Phase-based virtual image encryption and decryption system using Joint Transform Correlator

Dong-Hoan Seo[a], Kyu-Bo Cho[a], Se-Joon Park[a],
Woong-Ho Cho[b], Duck-Soo Noh[c] and Soo-Joong Kim[a]

[a]Department of Electronic Eng., Kyungpook Nat'l University, Taegu, Korea
[b]Department of Computer Science, Taegu technical college, Taegu, Korea
[c]Department of Electronic and Information Eng., Kyungil University, Taegu, Korea

Abstract: In this paper a phase-based virtual image encryption and decryption techniques based on a joint transform correlator (JTC) are proposed. In this method, an encrypted image is obtained by multiplying a phase-encoded virtual image that contains no information from the decrypted image with a random phase. Even if this encryption process converts a virtual image into a white-noise-like image, the unauthorized users can permit a counterfeiting of the encrypted image by analyzing the random phase mask using some phase-contrast technique. However, they cannot reconstruct the required image because the virtual image protects the original image from counterfeiting and unauthorized access. The proposed encryption technique does not suffer from strong auto-correlation terms appearing in the output plane. In addition, the reconstructed data can be directly transmitted to a digital system for real-time processing. Based on computer simulations, the proposed encryption technique and decoding system were demonstrated as adequate for optical security applications.

Keywords: optical security, image encryption, JTC, random phase, SLM, square law device

1. INTRODUCTION

Optical information processing systems are useful for security applications due to their ability for parallel and high-speed processing. And optical security systems present a good potential for those tasks, because they can provide a large degree of freedom to secure data. So many researches are currently focused on optical security systems[1-4]. The double random-phase encoding encryption technique[1] uses two statistically independent random phase masks in the input and Fourier planes to encrypt an image into stationary white noise. To recover the encrypted data, a key phase card, the complex conjugate of the random phase mask used in the encoding process, is used in the Fourier plane of a 4f-correlator system. This method requires an accurate optical alignment and an exact complex conjugate of the key mask used in the encoding process.

The joint transform correlator (JTC)[5-6] has been found to be a useful alternative to a 4-f correlator system since it can alleviate the need for an accurate optical axis alignment. If a JTC is used for optical security applications, the same key phase mask is used in the decoding process. In addition, the JTC has a good potential for real-time processing. However, the main drawback of a JTC system, when it is used in optical information processing, is that it always suffers from appearing strong auto-correlation terms in the output plane. It is very difficult to find cross-correlation terms before they are removed. A lot[7-8] of research has been focused on alleviating the drawback of a JTC both optical and digital. A simple and efficient method is subtracting the DC terms digitally. However, this requires some preprocessing before the subtraction operation is performed. Nonetheless, in spite of its drawback, the JTC is a very attractive architecture for optical information systems. Recently, an optical double random-phase encryption method using JTC architecture was proposed by T. Nomura and B. Javidi. In this method, an image with an input phase code attached is placed side by side with a key

code in the JTC input plane. The inverse Fourier transform of a random phase mask is used as the key code. The joint power spectrum (JPS) is then recorded as the encrypted data. The decryption process is performed by a 4f-correlator system. The key phase mask used on the input plane is Fourier transformed and then multiplied with the encrypted data in the Fourier plane. This method does not require the production of a complex conjugate of the key phase mask. However, since the decryption process is performed by a 4f-correlator system, it still has the optical axis alignment problem. Yet the encrypted JPS includes strong auto-correlation terms, which can disturb the identification of the decoded image, and since the JPS is real-valued function, so an intensity detector, such as a CCD camera and scanner, can copy the encrypted code.

In this paper a phase-based virtual image encryption and decryption techniques using joint transform correlator (JTC) are proposed. In this method, a virtual image which contains no information from the decrypted image is encoded into a phase function, and then the phase function to be encrypted is first multiplied by a random phase mask, Fourier-transformed. Even if this encryption process converts a virtual image into a white-noise-like image, the unauthorized users can permit a counterfeiting of the encrypted image by analyzing the random phase mask using some phase-contrast technique. However, they cannot reconstruct the required image because the virtual image protects the original image from counterfeiting and unauthorized access. And a Fourier transform of the phase encoded decrypting image that is generated by a kind of XOR operation rule is used as the key code. For decryption, the encrypted image is used for one half of the joint input plane, while the key code is used for the other half. After the joint input plane is inverse Fourier transformed, the required binary image can then be reconstructed on a square law device, such as a CCD camera. The proposed encryption technique does not suffer from strong auto-correlation terms appearing in the output plane. In addition, the reconstructed data can be directly transmitted to a digital system for real-time processing. Based on computer simulations, the proposed encryption technique and decoding system were demonstrated as adequate for optical security applications.

2. BINARY IMAGE ENCRYPTION

Let f(x,y), r(x,y), and e(x,y) denote the binary virtual image to be encrypted, binary random image, and the encrypted image, respectively. The original binary image has two values of '1' or '0'. In this method, the binary image is encoded into a phase function. Binary random noise-like patterns are then generated by a digital computing process and also encoded into a phase function. Both two-phase encoded images have two phase values of '0' and 'π' and a uniform amplitude transmittance. The encrypted image is obtained by multiplying the phase function with the random phase function. The encrypted imagee(x,y) is given by

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

The encrypted image also has a uniform amplitude transmittance. A Fourier transform of the encrypted image is used as the encrypted data $E(u,v)$, and a Fourier transform of the phase encoded decrypting image that is generated by a kind of XOR operation rule is used as the key code $D(u,v)$. The encrypted data and key code are fully complex-valued. They can be fabricated by a digital computing process and optical lithography, or they can be displayed on a spatial light modulator, such as a LCD. The complex-valued encrypted data is divided into an amplitude and phase component. The amplitude can be recorded on film and the phase component is recorded by optical lithography. When attached to each other, the encrypted data can be used on a credit card or ID card. Plus the original image can only be reconstructed with the correct decrypting key code because illegal users cannot reconstruct the required image because the virtual image protects the original image from counterfeiting and unauthorized access.

3. JTC DECRYPTION SYSTEM

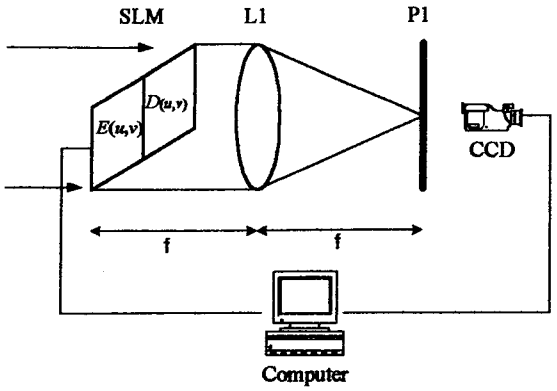

Fig. 1. Scheme of joint transform correlator.

The JTC decryption system is the same as in Fig.1. The encrypted data is used on the joint input plane along with the key code. They are seperated by a distance of $2u_0$, note that the joint input plane is a frequency-domain, as such, the joint input plane can be expressed as

$$\mathrm{JTC}(u, v) = E(u - u_0, v) + D_2(u + u_0, v) \quad (2)$$

Then the joint input plane is inverse Fourier transformed by L1, and is given by

$$\begin{aligned} \mathrm{jtc}(x, y) &= e(x, y)\exp[j2\pi(u_0 x, y)] \\ &\quad + d(x, y)\exp[-j2\pi(u_0 x, y)] \end{aligned} \quad (3)$$

where $\exp[j\,2\pi u_0\, x]$ is the phase shift term caused by the frequency shift term of Eq. (2). The CCD camera located at P1 plane captures the JPS, and the intensity is given by

$$\begin{aligned} &|\mathrm{jtc}(x, y)|^2 \\ &= |e(x,y)|^2 + |d(x,y)|^2 \\ &\quad + v_p(x,y) r_p(x,y) d(x,y)\exp[j4\pi(u_0 x, y)] \\ &\quad + v_p(x,y) * r_p(x,y) * d(x,y)^* \exp[-j4\pi(u_0 x, y)] \\ &= 1 + 1 \\ &\quad + \exp[j\pi\alpha(x,y)]\exp[j4\pi(u_0 x, y)] \\ &\quad + \exp[-j\pi\alpha(x,y)]\exp[-j4\pi(u_0 x, y)] \\ &= \begin{cases} 2 + 2\cos[4\pi(u_0 x, y)], & \alpha(x, y) = 0 \\ 2 - 2\cos[4\pi(u_0 x, y)], & \alpha(x, y) = 1 \end{cases} \end{aligned} \quad (4)$$

where $\alpha(x,y) = v_p(x,y) r_p(x,y) d(x,y)$

If the phase term sets to '1', then eq. (4) is

$$|jtc(x,y)|^2 = \begin{cases} 4, & \alpha(x, y) = 0 \\ 0, & \alpha(x, y) = 1 \end{cases} \quad (5)$$

This means that the negative image of the original image can be reconstructed on a CCD camera. Note that the auto-correlation terms of Eq. (4) contribute to reconstructing the original image rather than disturbing its identification. As such they are not irritating terms in the proposed encryption method. Accordingly, the proposed encryption method is very useful for JTC architecture

4. COMPUTER SIMULATION

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. 2(a), (b), and (c). These images were encoded into phase components. The encrypted image $e(x, y)$ is obtained by multiplying a phase-encoded virtual image and a phase-encoded random image as shown in Fig. 2(d). Note, $e(x, y)$ is a pure phase function and presented as amplitude-encoded data since it can not be seen. The encrypted image is similar to random noise-like patterns.

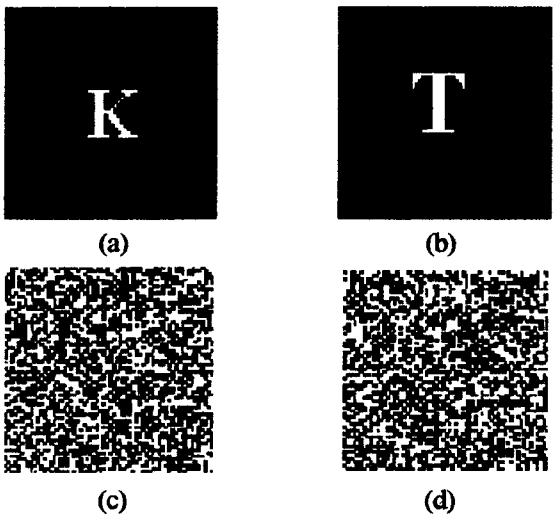

Fig. 2. Images used for proposed encryption technique: (a) an original image $f(x, y)$, (b) a virtual image $v(x, y)$ (c) random image $r(x, y)$, (d) encrypted image $e(x, y)$.

The encrypted data $E(u,v)$ is obtained by performing a Fourier transformation of the encrypted image, as shown in Fig. 3(a) and the key code is shown in Fig.

3(b). The size of each image is 64 × 64. In this case the size of the input plane was 64 × 128. The reconstruted image is shown in Fig. 3(c)

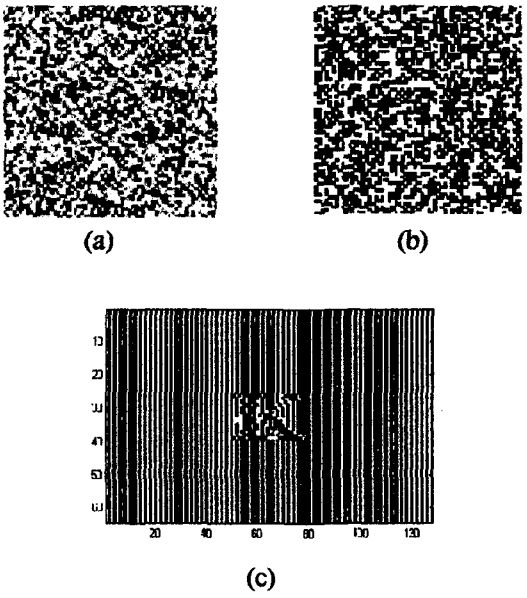

Fig. 4 Computer simulation results: (a) the encrypted data of Fig. 2(d), (b) the key code, (c) the reconstructed image

As such, the main drawback of JTC becomes a useful element in the proposed encryption technique. In addition, if the reconstruction is performed on a CCD camera, the image can be directly sent to digital equipment. Accordingly, the proposed technique is also useful for real-time processing.

5. CONCLUSION

In this paper an encryption technique that can utilize the advantages of JTC architecture which dose not require an accurate optical alignment and virtual image which does not contain any information of original image is proposed. For encryption, a binary virtual image is encoded into a purely phase component. Next, binary random noise-like patterns are generated by a digital computing process and also encoded into a phase function. An encrypted image is then obtained by multiplying the phase function with the random phase function. The encrypted data is a fully complex-valued function. As such, it can not be copied or reproduced by an intensity detector, such as a CCD camera or scanner. In addition, the original image can only be reconstructed with the correct key code. In the proposed method, the auto-correlation terms of the output plane contribute to reconstructing the original image rather than disturbing its identification, thereby solving the main drawback of JTC architecture. Finally, since the decryption process can be performed on a CCD camera, the obtained data can be directly transmitted to digital devices or communication lines. Accordingly, the proposed technique has good potential for real time processing.

References

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

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

[3]. L. G. Neto, "Implementation of Image Encryption using the Phase-Contrast Technique," *proceedings of SPIE*, vol. 3386, pp. 284-290, 1998.

[4]. C. S. Weaver and J. W. Goodman, "Technique for optically convolving two functions," *Appl. Opt.*, vol. 5, pp. 1248-1249, 1966.

[5]. S. Zhong, J. Jiang, S. Liu, and C. Li, "Binary joint transform correlator based on differential processing of the joint transform power spectrum," *Appl. Opt.*, vol. 8. pp. 1776-1780, 1997.

[6]. C. J. Kuo, "Joint transform correlation improved by means of the frequency selective technique," *Opt. Eng.*, vol. 33, no. 2, pp. 522-527, 1994.

[7]. W. Yu, K. Nakagawa, and T. Minemoto, "All-optical subtracted joint transform correlator with a holographic interferomer," *Appl. Opt.*, vol. 36, no. 35, pp. 9205-9210, 1997.

[8]. T. Nomura and B. Javidi, "Optical encryption using a joint transform correlator architecture," *Opt. Eng.*, vol. 39, No. 8, pp. 2031-2035, 2000.