Experimental encryption multiplexing based on a JTC scheme

Myrian Tebaldi,[*1] Carlos Vargas[3], Néstor Bolognini,[1,2] and Roberto Torroba[1]

[1]*Centro de Investigaciones Ópticas (CONICET-CIC) and UID OPTIMO, Facultad de Ingeniería, Universidad Nacional de La Plata, P.O. Box 3 C.P 1897, La Plata, Argentina,*
[2]*Facultad de Ciencias Exactas, Universidad Nacional de La Plata, La Plata, Argentina,*
[3]*Grupo de Óptica y Fotónica, Instituto de Física, Universidad de Antioquia, A.A 1226 Medellín, Colombia.*

Received October 21, 2010; accepted November 18, 2010; published December 31, 2010

Abstract—We present an alternative scheme to perform a multiple encrypting technique based on the use of a Joint Transform Correlator architecture. The basic approach relies on using an extra random phase mask placed before the correlator input plane, where we select different disjoint regions to encode each input object. In this way we avoid the cross talking when reconstructing the encoded objects. We experimentally validated the procedure using a photorefractive crystal as a storing medium.

Encryption techniques are of great importance for data protection [1, 2]. In particular, the development of optical encryption attracted increasing interest for its high processing speed and high security level. Conventional optical image-encryption methods are based on the 4-*f* correlator architecture that uses two random phase masks [1]. This scheme is known as Double Random Phase Encryption (DRPE). An experimental version of this set-up was implemented by using photorefractive crystals as storing media. During the decryption procedure, the phase-conjugated beams of the encrypted data allow to obtain the input image [3-5].

Several variations of the (DRPE) were proposed in the literature, for instance working in the fractional Fourier domain [6] and by using digital holography [7], to name a few.

Encryption techniques imply that the input image should not be recovered without employing the correct encoding key. It should be pointed out that the key code should not be inferred by hackers or unauthorized users. However, it was shown that encryption schemes present some weaknesses. In DRPE hackers demonstrated that they can access random phase keys in both the input plane and the Fourier plane. Chosen and known plaintext attacks [8, 9] were employed to efficiently obtain the encoding keys of the system.

The mentioned 4f scheme involves the generation of a phase conjugated beam to recover the input image. This holographic scheme requires precise alignment to be experimentally implemented. An alternative encryption technique based on JTC architecture (see Ref. [10]) introduces, in the input plane, both the object to be codified and the key code mask. In the decryption step, after an inverse FT of the joint power spectrum (JPS), which is illuminated by the FT of the exact key code mask, the input image is correctly recovered. This scheme can be also experimentally implemented by using a volume photorefractive intensity-sensitive crystal as storing media. Note that the JTC architecture is an inherent two step holographic set-up, avoiding the use of complex conjugate waves. It was also demonstrated the validity of algorithms for cracking the JTC encryption systems. However, multiplexing turns the system immune to the mentioned attacks, increasing therefore the encryption method security. Multiplexing techniques are based on encoding two or more input images and combining them into a single recording medium. Then, an intruder, who intercepts the encrypted multiplexed data, could not determine by simple observation the number of data included in the storing medium.

Several multiplexing alternatives were proposed in the literature. In Ref. [4-5, 11] multiplexing based on shifting the random phase mask, the use of multiple apertures and the change in the polarization state or the wavelength are proposed. In the present work, we present a modified version of the conventional JTC scheme. In this case, another random phase mask is inserted before the JTC input. The multiplexing of amplitude input images is introduced by using different non-overlapping regions of the mentioned new input random phase mask. The use of different non-overlapping regions of the input mask, besides introducing the multiplexing procedure, allows avoiding the cross talk of multiple images at the time of decryption. We experimentally demonstrate the validity of our proposal.

The scheme used to implement the multiplexing encryption and decryption procedure is schematized in Fig. 1. An Nd YAG laser (wavelength 532nm) is used as a coherent light source. The scheme is based on the JTC encryption architecture. However, another random phase mask is placed in the input plane. Therefore, the JTC double aperture arrangement is illuminated by a speckle pattern. The symbols O and R_1, R_2 and R_3 denote the input image to be encrypted and the random phase mask diffusers. The first random diffuser R_1 illuminated by a

* E-mail: myrianc@ciop.unlp.edu.ar

plane wave is located at the input plane. The random phase masks R_2 and R_3 are placed side by side at the double aperture plane. These random phase masks functions R_1, R_2 and R_3 are chosen to be statistically independent. The random phase diffuser is generated by a white sequence of phase that is uniformly distributed on the interval $[0, 2\pi]$. An input image is bonded to one aperture random mask (R_2). A structured beam generated by the first random phase mask R_1 illuminates the double aperture. The Fourier transform of the double aperture plane is recorded in an intensity sensitive recording media. The medium in our proposal is a photorefractive BSO crystal. This sample was 10mm x 10mm x 10mm in size. Then, a voltage of V=10 kV was applied between the $1\bar{1}0$ crystal faces, which are separated by a distance of 10mm, producing an electric field of 1kV/mm.

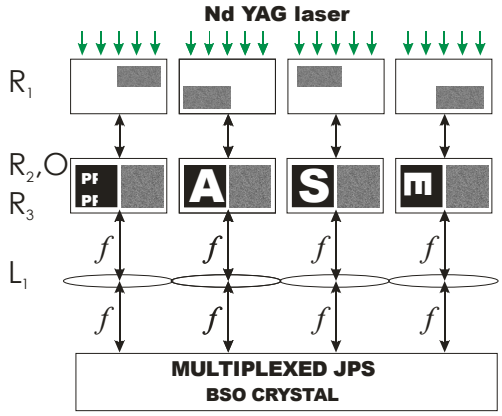


Fig. 1. Multiplexing encryption scheme (O: input object; R_1, R_2 and R_3: random phase masks; L_1: lens with focal length f)

The encrypted JPS is recorded into the photorefractive crystal to store the JPS as a volume hologram. The intensity distribution received by this crystal creates photocharges. Due to the low fringe frequency involved, the charges drift owing to the external electric field. These photocharges drift from the highly illuminated regions into the less illuminated ones where they are trapped. The photocharges generation rate is proportional to the light pattern received by the crystal. These charges develop a space-charge field that partially compensates the external field. A resulting internal field is obtained at each point and the system arrives at a steady-state situation. Thus, the intensity distribution received by the crystal is encoded as the spatial distribution of the resulting electric field strength at each point. This field induces, through the linear electro-optic effect the crystal exhibits, the corresponding spatial variation of the refractive index. Therefore, the JPS is stored as a refractive index change in the crystal.

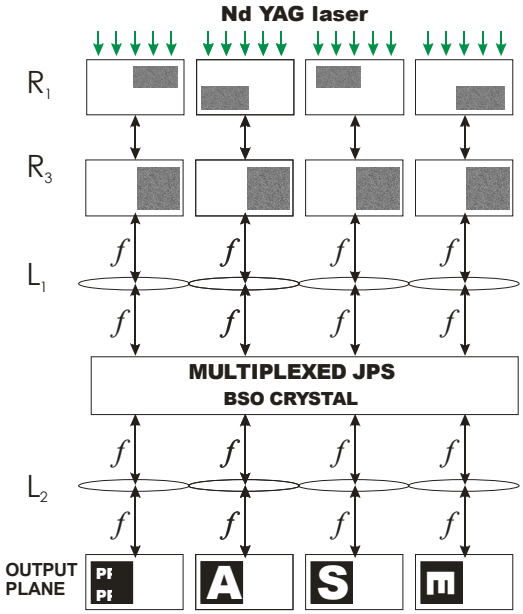
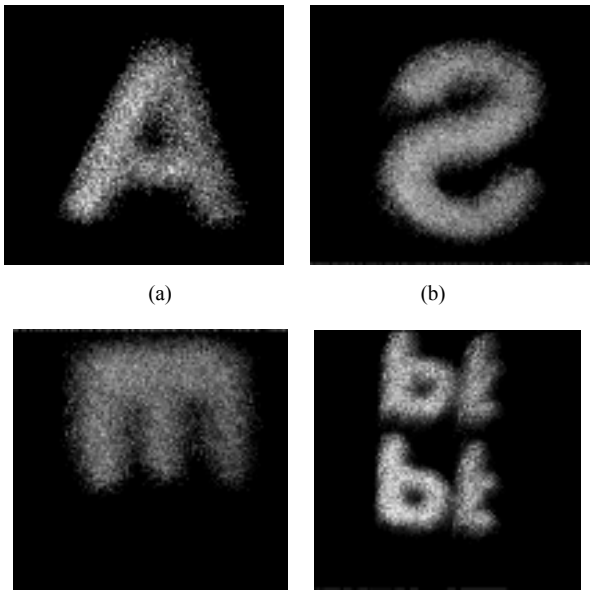


Fig. 2. Multiplexing decryption scheme (R_1, R_2 and R_3: random phase masks; L_1 and L_2: lenses with focal length f)

In the decryption step, the photorefractive crystal is illuminated by the Fourier transform of the correct input random phase masks, which is illuminated by a determined portion of the first random phase mask R_1 (see Fig. 2). Then, the beam passing through both masks R_1 and R_3 is imaged onto the photorefractive crystal and the diffracted light is collected at the back focal plane of L_2, reconstructing thereby the input. Note that the illumination wavelength must be the same one used during the encryption step. If the illumination wavelength changes during decryption but maintains the reference random phase key codes, the patterns in the decoding step change as well, avoiding the decoding of the original input data.

Both key code masks R_1 and R_3 must be employed during the decryption step. If the decryption process uses one incorrect key, for instance R_2 or R_3, the decryption fails. When the first mask R_2 is located at the incorrect position, the input data cannot be recovered and only noise appears at the output plane. In addition, diffusers should be placed at the same position that they occupied during the encryption. Then the introduction of this new mask increases the security of the system, acting as an extra encoding key. The proposed method has been investigated by using binary characters as an input image. The system behavior allows implementing a multiplexing operation. The photorefractive-material stores the multiple JPS generated by selecting different regions of the additional random phase mask R_1. The experimental

procedure consists in four exposures where the random phase mask position is modified between each exposure. During the encryption step, different regions of the key code mask are employed, where regions in each exposure do not overlap. In order to get an effective decryption of each input data, the region of the mask R_1 must be the same as that used in the encryption step. The results of Fig. 3 correspond to the decrypted images when different regions of the mask R_1 are utilized. Note that the decrypted data have comparable efficiency. In order to obtain comparable diffraction efficiencies in the multiple exposures, we take into account the recording-erasure response of the crystal. Then, the exposure times varied in each exposure in order to obtain approximately equivalent diffraction efficiency in all decrypted data.



(a) (b)

(c) (d)

Fig. 3. Experimental results

If during decryption step, we simultaneously use the masks used in two different objects, the encrypted data in both exposures are simultaneously reconstructed (see Fig. 4).

In summary, the new random phase mask R_1 provides new encryption key codes. The detailed new key could be advantageously employed to encrypt multiple information in the same medium. Note that each diffuser region can be used as a different information channel. The method is robust when confronted with known attacks, as hackers cannot infer the existence of a multiplexing procedure.

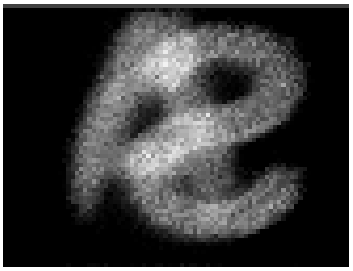


Fig. 4. Experimental results

This research was performed under grants CONICET No. 112-200801-00863 (Argentina), ANCYT PICT 1167 (Argentina), bilateral project CO/08/16 between MINCYT (Argentina) and COLCIENCIAS (Colombia), and Facultad de Ingeniería, Universidad Nacional de La Plata No. 11/I125 (Argentina).

References

[1] P. Refregier, B. Javidi, Opt. Lett. **20**, 767 (1995).
[2] E. Tajahuerce, O. Matoba, S. C. Verrall, B. Javidi, Appl. Opt. **39**, 2313 (2000).
[3] G. Unnikrishnan, J. Joseph, K. Singh, Appl. Opt. **37**, 8181 (1998).
[4] J. F. Barrera, R. Henao, M. Tebaldi, N. Bolognini, R. Torroba, Opt. Commun. **259**, 532 (2006).
[5] J. F. Barrera, R. Henao, M. Tebaldi, N. Bolognini, R. Torroba, Opt. Commun. **260**, 109 (2006).
[6] G. Unnikrishnan, J. Joseph, K. Singh, Opt. Lett. **25**, 887 (2000).
[7] E. Tajahuerce, B. Javidi, Appl. Opt. **39**, 6595 (2000).
[8] X. Peng, P. Zhang, H. Wei, B. Yu, Opt. Lett. **31** 1044 (2006).
[9] Y. Frauel, A. Castro, T. J. Naughton, B. Javidi, Opt. Exp. **15**, 10253 (2007).
[10] T. Nomura, B. Javidi, Opt. Eng. **39**, 2031 (2000).
[11] D. Amaya, M. Tebaldi, R. Torroba, N. Bolognini, J. Opt. A: Pure Appl. Opt. **10**, 104031 (2008).

