Virtual optical image encryption based on double random amplitude encoding

Binyao Gong

College of Energy Engineering, Yulin University, Yulin 719000, Shaanxi, China

gby56@sohu.com

Keywords: Image encryption; double random amplitude encoding; virtual optical system; blind deconvolution

Abstract. A new optical encryption system is presented in this paper. By replacing the random phase plates by random amplitude plates in the double random phase encoding system, a novel optical encryption system is formed. The Statistical characteristics of the autocorrelation function of the encoded image are investigated; we found that the original image had been changed into a complex-amplitude stationary white noise. As a result, this approach proved to be robustness against brute force attack. Computer simulations are performed and the results are consistent with theoretical analysis. Moreover, some properties of this method prior to double random phase encoding system are discussed.

Introduction

Along with the wide use of the Internet, the safety and secrecy of information has attracted much attention. Among various encryption strategies, the optical encryption technique is considered an important topic, since it possesses unique characteristics, such as multi-parameter capability and parallel processing [1-6]. The pioneering work on optical encryption, which was devoted by Refregier and Javidi in 1995, is based on double random phase encoding (DRPE) scheme [7]. This method uses two statistically independent random phase masks in the input and the Fourier planes to encrypt an image into stationary white noise. This DRPE scheme has spawned several variation techniques and has been applied in many situations. For instance, Unnikrishnan et al. [8] and Situ and Zhang [9] extended DPRE to Fractional Fourier and Fresnel domain, respectively, from the standard Fourier domain.

In this paper, we propose a new optical encryption method by replacing the random phase masks with random amplitude masks in the DRPE system and call it double random amplitude encoding (DRAE) scheme. We show that this system also allows one to encode a primary image into a stationary white noise. It deserves to be specially noted that this method has some superiorities over the DRPE scheme. For example, it decreases the demands of the statistical properties of the random masks, that is, the secret keys in the space domain and Fourier domain are more easily to be obtained. At the same time, this method behaves more robustly compared with the DRPE system while the secret key of the Fourier domain is disclosed.

Theoretical Analysis and Computer Simulation

The optical encryption scheme based on double random amplitude encoding is illustrated in Fig. 1. A standard of 4f optical signal processor that in was applied, in which a host image or plaintext, f(x, y), was placed on the input plane of the 4f system and an encrypted image was obtained at the output plane of the system. The encryption process can be briefly described as follows: the host image bonds with a random amplitude key, n(x, y); a random phase mask is used as one of the encryption keys; and the first-step encrypted image f(x, y) $\times$n(x, y) is then transformed to the spatial frequency domain,

Published by Atlantis Press, Paris, France.
© the authors

where it is further encrypted with another amplitude key b(μ, ν) to obtain the second-step encrypted image.

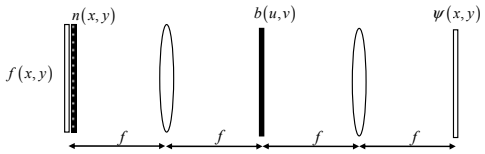


Fig. 1 Schematic of double random amplitude encoding optical encryption system.

In this system, the encryption keys are required to be mutually independent and have zero means. The output encryption of the plaintext is expressed as

$$\psi(x,y)=\left[f(x,y)n(x,y)\right]\otimes h(x,y) \tag{1}$$

Where $\otimes$ denotes the convolution operation and h(x, y) is defined as

$$h(x,y)=\mathrm{FT}^{-1}\left[b(u,v)\right] \tag{2}$$

Where FT-1 denotes the inverse Fourier transform. It will be shown in the following analysis that the encoded image ψ(x, y) is a stationary white noise.

First of all, let us consider the statistical properties of r(x, y), which is given by

$$r(x,y)=f(x,y)n(x,y) \tag{3}$$

It is easily shown that the expection of r(x, y) is zero. Then the autocorrelation function of ψ(x, y) can be calculated by

$$\begin{aligned}&E\left[r^*(x,y)r(x+\tau,y+\beta)\right]\\&=E\left[f^*(x,y)f(x+\tau,y+\beta)n^*(x,y)n(x+\tau,y+\beta)\right]\\&=f^*(x,y)f(x+\tau,y+\beta)E\left[n(x,y)n(x+\tau,y+\beta)\right]\end{aligned} \tag{4}$$

Where E stands for the expected value, * stands for complex conjugate, and (x, y) are shifts in the spatial domain. Because n(x, y) is a white noise with a zero mean, Eq. (4) could be further simplified

$$\begin{aligned}&f^*(x,y)f(x+\tau,y+\beta)E\left[n(x,y)n(x+\tau,y+\beta)\right]\\&=f^*(x,y)f(x+\tau,y+\beta)\delta(\tau,\beta)\\&=\left|f(x,y)\right|^2\end{aligned} \tag{5}$$

Where δ(τ, β) is the Kronecker delta function. Eq. (5) indicates that r(x, y) is nonstationary and its autocorrelation function is equal to the square of the host image. Since it is required that the encrypted image should be a stationary white noise to be robust against blind decryptions， another random amplitude mask b(μ, ν) is necessary for the encryption of the host image[7]. According to the definition of discrete convolution, ψ(x, y) is given by

$$\psi(x,y)=\sum_{\eta=0}^{N-1}\sum_{\zeta=0}^{M-1}f(\eta,\xi)n(\eta,\xi)h(x-\eta,y-\xi) \tag{6}$$

Then we have

$$\begin{aligned}&E\left[\psi^*(x,y)\psi(x+\tau,y+\beta)\right]=\sum_{\eta=0}^{N-1}\sum_{\xi=0}^{M-1}\sum_{\lambda=0}^{N-1}\sum_{\gamma=0}^{M-1}f^*(\eta,\xi)f(\lambda,\gamma)\\&E\left[n(\lambda,\gamma)n(\eta,\xi)\times h^*(x-\eta,y-\xi)h(x+\tau-\lambda,y+\beta-\gamma)\right]\end{aligned} \tag{7}$$

However, because n(x, y) and b(μ, ν) are independent, then

$$\begin{aligned}&E\left[\left(n(\lambda,\gamma)n(\eta,\xi)\right)\times h^*(x-\eta,y-\xi)h(x+\tau-\lambda,y+\beta-\gamma)\right]\\&=E\left[n(\lambda,\gamma)n(\eta,\xi)\right]E\left[h^*(x-\eta,y-\xi)h(x+\tau-\lambda,y+\beta-\gamma)\right]\end{aligned} \tag{8}$$

And it has been shown in Eq. (5) that

© the authors

$$E\left[n(\lambda,\gamma)n(\eta,\xi)\right]=\delta(\lambda\text{-}\eta,\gamma\text{-}\xi) \tag{9}$$

Because h(x, y) could be expressed according to the definition of discrete Fourier transform, we have

$$h(x,y)=\frac{1}{M\times N}\sum_{u=0}^{N-1}\sum_{v=0}^{M-1}b(u,v)\exp\left[j2\pi(xu+yv)\right] \tag{10}$$

Then it can be shown that

$$\begin{aligned}&E\left[h^{*}(x-\eta,y-\xi)h(x+\tau-\lambda,y+\beta-\gamma)\right]\\&=\frac{1}{M^{2}N^{2}}\sum_{u=0}^{N\text{-}1}\sum_{v=0}^{M\text{-}1}\sum_{u'=0}^{N\text{-}1}\sum_{v'=0}^{M\text{-}1}E\left[b(u,v)b(u',v')\right]\exp\left\{i2\pi\left[u'(x+\tau-\lambda)-u(x-\eta)\right]\right\}\\&\times\exp\left\{i2\pi\left[v'(y+\beta-\gamma)-v(y-\xi)\right]\right\}\end{aligned} \tag{11}$$

Eq. (9) can be simplified from Eq. (7)

$$\begin{aligned}&E\left[h^{*}(x-\eta,y-\xi)h(x+\tau-\lambda,y+\beta-\gamma)\right]\\&=\frac{1}{M^{2}N^{2}}\sum_{u=0}^{N}\sum_{v=0}^{M}\exp\left[i2\pi(u\tau+v\beta)\right]\\&=\frac{1}{M^{2}N^{2}}\delta(\tau,\beta)\end{aligned} \tag{12}$$

According to Eq. (9), Eq. (5), Eq. (6) we obtain

$$E\left[\psi^{*}(x,y)\psi(x+\tau,y+\beta)\right]=\sum_{\eta=0}^{N-1}\sum_{\xi=0}^{M-1}\frac{1}{M\times N}\left|f(\eta,\xi)\right|^{2}\delta(\tau,\beta) \tag{13}$$

It is obvious from Eq. (13) that a double amplitude encoded image is white with a zero mean and variance of

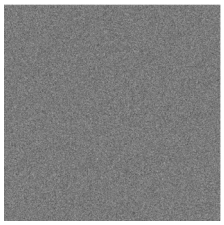
$$\sum_{\eta=0}^{N-1}\sum_{\xi=0}^{M-1}\frac{1}{M\times N}\left|f(\eta,\xi)\right|^{2} \tag{14}$$

It can be conclude that this scheme had the similar encryption results with the DRPE method. Because of this property, it is impossible to recover the hidden image with one of the phase recovery algorithms.

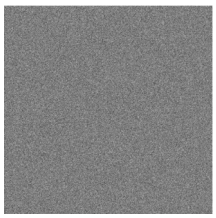
To decode a double amplitude encoded image, the Fourier transform of the encrypted image is multiplied by 1/b(μ, ν), then inverse Fourier transformed, which produces n(x, y)×f(x, y), Finally, f(x, y) can be recovered when we multiply it by 1/n(x, y).

Computer simulations were conducted to investigate the performance of the proposed optical systems. A picture of a beautiful woman Lena is used as an original input image with 512×512 pixels as shown in Fig. 2(a). The real and the imaginary parts of the encoded images are shown in Figs. 3(b) and 3(c). In this simulation the keys are both normally distributed and have mean 0 and standard deviation 1.

(a) Image to be encoded



(b) Real part of the encoded image.



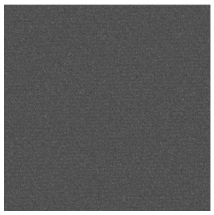
(c) Imaginary part of the encoded image

Fig. 2 Encoded images by double amplitude encoding system.

It is also interesting to analyze the robustness of this encoding technique against blind deconvolution. Let us assume that the attacker intercepted the ciphertext and attempts to retrieve the true plaintext without the knowledge of secret keys. He might try to decode the plaintext with decrypt

© the authors

the ciphertext by randomly picking a key from the key space. Fig. 3(a) shows that this attempt will fail. Only when the true pair of decryption keys is known, the original image of Fig. 3(b) can be retrieved.

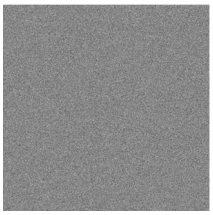
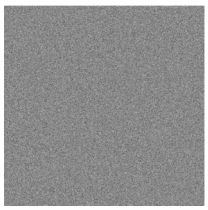



(a) (b)

Fig.3 Decoded image with the wrong (a) and right (b) keys

Discussions

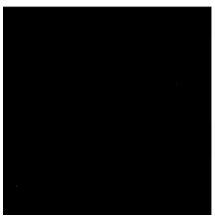
In Refregier and Javidi's classical letter, the random phase mask is demanded to be uniformly distribute in [0, 2π] [7], thus attackers know exactly the statistical properties of the random phase mask. This could be considered as a great potential threat to the DRPE system. By contrast, the DRAE has lower requirements for keys. From the analysis of part 2, both amplitude masks in the space and Fourier domain are expected white noises with zero means without any restriction of their probability density functions. Therefore, the idea gives more flexibility to one to encrypt an image. For instance, we can assign normally distributed numbers to one of the secret keys but assign uniformly distributed random numbers to another. By following this idea the encryption results of Fig. 2(a) are shown in Fig. 4(c) and 4(d), from which the correctness of the theoretical analysis was further verified. From the perspective of cryptanalysis, the expansion of the key space will induces the security enhancement compared with the DPRE scheme.

(a) Real part of the encoded image. (b) Imaginary part of the encoded image

Fig. 4 Encoded images by random amplitude keys with uniform distributions.

In addition, we investigate the robustness of the proposed optical security system. Suppose a positive host image is encrypted by use of the DRPE method, it can be easily shown that attackers can completely acquire the plaintext only with the true key of the Fourier plane. This is the fatal defect of the DRPE system. However, this should never occur with the DRAE method since the amplitude of the image was directly modulated by a random mask. Even if the opponent knows the secret key in the Fourier domain, it is still impossible for him to recover the original plaintext. Fig. 5(a) and 5(b) show the retrieved plaintext with the true key of the Fourier domain but the wrong key of the space domain from the encoded images with DRPE and DRAE methods, respectively. It can be obviously shown that the former is in conformity with the original image but the latter is totally different from it, therefore it was confirmed that the DRAP system shows higher robustness.

(a) (b)

Fig.5 Decoded image with the right key of the Fourier domain. (a) DRPE scheme (b) DRAE scheme

Published by Atlantis Press, Paris, France.
© the authors

In the DAME system, we require that the random amplitude mask is a white noise with a zero mean. That is, there are inevitable minuses in the random amplitude mask. However, we will never get a wave with negative amplitude. Thus the DRAE system could only be performed by digital method namely virtual optical system. This is the limitations of it.

Conclusion

In conclusion, we have proposed a virtual optical encryption system referred to as double random amplitude encoding scheme. By this method, one can transform an image into a white noise that is free from blind deconvolution attack. Compared with DRPE method, it reduces the requirements of the statistical properties of the secret keys in the space domain and Fourier domain. Consequently, the flexibility in choose the secret keys can be served as additional keys to further enhance the security of the system. In addition, it shows robustness against partial key exposure attack that makes it more suitable for image encryption. However, since the negative modulation of amplitude can not be physically realized, this scheme could only be performed digitally.

References

[1] W. Qin, and X. Peng, "Asymmetric cryptosystem based on phase-truncated Fourier transforms," Opt. Lett., vol. 35, pp. 118, 2010.

[2] X. Wang, and D. Zhao, "Security enhancement of a phase-truncation based image encryption algorithm," Appl. Opt. vol. 50, pp. 6645, 2011.

[3] W. Chen, X. Chen, and C. J. R. Sheppard, "Optical image encryption based on diffractive imaging," Opt. Lett., vol. 35, pp. 3817, 2010.

[4] H. Kim, D. Kim, and Y. H. Lee, "Encryption of digital hologram of 3-D object by virtual optics," Opt. Express, vol. 12, pp. 4912, 2004.

[5] N. K. Nishchal, and T. J. Naughton, "Flexible optical encryption with multiple users and multiple security levels," Opt. Comm., vol. 284, pp. 735, 2011.

[6] S. Kishkand, and B. Javidi, "Information hiding technique with double phase encoding," Appl. Opt., vol. 41, pp. 5462, 2002.

[7] P. Refregier, and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. vol. 20, pp. 767, 1995.

[8] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," Opt. Lett., vol. 25, pp. 887, 2000.

[9] G. Situ, and J. Zhang, "Double random-phase encoding in the Fresnel domain," Opt. Lett., vol. 29, pp. 1584, 2004.

Published by Atlantis Press, Paris, France.
© the authors