ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Optics Communications 221 (2003) 43–47

OPTICS COMMUNICATIONS

www.elsevier.com/locate/optcom

Fully digital encryption technique

Ricardo Arizaga[a], Rodrigo Henao[b], Roberto Torroba[a,*]

[a] *Centro de Investigaciones Opticas (CIOp) and OPTIMO, Facultad de Ingeniería, Universidad Nacional de La Plata, C.C. 124, B1902WAB La Plata, Argentina*

[b] *Institute of Physics, Antioquia University, Medellín, Colombia*

Received 12 September 2002; received in revised form 11 March 2003; accepted 24 March 2003

Abstract

We propose an alternative fully digital encryption technique based on using the Fourier transform of the original object to be processed and a speckled reference wave as encryption mask. Once encrypted, the Fourier transform spectrum of the object is holographically stored. The original-data recovering is performed by digital reconstruction using the same encryption mask, which is also holographically stored. Quality of reconstructed data is evaluated as a function of the sensed encrypted data. Computer simulations and experimental results are presented to demonstrate the method.

Keywords: Optical data processing; Information processing; Encryption and validation procedures

1. Introduction

In recent years, several proposals on information security using optical techniques were published [1–6]. Optical encryption have the added property that a large amount of data can be stored or retrieved in parallel and at high speed. The first to be used were techniques related to analog encryption methods based on different correlation architectures [7,8]. These setups can be considered as the basis for the design of real-time optical security devices. Most optical correlators use 2-D input images and are designed around a 2-D optical processing architecture. However, the presence of complex or expensive elements complicates the creation of simple and low-priced devices of this type. These correlators can be used for instance to secure entry systems that identify individuals for access to a restricted area. In security systems, the image, such as a picture of a face or a fingerprint, is used for the same purpose. They include memory units for storing key code images that are used to verify the authenticity of the input image. It is impossible to verify the encoded documents without knowing the key mask that have been used in the encoding. Furthermore, key codes have to be unique to be a full-proof, reliable accurate, ready to implement as well as to meet the goal of putting the counterfeits and frauds to a complete halt.

[*] Corresponding author. Fax: +54-221-4712771.
E-mail address: robertot@ciop.unlp.edu.ar (R. Torroba).

0030-4018/03/$ - see front matter © 2003 Elsevier Science B.V. All rights reserved.
doi:10.1016/S0030-4018(03)01462-7

The systems are also integrated to a network. If the memory units are stolen or if important data are intercepted by monitoring the transmission line in the network, however, an unauthorized person can extract vital information easily. It is becoming increasingly simple to reproduce the input data of the security system. Therefore, data protection has become necessary. The most preferred method is that of double random phase encryption [9]. In the encryption process input data (positive real-valued image) is multiplied by a random phase function, then Fourier transformed and finally multiplied by another random phase function. We can obtain a decrypted image by first multiplying by the complex–conjugate of the second encoding phase function and taking a Fourier transform. Many related contributions were generated, including the use of a Joint-transform correlator (JTC) [10] or optical arrangements using photorefractive crystals [11]. The content of the proposals was extended to include subjects as stream ciphers [12], other configurations of optical correlators [13], optical memory cards [14], even several optical parameters can be used as encryption–decryption keys, as for example multidimensional keys [15]. In this context, Javidi et al. first introduced digital holography in the field of information securing. This technique has important benefits as enables to store, transmit, and decrypt the encrypted data digitally. Another benefit of the proposed system compared with electronic encryption is that optical processing provides many degrees of freedom for securing information [16].

The setup is a Mach-Zender configuration using the double-encoding phase mask. More recently the proposal was extended to an optical retrieval system for secure real-time display. The images in all these correlators are normally intensity representations.

In this paper, the idea is to present an alternative fully digital technique with a single-random encryption. The object is directly Fourier transformed. At the Fourier plane we place a lensless CCD sensor. We record and simultaneously encrypt the data using an interference with a speckled reference wave. Then a digital hologram of the encrypted object Fourier transform is made, which will be reconstructed also digitally. The decryption key is also recorded as a digital hologram as described in the following section. This second stored frame is sent to all possible clients to be kept as decoding key The retrieval is operated by all-digital means. The whole technique is simpler than the previous ones. Since the process is performed on a CCD camera, the obtained data can be directly transmitted to digital devices or communication lines. Accordingly, the technique has potential for near real-time processing. The influence of the encrypted spectrum content vs the CCD array area is also evaluated. Theoretical explanation, computer simulations and experimental results are presented.

2. Principle of the method and results

In the following, we describe in detail the proposed encryption procedure and the way to experimentally implement it.

Let $i(x,y)$ denote the original image to be encrypted. The proposed experimental setup for the digital encryption is schemed in Fig. 1. A He–Ne laser is used as a coherent light source. A lensless CCD array is directly placed in the lens L Fourier plane. The image of a speckled screen is used as the encryption mask needed for the process. This screen is imaged on the CCD array. Let $s(\mu,\eta)$ denotes the speckle screen at the CCD plane. Precisely, this is the reference wave used in the generation of the digital hologram. If we denote by

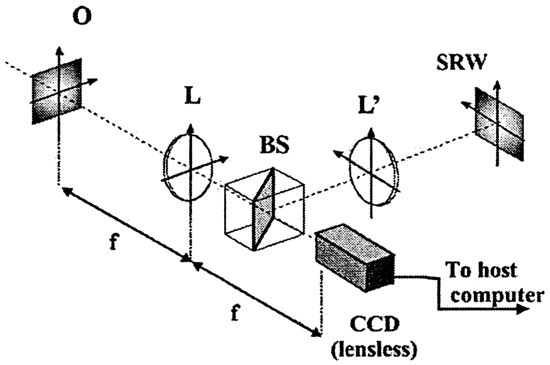

Fig. 1. Setup for the encryption procedure. Laser light illuminates the object to be encrypted O, L transforming lens, SRW speckled reference wave, and CCD lensless sensor array.

$I(\mu,\eta)$ the Fourier transform of $i(x,y)$ at the CCD plane coordinates, the intensity $h(\mu,\eta)$ of the digital hologram created by the interference between these two waves in the Fourier domain is expressed by

$$\begin{aligned} h(\mu,\eta) &= |I(\mu,\eta)+s(\mu,\eta)|^2 \\ &= |I(\mu,\eta)|^2 + |s(\mu,\eta)|^2 + I^*(\mu,\eta)s(\mu,\eta) \\ &\quad + I(\mu,\eta)s^*(\mu,\eta). \end{aligned} \tag{1}$$

Similarly, by removing both the original object and the transforming lens L of the setup and illuminating with a plane wave of uniform unitary amplitude, we get

$$\begin{aligned} k(\mu,\eta) &= |1+s(\mu,\eta)|^2 \\ &= |1|^2 + |s(\mu,\eta)|^2 + s^*(\mu,\eta) + s(\mu,\eta). \end{aligned} \tag{2}$$

When extracting the holographic data from Eqs. (1) and (2), retaining the fourth term in both equations and multiplying them, we get $I(\mu,\eta)$. Finally we perform the inverse Fourier transform of this last term for recovering the function $i(x,y)$ and subsequently the original image

$$\begin{aligned} &I(\mu,\eta)s^*(\mu,\eta)s(\mu,\eta) \to I(\mu,\eta) \\ &\qquad \Rightarrow FT^{-1}[I(\mu,\eta)] = i(x,y). \end{aligned} \tag{3}$$

In Fig. 2, we show a computer simulation of the method. The intensity of the original image 2(a) and its encryption 2(b) are shown. The results of using the right decoding key 2(c) and a wrong key 2(d) are also displayed. The right decoding key can retrieve the original image, but a noise-like image remains by the wrong key.

In Fig. 3, we experimentally demonstrate the procedure. We show the intensity images of 3(a) the input object, 3(b) the encrypted image, and 3(c) the correct digital reconstruction of the input.

The main limiting aspect is the size of the spectrum the CCD array is able to sense. We investigated then the influence of capturing a smaller area of the total encrypted spectrum. In this case we use an algorithm to calculate the mean square error, which is given by

$$\mathrm{Err} = \frac{\sum_{m=1}^{M}\sum_{n=1}^{N}|i(m,n)-i'(m,n)|^2}{M\times N},$$

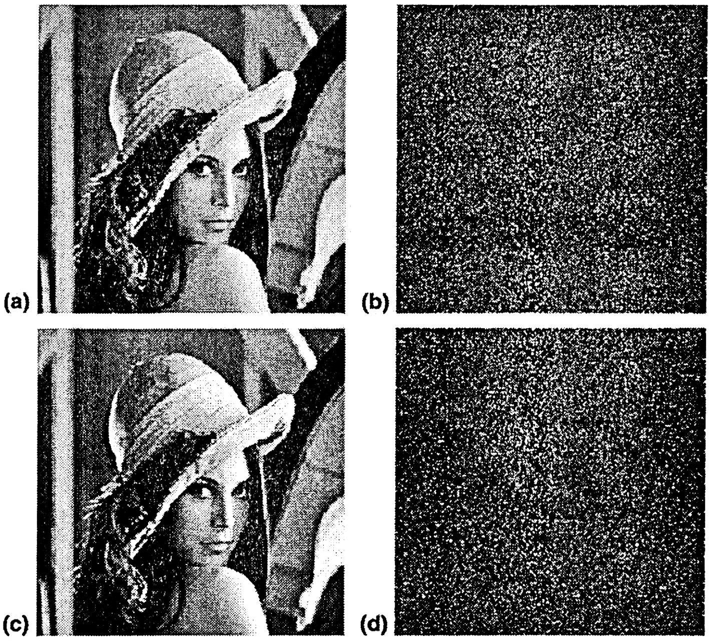

Fig. 2. Results of a computer simulation: (a) original image, (b) encrypted image, (c) retrieved image by the right decoding key, and (d) retrieved image by a wrong decoding key.

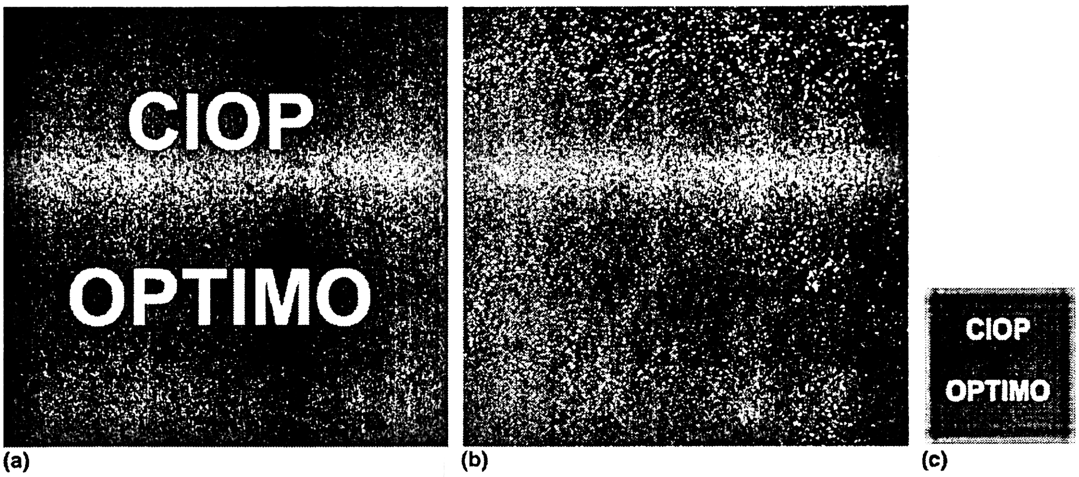

Fig. 3. Experimental results showing (a) the object to be encrypted, (b) the resulting encrypted image, and (c) the reconstructed image after the right decoding process.

where (m, n) are the pixel coordinates, $M \times N$ is the number of pixels of the original image $i(m, n)$, and $i'(m, n)$ is the decrypted information obtained when blocking the area of the CCD sensor.

Evidently, some frequency information is lost due to the limited CCD sensor size. Ideally, all collected data must remain within the CCD array but it depends both on the original image frequency content and on the optical parameters of the imaging system. So, the optical system must be chosen as to fit the object Fourier transform spectrum on the CCD array. On the other hand, for a fixed Fourier spectrum size, a better sensor resolution will only help if lower object frequencies are of importance in recognizing the whole information. In standard conditions, only bulk objects are expected to be recognized.

In the following we investigate the difference in quality of decrypted data when limiting the physical size of the CCD array. In this analysis we use the same test image (same frequency content) and using a varying blocking mask over the CCD array, and centered around it. Actually the problem is the opposite, because the sensor is always the same and the frequency spectrum varies from one object to another, but the situation is illustrated in the same way in our example.

We assume that the Fourier transform field information is properly sampled. Besides we suppose the intensity levels to be adequate to avoid saturation, or they are well above the detector minimum level. In this way, these parameters has little or no influence in the resulting decryption. The optical system we use produces a Fourier transform field whose detectable intensity fits completely into the sensor array without the covering mask in place.

The result are shown in the plot of Fig. 4. This figure shows the mean squared errors as a function of the blocked proportion of the CCD array. When the mean squared error gives around 4×10^3, a visual inspection of the resulting image shows a very poor correlation with the original image. Image

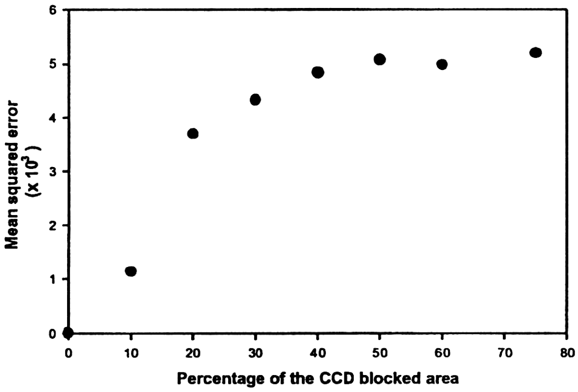

Fig. 4. Plot of the mean squared error versus the proportion of the detector blocked area. It is clearly shown that reconstructed image quickly deteriorates, even when only the 10% of the detector area is blocked.

quality quickly deteriorates as the blocked area increases. As a consequence, care must be taken in choosing the right transforming lens as to fit the object spectrum on the sensor area, although some minor tolerance can be accepted.

Advantages over existing proposals are: (a) there is no need for additional experimental equipment at the decryption stage, (b) it only needs the right decoding key, which is the same for both coding and decoding processes (other methods need the conjugate of the decoding key), (c) is independent of diffraction efficiencies, and (d) requires no filtering

In our case, the signal-to-noise ratio is given in terms of the visibility of the resulting decrypted output.

Acknowledgements

The Grants from CONICET (PICT No. 008/98), from Universidad Nacional de La Plata and CODI-Universidad de Antioquia are gratefully acknowledged.

References

[1] B. Javidi, E. Ahouzi, Appl. Opt. 37 (1998) 6247.
[2] N. Towghi, B. Javidi, J. Opt. Soc. Am. A 16 (1999) 1915.
[3] O. Matoba, B. Javidi, Appl. Opt. 38 (1999) 7288.
[4] X. Tan, O. Matoba, T. Shimura, K. Kinoda, B. Javidi, Appl. Opt. 39 (2000) 6689.
[5] S. Lai, M. Neifield, Opt. C. 178 (2000) 283.
[6] O. Matoba, B. Javidi, Opt. Lett. 27 (2002) 321.
[7] T. Grycewich, B. Javidi, Opt. Eng. 35 (1996) 2519.
[8] L. Muravsky, T. Voronyak, V. Fitio, M. Shovgenyuk, Opt. Eng. 38 (1999) 25.
[9] P. Rèfrègier, B. Javidi, Opt. Lett. 20 (1995) 767.
[10] B. Soon, M. Karim, M. Alam, Opt. Eng. 38 (1999) 39.
[11] G. Unnikrishnan, J. Joseph, K. Singh, Appl. Opt. 37 (1998) 8181.
[12] S. Zhang, M. Karim, Opt. Eng. 38 (1999) 20.
[13] B. Javidi, J. Wang, Opt. Eng. 35 (1996) 2479.
[14] J. Horner, B. Javidi, Opt. Eng. 38 (1999) 8.
[15] O. Matoba, B. Javidi, Opt. Lett. 24 (1999) 762.
[16] B. Javidi, T. Nomura, Opt. Lett. 25 (2000) 28.