Review Article
Volume 9:6, 2022

Journal of Lasers, Optics & Photonics

ISSN: 2469-410X
Open Access

Optical Security System using Random Gratings for Optical Coding and Multiplexing

Mohammad Sohail*

Department of Physics, University of Lahore, Sargodha, Pakistan

Abstract

In the modern age, due to the rapid development of communication techniques, individuals can be secured by the application optical signal processing technology. In this paper, we have proposed a new technique that is using a multiplexing tactic for optical encrypting mechanism to secure the individuals for multiple users. Here in this paper, we are modifying the classical joint transform correlator to provide more security which is easy in implementation. Our proposed technique that is using encoding and decoding procedure provides more security than the previous techniques. In this approach, amplitude random mask was used for encoding as well as decoding procedure but in a holographic format that modulates the input information and enables us to recover the input information from modulated signal which is difficult for other people. For encoding process, we project the spectrum of the scattered beam of the amplitude random mask on the object that capture the object information in random manner and Fourier transformation gives the spectrum of the coded object. The split beam of the mask is multiplexed to the coming spectrum at the CCD plane for the decoding process unlike the classical joint transform architecture discussed. There is no need of the mechanical moment of the mask. This technique is more efficient than the techniques available in the literature because the advantage of the method introduced in this paper is the decryption performed using the same key code. We present a theoretical explanation, along with computer simulations results that support our proposal.

Keywords: Superresolution • Optical security and encryption • Amplitude random gratings • Optical information processing • Multiplexing

Introduction

In the modern world, security of the valuable things is not limited to the physical lock but to secure using simply entry data, like doors and some important information to safe. The most basic definition of any security system is found in its name. It is literally a means or method by which something is secured through a system of interworking components and devices.

Security systems involve the application of various means, devices and sometimes also human force to protect individuals and property from various hazards such as fire, crime and loss. It is quite clear that modern security system needs the application of cryptography and biometrics for strong authentication, data integrity and information confidentiality to be realized in embedded digital systems.

Optics can take advantage of their inherent parallel processing nature and encoding of Three-Dimensional (3D) information by use of amplitude and phase distributions. Many studies related to 3D display and 3D object recognition by use of digital holograms and integral imaging has appeared in the literature [1].

Due to the use of the optical components, the high speed calculation in a parallel manner makes possible that such type of security system are more suitable in practice. Moreover, due to the application of optics, it can provide higher security than digital system because the optical components such as holograms and phase masks are hard to break or to duplicate [2-4]. Security systems can be classified by their application, 1) Optical component that encodes the information and 2) verification part. We need to use encoding and decoding techniques. The need to encode information, in a way that will make it protected from decoding by unauthorized person. Recently, due to their parallelism and high spatial resolution, a few interesting encoding techniques were investigated and implemented by optical means. Some of these techniques are described.

Digital holography can be considered as a technique not only to visualize but also to secure 3D objects. Apart from DRPE, many algorithms and infrastructures, such as photon counting imaging, a symmetric cryptosystem based on amplitude- and phase-truncation approaches and polarization-based encryption, have been developed for security purposes.

***Address for Correspondence:** Dr. Mohammad Sohail, Department of Physics, University of Lahore, Sargodha, Pakistan; E-mail: mohammad.sohail@phys.uol.edu.pk*

Received: 14-Jan-2021, Manuscript No. JLOP-21-001-PreQC-21; **Editor assigned:** 19-Jan-2021, Pre QC No JLOP-21-001-PreQC-21 (PQ); **Reviewed:** 02-Mar-2021, QC No. JLOP-21-001-PreQC-21; **Revised:** 09-Jan-2022, Manuscript No. JLOP-21-001-PreQC-21(R); **Published:** 16-Mar-2022, DOI: 10.37421/ 2469-410X.2022.09.26

Some of these techniques calculate the comparison between two phase masks by optical correlator. In the given techniques, one uses the first optical mask as the system's lock, located in the optical correlator to make the original signal noisy. The other optical mask is working as the system's key to recover the original signal and such a system is used by the user for the verification purpose. These security systems provide the authenticity of the input signal by comparing the output correlation peak with a predefined threshold value. Some of them use the encoding and decoding input signal procedures. In encoding process, different people use different element like random phase mask etc. to make the information noise-like data for security. In decoding process, the same element can be used to recover the required original information. We need that security techniques must be reliable and faithful in reproducing the information to its authorized users only, operate fast and involve simple architecture. Optics-based security techniques have been of great interest because of their very fast operation and reliable performance.

In classical JTC, lateral shift multiplexing technique is used to eliminate the problem of some experimental constraints. These constraints arise from invariance intrinsic to lateral shifts that restrict the multiplexing capabilities. Some modification in the architecture was made to avoid this restriction and by mask-shifting multiplexing in the JTC system. Lateral shifting selectivity of the decryption phase mask in the system depends not only on its correlation length but also on the dimensions of the recording medium and on the distance between the phase mask and the hologram. But the movement of the diffuser creates different problems [5-7].

Here we present the new approach that using the same encoding and decoding procedure but provides more security and easy in implementation than the previous techniques. In this approach amplitude random mask was used for encoding and decoding. The diffuser scattered beam coming from the mask is divided into two beam, one is used as reference beam for the decoding process and the other beam is passed through the lens to illuminate the object to carry the object information that gives the modulated input signal and the second beam is used to recover the input information from modulated power signal which is in sampled and noised form and difficult for unauthentic people. The joint transform correlator is used to correlate the output data with input stored signal. The mathematical model and simulation results were presented.

Literature Review

We present the mathematical model for the encoding and decoding data that mostly help to secure the access of unauthorized person to the information. In this technique, we are modifying the classical joint transform correlation technique in imaging system. The modified joint transform correlation sketch is shown in Figure 1.

Let we have an input object represented. The diffuser is used as input random amplitude mask is placed at the front focal plane of the convex.

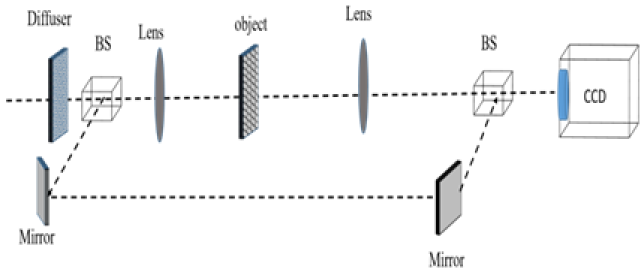

Figure 1. Experimental setup for modified joint transforms correlation.

Lens that produces the spectrum at the back focal plane. The values of the input random mask in the interval. The mathematical representation of the input random mask is given

$$D(x)=\sum_{m=-\infty}^{m=\infty} M(x-mx_o) \quad \text{...............} (1)$$

Where the period and m is the random location of transmission apertures in the random amplitude mask. The Fourier transform of the random mask is given by:

$$\tilde{D}(u)=\frac{1}{x_o}\sum_{m=-\infty}^{m=\infty} M(u-mu_o) \quad \text{.............} (2)$$

Where x and u are the coordinate in frequency and space domain and the relation between x and u. The beam passing through the input random grating is divided by the beam splitter. One part of the diffuser spectrum is used to pass through the convex lens to shine the object. The other part of the spectrum known as reference beam is reflected from different mirrors to fall on the coming beam passes through the security imaging system and is combined to extract the object information. The Fourier spectrum of the random amplitude mask is given in equation (2). The object information after illumination by the beam coming from the first Fourier lens to encode or to modulate the object data for the security purpose. The object after the scattered beam illumination is given by:

$$E(x)=g(x)\sum_{m=-\infty}^{m=\infty} M(x-mx_o) \quad \text{.............} (3)$$

Here we are working in the space domain; we are using the space coordinate x in one dimension for the sake of simplicity. The encoded object is in the sampled form because of the random amplitude mask. The convex lens produces the spectrum of the encoded object is given by

$$\tilde{E}(u)=G(u)\otimes\frac{1}{x_o}\sum_{m=-\infty}^{m=\infty} M(u-mu_o) \quad \text{...............} (4)$$

is the Fourier spectrum of the input object and "" is used for the convolution sign. The spectrum of the input object replicated at each point of the amplitude random mask.

In the decryption procedure, only the decryptions mask which the Fourier of the amplitude random mask corresponding to the encryption mask is placed at spectrum plane. The spectrum of the encoded object in the Fourier plane is multiplied to the Fourier scattered spectrum of the diffuser that result the decoding spectrum is given by.

$$\tilde{E}(u)=\left\{G(u)\otimes\frac{1}{x_o}\sum_{m=-\infty}^{m=\infty}M(u-mu_o)\right\}\frac{1}{x_o}\sum_{m=-\infty}^{m=\infty}M(u-mu_o) \quad \text{.....................} (5)$$

$$\tilde{E}(u)=\left\{G(u)\otimes\left(\frac{1}{x_o}\sum_{m=-\infty}^{m=\infty}M(u-mu_o)\right)^2\right\} \quad \text{.................} (6)$$

Eq. 5 shows that both the masks are aligned and the multiplication of the two masks give a single mask that sample the object spectrum. CCD is an electronic device that converts the optical signal into electronic signal. CCD is an array of pixel represented by the Dirac delta function in ideal case. CCD can be represented mathematically in one dimension as

$$CCD(u)=\sum_{n=-\infty}^{n=\infty}\delta(u-nX) \quad \text{.................} (7)$$

Since the CCD sampled the spectrum of the object mean the intensity image, the CCD sampled spectrum is as given below

$$R(u)=\left\{G(u)\otimes\frac{1}{x_o}\sum_{m=-\infty}^{m=\infty}M(u-mu_o)\right\}\sum_{n=-\infty}^{n=\infty}\delta(u-nX) \quad \text{..................} (8)$$

The inverse Fourier transformation of the CCD sampled spectrum produces multiple replicas of the object image at the focal plan of the imaging convex lens but this time on computer i.e.

$$r(x)=\left\{g(x)\sum_{m=-\infty}^{m=\infty}M(x-mx_o)\right\}\otimes\frac{1}{X}\sum_{n=-\infty}^{n=\infty}\delta\left(x-\frac{n}{X}\right) \quad \text{..................} (9)$$

Equation 8 gives the series of replicas of the object image with varied amplitude due to the multiplication of 1/X to the obtain image. To select a single replica of the object image, we have put n=0, Equation 8 takes the form,

$$r(x)=\frac{1}{X}\delta(x)\left\{g(x)\sum_{m=-\infty}^{m=\infty}M(x-mx_o)\right\} \quad \text{..................} (10)$$

Equation 9 gives the image of the object in sampled form. To fill the missing point in the image, we have used interpolation technique that gives a continuous image. A correlation technique is used to compare the output image with original reference object, we find that the output image of the object having better correlation with the original object [8-10].

Discussion

For the simulation of proposed technique we have chosen a biohazard image as the input object which is shown in Figure 2A. All the simulation work carried out in mathematical software. The amplitude grating having random and integral transmission ranging from zero to unit as shown in Figure 2B. The scattered random beam coming from diffuser is divided into two beams by using beam splitter, one beam passed through the convex lens of focal length f=200nm that gives the beam of the random amplitude grating at the input object plane to illuminate and coded the object information as shown in Figure 2C and the other beam of the scattered spectrum of the diffuser is used as reference beam or for decoding process to recover the coded information.

In the previous work, half of the grating was covered and the object was illuminated and half part of the random grating was used for the recovery of the image of the object and then moved and the same procedure is repeated for the remaining part of the object, added to remove the invariance effect. But here in our approach, we illuminate the object with no covering sheet as well as no motion of the grating. The convex lens produces the spectrum of the coded object at the back focal plane as shown in Figure 2D, the decoding or the reference beam are focused on the spectrum of the coded object as shown in Figure 2E by using the beam splitter that recovers the object spectrum information. The CCD sampled the intensity image that is spectrum as shown in Figure 2F. A CCD camera is placed at the back focal plane of the lens where the decoding beam shines the spectrum of the coded object information. A CCD is an array of pixels in regular arrangement represented by Dirac delta function. Pixel is a photo-detector that converts the optical signal into electric signal and sends to computer for further process. But the CCD sampling means that the pixel pitch also degrades the data falling on each pixel and is integrated and the data bits at a pixel are lost and only integrated data is recovered. The CCD sampled the object spectrum as shown in the Figures 2E and 2F. The inverse Fourier transformation of the figure is shown in the Figures 2F and 2G. We have obtain output image with better resolution without any motion of the amplitude random mask and no need of the covering sheet (Figures 2A-2H).

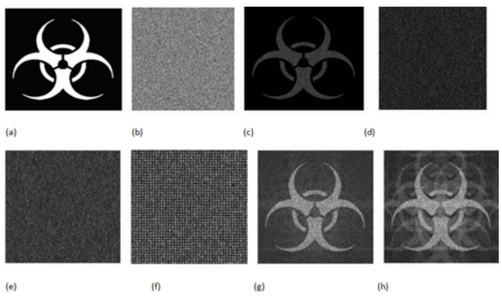

Figure 2. Simulation of proposed technique. A. Input object; B. Amplitude random mask; C. Coded object; D. Fourier spectrum of the coded object; E. Effect of the multiplication of mask on (d); F. CCD sampled the figure (e); G. Inverse Fourier of the (f); H. Output image using diffuser for coding and using covering sheet and movement of the diffuser.

Conclusion

In the past security system they have used amplitude random transmission mask for encoding and decoding process and to secure the information. We have followed the work given in but they have used a window of the mask that allows the half portion of the object, moved the window mask for the remaining portion of the object and repeat the same procedure.

At the final stage they added the images to obtain the output image but we have performed the same procedure without any motion of the mask and with our using covering sheet which make difficult the procedure and we have obtain output image with better resolution.

In our technique, we have used the beam coming from the mask for the encoding process and for the decoding procedure the same mask pattern was used that enable us to recover the image with better resolution as discussed. We checked the correlation of the recovered signal and the input object having a good correlation. This approach is better and easy coding technique than the techniques available in the literature.

Acknowledgment

We are thankful to University of Lahore Main campus Lahore (UOL) for funding this project and also to the University of Lahore, Sargodha Campus (UOL) for providing research facilities.

References

1. Schnars, Ulf and Juptner Werner. “Digital Holography: Digital Hologram Recording, Numerical Reconstruction and Related Techniques.” New York: Springer, United States. (2005).
2. Joseph, Horner and Bahram Javidi. “Guest Editorial: Special Section on Optical Security.” *Opt Eng* 38(1999): e1.
3. Philippe, Refregier and Bahram Javidi. “Optical Image Encryption based on Input Plane and Fourier Plane Random Encoding.” *Opt Lett* 20(1995): 769.
Joseph, Goodman. “Introduction to Fourier Optics.” Colorado: Roberts and Company Publishers, United States. (1996).
4. Takanori, Nomura. “Phase Encoded Joint Transform Correlator as an Optical Encryption Decoder.” SanDiego SPIE 21(1998): 246-252.
5. Tajahuerce, Enrique and Javidi Bahram. “Encrypting Three-dimensional Information with Digital Holography.” Appl Opt 39(2000): 6595-6601.
6. Javidi, Bahram and Nomura Takanori. “Securing Information by use of Digital Holography.” Opt Lett 25(2000): 28-30.
7. Nishchal, Naveen, Joseph Joby and Singh Kehar. “Fully Phase Encryption using Digital Holography.” Opt Eng 43(2004): 2959-2966.
Wang, Xiaogang, Zhao Daomu and Chen Linfei. “Image Encryption based on Extended Fractional Fourier Transform and Digital Holography.” Technique Opt Commun 260(2006): 449-453.
8. Nelleri, Anith, Joseph Joby and Singh Kehar. “Digital Fresnel Field Encryption for Three-dimensional Information Security.” Opt Eng 46(2007): 45801.

How to cite this article: Mohammad Sohail. "Optical Security System using Random Gratings for Optical Coding and Multiplexing". *J Laser Opt Photonics* (9): (6) (2022) :026