Optical encryption using phase-shifting interferometry in a joint transform correlator

Cecilia La Mela and Claudio Iemmi

Departamento de Física, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Pabellón 1, Ciudad Universitaria, 1428 Buenos Aires, Argentina

Received April 3, 2006; revised May 16, 2006; accepted May 23, 2006; posted June 12, 2006 (Doc. ID 69601); published August 9, 2006

We propose an optical encryption technique where the encrypted field and the decrypting key are obtained by three-step phase-shifting interferometry and registered as digital Fresnel holograms in a joint transform correlator architecture. Decryption can be achieved by digital or optical means. The technique allows the complete process to be achieved at high speed and data to be transfered via digital communication channels. Experimental implementation is performed in a system based on a programmable liquid-crystal TV display working in pure phase mode to represent the input data and to introduce the required phase shifts. A CCD is used to register the output data. © 2006 Optical Society of America

OCIS codes: 100.4550, 100.3010, 090.2880, 120.5050, 230.3720, 070.4560.

Most of the proposed techniques for optical data encryption, among which double random phase encoding is one of the most used,[1] include phase encoding of information by use of random phase masks.[2–8] These methods in general involve complex encrypted data that need to be registered holographically.[9] The recent growing interest in transmission of secure information via digital communication channels made that different encryption techniques, based on digital holography,[10] were developed.[2–8]

In this Letter we present an optical encryption technique, based on the double random phase encoding, that uses phase-shifting interferometry[11] in a joint transform correlator[12] (JTC) system. The data can be transferred via digital communication channels and the complete encryption–decryption process can be achieved at high speed. Most of the encryption methods involving phase-shifting interferometry have been developed to operate in systems based on Mach–Zehnder interferometers, generally including optical phase retarders and the use of phase masks that usually require accurate alignment of the system.[2,6] The encryption process that we propose is performed by means of a JTC-based architecture schematized in Fig. 1(a), where the scene is encrypted at a Fresnel plane by means of a random phase reference. The encrypted field and the decrypting key, registered as Fresnel holograms, are obtained by three-step phase-shifting interferometry in the JTC.[13] Here, the position of the Fresnel plane is an additional security parameter. A CCD is used for the registering process. A benefit of the encryption method that we propose is that no alignment drawbacks are present, as it can be implemented in a very simple and robust system, where a programmable liquid-crystal television display (LCTV) working in pure phase mode is used for both input signal displaying and phase shifting. Some other optical encryption methods, based in a JTC architecture, have been proposed but they, in general, require precise alignment in the decryption process as they use a 4-*f* correlator.[4,5,8] In addition, they suffer from autocorrelation terms present in the output plane. The method that we present, and the system that we propose to implement it, allow us to overcome these drawbacks. In our technique, once the Fresnel holograms of the encrypted field and the decrypting key are registered and sent to the receiver, and after simple digital operations, the receiver can obtain the phase information of the field diffracted by the scene at the Fresnel plane. The scene information can be retrieved by simply performing a Fresnel propagation process over that phase distribution.[14] The system used for decryption is a simple architecture, schematized in Fig. 1(b), where no alignment drawbacks are present. This process can be performed both digitally or by optical means, as will be shown.

Both optical encryption and optical decryption are performed by using the same experimental setup. The collimated beam of the 457 nm line of an Ar laser is used to uniformly illuminate the input plane of the system, which is represented in a Sony LCTV model LCX012BL extracted from a commercial video projector. This display, in combination with the adequate

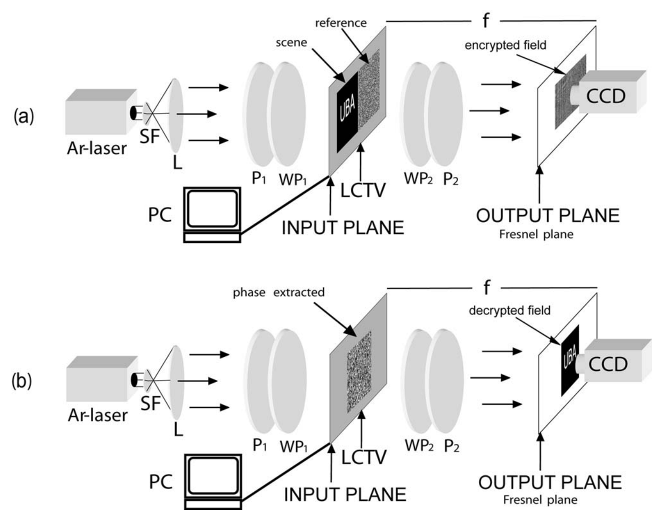

Fig. 1. Scheme of the system for (a) encryption process and (b) decryption process. SF, L, P_s, and WP_s denote spatial filter, lens, polarizers, and wave plates, respectively. A personal computer is used to drive the LCTV and the CCD.

state of light polarization (provided by polarizers P_1, P_2 and the wave plates WP_1, WP_2), allows us to reach a phase modulation near 2π under blue illumination.[15] Then the LCTV, together with the polarizers and wave plates, conform the spatial light modulator that provides the input signal. This field propagates up to the output plane, which is a Fresnel plane, in this case set at a distance $f=700$ mm from the LCTV. The output information is recorded and digitalized by means of a CCD and a frame grabber.

The encryption method that we propose is based on the well-known double random phase encoding technique. Implementation of this process in a JTC architecture requires use of complex distributions for scene and reference to obtain the encrypted field.[5] In our case, as the input signals are displayed in a pure phase modulator, it is necessary to develop a technique to introduce the amplitude information. As a scene, we use a phase-only distribution and emulate a binary amplitude by conveniently programming a convergent lens on the LCTV. As a reference, we use a random phase distribution that generates, at the Fresnel plane, a complex field also characterized by a random phase. The process can be mathematically described as follows. Let us represent by $f(x,y)$ the binary function in the $[0,1]$ range corresponding to the image to be encrypted, by $n(x,y)$ a white noise distribution also in the $[0,1]$ range, and by $l(x,y)$ a quadratic phase distribution corresponding to a convergent lens of focal distance f for wavelength λ. Coordinates at the input plane are represented by (x,y). We chose the scene distribution as

$$e(x,y)=\exp\{i2\pi[f(x,y)n(x,y)]\}\times\exp\{l(x-a,y-b)[1-f(x,y)]\}. \quad (1)$$

It can be seen from this expression that each time that $f(x,y)$ takes the value 1, $e(x,y)$ is a random phase distribution, and each time $f(x,y)$ takes the value zero, this distribution becomes a convergent lens with the optical axes centered at $x=a$, $y=b$. When $e(x,y)$ is represented in the input plane and is illuminated by a uniform plane wave of wavelength λ, the light passing through the zero-valued places of $f(x,y)$, after freely propagating a distance f, is focused onto a small region centered at coordinates $p=a$, $q=b$, where (p,q) stand for the output plane coordinates. If we conveniently set a and b, we can concentrate the light out of the region of interest and then we can consider that no light arrives to the output plane when $f(x,y)$ is zero valued. It is important to clarify that, as the LCTV can represent phase distributions in the $[0,2\pi]$ range, to program the convergent lens we perform a 2π modulus operation over the phase distribution $l(x,y)$. Then, by representing on the LCTV the phase-only distribution $e(x,y)$ given in Eq. (1), we can emulate a complex distribution where the amplitude is given by $f(x,y)$ and the phase by $n(x,y)$. Under this approximation, let us mathematically represent the scene distribution by

$$e(x,y)=f(x,y)\exp[i2\pi n(x,y)]. \quad (2)$$

As the reference wave needed to encrypt the scene, we use a random-phase distribution $r(x,y)=\exp[i2\pi\varphi_r(x,y)]$, where $\varphi_r(x,y)$ is a white noise distribution in the $[0,1]$ range and it is statistically independent from $n(x,y)$. We represent scene $e(x,y)$ and reference $r(x,y)$ distributions side by side at the input plane, centered at $(c,0)$ and $(-c,0)$, respectively, as shown in Fig. 1(a). When we uniformly illuminate them, after freely propagating a distance f, the encrypted field arrives to the output plane. The intensity can be represented as

$$I_0(p,q)=|E(p,q)+R(p,q)|^2, \quad (3)$$

where $E(p,q)=|E(p,q)|\exp[i2\pi\varphi_E(p,q)]$ and $R(p,q)=|R(p,q)|\exp[i2\pi\varphi_R(p,q)]$ represent, respectively, the diffracted fields of scene $e(x,y)$ and reference $r(x,y)$ at the Fresnel plane.

It is important to mention that the random phase distribution $n(x,y)$ introduced on the scene distribution given by Eq. (2), allows reconstruction of the encoded function $f(x,y)$ by using only the phase of the field diffracted by the scene at the Fresnel plane. Thus the decryption process is based on obtaining the phase information of $E(p,q)$. This is achieved by performing two phase extraction processes, by means of the three-step phase-shifting technique, as explained below.

First, we extract the phase difference between $E(p,q)$ and $R(p,q)$. To implement the three-step phase-shifting technique, phase shifts of 0, $2/3\pi$ and $4/3\pi$ are performed on the reference distribution $r(x,y)$ by programming them directly on the LCTV as it is working in a pure phase mode. We record the corresponding intensity patterns at the Fresnel plane, which are given by

$$I_j(p,q)=|E(p,q)|^2+|R(p,q)|^2+2|E(p,q)||R(p,q)|\times\cos[\varphi_R(p,q)-\varphi_E(p,q)+j\pi-2cp], \quad (4)$$

where j takes the values $j=0$, 2/3, and 4/3. It can easily be seen that

$$\varphi_R(p,q)-\varphi_E(p,q)-2cp=\arctan\left\{\frac{[I_{4/3}-I_{2/3}]\sqrt{3}}{2I_0-I_{4/3}-I_{2/3}}\right\}. \quad (5)$$

Equation (5) represents the phase of $E(p,q)$ encrypted by the phase of $R(p,q)$. To recover the phase information of $E(p,q)$, we need to know the phase information of the encrypting field $R(p,q)$. This phase is obtained by again performing the three-step phase-shifting process, but now using a constant distribution as the scene, while the key remains as the reference. We then represent a constant phase and the key distribution side by side at the input plane. If the field diffracted by the constant scene, at the output plane, is represented as $C(p,q)=\exp[i\varphi_C]$, where φ_C is a constant, the new output intensity patterns can be deduced, from Eq. (4), by replacing $E(p,q)$ by $C(p,q)$, as

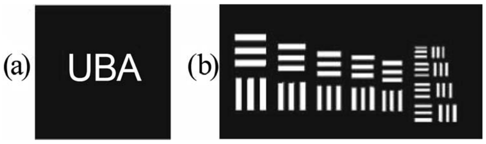

Fig. 2. Images used for the encryption process.

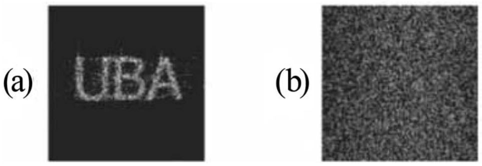

Fig. 3. Results obtained when the complete encryption–decryption process is numerically simulated. The decrypted image is shown when (a) the correct key is used and (b) the incorrect key is used.

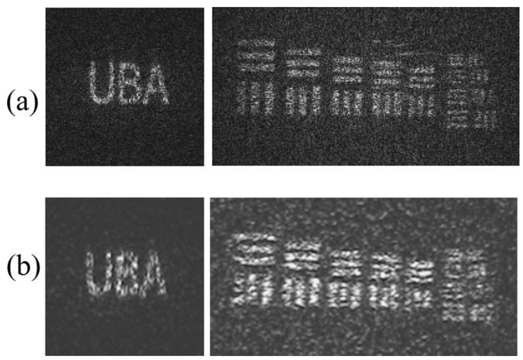

Fig. 4. Results obtained when the encryption has been optically performed and decryption has been achieved (a) digitally and (b) optically.

$$I'_j(p,q) = 1 + |R(p,q)|^2 + 2|R(p,q)| \times \cos[\varphi_R(p,q) - \varphi_C + j\pi - 2cp], \quad (6)$$

where again j takes the values $j=0$, $2/3$, and $4/3$. We can calculate

$$\varphi_R(p,q) - \varphi_C - 2cp = \arctan\left\{ \frac{[I'_{4/3} - I'_{2/3}]\sqrt{3}}{2I'_0 - I'_{4/3} - I'_{2/3}} \right\}, \quad (7)$$

and then, by subtracting Eq. (5) from Eq. (7), we obtain $\varphi_E(p,q)$ added to a constant term that can be ignored.

The different intensity patterns can be obtained at the video rate. Then, after the sender transmits the six intensity distributions together with the information of λ and f, the receiver can successfully complete the decryption process digitally or optically. To digitally recover the encrypted image $f(x,y)$, we numerically perform an inverse Fresnel propagation over $\tilde{E}(p,q)=\exp[-i\varphi_E(p,q)]$, which is the complex conjugate of the phase-only information, at the Fresnel plane, of the field diffracted by the scene $e(x,y)$ given by Eq. (2). To optically recover the image, $\tilde{E}(p,q)$ is represented on the LCTV operating in pure phase mode at the input plane, as shown in Fig. 1(b), and it is uniformly illuminated to obtain the decrypted image at the output plane.

The two images used for the process are shown in Figs. 2(a) and 2(b). To test the robustness of the encryption technique, we performed a numerical simulation of the complete encryption–decryption process for the image of Fig. 2(a). The result obtained when the correct key is used is shown in Fig. 3(a) while the result obtained when the incorrect key is used is shown in Fig. 3(b). It can be seen that the image cannot be decrypted if the incorrect key is used. In Fig. 4(a) we show the results when the encryption process is optically performed but the decrypted images are obtained by digital means. The results obtained when both encryption and decryption processes are optically performed are shown in Fig. 4(b).

In summary, we have developed and implemented an optical encryption technique where the encrypted field and the decrypting key, registered as Fresnel holograms, are obtained by three-step phase-shifting interferometry in a JTC architecture. The decryption has been achieved optically and digitally by a simple free propagation process. The technique allows a high-speed encryption–decryption process for binary data and is able to operate in a robust and extremely simple optoelectronic system. The security of the process, which is based on the use of double random phase encoding, can be increased if we consider that the encrypting key can be updated at high speed.

This paper was financed by Universidad de Buenos Aires and Consejo Nacional de Investigaciones Científicas y Técnicas, Argentina. C. La Mela's e-mail address is cecilm@df.uba.ar.

References

1. P. Refregier and B. Javidi, Opt. Lett. **20**, 767 (1995).
2. E. Tajahuerce, O. Matoba, S. Verrall, and B. Javidi, Appl. Opt. **39**, 2313 (2000).
3. O. Matoba and B. Javidi, Opt. Lett. **27**, 321 (2002).
4. T. Nomoura and B. Javidi, Appl. Opt. **39**, 4783 (2000).
5. T. Nomoura and B. Javidi, Opt. Eng. **39**, 2031 (2000).
6. S. Lai and M. A. Neifeld, Opt. Commun. **178**, 283 (2000).
7. B. Javidi and T. Nomura, Opt. Lett. **25**, 28 (2000).
8. T. Nomura, S. Mikan, Y. Morimoto, and B. Javidi, Appl. Opt. **42**, 1508 (2003).
9. H. J. Caulfield, ed., *Handbook of Optical Holography* (Academic, 1979).
10. U. Schnars, J. Opt. Soc. Am. A **11**, 2011 (1994).
11. J. H. Burning, D. H. Herriott, J. E. Gallagher, D. P. Rosenfeld, A. D. White, and D. J. Barangaccio, Appl. Opt. **13**, 2693 (1974).
12. C. S. Weaver and J. W. Goodman, Appl. Opt. **5**, 1248 (1966).
13. G. Lu, Z. Zhang, S. Wu, and F. T. S. Yu, Appl. Opt. **36**, 470 (1997).
14. O. Matoba, T. J. Naughton, Y. Frauel, N. Bertaux, and B. Javidi, Appl. Opt. **41**, 6187 (2002).
15. A. Marquez, C. Iemmi, C. Moreno, J. Davis, J. Campos, and M. Yzuel, Opt. Eng. **40**, 2558 (2001).