Journal of the Optical Society of Korea, Vol. 6, No. 4, December 2002, pp. 156-160

Image Encryption Using Phase-Based Virtual Image and Interferometer

Dong-Hoan Seo* and Soo-Joong Kim

Dept. of Electronic Engineering, Kyungpook National University,
Daegu 702-701, KOREA

(Received September 10, 2002)

In this paper, we propose an improved optical security system using three phase-encoded images and the principle of interference. This optical system based on a Mach-Zehnder interferometer consists of one phase-encoded virtual image to be encrypted and two phase-encoded images, encrypting image and decrypting image, where every pixel in the three images has a phase value of '0' and 'π'. The proposed encryption is performed by the multiplication of an encrypting image and a phase-encoded virtual image which dose not contain any information from the decrypted image. Therefore, even if the unauthorized users steal and analyze the encrypted image, they cannot reconstruct the required image. This virtual image protects the original image from counterfeiting and unauthorized access. The decryption of the original image is simply performed by interfering between a reference wave and a direct pixel-to-pixel mapping image of the encrypted image with a decrypting image. Computer simulations confirmed the effectiveness of the proposed optical technique for optical security applications.

OCIS codes : 070.2580, 100.0100.

I. INTRODUCTION

Optical processing techniques have recently been employed in security applications due to their ability for rapid transmission of information and a large degree of freedom to encode data. These advantages of an optical security system include the controllability of phase components of the image which can be fabricated by optical devices, such as liquid crystal devices (LCD), computer generated holograms (CGH), or lithography [1–4]. Optical encryption methods convert an original image into a complex image or pure random phase image. Since the resulting phase components are difficult to detect by intensity detectors, they are more difficult to copy or reproduce. So various approaches for optical security systems, based on optical correlations, have been proposed [5–10].

Representative techniques for the implementation of optical encryption such as double random-phase encryption, with Javidi and co-workers, have been proposed. This method converts an original image into a random-noise-like image by using two random-phase masks located in the input and Fourier planes of a $4f$ correlator. In the decoding process, the phase mask, which is the complex conjugate of the random phase mask used for encryption in the Fourier plane, is used in the frequency plane as the key for decryption. So this technique requires high alignment accuracy and an accurately fabricated complex conjugate key. We also know that the previous approaches have some drawbacks, because unauthorized users can permit a counterfeiting of the encrypted image by analyzing the random phase mask using some phase measurement technique. Other approaches using the random phase-coding method based on the iterative algorithm have been proposed [11,12]. These methods encrypt an original image using two random phase masks generated by computer, where the encoded random phase image contains no information from the input phase image or the Fourier plane filter that is required during the decoding process. These approaches have shown computer-simulation results that suggest that they are suitable for security applications. However, these systems require a phase mask obtained by an accurately iterative computation for a fine control of the multivalued phase and high alignment accuracy so that no satisfactory experimental results are obtained.

II. PRINCIPLE OF INTERFERENCE

Let the two plane waves propagating in the z-direction with the same frequency ω, wavelength λ, amplitude E_0, and polarization be

$$\begin{aligned} E_1(z,t) &= E_0\cos(kz-\omega t+\phi_1) \\ E_2(z,t) &= E_0\cos(kz-\omega t+\phi_2), \end{aligned} \quad (1)$$

where ϕ_1 are ϕ_2 the initial phases, and k is the propagation constant. The intensity of the superposition wave of the two waves at an instantaneous time can be written as

$$\begin{aligned} I &= \langle E^2\rangle \\ &= \langle (E_1+E_2)\overline{(E_1+E_2)}\rangle \\ &= \langle E_1^2\rangle + \langle E_2^2\rangle + 2\langle E_1E_2\rangle \\ &= I_1+I_2+I_{12} \end{aligned} \quad (2)$$

The interference term is then

$$I_{12} = 2E_0^2\cos\triangle, \quad (3)$$

where the phase difference ($\triangle$) arises from a combined path length and initial phase angle difference. That is

$$\triangle = k(z_1-z_2)-(\phi_1-\phi_2) \quad (4)$$

At various points in space, the resultant irradiance depends on $\triangle$. The maximum irradiance is obtained when $\cos\triangle = 1$. Therefore, if the phase difference between the two waves is an even multiple of π or an odd multiple of π, the intensity is maximized or minimized, respectively. Consider the case where two phase-only images have pixel values of '0' or 'π'. If two pixels with the same phase value interfere with each other, the corresponding intensity value will become the maximum value, while two pixels with a different phase value will result in the minimum value. As such, the binary intensity image can be obtained by interfering two phase-encoded images with each other. This principle is similar to a kind of digital XOR logic operation and is applied for encryption and decryption in the proposed system.

III. PROPOSED IMAGE ENCRYPTION AND DECRYPTION

1. Image encryption process

Let $f(x,y)$, $v(x,y)$, $r(x,y)$, $d(x,y)$, and $e(x,y)$ denote the original image, the binary virtual image to be encrypted, binary random image, binary decrypting image, and the encrypted image, respectively. The original image is divided into three images, virtual image, random image, and decrypting key, and given by

$$f(x,y) = v(x,y)+r(x,y)+d(x,y) \quad (5)$$

The virtual image $v(x,y)$, the random image $r(x,y)$ and the decrypting key $d(x,y)$ have two values of '0' and '1'. In the encryption process, to prevent counterfeiting and unauthorized access by analyzing the encrypted image, the virtual image to be encrypted and the random image are combined with the encrypted image. The virtual image and the random image are encoded into a phase function. Therefore the two phase-encoded images have two phase values of '0' and 'π' and a uniform amplitude transmittance and are given by

$$\begin{aligned} v_p(x,y) &= \exp[j\pi v(x,y)], \\ r_p(x,y) &= \exp[j\pi r(x,y)]|v_p(x,y)|^2 \\ &= |r_p(x,y)|^2 = 1, \end{aligned} \quad (6)$$

where subscript 'p' denotes the phase encoded image. The encrypted image $e(x,y)$ is obtained by multiplying two phase-encoded images with each other. Therefore, the original image $f(x,y)$ is protected from counterfeiting and unauthorized access. And it also has a uniform amplitude transmittance. And it is given by

$$\begin{aligned} e(x,y) &= v_p(x,y)r_p(x,y) \\ &= \exp[j\pi\{v(x,y)+r(x,y)\}] \end{aligned} \quad (7)$$

the optical encryption method is shown as a block diagram in Fig. 1. The virtual image and random image are fully phase-valued, so they can not be copyed by an intensity detector such as a camera, scanner and so on. And then even if illegal users steal and decipher the encrypted image, most of them will recognize the virtual image as an original image. Therefore whitout

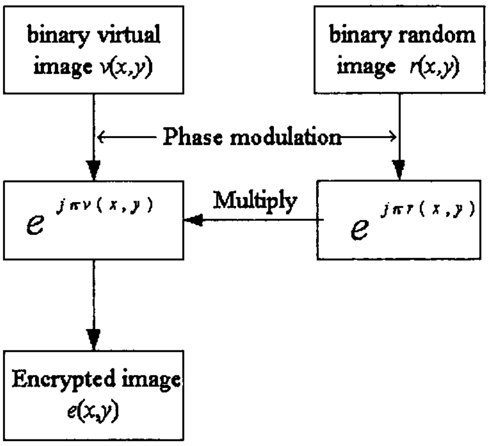

FIG. 1. Block diagram for encryption procedure.

the correct decrypting key, the original image cannot be reconstructed. These phase images can be fabricated using computer processing and optical lithography, or displayed on a spatial light modulator, such as an LCD.

2. Image decryption process

The decryption of the original image is simply performed by interfering between a reference wave and a direct pixel-to-pixel mapping image of the encrypted image with a decrypting image, which can be made by a kind of XOR operation rule, and it can be optically recovered by a simple Mach-Zehnder interferometer architecture. Let $M(x,y)$, $R(x,y)$, and $d_p(x,y)$ denote the direct pixel to pixel mapping image, reference wave, and the decrypting phase key, respectively. The direct pixel-to-pixel mapping image is given by

$$\begin{aligned} M(x,y) &= e(x,y)d_p(x,y) \\ &= v_p(x,y)r_p(x,y)d_p(x,y) \\ &= \exp[j\pi\{v(x,y)+r(x,y)+d(x,y)\}]. \end{aligned} \tag{8}$$

In Eq. (8), we can see the phase values of the mapping image $M(x,y)$ become a linear summation of virtual image, random image and decrypting key. To obtain the original image $f(x,y)$, the three phase-encoded images are then fabricated by phase assignment rule using an XOR logic operation. As a result, the decrypting key $d(x,y)$ can be obtained by an XOR operation with three phase-encoded images: phase-encoded virtual image, phase-encoded random image, and phase-encoded original image. And then the interference of the two optical paths is given by

$$\begin{aligned} I(x,y) &= |R(x,y)+R(x,y)M(x,y)|^2 \\ &= |R(x,y)|^2|1+\exp[j\pi\{v(x,y) \\ &\quad + r(x,y)+d(x,y)\}]|^2 \\ &= |R(x,y)|^2|1+\exp[j\pi f(x,y)]|^2 \\ &= |E|^2\begin{cases} 4 & f(x,y)=0 \\ 0 & f(x,y)=1 \end{cases} \end{aligned} \tag{9}$$

where the phase value is $f(x,y)=v(x,y)+r(x,y)+d(x,y)$ and the reference wave is where E is the amplitude and φ is the initial phase of the plane wave

$$\begin{aligned} R(x,y) &= E\exp(j\varphi), \quad |R(x,y)|^2 \\ &= |E\exp(j\varphi)|^2 = |E|^2 \end{aligned} \tag{10}$$

and also the reference wave has a uniform amplitude transmittance. In Eq. (9), if the summation of the each pixel value of the mapping image is '0', the intensity is maximum. if the pixel value is '1', the intensity is minimum. This means that the negative image of the original image can be obtained in the detector by placing the mapping image on one path of the Mach-Zehnder interferometer, as shown in Fig. 2. Here, we suppose that the optical path difference between two arms is an integer multiple of 2π to prevent interference due to differences between beam paths. In the proposed system, to reduce the diffraction effect between the encrypted image and the decrypting key, they are exactly superimposed in the experimental system and then we can improve the quality of the decrypted image As a result, the coherent light that

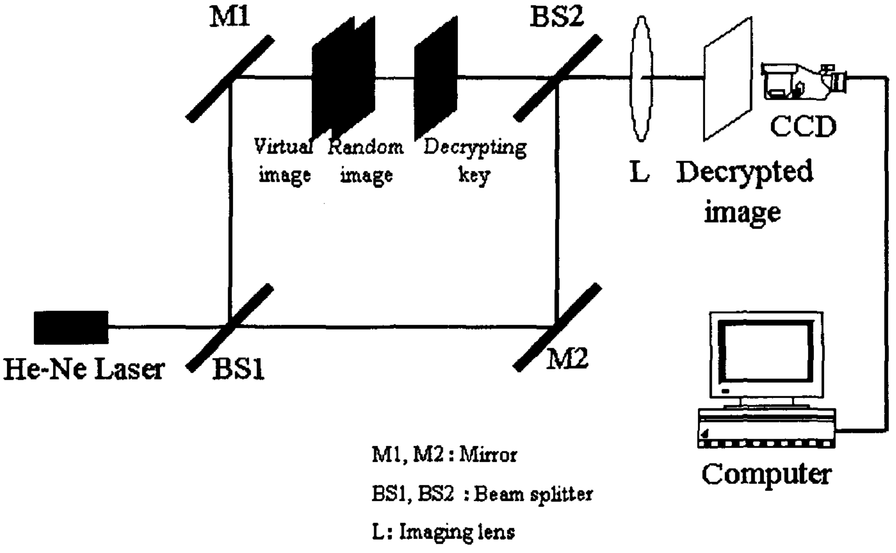

FIG. 2. Mach-Zehnder interferometer for image decryption system.

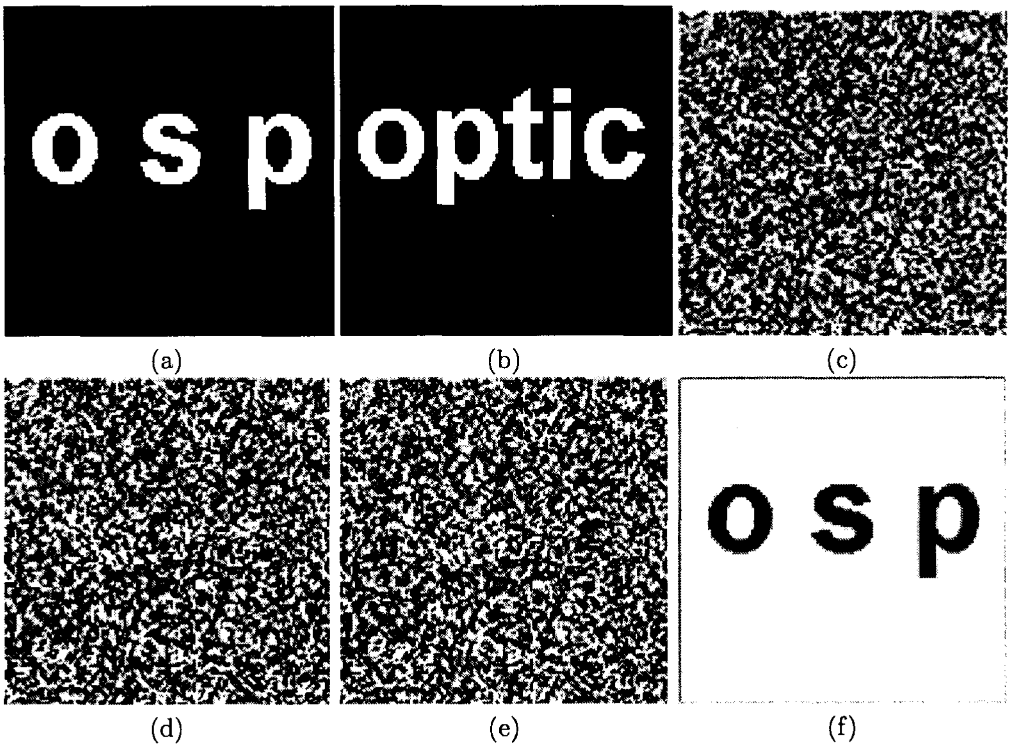

FIG. 3. Computer simulations: (a) original image, (b) virtual image, (c) random image, (d) encrypted phase image, (e) decrypting image, and (f) reconstructed image.

passes each pixel of the encrypted image and the decrypting key will have the same phase delay as the pixel value. And then the phase-delayed lights interfere with reference wave.

IV. COMPUTER SIMULATIONS

Let's consider an original image $f(x,y)$, a virtual image $v(x,y)$, and a random image $r(x,y)$ that is randomly generated by using computer processing, as shown in Fig. 3(a), (b), and (c). The size of the images is 128×128. Here, to reduce the phase difference due to the thickness and surface of the phase masks, it is important to fabricate the three phase masks precisely in the optical experiment. The virtual image and the random image are encoded into pure phase functions. The encrypted image is obtained by multiplying the phase-encoded images with each other, as shown in Fig 3(d). Fig. 3(e) represents the decrypting key that is made by the phase assignment rule using an XOR logic operation to obtain the original image. These images cannot be seen and copied by an intensity detector. Conveniently, we represent that the white pixel of these images is 0 phase value and the black pixel is p phase value. Consequently, the interference pattern between phase-delayed wave that passes through three phase-encoded images and reference wave is detected in the output plane, such as a CCD, as shown in Fig. 3(f). The inversion of the output result was the same as the original image.

V. CONCLUSION

We proposed an improved optical security system using a phase-based virtual image and optical interference principle in the space domain. A virtual image is encrypted into a binary phase-only image by multiplying with a random phase image and then decrypted by using the decrypting image in the optical decryption system. The advantage of this technique is that we use a reference wave to solve optical alignment and pixel-to-pixel mapping problem in the interferometer and only three phase masks are required to reconstruct the decrypted image without any decryption filter. And also even if illegal users analyze the encrypted image and know the expected image in the output plane, they will reconstruct the virtual image that does not include any information on the original image. This virtual image protects the required information from counterfeiting and unauthorized access. Therefore it cannot be regenerated from the encrypted image without information on the decrypting image. Computer simulation demonstrated that the proposed method can be applied for optical security systems.

VI. ACKNOWLEDGEMENT

This work was supported by the Institute of Information Technology Assessment in South Korea, project C1-2002-012-0-3.

*Corresponding author : dhseo@palgong.knu.ac.kr.

REFERENCES

[1] B. Javidi and J. L. Horner, Opt. Eng. **33**, 1752 (1994).

[2] P. Refregier and B. Javidi, Opt. Lett. **20**, 767 (1995).

[3] B. Javidi, G. Zhang, and Jian Li, Opt. Eng. **35**, 2506 (1996).

[4] R. K. Wang, I. A. Watson, and C. Chatwin, Opt. Eng. **35**, 2464 (1996).

[5] S. Lai, Opt. Eng. **35**, 2470 (1996).

[6] L. G. Neto, Proc. SPIE **3386**, 284 (1998).

[7] B. Javidi and E. Ahouzi, Appl. Opt. **37**, 6247 (1998).

[8] J. W. Han, D. H. Ryu. D. S. Park, and E. S. Kim, Opt. Eng. **38**, 47 (1999).

[9] T. Nomura and B. Javidi, Opt. Eng. **39**, 2031 (2000).

[10] B. javidi and T. nomura, Opt. Lett. **25**, 28 (2000).

[11] T.Sasaki, H. Togo, J. Tnida, and Y. Ichioka, Appl. Opt. **39**, 2340 (2000).

[12] Hsuan T. Chang, Opt. Eng. **40**, 2165 (2001).