Optical Cryptography System Based on Joint Transform Correlation

M. Nazrul Islam
Email: islamn@farmingdale.edu
Security Systems, Farmingdale State University of New York, 2350 Broad Hollow Road, Farmingdale, New York

Abstract: The paper presents a review of optical cryptography techniques using joint transform correlation (JTC) algorithm. The given input image contains confidential information, such as personal identification, photo, which is then encrypted using an encryption key. Optical JTC technique is employed to perform the encryption and decryption processes using optical lenses and other equipments. The input image and the key are introduced to the same input plane which is then Fourier transformed. Joint power spectrum (JPS) of the resultant signal is recorded and inverse Fourier transformed to derive the encrypted signal. At the receiving end, the received encrypted signal is first Fourier transformed and multiplied by the key used in encryption. Inverse Fourier transformation retrieves the original information without any distortion. The JTC techniques are simple and fast, which would offer excellent and efficient cryptography systems for real-time applications.

Key Words: security systems, encryption, decryption, address code, joint transform correlation, fringe-adjusted filter.

Introduction

Information security has been drawing significant research interest recently because of a number of malicious activities in the computer network. Also the topic is getting more involved into the engineering curriculum in order to prepare the future engineers and scientists to efficiently handle the emerging security threats. One of the most important objectives of information security systems is to secure the confidential information, which includes personal identification number, personal data, as well as graphical information like photo, fingerprint. Securing information can only be done through the use of cryptography technology, which involves encryption of the information before transmission and then successful reproduction of the information at the receiving end. Traditional encryption schemes suffer from poor security because a random code has the probability to retrieve all or some of the secure information. Optical joint transform correlation (JTC) offers a nonlinear encoding process which is very difficult to break without knowing the code as well as the process [1]. Also it does not require any complex conjugate of the address code for decryption purpose and accurate alignment of devices for implementation of the technique in optical domain. Several other optical information security systems have been proposed in the literature, which include double phase-encoding with random masks [2], polarization encoding [3], multiplexed minimum average correlation energy phase-encrypted filter [4], exclusive-OR encryption [5], fractional Fourier transformation [6], shifted phase-encoded JTC [7], and multiple phase-shifted reference-based JTC [8].

The main objective of this paper is to compare the optical cryptography techniques. The techniques are investigated using computer simulation and then their performances are compared to evaluate the development of the research in the field and to identify the future directions on how to improve the techniques for efficient practical implementations. The paper also focuses on

efficient teaching of optical cryptography techniques in the engineering as well as science curriculum.

Analysis

Classical JTC

Optical image processing systems employ optical lenses, spatial light modulator, laser light source and CCD camera, which offer extremely fast processing of information. Optical security system based on classical JTC technique introduces the input image, $t(x, y)$, and the address code, $c(x,y)$, side-by-side in a joint image plane, which is given by

$$f(x,y) = t(x,y) + c(x,y) \tag{1}$$

Application of Fourier transformation to Eq. (1) yields the joint power spectrum (JPS) as follows.

$$E_1(u,v) = |F(u,v)|^2 = |T(u,v)|^2 + |C(u,v)|^2 + T(u,v)C^*(u,v) + T^*(u,v)C(u,v) \tag{2}$$

where $F(u,v)$, $T(u,v)$ and $C(u,v)$ denote the Fourier transforms of $f(x,y)$, $t(x,y)$ and $c(x,y)$, respectively, and the superscript * represents a complex conjugate of the original signal. It is assumed that the code $C(u,v)$ is a phase-only signal and therefore, $|C(u,v)|^2$=1.0. The JPS, $E(u,v)$, is inverse Fourier transformed to obtain the encrypted data as given by

$$e_1(x,y) = t(x,y) \otimes t(x,y) + \delta(x,y) + t(x,y) \otimes \delta(x,y) + t(x,y) \otimes \delta(x,y) \tag{3}$$

where $\otimes$ denotes the convolution operation.

Then, for decryption purpose, the encrypted image is first Fourier transformed and then multiplied by the same address code. It produces the output as

$$D_1(u,v) = E(u,v)C(u,v) = |T(u,v)|^2 C(u,v) + C(u,v) + T(u,v) + T^*(u,v)C(u,v)C(u,v) \tag{4}$$

Inverse Fourier transformation to Eq. (4) yields the decrypted image. It can be observed from Eq. (4) that the output plane contains unwanted noisy signals in addition to the original image.

JTC with Fourier Plane Power Subtraction

To overcome the effect of auto-correlation terms, which produces noisy signal in the output plane of the classical JTC technique, the JPS signal is modified using the following relation.

$$E_2(u,v) = E_1(u,v) - |T(u,v)|^2 - |C(u,v)|^2 = T(u,v)C^*(u,v) + T^*(u,v)C(u,v) \tag{5}$$

This process requires evaluation of the autocorrelation of the input image and that of the address code, which could be in parallel channel to the main JTC processing channel. The encrypted image is given by

$$e_2(x,y) = t(x,y) \otimes \delta(x,y) + t(x,y) \otimes \delta(x,y) \tag{6}$$

The original image can now be retrieved from Eq. (6) by first Fourier transforming the received signal, multiplying it with the address code and finally taking inverse Fourier transformation. Thus the output signal is given by

$$d_2(x,y) = t(x,y) + t(x,y) \otimes \delta(x,y) \tag{7}$$

It can be observed from Eq. (7) that there still exists an unwanted correlation term in the output signal which might produce noises.

Shifted Phase-Encoded JTC

Here the address code is first phase-encoded using a random phase mask, $\phi(x, y)$. The phase-encoded address codes can be expressed as

$$c_2(x,y) = c(x,y) \otimes \phi(x,y) \tag{8}$$

Next, the phase-encoded address code is fed to two channels where one channel introduces a phase shift of 180^0. The input image is introduced to both the channels to form two input joint images as given by

$$f_1(x,y) = c(x,y) \otimes \phi(x,y) + t(x,y) \tag{9}$$

$$f_2(x,y) = -c(x,y) \otimes \phi(x,y) + t(x,y) \tag{10}$$

After applying Fourier transformation to Eqs. (9) and (10), two JPS signals can be obtained which are then combined to get a modified JPS signal as stated in the following equation.

$$E_3(u,v) = \left[|F_1(u,v)|^2 - |F_2(u,v)|^2 \right] = 2 \times \left[T(u,v) C^*(u,v) + T^*(u,v) C(u,v) \right] \tag{11}$$

where it is assumed that $|\Phi(u,v)|^2=1.0$, because $\Phi(u,v)$ is a phase-only mask. The encrypted image can be obtained by applying inverse Fourier transformation to Eq. (11).

$$e_3(x,y) = 2\left[t(x,y) \otimes c^*(x,y) \otimes \phi^*(x,y) + t^*(x,y) \otimes c(x,y) \otimes \phi(x,y) \right] \tag{12}$$

For decryption purpose, the encrypted image is first Fourier transformed and then multiplied by the phase mask and the address code. Thus the output can be written as

$$D_3(u,v) = E_3(u,v) C(u,v) \Phi(u,v) = 2\left[T(u,v) + T^*(u,v) C(u,v) C(u,v) \Phi(u,v) \Phi(u,v) \right] \tag{13}$$

It can be observed from Eq. (13) that the first term yields the decrypted image without any distortion. The second term may result in noisy signals in the output plane, but as it is multiplied by the random phase mask twice in the Fourier domain, it will be scattered in various directions in the spatial domain and thus have minimal impact on the decryption process.

Multiple Phase-Shifted Reference-based JTC

This technique feeds the address code to four parallel processing channels with phase shifting by 0^0, 90^0, 180^0, and 270^0, respectively. Then the input image is introduced to each of the phase-shifted codes to form four joint images as given by

$$f_1(x,y) = c(x,y) + t(x,y) \tag{14}$$

$$f_2(x,y) = jc(x,y) + t(x,y) \tag{15}$$

$$f_3(x,y) = -c(x,y) + t(x,y) \tag{16}$$

$$f_4(x,y) = -jc(x,y) + t(x,y) \tag{17}$$

The joint images result in four JPS signals after Fourier transformation. The JPS signals are again phase-modulated and combined to form a modified JPS as given by

$$E_4(u,v) = |F_1(u,v)|^2 + j|F_2(u,v)|^2 - |F_3(u,v)|^2 - j|F_4(u,v)|^2 = 4C^*(u,v) T(u,v) \tag{18}$$

Then the encrypted image can be produced from inverse Fourier transform of the JPS in Eq. (18) as given by

$$e_4(x,y) = 4c(x,y) \otimes t(x,y) \tag{19}$$

Then the received encrypted image is Fourier transformed and multiplied with the Fourier transformation of the address code to obtain the decrypted image.

$$D_4(u,v) = E_4(u,v) C(u,v) = 4T(u,v) \tag{20}$$

Fringe-Adjusted Filter

The decrypted output can be made distortion-free by employing a fringe-adjusted filter (FAF) before applying the inverse Fourier transform operation. The FAF transfer function is given by

$$H(u,v) = \frac{a(u,v)}{\left[b(u,v) + |C(u,v)|^2\right]} \tag{21}$$

where $a(u,v)$ and $b(u,v)$ are either constants or functions of u and v. The parameter $a(u,v)$ is used to avoid having an optical gain greater than unity, while $b(u,v)$ is used to overcome the pole problem otherwise associated with a normal inverse filter. Since the power spectra of the address code can be pre-calculated, implementation of this filter does not deteriorate the system processing speed. Therefore, the filtered image can be written in the Fourier domain as

$$D_f(u,v) = D(u,v)H(u,v) \tag{18}$$

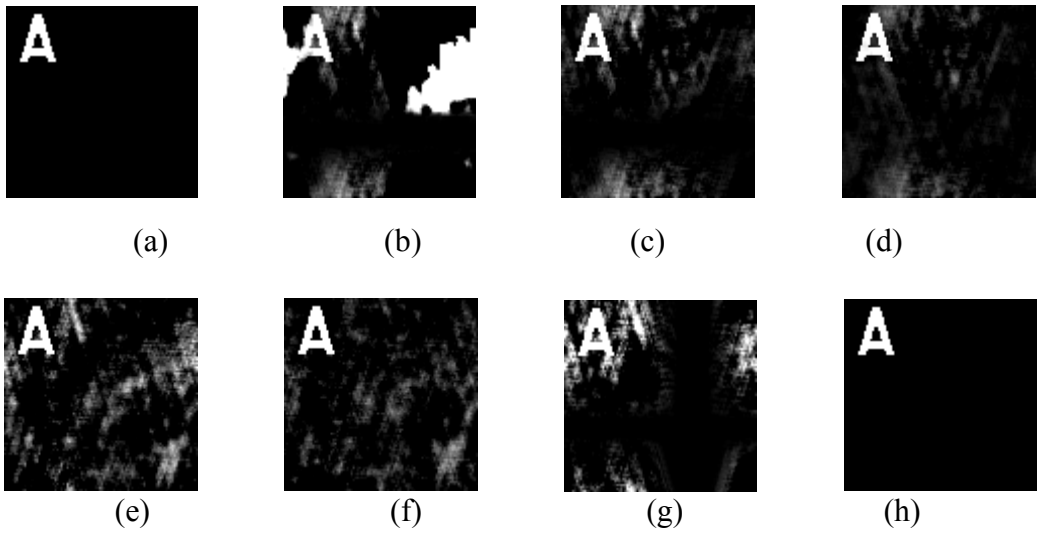


Figure 1: Encryption and decryption performance of different optical security systems involving a single binary character: (a) input image, (b) decrypted image using classical JTC technique, (c) decrypted image using JTC with power subtraction, (d) decrypted image using JTC with power subtraction and FAF, (e) decrypted image using SPJTC technique, (f) decrypted image using SPJTC technique and FAF, (g) decrypted image using MRJTC technique, and (f) decrypted using MRJTC and FAF

Simulation Results

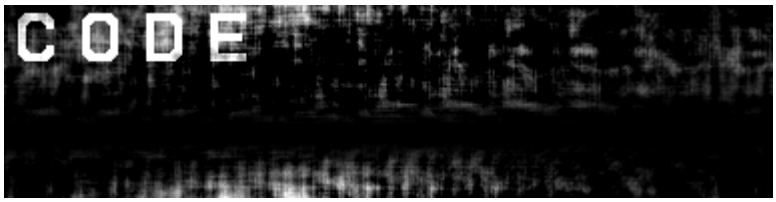
The optical information security systems were investigated using a computer simulation program developed in MATLAB. The FAF filter was designed with $a(u,v) = 1.0$ and $b(u,v) = 10^{-4}$. Figure 1(a) shows the input binary image which is fed to encryption technique along with a random code. The decrypted image using a classical JTC is shown in Fig. 1(b) which indicates that the technique fails in successfully retrieving the whole original information. Figure 1(c) shows the decrypted image obtained from the JTC technique with Fourier plane power subtraction, which represents a significant improvement over the classical JTC technique by removing extraneous autocorrelation noisy signals. Further improvement in the decrypted image can be observed from

Fig. 1(d) after applying FAF operation. The decrypted image shown in Fig. 1(e) employs the SPJTC algorithm which is successful in recovering the information with less amount of noise as compared to the previous two techniques. But after introducing the FAF operation, a much better and faithful reproduction of the original information has been observed as depicted in Fig. 1(f). Finally, the MRJTC technique produces the decrypted image as shown in Fig. 1(g). However, incorporation of the FAF in the MRJTC technique yields the best decryption of original image as depicted in Fig. 1(h), with almost negligible amount of noise.

Next a string of binary characters "CODE" was considered for investigation as shown in Fig. 2(a). The classical JTC technique is not at all successful in retrieving the original information as shown in Fig. 2(b). The filter FAF could improve the performance of the JTC technique as we can see in Fig. 2(c). Other techniques, namely, JTC with power subtraction, SPJTC and MRJTC, are observed to perform better as shown in Figs. 2(d) – 2(h). It can be obvious that the MRJTC technique with FAF offers the best security performance.

(a)

(b)



(c)

(d)

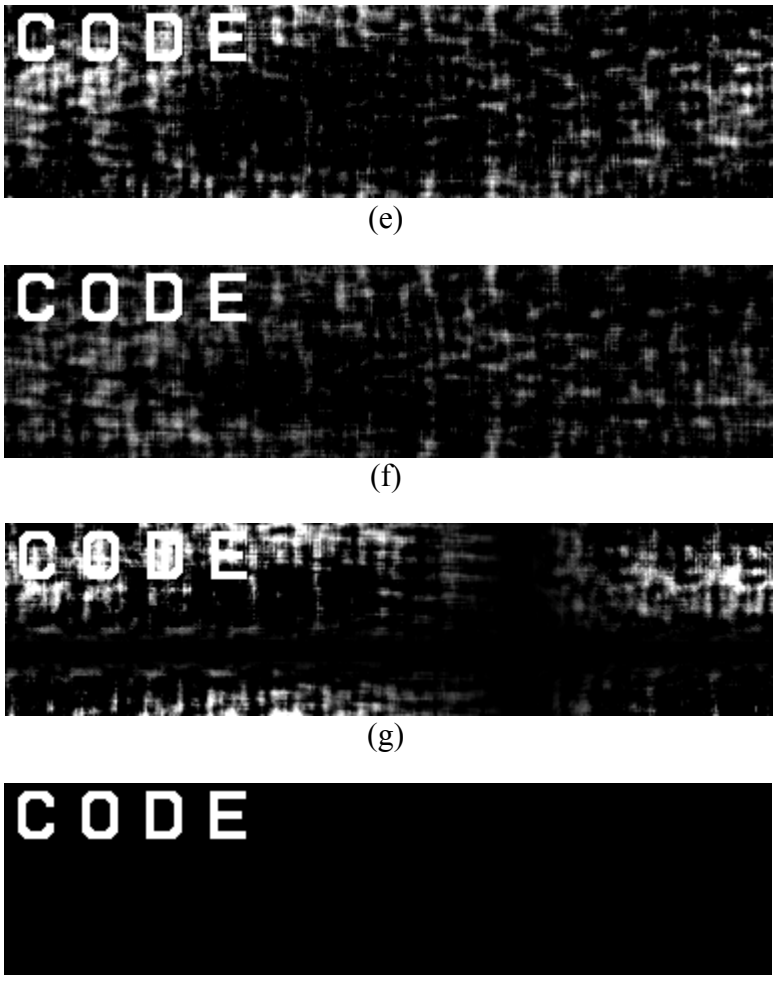


Figure 1: Encryption and decryption performance of different optical security systems involving a single binary character: (a) input image, (b) decrypted image using classical JTC technique, (c) decrypted image using JTC with power subtraction, (d) decrypted image using JTC with power subtraction and FAF, (e) decrypted image using SPJTC technique, (f) decrypted image using SPJTC technique and FAF, (g) decrypted image using MRJTC technique, and (f) decrypted using MRJTC and FAF

Conclusion

Four optical cryptography techniques have been analyzed and simulated in this paper, which includes classical joint transform correlation (JTC), JTC with power subtraction, shifted phase-encoded JTC (SPJTC) and multiple phase-shifted reference-based JTC (MRJTC). Each of the techniques has also been investigated with incorporation of a fringe-adjusted filter (FAF). Performances of the cryptography techniques have been evaluated using test images. It has been observed that classical JTC performs the worst because it includes lots of noises in the recovered image. If the number of characters in the information gets larger, the JTC technique even fails in retrieving any information. On the other hand, the MRJTC technique yields the best performance

if incorporated with the filter FAF, which recovers the whole information with almost no noise in the output plane. The only problem with the MRJTC technique is that it might be slower because of four parallel processing channels. Future research should be carried out in reducing the number of processing steps while producing a faithful and efficient cryptography performance.

Optical cryptography techniques would be excellent topics in engineering and science curriculum because they offer real-time processing of information and hence making a decision. The topic may be presented efficiently using block diagrams of optical systems and simulation results of the security features offered by the techniques, where a significant interest of the students can be developed.

References

[1] T. Nomura and B. Javidi, "Optical encryption using a joint transform correlator architecture," *Optical Engineering*, vol. 39, no. 8, pp. 2031–2035, 2000.

[2] 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.

[3] B. Javidi and T. Nomura, "Polarization encoding for optical security systems," *Optical Engineering*, vol. 39, no. 9, pp. 2439 – 2443, 2000.

[4] Y. H. Doh, J. S. Yoon, K. H. Choi and M. S. Alam, "Optical security system for the protection of personal identification information," *Applied Optics*, vol. 44, no. 5, pp. 742 – 750, 2005.

[5] B. Javidi, L. Bernard and N. Towghi, "Noise performance of double-phase encryption compared to XOR encryption," *Optical Engineering*, vol. 38, no. 1, pp. 9 – 19, 1999.

[6] A. Sinha and K. Singh, "Image encryption by using fractional Fourier transform and jigsaw transform in image bit planes," *Optical Engineering*, vol. 44, no. 5, pp. 057001-1 – 057001-6, 2005.

[7] M. N. Islam and M. S. Alam, "Optical security system employing shifted phase-encoded joint transform correlation," *Optics Communications*, vol. 281, pp. 248 – 254, 2008.

[8] M. N. Islam, M. A. Karim, M. S. Alam and K. V. Asari, "Optical security system using multiple phase-shifted reference-based joint transform correlation," (invited paper), *Proceedings of SPIE in Optical Pattern Recognition XXI*, 2010.