Secure sharing method for a secret binary image and its reconstruction system

Sang-Su Lee*, and Jong-Wook Han**

* Information Security Research Division, ETRI, Taejeon, Korea
(Tel : +82-42-860-1613; E-mail: sangsu@etri.re.kr)
** Information Security Research Division, ETRI, Taejeon, Korea
(Tel : +82-42-860-4940; E-mail: hanjw@etri.re.kr)

Abstract: In this paper, an encryption method to share a secret binary image is proposed. It divides the image to be encrypted into an arbitrary number of images and encrypts them using XOR process with different binary random images which was prepared by the means of the XOR process, too. Each encrypted slice image can be distributed to the authenticated ones. However, we transfer the encrypted images to the binary phase masks to strengthen the security power, that means phase masks can not be copied with general light-intensity sensitive tools such as CCDs or cameras. For decryption, we used the Mach-Zehnder interferometer in which linearly polarized two light beams in orthogonal direction, respectively. The experimental result proved the efficiency of the proposed method.

Keywords: optical security, XOR, phase, interferometer, polarization

1. INTRODUCTION

Many optical image encryption methods including random phase encryption, optical XOR image encryption and digital optical stream cipher have been suggested[1]-[3]. They used and focused on the intrinsic parallelism and ultra-fast processing speed of light. Especially, double random phase encoding in the input plane and the Fourier domain is the most common optical image encryption technique proposed by P. Refregier and B. Javidi. They used two statistically independent random phase masks in the input and Fourier domain to encrypt an image into stationary white noise. To recover the original image from the encrypted data, a key phase card, the complex conjugate of the random phase mask used in encoding process, is put in the Fourier plane of the 4f-correlator system. It is very difficult to decode the encoded data without the key, or with intensity sensitive detectors. Optical implementation of the double random phase encoding method has been demonstrated[4]-[8],. The security of an encryption technique depends on the size of the key used. Techniques have been proposed to use the additional degrees of freedom offered by an optical system to enlarge the key size. Matoba and Javidi proposed a method in which the random phase codes are used in the Fresnel domain[5]. The random phase codes along with their position form a three dimensional key. The wavelength of light can be used as a key for encryption and decryption[6]. T. Nomura proposed a phase encoded joint transform correlator (JTC) to decode the encrypted image with the same random phase mask used in the encryption procedure[9].

A majority of optical encryption system proposed up to date are based on the Fourier transform configuration. Recently, J.Y. Kim, S.J. Kim, et al., proposed a new optical image encryption method using the interferometer and encrypted phase masks[10]. They encrypted an binary image by XOR with a random binary image. They also proposed the rule about assigning phase according to the value of encrypted pixel. For instance, the pixels which are white in the encrypted image can have the phase value of ‘p’. On the other hand, the other black pixels can have the phase value of ‘0’. For decryption, the encrypted phase mask, converted from the encrypted binary image by the phase-assign rule, should be placed in one of arms in Mach-Zehnder interferometer, and in the other arm, the phase mask, converted from the encrypted key by the phase-assign rule, be placed. Finally, the original binary image can be obtained in the output plane by the interference between phase-delayed two beams.

In this paper, we proposed an encryption method to share a secret binary image was proposed. This divides the image to be encrypted into an arbitrary number of images and encrypts them using XOR process with different binary random images which was prepared by the means of the XOR process, too. Each encrypted slice image can be distributed to the authenticated ones. However, we transfer the encrypted images to the binary phase masks to strengthen the security power, that means phase masks can not be copied with general light-intensity sensitive tools such as CCDs and cameras. For decryption, we used the Mach-Zehnder interferometer in which linearly polarized two light beams in orthogonal direction, respectively. The experimental result proved the efficiency of the proposed method. When polarized beams are used, much of noise due to the vibration of light or scattering of light by fine particles in air can be removed effectively by the analyzer placed in output plane of the interferometer.

In Section 2 we describe the proposed method for encrypting a secret binary image and transforming into phase masks. In Section 3, for better understanding how to recover the original image, we discuss the polarization of light and then describe the decryption system.

2. THE PROPOSED ENCRYPTION METHOD

2.1 Slicing a binary image to be encrypted

A secret binary image to be encrypted can be divided into arbitrary number of n slide images and then one must prepare (n-1) random keys. However, the n-th random key can be obtained by XOR process with all (n-1) random keys. One can see that XOR of all random keys will give just white image and this property play the key role on encryption and decryption. Each slide image is encrypted by XOR operation with each random key. Figure 1 shows the case when n equals 5. In the figure, an original image is divided into the other five different slide images as shown in figure 1(a). To encrypt slide images, four random keys are generated and another random key is obtained by XOR processing them as shown in figure 1(b). The XOR process between each slide and random key generated five encrypted slides as shown in figure 1(c). To obtain the original image showed in figure 1(d), one must conduct XOR process with all of encrypted images. If even any of them is missed, it is impossible to get the original image. So, this encryption scheme can be applied to sharing information field such as military security.

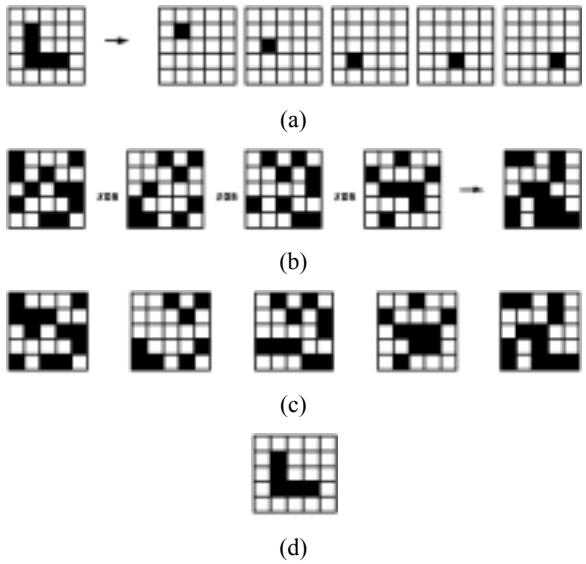

Fig. 1. Example of two-phase method for n = 5: (a) original image and its divided images, (b) 4 random keys and another random key generation, (c) encrypted images, (d) decrypted image

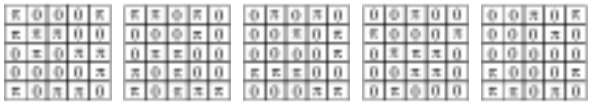

Fig. 2. The phase masks converted from encrypted images of figure 1(c)

2.2 The transformation of encrypted slides to phase masks

Although the encryption method described above is efficient enough, there is a threat that encrypted pattern can be copied easily. For protect the threat, we transform the encrypted slide consisted of binary pixels into the phase masks with binary phase values. In detail, the phase mask corresponding to each encrypted image can be made by using the way that assigned '0' or 'p' to white or black pixels of the encrypted image, respectively. For example, the phase masks for encrypted images in figure 1(c) will be like figure 2. These phase patterns are printed in transparent glass through the process of optical lithography and chemical etching. Thus, one can not read the patterns with human eyes, CCDs, or cameras because the patterns are pure phase distribution. In this sense, the proposed scheme is protected from illegal copy attack by attackers. Figure 3 shows the flow step of the encryption method described.

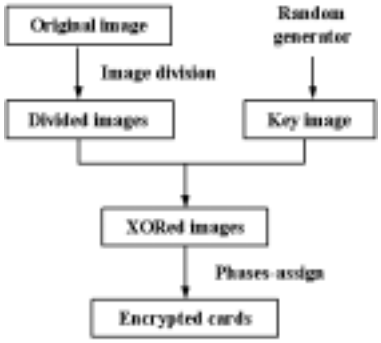

Fig. 3. The process of the proposed encryption method

3. THE PROPOSED DECRYPTION SYSTEM

3.1 Polarization of light

To understand the linear polarization of light, consider two light waves, one polarized in the y-z planes and the other in x-y plane. If the waves are in phase, which means they reach their maximum and minimum points at the same time, their vector sum leads to one wave, linearly polarized at 45 degrees. Similarly, if they are out of phase, which their phase difference is 180 degrees, the result is linearly polarized at 45 degrees in the opposite sense. In this sense, if one can control the phase of two beams polarized in orthogonal direction to each other, he can obtain a linearly polarized light with desirable degree. Table 1 offers the summary of the relationship between the phase values of polarized beams and the resultant direction of the linearly polarized beam.

Note that this result is very similar with the logical XOR operation. When the two lights have the same phase value, the polarization angle is opposite to the angle when the two lights have the phase difference of π. So, one can use this optical XOR concept when logical XOR operation is needed for decrypting an information.

Table 1. The relationship between the phase values of two orthogonally polarized light beams and the resultant polarization

Phase of light wave		Electric vector		Resultant Porarization
X-axis	Y-axis	X-axis	Y-axis	
0	0	→	↑	↗
0	π	→	↓	↘
π	0	←	↑	↖
π	π	←	↓	↙

3.2 Decryption system based on polarization of light

We used Mach-Zehnder interferometer using two orthogonally polarized beams as the decryption system shown in figure 4. Two lights splitted from polarization beam splitter (PBS) are polarized in orthogonal to each other. Encrypted phase masks can be any path of interferometer, and analyzer placed in output plane passes the linearly polarized light only with desirable polarization direction, for example, 45 or 135 degrees. In this way, the captured image by CCD can show decrypted image, of course, the image is the same as the original binary image. Actually, vibration of air or very fine particles in air can cause phase distortion of propagating light beam.

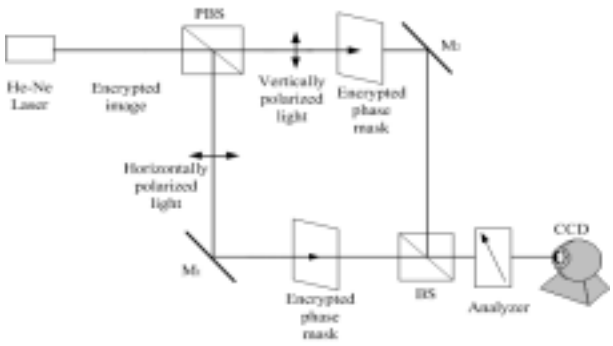

Fig. 4. The proposed decryption system using PBS

4. OPTICAL EXPERIMENTS

We conducted a simple optical experiment to prove the effectiveness of the proposed method. In our experiment, the original binary image was divided into two slide images as shown in figure 5(a), (b), and (c). And a random images used as an encryption key and encrypted images through XOR process with the key are shown in figure 5(d), (e), and (f), respectively. The phase masks corresponding to the encrypted images are figure 6(a) and (b), respectively. For decryption each phase mask was placed on any of the two optical paths of a Mach-Zehnder interferometer. The combined light by BS has the polarization statement as shown figure 7(a). Some of light, which has the same polarization angle as the angle of analyzer shown in figure 7(b), can be passed through the analyzer and its intensity is detected by CCD, while the others which have opposite polarization angle can't be passed. Figure 8 shows the captured image in CCD and one can see that it is the same as the original image of figure 5(a).

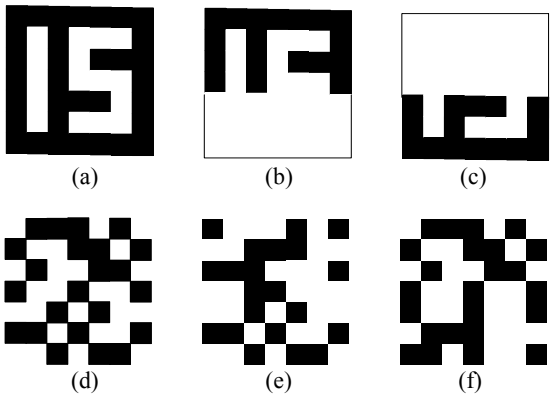

Fig. 5. Images and phase patterns for experiment: (a) original image; (b) and (c) divided images; (d) random key; (e) = (b) XOR (d); (f) = (c) XOR (d)

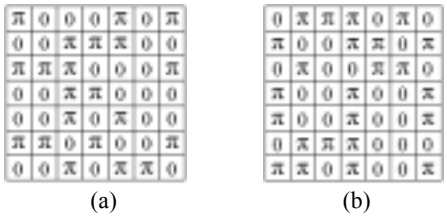

Fig. 6. (a) and (b) are phase patterns corresponding to the figure 6(e) and (f), respectively

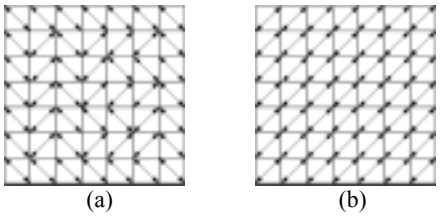

Fig. 7. Polarization angles: (a) the resultant polarization angle controlled by the encrypted phase masks, (b) the angle with which light can pass through analyzer

Fig. 8. The detected image

5. CONCLUSIONS

In this paper, we used the simple encryption method based on traditional XOR. However, by converting the encrypted slide images to phase masks, the better safety against illegal copy is obtained. Decryption is achieved by controlling the phase of two orthogonally polarized lights and the result image shows the original binary image. Thus, the proposed encryption method and decryption system can be an application to share a secret information, especially an binary image.

ACKNOWLEDGMENTS

We acknowledge the help of Optical Signal Processing Laboratory in Kyungpook National Univ., Korea, for the use of phase masks needed to our optical experiments.

REFERENCES

[1] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Optics Letters, Vol. 20, No. 7, pp. 767-769, 1995.

[2] J.W. Han, C,S, Park, D.H. Ryu, and E.S. Kim, "Optical image encryption based on XOR operations," Optical Engineering, vol.38, no.1, pp.47-54, 1999.

[3] J.W. Han, S.H. Lee, and E.S. Kim, "Optical key bit stream generator," Optical Engineering, Vol. 38, No. 1, pp. 33-38, 1999.

[4] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption system that uses phase conjugation in a photorefractive crystal," Applied Optics, vol. 37, pp. 8181-8185, 1998.

[5] O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," Optical Letters, vol. 24, pp. 762-764, 1999.

[6] O. Matoba and B. Javidi, "Encrypted optical storage with wavelength-key and random phase codes," Applied Optics, vol. 38, pp. 6785-6790, 1999.

[7] O. Matoba and B. Javidi, "Encrypted optical storage with angular multiplexing," Applied Optics, vol. 38, pp.7288-7293, 1999.

[8] L.G. Neto and Y. Sheng, "Optical implementation of image encryption using random phase encoding," Optical Engineering, vol.35, pp.2459-2463, 1996.

[9] T. Nomura, "Phase encoded joint transform correlators as an optical encryption decoder." San Diego SPIE Meeting, pp.246-252, 1998.

[10] J.-Y. Kim, S.-J. Park, C.-S. Kim, J.-G. Bae, and S.-J. Kim, "Optical image encryption using interferometry-based phase masks," Electronics Letters, vol.36, no.10, pp. 874-875, 2000.

[11] Dong-Hoan Seo, Jong-Yun Kim, et al., "Visual

Cryptography based on optical interference encryption technique," proceedings of SPIE, vol. 4386, pp. 172-180, 2001.

[1] http://plc.cwru.edu/tutorial/enhanced/files/lc/light/light.htm

[2] Hecht, *Optics*, 2nd Ed, Addison-Wesley, Ch. 9, 1987.