A robust optical security system using polarization and phase masks

Jae-Hyun Kim*, Chang-Mok Shin, Dong-Hoan Seo, Jong-Yun Kim,
Se-Joon Park, Soo-Joong Kim

Dept. of Electronic Engineering, Kyungpook National University, Taegu 702-701, Korea
Tel : +82-53-940-8611, Fax : +82-53-950-5505
E-mail : azalea73@hanmail.net

Abstract: A robust optical security technique using orthogonally polarized lights in the interferometer is proposed. We use orthogonally polarized lights in order to minimize the noise generated by the refractive index change due to vibration, flow of air, change of temperature etc. To make orthogonally polarized lights the first beam splitter in the Mach-Zehnder interferometer is substituted by a polarizing beam splitter(PBS). Because of incoherence of orthogonally polarized lights, the noise generated by the change of refractive index is minimized. To encrypt an image we use the random partition and the diffusing of pixel. Finally we make Phase-only-filters of each image which is randomly partitioned and diffused pixel by pixel. Simulation results show the proposed system has the ability of encryption and decryption of an image.

1. Introduction

The security is a serious and widespread problem in many fields of an information society. So many banks, businesses, and consumers want the system to be well prevented from counterfeiting. But the counterfeit parts, such as computer chips, machine tools, etc., are becoming ever more prolific with the rapid advances in computers, CCD technology, image-processing hardware and software, printers, scanners, and copiers for producing logos, symbols, money bills, or patterns. Nowadays credit cards and passports use holograms for security as they can be inspected the by human eye. This type of holographic pattern can be easily acquired from a credit card (photographed or captured by a CCD camera) and then a new hologram synthesized. Recently, various optical processing systems have been proposed for encryption, security systems, and the anti-counterfeiting and verification of biometrics' [1-6]. In addition, the system, which uses only phase holograms in the Mach-Zehnder interferometer, is proposed. However this system is very sensitive to a noise which is generated by the refractive index change [7,8].

In this paper, a robust optical security system using orthogonally polarization and phase masks is proposed. The encryption of an image is done by using a random partition, a random diffusing of pixels, and phase-only-filters. Two encrypted phase masks and two Fourier lenses are located in the Mach-Zehnder interferometer. And then the first beam splitter in the interferometer is substituted by a PBS. So two lights in each path are orthogonally polarized. Therefore the output image is the one which is a simply sum of intensity images of inverse Fourier transform of each phase mask. Because of the incoherence of orthogonally polarized lights, the interference of two lights can be removed. So the interference noise generated by environmental refractive index change can not be present. In this manner, we can use the optical security system that is robust for the interference noise of environmental imperfection.

2. Interference noise in the interferometer

In coherent optical systems, interference patterns, included noises, are inevitable phenomena, although Fourier transform, a correlation process and etc. can be easily carried out. Contrarily, in incoherent systems, interference patterns are not present, but Fourier transform of an image can not be performed. So sometimes we are used to need an appropriate trade-off.

In order for the encryption of an image, the system using binary phase holograms was proposed [8]. That system is coherent system. Binary phase masks, which have 0 or π phase, were used in that system. And Mach-Zehnder interferometer was also used. In that system, the difference of optical length of each path in the interferometer must be 0 or π. If not, the correct output image can not be obtained without other process. Generally vibration, flow of air, change of temperature and etc. are sources of optical path variation. So if these noises are not removed, the stable output images can not be obtained easily.

In this paper, we use PBS instead of the first beam

splitter in the Mach-Zehnder interferometer in order to make two orthogonally polarized lights. In doing so, we can remove the interference noise, because orthogonally polarized lights are incoherence each other. But each light of two lights in the interferometer is self-coherent. In proposed system, we need different encryption and decryption method.

3. Encryption, Decryption and the optical setup

3.1 Encryption

In our simulation, all images are 256 gray images and 256×256 pixel sized. Fig. 1 is a binary image of a capital letter T (White is 255 gray level and black is 0 gray level).

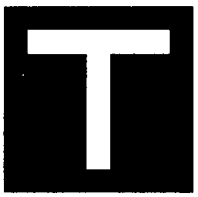

Fig. 1. The original binary image

Binary images are a easy image to process. So we use the binary image as the original image. Fig. 1 is divided into two images. Each pixel of Fig. 1 is assigned to one of two divided images randomly. Pixels, which are not assigned, are zero valued in the divided images. Then two divided images (Fig. 2(a) and Fig. 2(b)) are generated. For convenience' sake images are assigned by 16×16 pixels in our simulation. If Fig. 2(a) and Fig. 2(b) are added, Fig. 1 can be obtained. Each white pixel of Fig. 2(a) and 2(b) is shifted with a random direction and a random distance in a limited range. In doing so, two diffused images of Fig. 2(a) and Fig. 2(b) are generated (Fig. 2(c) and Fig. 2(d)). These diffused images are similar to ensembles of additive noises. But these images have similar geometric characteristics of Fig. 2(a) and Fig. 2(b) in shape. If we have only to consider the recognition problem, the nice shape of the image to be recognized is not needed. Phase-only-filters of two diffused images are Fig. 2(e) and Fig. 2(f)(The variation of phase from 0 to 2π is represented by gray levels). We use Fig. 2(e) and Fig. 2(f) as phase masks. These two encrypted phase masks can be implemented with a optical lithography technique or Liquid crystal display(LCD). But accurate implementation is very difficult and remained.

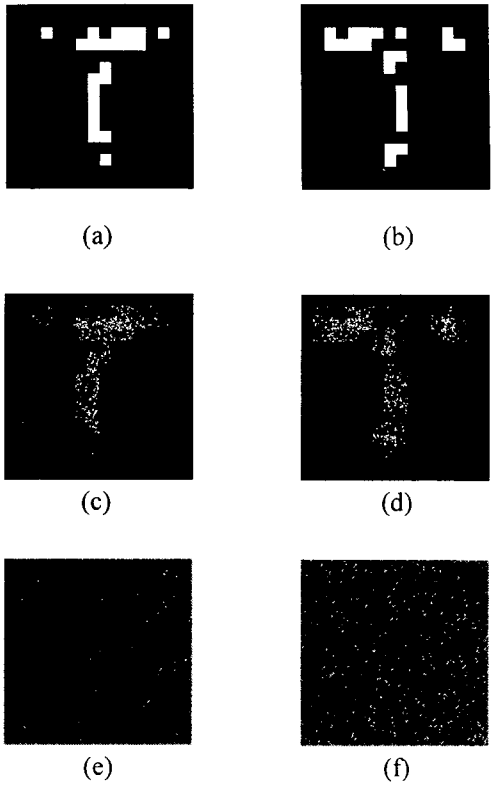

Fig. 2. Encryptin method
(a),(b) Two divided images
(c),(d) Two diffused images
(e),(f) Phase-only-filters of (c) and (d)

3.2 Decryption

Fig. 3(a) and Fig. 3(b) are intensity images of inverse Fourier transform of Phase-only-filters. Fig. 3(a) and Fig. 3(b) are still similar shape of Fig. 2(a) and Fig. 2(b). Besides these images have only Fourier phase component. Generally if an image is randomly diffused, the Fourier phase component has more information than the Fourier modulus. The reason for that each randomly diffused pixel

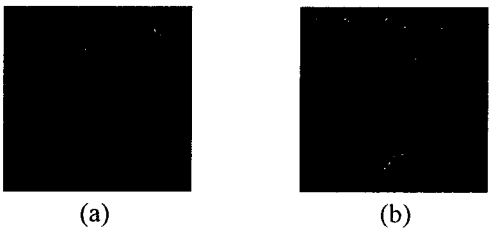

Fig. 3. Two Intensity images of inverse Fourier transform of Fig. 2(e) and Fig. 2(f)

acts as a random additive noise. So the Fourier transform of a diffused image can be roughly thought as a linear combination of the Fourier transform of each additive noise. So Fourier modulus component can be roughly constant in reasonable ranges. Therefore the image reconstructed using only phase information is similar with the original image in shape. The final image to be recognized is Fig. 4. This final image is a simply added version of Fig. 3(a) and Fig. 3(b) and has a similar shape of the original binary image. Fig. 3 is a target image to be detected in the optical setup. After obtaining this target image, we can postprocess the image. For example, a binarization, a morphology process, and any other optical processing can be followed in order to make the target image resemble the original binary image. If we perform correlation process by computer, auto-recognition can be realizable. Because Fig. 4 is generated by two phase-only-masks, these masks can not be copied by an intensity modulator. These masks can be invisible parts of credit cards and also be well encrypted.

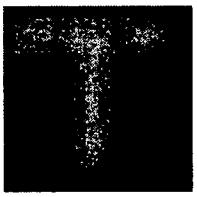

Fig. 4. The target image

3.3 The optical setup

If two lights are orthogonally polarized and these are added, the total light U(t) can be written as

$$\boldsymbol{U}(t) = \mathbf{X}\, A\cos(\omega t) \quad + \quad \mathbf{Y}\, B\cos(\omega t - \phi) \qquad (1)$$

Where

X : x-axis unit vector, **Y** : y-axis unit vector

A, B : the amplitude of each light

ω : angular frequency, ϕ : the phase difference

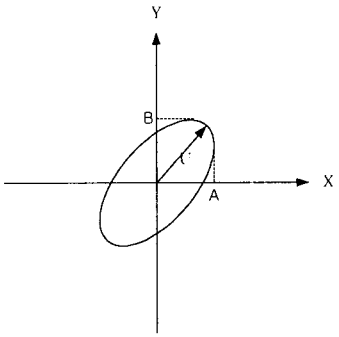

Fig. 5. The sum of two orthoganally polarized lights

Figure 5 presents the amplitude of (1) in the x-y plane. The vector $\boldsymbol{U}(t)$ can rotate in counterclockwise or clockwise. The intensity of $\boldsymbol{U}(t)$ is proportional to time average of square of amplitude $\boldsymbol{U}(t)$. We can verify that the intensity of the sum of two orthogonally polarized lights is proportional to sum of each intensities of two lights through the one period integration of the square of the $\boldsymbol{U}(t)$,i.e. incoherent. So in order to minimize undesired interference noises owing to the refractive index change, we can substitute first beamsplitter in the interferometry with a PBS.

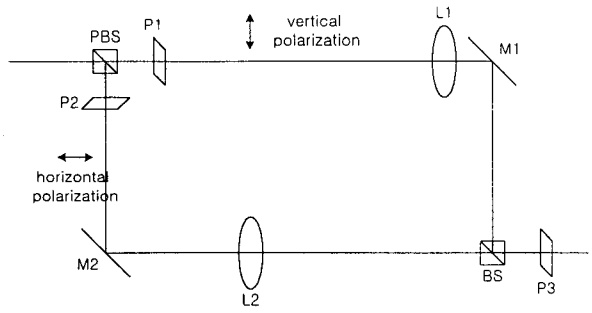

Fig. 6. The optical setup

Fig. 6 is the proposed decryption optical setup. We use Mach-Zejnder interferometer and first beam splitter is substituted with a PBS. P1 and P2 is the location of phase-masks (Fig. 2(e) and Fig. 2(f)). And P3 is the output plane. In P3 plane we can detect the target image. Because two light in each path are orthogonally polarized, two intensity images of inverse Fourier transform of phase mask images in P1 and P2 are added in P3 plane in the sense of intensity. L1 and L2 have same focal length. The distances from P1 to L1 , from P2 to L2 and from P3 to each lens are all same. If wrong mask is loaded in P1 and P2 planes, the output images is different from the target image. The image in the P3 plane can be captured by CCD camera. This obtained image is correlated with the target images already stored in the computer. When the image is captured by CCD camera, it is expected to be free from the noise.

4.Conclusion

In this paper, we encrypted images by using a random partition and a random diffusing. And we propose the method of minimization the noise of refractive index change by using orthogonally polarized lights. The production of actual phase masks and optical experiments are remained.

References

[1] B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification", vol. 33, no. 6, pp. 1752-1756, 1994. 6.

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

[3] B. Javidi, "Optical Information Processing for Encryption and Security Systems", Optics & Photonics News, pp. 28-33, 1997. 3.

[4] R. K. Wang, I. A. Watson, and C. Chatwin, "Random phase encoding for optical security", Opt. Eng., vol. 35, no. 9, pp. 2464-2469, 1996. 9.

[5] B. Javidi, "Optical spatial filtering for image encrpytion and security systems", Proc. of SPIE, vol. 3386, pp. 14-23, 1998. 4.

[6] T. Nomura, "Encryption using joint-transform correlator architecture for robust alignment", SPIE's newsletter, p. 4, 1998. 12.

[7] J.-Y. Kim, S.-J. Park, S.-J. Kim, J.-G. Bae, Y.–H. Doh, and C.-S. Kim, "Optical Encryption System using a Computer Generated Hologram", Journal of the OSK, vol. 4, no. 1, pp.19-22, 2000. 3.

[8] J.-Y. Kim, S.-J. Park, J.-G. Bae, C.-S. Kim, and S.-J. Kim, "Optical image encryption using interferometry-based phase masks", To be published in Electronics Letters.