Experimental color encryption in a joint transform correlator architecture

Myrian Tebaldi[2], Sergi Horrillo[1], Elisabet Pérez-Cabré[1] María S. Millán[1], Dafne Amaya[2], Roberto Torroba[2], Néstor Bolognini

1 Departamento de Óptica y Optometría de la Universidad Politécnica de Cataluña, Terrasa (España)
2 Centro de Investigaciones Ópticas (CONICET La Plata-CIC) and UID OPTIMO, Facultad Ingeniería, Universidad Nacional de La Plata (Argentina)
3 Facultad Ciencias Exactas, Universidad Nacional de La Plata, La Plata (Argentina)

Corresponding author: myrianc@ciop.unlp.edu.ar

Abstract. We present an experimental color image encryption by using a photorefractive crystal and a joint transform correlator (JTC) architecture. We achieve the color storing by changing the illumination wavelength. One JTC aperture has the input image information corresponding to a determined color channel bonded to a random phase mask (object aperture), and the other JTC aperture contains the key code mask. The joint power spectrum is stored in a photorefractive crystal. Each color data is stored as a modulation of birefringence in this photosensitive medium. The adequate wavelength change produces a corresponding power spectrum modification that avoids image encryption cross talk in the read out step. An analysis in terms of the sensitivity of the photorefractive silenite crystal for different recording wavelengths is carried out. It should be highlighted that the multiplexed power spectrum shows neither the multiplexing operation nor the amount of stored information increasing the system security. We present experimental results that support our approach

1. Introduction

In the last years, the development of secure transmission systems has received much attention [1-14]. Among these methods, encryption techniques, which consist of transforming original data to a non recognizable data (encrypted information) are interesting. To retrieve the original data, encryption keys and encryption machine must be known. The encryption systems can be implemented optically by taking advantage of high-speed parallel encryption of two dimensional image data achievable with optical processing. [2-5]. Several authors demonstrated different optical encryption systems for information security applications, based on optical correlations. There are many other optical image encryption proposed in the literature, such as double-random-phase encryption (DRPE) [2], joint transform correlator (JTC) [3] and encryption with digital holography [4]. In the DRPE scheme based on a 4f lens arrangement, an input image can be encoded into a white-noise like image (encrypted image) by use of two random phase masks located at the input and Fourier planes, respectively. The key code mask is required for successful retrieval of the original data. This scheme bases their success in the use of diffuser random phase masks. A speckle pattern is generated by the multiple interference among the wavefronts scattered from each diffuser element of a random phase masks illuminated by coherent light. The speckle pattern characteristics depend on the illumination wavelengths, original diffusers, optical system, polarization, and relative optical position. It is impossible to generate an identical speckle pattern using different optical parameters, even by using the same random diffuser. For instance, the wavelength of the decryption beam can be used as a new key [6]. It is difficult to decrypt the data without knowledge of both the wavelength and the phase key. It should be pointed out that the DRPE scheme needs to produce a conjugate of the encryption data in order to retrieve the input data, requiring an extremely precise alignment [7, 8]. However, the JTC architecture alleviates the alignment problem. The JTC architecture is an inherent two-step holographic set-up avoiding the use of complex conjugate waves.

Recently, wavelength, polarization, and position multiplexing methods using a double random phase [7, 8] and JTC [9] have been proposed. The main idea of multi-encryption methods consists of encoding several input images and storing them into a single medium. The advantage of multiple image encryption is that it can encrypt and decrypt several images in parallel. The multiplexing proposal exhibits better security because an intruder, which intercepts the encrypted multiplexed images, could not determine by simple observation the number of images included in the storing medium.

In previous works, the input images are illuminated by monochromatic light and the color information of the input image is lost. However, the color information is useful in practical applications. Zhang and Karim [10] introduced a method for color image encryption based on Fourier transform. Likewise, Chen et al. proposed a technique using wavelength multiplexing and lensless Fresnel transform hologram [11]. In this last case, the image is separated into red, green and blue components and encryption is carried out in each channel. The free space propagation distance and cascade random phase codes are used as keys for image encryption. Joshi et al. proposed an alternative of the mentioned method based on the 4f encoding technique that includes the fractional Fourier transform as an extra key [12]. Phase conjugation operation is applied in this arrangement to the second random phase mask. On the other hand, a single-channel color encryption technique based on color image format conversion has also been described in Ref [13].

However, secure data recording of color images under a wavelength multiplexing technique is possible in a JTC arrangement. In Ref. [14], we evaluated the performance of the decrypting procedure when decrypting with a wavelength different from that employed in the encryption step. This analysis revealed that the wavelength is a valid parameter to conduct image-multiplexing encoding with a JTC architecture. Further, we determined the minimum wavelength change that prevented decoding cross talk. However, to our knowledge, there are no communications reporting color encrypted experimental results. In our work, we present an experimental encryption method for color images. As in previously mentioned contributions, each color channel is encrypted independently, and is multiplexed in a single medium using a JTC scheme. Multiplexing is achieved by keeping the same random phase masks in each encrypting step and only changing the illuminating wavelength. This approach could be considered as an extension of the conventional encryption, using JTC architecture, now including the wavelength multiplexing.

We propose what we believe are the first experimental results of color image encryption by use of wavelength multiplexing based on the JTC architecture. Three images are independently encrypted in three different channels by using three different wavelengths (red, green, and yellow). In all cases, the same random phase mask is employed. The wavelength in each channel can be considered as a key in image encryption and decryption. The joint power spectrum is stored in an intensity sensitive medium.

In Section 2, image encryption/decryption schemes and their experimental optical implementations are described. Also, experimental and simulated results are presented to demonstrate the validity of the proposal. Some concluding remarks are summarized in the final section.

2. Experimental set-up description

In this section, we describe color encryption techniques. Based on the conventional JTC scheme, an optical architecture of color image encryption is proposed. Each color acts as a different channel in our proposal.

The conventional JTC encryption architecture contains two apertures, one with the input data bonded to a random phase mask, while the other aperture contains the key code mask. This arrangement performs the correlation between the convolution of the input image along with a random mask both included in one aperture, and a random phase encoding mask in the other aperture. We denote r(x) as the input random-phase mask, g(x) as the input image and h(*x*) as the key code mask, which are positioned at coordinates (-a); (-a); (a), respectively. We use one-dimensional notation for simplicity. The random phase diffusers are statistically independent and they have random phase values uniformly distributed on the interval [0, 2π]. The joint power spectrum (JPS) (encrypted power spectrum) corresponding to one wavelength signal encryption is given by,

$$JPS(\nu)=\left|FT\left[r(x-a)g(x-a)+h(x+a)\right]\right|^2 \tag{1}$$

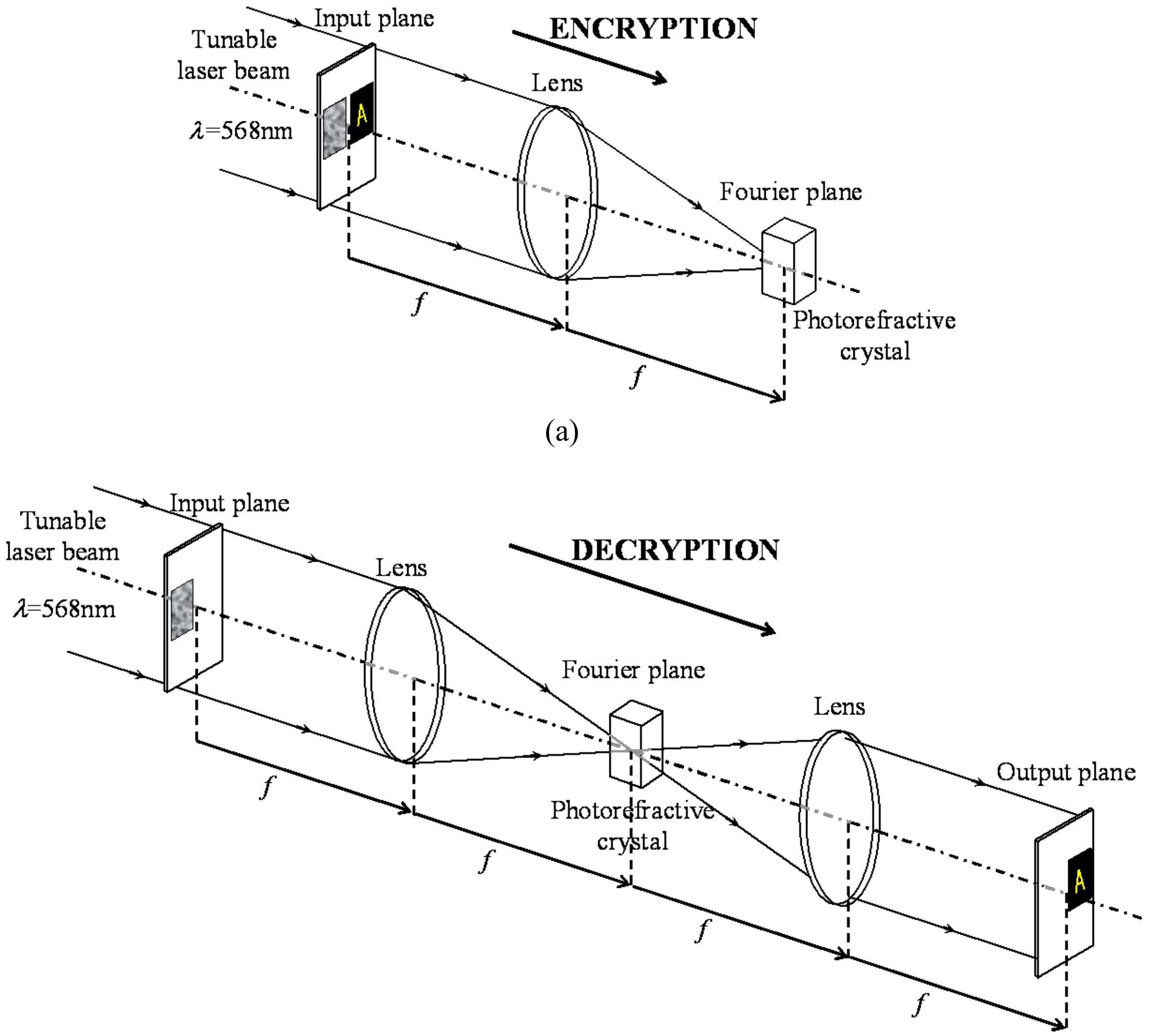
where *F*[ ] represents the Fourier transform operation. The *JPS(ν)* can be regarded as the encrypted data as it exhibits a white noise distributed over the frequency domain. The JPS characteristics depend on the illumination wavelengths, original diffusers, etc. Then, with the same phase mask and different wavelengths, the system can produce many JPS by the introduction of different laser wavelengths. Therefore, the system can provide different color information channels to the authorized person. Thus, it is possible to implement a multiplexing operation. All color channels are encrypted using the same scheme. In our proposal, the encryption procedure uses three illuminating wavelengths. The basic experimental scheme is depicted in Figure 1. The different color components are obtained by using a tunable Ar-Kr laser. Holographic storage media represent an interesting option in order to implement experimentally the mentioned JTC optical encryption scheme. In particular, photorefractive materials with their parallel read/write capabilities, high information retrieval rate, high-capacity storage and phase conjugation capability are a valid alternative. The optical implementation is realized by using a BTO silenite crystal as recording medium. The crystal is cut in the transverse electro-optic configuration. The directions $(1\bar{1}0)$, (001), and (110) of the crystal coincide with the XYZ axes and the linear dimensions are L_X =L_Y= L_Z= 8 mm, respectively. It should be highlighted that the use of a random phase mask in photorefractive volume storage medium powers the multiplex capability simultaneously preventing from unauthorized users.

As expected, if the illumination wavelength changes though maintaining the reference random phase key code, the encrypted spectrum changes as well. To proceed with the multiplexing, each input object, encrypted with a different wavelength, is sequentially recorded at the output plane. Each *JPS* associated to each channel is stored in the same medium, thereby generating the multiplexed joint power spectra.

In the experiments, the wavelengths 647 nm, 556nm and 520nm are used. Among the available Ar-Kr tunable laser lines the selection of wavelengths was based on the power of each line and the highest diffraction efficiency. Note that the diffraction efficiency in BTO crystal includes an absorption factor. In the case of the blue lines the absorption coefficient is very high. Therefore, the diffraction efficiency of those lines is severely decreased and they were disregarded in our experiment.

All keys in all channels should be correct; otherwise, we could not correctly recover the complete information. If the incident wavelength of each channel is close to the wavelength of the basic colors, the real color information can be recovered at the output plane. In Ref. [14] the wavelength selectivity is numerically evaluated.

The three color encrypted images add together, written on a BTO crystal. Each color channel is independently encrypted. This pure optical setup can realize the encryption in real time. The encoding processes are the same as above described.



(a)

(b)

Figure 1 a) Experimental encryption scheme b) experimental decryption scheme

The photorefractive-material stores the JPS, which is the interference pattern between the Fourier transform of: both the key random diffuser and the product of a diffuser and the input object. This operation is achieved by means of lens L_1 whose focal length is 100 mm.

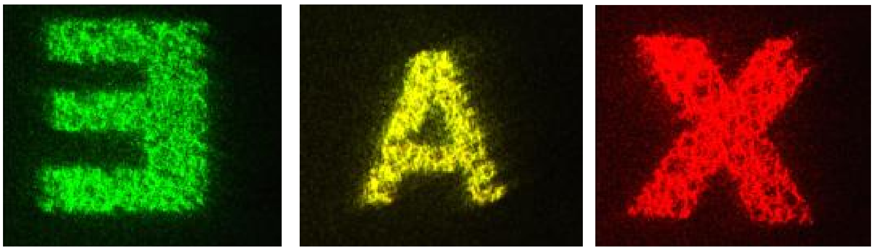
In wavelength multiplexing, each input image is firstly encrypted into the same encoding media by the same phase keys under coherent illumination with different wavelength λ_n. Then all the encrypted data are superimposed to yield the final single multiplexed encrypted data.

A plane wave illumination is necessary, to implement the decryption procedure. During decoding process, the key code is located in the input plane to decode the encrypted JPS and then retrieve the input image. Thus, we obtain the decrypted image in the output plane. Note that the remaining terms are noise.

If the phase key (random phase mask and/or wavelength) is unauthorized, the intensity distribution obtained by CCD is a noisy pattern, and nothing could be retrieved from the BTO crystal. The decoding image appeared only when both keys match.

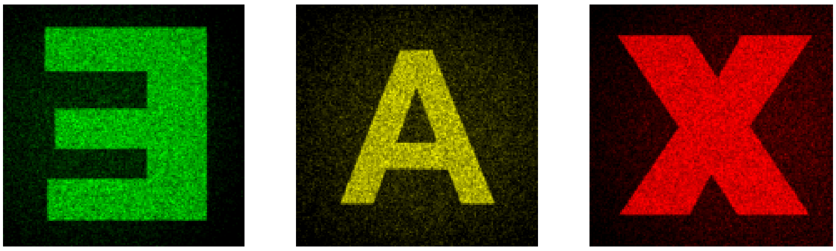
Each image can be obtained by decoding a single JPS (encrypted data) with the corresponding wavelength λ_n. There will be cross-talk noise in each decrypted image. The cross-talk noise deteriorates the decrypted results as the number of encrypted images increases. The cross-talk noise is unavoidably present in decrypted results from non-decrypted images. Then, the system has a limited multiplexing encryption capacity.

Explicitly, the principle of our proposal is to encrypt three different color objects with a coding mask and different wavelengths. We employ the same experimental set-up for decryption. Figure 2 shows three experimentally decrypted images by using the proposed encrypted optical memory with a given wavelength and random phase coding. For a given wavelength, the corresponding color image is clearly obtained with a low level of noise in its background. These results show the feasibility of multiple image encryption by spectral multiplexing in a JTC configuration. In Figure 3 we present some simulation results to illustrate the wavelength multiplexing procedure and to show their agreement with the experimental counterpart.



(a) (b) (c)

Figure 2: Experimental color decrypted images corresponding a) green channel (λ_1 = 520 nm) b) yellow channel (λ_2 =568 nm); c) red channel (λ_3 =647 nm)



(a) (b) (c)

Figure 3: Simulated color decrypted images corresponding a) green channel (λ_1 = 520 nm) b) yellow channel (λ_2 = 568 nm); c) red channel (λ_3 = 647 nm).

3. Conclusions

A simple method for color image encryption is presented. The encryption method is based on a JTC architecture. The encrypted data or JPS depend on the input illumination wavelength. The spectral-dependent JPS, allows multiple encryption storing, avoids the need of different random phase masks, and let parallel image handling.

Then these parameters act as a new key code. This idea is useful in a multiplexing scheme to encrypt several input data, providing that different wavelengths are introduced.

The random phase masks and the wavelength in each channel are important keys in encryption and decryption. The user should receive the encrypted information, the phase mask, and the wavelength information to retrieve the input data. The wavelength information can be sent to each authorized users via a separate channel other than the one used to send the master mask. When the keys are incorrect in decryption, noise like information appears at the output plane. If we attempt to recover the information with only one or two wavelength correct channels, we cannot obtain the complete information. The information can be encrypted, stored, and transmitted with high security.

A problem associated with multiplexing operations is the possible cross talk between the recovered images that would distort the final outputs. The encryption of multiple images implies that multiple coded data being added together in the same storing media. The additive cross talk arising from their mutual disturbances results in the decreasing of the quality of the multiple decrypted data. Therefore, the performance of a multiple image security system will be improved by reducing cross talk.

The expected advantage of a JTC-based security system is the invariance of the system to in-plane shifts of the random phase masks. In addition to this, the JTC scheme configuration offers some advantages over the 4f optical implementation, such as its simplicity and easy realization. The proposal can be implemented in real time.

Acknowledgments

This research was performed under the grants: CONICET No. 863 (Argentina), ANCYT PICT 1167 (Argentina), Facultad de Ingeniería, Universidad Nacional de La Plata No. 11/I125 (Argentina). It also received financial funding from the Spanish Ministerio de Ciencia e Innovación y Fondo FEDER (project DPI2009-08879).

References

[1] Millán M S, Pérez-Cabré E and Javidi B 2006 *Opt. Lett*. **31** 721
[2] Refregier P and Javidi B 1995 *Opt. Lett.* **20** 767
[3] Amaya D, Tebaldi M, Torroba R and Bolognini N 2008 *Appl. Opt.* **47** 5903
[4] Tajahuerce E and Javidi B 2000, *Appl. Opt*. **39** 6595
[5] Tebaldi M, Furlan W D, Torroba R and Bolognini N 2009 *Opt. Lett*. **34** 316
[6] Matoba O. and Javidi B.1999 *Appl. Opt*. **38** 6785
[7] Barrera J F, Henao R, Tebaldi M, Bolognini N and Torroba R 2006,*Opt. Commun*. **259** 532
[8] Barrera J F, Henao R, Tebaldi M, Bolognini N and Torroba R 2006 *Opt. Commun*. **261** 29
[9] Amaya D, Tebaldi M, Torroba R and Bolognini N 2009 *Appl. Opt*. **48** 2099
[10] Zhang S and Karim M A 1999 *Microwave Opt. Technol. Lett.* **21** 318
[11] Chen L and Zhao D 2006 *Opt. Express* **14** 8552
[12] Joshi M, Chandrashakher and Singh K 2007 *Opt. Commun*. **279** 35
[13] Joshi M, Chandrashakher and Singh K 2008 *Opt. Commun*. **281** 5713
[14] Amaya D, Tebaldi M, Torroba R and Bolognini N 2009 *Appl. Opt*. **48** 2099