mathrm{FT}^{-1}\{\mathrm{FT}[f(x, y)N(x, y)]B(\xi, \eta)\} \tag{1}$$

where $N(x, y)$ and $B(\xi, \eta)$ are two random phase masks in the spatial domain and frequency domain, respectively. They can be viewed as the secret key for the DRPE-based image encryption. FT and FT^{-1} represent Fourier transform and inverse Fourier transform, respectively.

The encoded image $\phi(x, y)$ is complex-valued, which can be denoted as:

$$\phi(x, y) = \phi_{\mathrm{R}}(x, y) + j\phi_{\mathrm{I}}(x, y) \tag{2}$$

where $\phi_{\mathrm{R}}(x, y)$ and $\phi_{\mathrm{I}}(x, y)$ are the real part and the imaginary part of $\phi(x, y)$, respectively.

Step 2. Enlarge the host image

Each pixel in the original host image $h_0(x, y)$ with size of $M \times N$ is enlarged to a 2×2 image block as Eq. (3) shows to obtain the enlarged image $h_{\mathrm{e}}(x, y)$ with size of $2M \times 2N$.

$$\begin{cases} h_{\mathrm{e}}(2x, 2y) = h_0(x, y) \\ h_{\mathrm{e}}(2x, 2y+1) = h_0(x, y) \\ h_{\mathrm{e}}(2x+1, 2y) = h_0(x, y) \\ h_{\mathrm{e}}(2x+1, 2y+1) = h_0(x, y) \end{cases} \quad x = 0, 1, 2, \ldots, M-1, \quad y = 0, 1, 2, \ldots, N-1 \tag{3}$$

Step 3. Hide the encoded image into the enlarged host image via superimposition

The encoded image $\phi(x, y)$ is hidden into the enlarged host image $h_{\mathrm{e}}(x, y)$ via superimposition as Eq. (4) shows to obtain the stego-image $h_{\mathrm{s}}(x, y)$.

$$\begin{cases} h_{\mathrm{s}}(2x, 2y) = h_{\mathrm{e}}(2x, 2y) + \alpha\phi_{\mathrm{R}}(x, y) \\ h_{\mathrm{s}}(2x, 2y+1) = h_{\mathrm{e}}(2x, 2y+1) - \alpha\phi_{\mathrm{I}}(x, y) \\ h_{\mathrm{s}}(2x+1, 2y) = h_{\mathrm{e}}(2x+1, 2y) + \alpha\phi_{\mathrm{I}}(x, y) \\ h_{\mathrm{s}}(2x+1, 2y+1) = h_{\mathrm{e}}(2x+1, 2y+1) - \alpha\phi_{\mathrm{R}}(x, y) \end{cases} \quad x = 0, 1, 2, \ldots, M-1, \quad y = 0, 1, 2, \ldots, M-1 \tag{4}$$

where α is the superposition coefficient, which can be viewed as the secret key for superimposition.

2.1.2. Extract and recover the secret image

Following Eqs. (3) and (4), the encoded image $\phi(x, y)$ can be extracted from the stego-image $h_{\mathrm{s}}(x, y)$ as:

$$\begin{aligned} \phi_{\mathrm{R}}(x, y) &= \left[\frac{h_{\mathrm{s}}(2x, 2y) - h_{\mathrm{s}}(2x+1, 2y+1)}{2\alpha}\right] \\ \phi_{\mathrm{I}}(x, y) &= \left[\frac{h_{\mathrm{s}}(2x+1, 2y) - h_{\mathrm{s}}(2x, 2y+1)}{2\alpha}\right] \\ \phi(x, y) &= \phi_{\mathrm{R}}(x, y) + j\phi_{\mathrm{I}}(x, y) \end{aligned} \tag{5}$$