Master key generation to avoid the use of an external reference wave in an experimental JTC encrypting architecture

Edgar Rueda,[1] Carlos Ríos,[1] John Fredy Barrera,[1,*] and Roberto Torroba[2]

[1]Grupo de Óptica y Fotónica, Instituto de Física, Universidad de Antioquia, Medellín, Colombia

[2]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

*Corresponding author: jbarrera@fisica.udea.edu.co

Received 5 December 2011; revised 9 February 2012; accepted 10 February 2012; posted 10 February 2012 (Doc. ID 159493); published 10 April 2012

In experimental optodigital encrypting architectures, the use of a reference wave is essential. In this contribution, we present an experimental alternative to avoid the reference wave during the encrypting procedure in a joint transform correlator architecture by introducing the concept of a master key. Besides, the master key represents an additional security element for the entire protocol. In our method, the master key is holographically processed and used during the encryption process with the encrypting key. We give the mathematical description for the process in case of a single input object and then we extend it to multiple input objects. We present the experimental demonstration of the proposed method including two examples where this technique is successfully applied for several input objects.

OCIS codes: 060.4785, 070.4560.

1. Introduction

Various techniques were proposed for optical encryption [1,2]. Conventionally, we find the double random phase encryption (DRPE) in the Fourier domain [3], with extensions to the fractional Fourier domain [4] and the Fresnel domain [5], to name a few. All these techniques present interesting properties, for instance they are sensitive to translations [6], polarization [7], and wavelength [8]. Nevertheless, there is also another architecture actively used, the joint transform correlator (JTC) [9]. In the JTC, the encrypted information is stored as intensity distribution in the recording media. The JTC is robust, as it does not require an accurate optical alignment. The image with an input phase mask attached is placed side by side with a key mask in the JTC input plane. The joint power spectrum (JPS) represents the encrypted data. That is, the encrypted data are recorded as the magnitude squared of the amplitude and phase information. An advantage of the JTC is that the decryption is performed using the same key mask, which removes the need to produce an exact complex conjugate of the key.

Experimental demonstrations for security verification show that a JTC can be applied successfully. The joint transform correlator has some advantages compared with a $4f$ correlator. Primarily, alignment and resolution requirements are relaxed, and spatial filter synthesis is avoided. Furthermore, this optical setup is compact because the object and reference beams share a single $2f$ system. That is, the encrypted data are recorded as an intensity basis.

The comparative analysis of the JTC and the $4f$ architectures is useful for improving well-known methods and developing new methods for optical security. In addition, that comparative analysis is useful

1559-128X/12/111822-06$15.00/0

for designing and creating new high-performance security systems based on a JTC architecture [10].

In the context of optical encryption, several digital holography methods in 4*f* or JTC were used to record fully complex information with electronic cameras and displays [10–16]. Besides, digital recording of holograms has advantages over traditional methods, thanks to the advances in using computer image-acquisition devices. By storing the holograms in a computer, we can reduce the noise through image processing techniques, and numerically reconstruct and handle the object with arbitrary potentials. The digital format of the holographic data can be transmitted to receivers through data communication channels. After the transmission of the encrypted data authorized remote users, who use a correct digital hologram, we are able to reconstruct correctly the original data through optical correlation. If one does not have the key hologram, the reconstructed data will be noise-like.

In a classical digital holographic configuration, the JTC architecture is a Mach–Zehnder interferometer, with a JTC in one arm and a reference wave in the other.

In [10], we find a discussion on the advantages of this arrangement in optical encryption, stressing the stage of image transmission. This arrangement is more advantageous in the sense that we do not require the use of spatial light modulators (SLMs) to project the joint power spectrum (JPS) or photorefractive components in the storing and recovering processes.

The influence of intensity saturation on the CCD recording device was addressed, as this issue has an important effect on the noise in the recovered information. Besides the control of the intensity levels, we identify and filter the unwanted terms in order to prevent noise due to saturation of the CCD.

It is worthwhile to recall the fact that any interferometric system requires stability and solid alignment conditions. Additionally, the optical architecture involves supplementary optical elements and a larger working space. Because of these issues, it is important to develop other effective experimental schemes where the interferometric architecture could be austerely employed, said only once, thus overall using fewer elements and relaxing the stability and alignment requirements for the entire process.

This is the first paper, to the best of our knowledge, to report the implementation of an optical construction–reconstruction encrypting protocol by the use of a JTC architecture without the need of an external reference wave. To accomplish this advantage, we first manufacture a master key by using a Mach–Zehnder scheme with the JTC architecture in one arm. Thereafter, by only working with the JTC we proceed to complete the encrypting technique. The master key works as an additional random phase mask to the conventional encrypting processes. In any case, the retrieval process enables us to implement a secure system without altering the original encrypting protocols. We include a theoretical supporting section, along with a technical description of the method. Finally, we present two practical applications in encryption: one in a multiplexing process [17] and the other in a subsampling operation [18].

2. Master Key

In this contribution, we manage the concept of a master key, which has not been used so far in the context of experimental optical encryption. The master key is an additional random phase mask to the conventional encrypting processes. Its inclusion allows us to primarily generate an additional secure instrument in the JTC encrypting process. It also permits, in the same process, implementation of an actual experimental procedure involving digital holography, without the need of an external reference wave. Another major advantage is that when eliminating the reference wave, we do not alter the basic JTC setup, therefore we are keeping the basic encrypting structure.

In the following, we discuss the experimental process to register the Fourier transform (FT) of the master key. Referring to Fig. 1, where we display a basic Mach–Zehnder scheme, the ground glass placed at plane O brings the master key through the respective windows. Using a plane wave illumination, the first beam splitter divides the input beam into two paths, the object wave and the reference wave. The CCD camera placed after the second recombination beam splitter records the digital hologram of the Fourier transform (FT) of the master key $I_{MK}(u,v)$. The resulting intensity is

$$\begin{aligned} I_{MK}(u,v) = {} & |P(u,v)|^2 + P^*(u,v)MK(u,v)\exp(i2\pi ua) \\ & + P(u,v)MK^*(u,v)\exp(-i2\pi ua) \\ & + |MK(u,v)|^2, \end{aligned} \tag{1}$$

where a is the distance between the master key and the optical axis, $*$ denotes the complex conjugate, $MK(u,v)$ is the FT of the master key $mk(x,y)$, and $P(u,v)$ represents the reference plane wave. Here (x,y) represent the spatial coordinates and $(u = x/\lambda f_L, v = y/\lambda f_L)$ denotes the coordinates in the Fourier domain. As we want to retain the second term of Eq. (1) we need to cancel the other three terms. First,

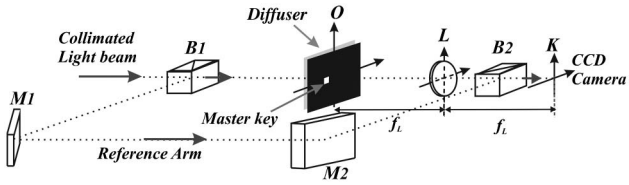

Fig. 1. Experimental setup to store holographically the FT of the master key: O: input plane; B: beam splitter; M: mirror; diffuser: ground glass; master key: random phase mask; L: lens; f_L: focal length of L; K: output plane where the CCD camera is placed.

we record the intensity term $|P(u,v)|^2$ by blocking the object wave and then by blocking the reference wave we record the term $|MK(u,v)|^2$. Applying the subtracting operation of these terms from Eq. (1), we retain the second and third terms.

Now we want to remove the third term but also we want to position the second term in the center of the optical axis. To do so, we perform an FT leading to

$$i_{MK}(x,y) = mk(-x,-y) \otimes \delta(x-2a,y) + mk^*(x,y) \otimes \delta(x+2a,y), \quad (2)$$

where $\otimes$ represents convolution. The second term of Eq. 2 is spatially placed by a delta function, therefore a simple filtering removes it. Finally, the remaining term is digitally positioned at the center of the coordinate system, thus by an inverse FT, we get

$$I'_{MK}(u,v) = MK(u,v). \quad (3)$$

Equation (3) represents the FT of the master key centered at the optical axis. This master key will be an additional security coding-mask when included in a conventional JTC encrypting architecture. In order to probe the potentiality of this new concept, in the next sections we will develop the optodigital procedure to carry out an encrypting protocol using the concept of master key; next we present two applications of the master key in a multiplexing procedure [17] and a subsampling technique [18].

3. Encryption Process Using the Master Key

In the conventional JTC encrypting implementation by using digital holography, an explicit reference wave is needed. In this section, we will develop a JTC encrypting tactic but this time taking advantage of the master key to avoid the reference wave. We now give a brief description of the procedure.

Using only the object path of the Mach–Zehnder of Fig. 1, we are employing the total amount of intensity from the original plane wave over the JTC encrypting architecture. Obviously this is a noninterferometric scheme and now we replace the master key for the object to be encrypted $o(x,y)$ multiplied by a random phase mask $h(x,y)$; afterward we open the other JTC window, where we placed the random phase encoding mask $k(x,y)$ separated by a distance $2a$ (Fig. 2). The amplitude distribution in this input plane is described by

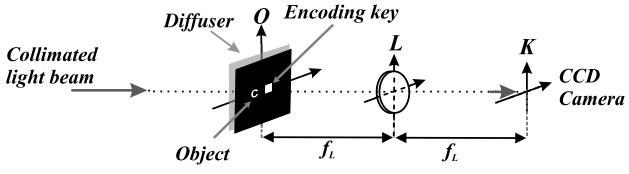

Fig. 2. Experimental arrangement to encrypt the input object. Object path of the Mach–Zehnder interferometer.

$$e(x,y) = f(x,y) \otimes \delta(x+a,y) + k(x,y) \otimes \delta(x-a,y), \quad (4)$$

where $f(x,y) = o(x,y)h(x,y)$ is the transmittance given by $o(x,y)$ in contact with the random phase mask $h(x,y)$. The CCD camera then records the respective JPSs that essentially represent the encrypted object $E(u,v)$, given by

$$E(u,v) = |K(u,v)|^2 + F^*(u,v)K(u,v)\exp(-i4\pi ua) + F(u,v)K^*(u,v)\exp(i4\pi ua) + |F(u,v)|^2, \quad (5)$$

where $K(u,v)$ and $F(u,v)$ denote the FTs of the encoding keys $k(x,y)$ and $f(x,y)$, respectively.

Following a similar procedure as the one used for the master key in Eqs. (1)–(3), we remove all but the third term and center it. In this case, we block the object window to obtain $|K(u,v)|^2$ and we block the encoding key window to get $|F(u,v)|^2$

$$E'(u,v) = F(u,v)K^*(u,v). \quad (6)$$

In the following step, we change the object, in the experimental arrangement of Fig. 2, by the master key in order to record the JPS information between the encoding key and the master key. By filtering, keeping only the relevant decoding information, and repositioning at the center of the plane, we get

$$G(u,v) = MK^*(u,v)K(u,v). \quad (7)$$

In the decrypting step we multiply the FT of the master key [Eq. (3)], the encrypted object [Eq. (6)], and the processed JPS between the master key and the encoding key [Eq. (7)], to obtain after an inverse FT:

$$d(x,y) = f(x,y) \otimes [k^*(-x,-y) \otimes k(x,y)] \otimes [mk^*(-x,-y) \otimes mk(x,y)]. \quad (8)$$

According to standard mathematical procedures [19], Eq. (8) reduces to

$$d(x,y) = f(x,y). \quad (9)$$

This reproduces the original input object-window content. In this way, we probed that our method allows carrying out of an encrypting process using the interferometric setup only in the first step, in which the information of the master key [Eq. (3)] is obtained. Therefore, in the next steps the optical setup is a JTC conventional processor.

In the actual experimental setup, the master key window is projected using a translucent Holoeye LC2002 SLM with a pixel size of 32 μm. We used a laser with wavelength 632 nm, a lens with focal distance 200 mm, and a PULNIX TM6703 CCD with 640×480 pixels and pixel size of 9 μm. The master key is generated employing a ground glass and is limited by the master key window. We obtain the encrypted object using the same experimental setup as in Fig. 1 but without the reference arm (Fig. 2). In this case, the area of both the encoding key window

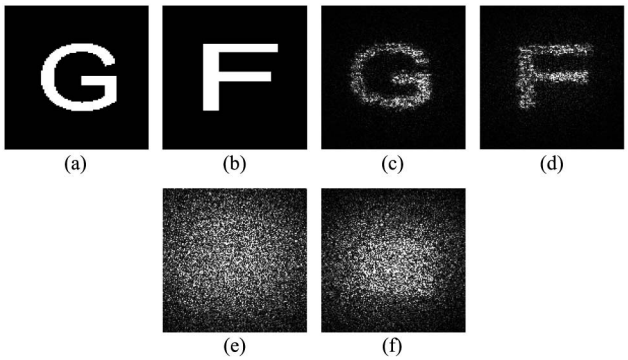

Fig. 3. Images (a) and (b) represent the input objects. Experimental results: (c) and (d) are the right decrypted images of (a) and (b) employing the same master key and their respective encoding keys. By contrast, (e) is the wrong decrypted output using the incorrect encoding key but the right master key of (a), while (f) is the wrong decrypted output using the correct encoding key but the wrong master key of (b).

and the object window is 2.0 mm × 2.0 mm, and the distance between windows is 2.6 mm.

In Figs. 3(a) and 3(b) we show the objects to be encrypted, and in Figs. 3(c) and 3(d) we show the result of the recovering procedure employing the right encoding and master keys, respectively. The master key is the same for both objects, while the encoding key is different for each object. From the experimental point of view, once we obtain the FT of the master key, the beam splitters and the mirrors are dismounted from the original interferometric scheme of Fig. 1. Note that in Figs. 3(c) and 3(d) there is some degradation due both to the limitation in the experimental resolution and to the inherent speckle noise.

In Figs. 3(e) and 3(f), the master key represents an additional key for the process, leading to an increase of the security of the method. The advantages we found with this architecture are evident from the experimental results presented in Fig. 3. The system is more compact, as we do not require an external reference beam; and at the same time, security is enhanced.

4. Applications of the Protocol to Encrypt Multiple Data

The multiplexing operation in the context of encryption allows getting into a single dataset the information of multiple encrypted objects. Using the master key protocol described above, in this section, we encrypt and multiplex encrypted images. For this purpose, we change the encoding key during the encryption of each object. Following the same encryption process of Section 3, the object $o_n(x,y)$ and its corresponding encoding key $k_n(x,y)$ are placed side by side, as shown in Fig. 2. Then, the JPS is [Eq. (5)]

$$E_n(u,v) = |K_n(u,v)|^2 + F_n^*(u,v)K_n(u,v)\exp(-i4\pi ua) + F_n(u,v)K_n^*(u,v)\exp(i4\pi ua) + |F_n(u,v)|^2 \tag{10}$$

where $K_n(u,v)$ and $F_n(u,v)$ denote the FT of the encoding key $k_n(x,y)$ and $f_n(x,y) = o_n(x,y)h(x,y)$. Then subtracting the first and fourth terms and performing an FT we get

$$e_n(x,y) = f_n^*(x,y) \otimes k_n(-x,-y) \otimes \delta(x+2a,y) + f_n(-x,-y) \otimes k_n^*(x,y) \otimes \delta(x-2a,y), \tag{11}$$

with the two terms spatially separated. Now we are able both to remove the first term and to reposition the pertinent information around a desired point (x_n,y_n). Each (x_n,y_n) pair of coordinates are chosen in such a way that each object is placed, inside the recovering plane, in its relative original position, thus avoiding mismatching of any kind. Therefore, we get

$$e_n'(x,y) = f_n(-x,-y) \otimes k_n^*(x,y) \otimes \delta(x-x_n,y-y_n). \tag{12}$$

Finally, performing an inverse FT we retain the encrypted object without the unwanted terms

$$E_n'(u,v) = F_n(u,v)K_n^*(u,v)\exp[i2\pi(x_nu + y_nv)]. \tag{13}$$

In case we have N different objects, we encrypt each one independently with different encoding keys. Then, the multiplexing of the corresponding N encrypted images is

$$M(u,v) = \sum_{n=1}^{N} F_n(u,v)K_n^*(u,v)\exp[i2\pi(x_nu + y_nv)]. \tag{14}$$

Next, we record the JPS between each encoding key and the master key [Eq. (7)] to obtain

$$G_n(u,v) = MK^*(u,v)K_n(u,v). \tag{15}$$

In the decryption process of the object l, we multiply the multiplexing that contains all the encrypted objects [Eq. (14)], the processed JPS between the encoding key l and the master key [from Eq. (15)], and the FT of the master key [Eq. (3)]. Then, after an inverse FT, we get

$$d_l(x,y) = f_l(x,y) \otimes [k_l^*(-x,-y) \otimes k_l(x,y)] \otimes [mk^*(-x,-y) \otimes mk(x,y)] \otimes \delta(x-x_l,y-y_l), \tag{16}$$

thus finally leading to the object l in the chosen position (x_l,y_l),

$$d_l(x,y) = f_l(x,y) \otimes \delta(x-x_l,y-y_l). \tag{17}$$

At this point, we want to highlight that Eq. (17) shows each decrypted object in a previously desired

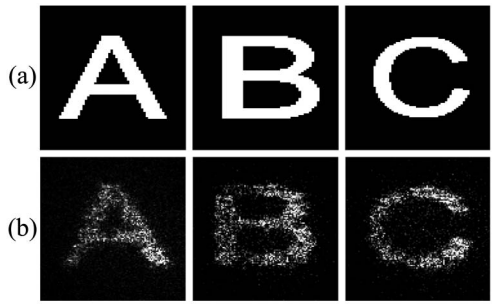

Fig. 4. Multiplexed encrypted objects. Line (a) corresponds to the original objects and line (b) corresponds to the decrypted objects.

position defined when handling Eq. (12). This procedure avoids the influence of cross-talk and noise over the recovered information.

The objects of Fig. 4 line (a) are encrypted and then multiplexed according to the procedure described above. After the optodigital decrypting process, we recover the original data [Fig. 4, line (b)] without cross-talk or noise. It is important to take into account that the noise is avoided by means of subtracting the DC terms, and the cross-talk is suppressed employing the repositioning scheme.

5. Multiplexing Encryption in a Subsampling Protocol

Optical systems have a limited resolution. Consequently, we get somewhat degraded images. These limitations are present in the actual experimental setups employed to encrypt and to decrypt information. This image deterioration is partly due to the natural speckle noise as well as the practical limitations arising from the optical elements composing the setup. In a recent contribution [18], we proposed and implemented an experimental protocol that allows obtaining a better-decoded image without losing the security advantages of the encrypting protocols, complicating the recording system or the reconstruction algorithm, moving the CCD device. This protocol is based on an optical image synthesis with digital holography using enlarged subsamples of an entire image together with a multiplexing technique [18]. Calling the input image a *sample,* by *subsample* we mean each equally subdivided part of the sample.

Our purpose in this section is to apply the concept of a master key in a subsampling encrypting technique without altering the standard security levels. This method avoids the eventual joint misplacement of the subsamples when reconstructing, thus preventing quality degradation.

Using the experimental setup of Fig. 2 we encrypt all subsamples with the same encrypting key. In order to obtain the encrypted data, each subsample and the encrypting key in the input plane are separated by a distance $2a$. As in the procedure described in Section 4, after subtracting the DC terms and repositioning the term of interest, the encrypted information of each subsample is obtained and then all the encrypted subsamples are multiplexed:

$$M(u,v)=\sum_{n=1}^{N}F_n(u,v)K^*(u,v)\exp[i2\pi(x_nu+y_nv)]. \quad (18)$$

In this application, $K(u,v)$ denotes the FT of the encoding key $k(x,y)$ and $F_n(u,v)$ represents the FT of $f_n(x,y)=o_n(x,y)h(x,y)$, where $o_n(x,y)$ is the transmittance of the n subsample. In this case, there is only one encoding key for all subsamples. This implies that we need only once get the processed JPS between the master key and the encoding key, as was noted in the case of a single object encryption [Eq. (7)].

The information contained in Eq. (18) is sent to the end user together with the processed JPS between the master key and the encoding key [Eq. (7)] and the FT of the master key [Eq. (3)]. Finally, the user multiplies this information and performs an inverse FT to recover the entire sample:

$$d(x,y)=\sum_{n=1}^{N}f_n(x,y)\otimes\delta(x-x_n,y-y_n). \quad (19)$$

Eq. (19) shows each decrypted subsample in a chosen position. Such position is controlled pixel wise, the same pixel partition made when generating the subsamples, therefore during decryption we are not introducing any mismatching between subsamples. The final procedure reconstructs all parts of the sample in their right places at the same time.

The experimental results of this application are displayed in Fig. 5. In the experimental procedure the original sample [Fig. 5(a)] is projected in the SLM and the JPS between the object and the encoding key is recorded in the CCD camera. Then, the information of the FT of the encoding key is also registered in the camera. After following all the steps described in the previous section and performing the right decryption process, the recovered information is obtained [Fig. 5(b)]. The original encrypting procedure, besides the usual frequency lost due to the numerical aperture involved, also presents speckles whose sizes override frequency bands. Therefore, we cannot recognize all original traces.

In the next step, we divided the entire sample into four subsamples [Fig. 5(c)], and then each subsample

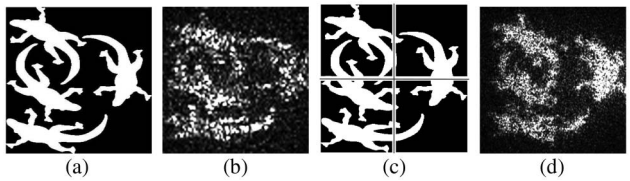

Fig. 5. Improving decrypted image quality using the subsampling technique. (a) Sample, (b) right experimental decryption using the entire sample without the subsampling protocol, (c) sample divided into four subsamples, and (d) decrypted image employing the subsampling technique.

was rescaled so as to occupy the same size as the original sample. Using the entire subsampling procedure to encrypt and multiplex the subsample data and the correct decrypting procedure, the decryption leads to recovering of the entire sample [Fig. 5(d)]. After applying our technique, the recognition of the entire subsample is improved.

6. Conclusions

With the introduction of a master key, we demonstrated that we actually reduce the application of an external reference wave to only once during the completely experimental procedure in a JTC encrypting architecture. Besides, we reinforce the security of the double random phase mask encoding method. We presented experimental results supporting our approach, including several examples as a single image encryption, a multi-user application, and a subsampling protocol.

As mentioned, the main advantage of the method is avoidance of the reference wave in an encryption protocol that employs an actual digital holographic scheme. Once the information of the master key is holographically registered, the rest of the experimental steps are performed by means of a classical JTC architecture alone. Therefore, the experimental setup to implement our proposal is compact and robust, as it does not require an accurate optical alignment.

This research was performed under grants from CODI—Universidad de Antioquia (Colombia), TWAS-UNESCO Associateship Scheme at Centres of Excellence in the South, CONICET no. 112-200801-00863 (Argentina), ANCYT PICT 1167 (Argentina), and Facultad de Ingeniería, Universidad Nacional de La Plata no. 11/I125 (Argentina).

References

1. A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," Adv. Opt. Photon **1**, 589–636 (2009).
2. O. Matoba, T. Nomura, E. Pérez-Cabré, M. S. Millán, and B. Javidi, "Optical techniques for information security," Proc. IEEE **97**, 1128–1148 (2009).
3. O. Matoba and B. Javidi, "Encrypted optical storage with angular multiplexing," Appl. Opt. **38**, 7288–7293 (1999).
4. G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," Opt. Lett. **25**, 887–889 (2000).
5. O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," Opt. Lett. **24**, 762–764 (1999).
6. J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, "Multiplexing encryption-decryption via lateral shifting of a random phase mask," Opt. Commun. **259**, 532–536 (2006).
7. J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, "Multiplexing encrypted data by using polarized light," Opt. Commun. **260**, 109–112 (2006).
8. G. Situ and J. Zhang, "Multiple-image encryption by wavelength multiplexing," Opt. Lett. **30**, 1306–1308 (2005).
9. T. Nomura and B. Javidi, "Optical encryption using a joint transform correlator architecture," Opt. Eng. **39**, 2031–2045 (2000).
10. E. Rueda, J. F. Barrera R., R. Henao, and R. Torroba, "Optical encryption with a reference wave in a joint transform correlator architecture," Opt. Commun. **282**, 3243–3249 (2009).
11. E. Tajahuerce, O. Matoba, S. C. Verrall, and B. Javidi, "Optoelectronic information encryption with phase-shifting interferometry," Appl. Opt. **39**, 2313–2320 (2000).
12. C. La Mela and C. Iemmi, "Optical encryption using phase-shifting interferometry in a joint transform correlator," Opt. Lett. **31**, 2562–2564 (2006).
13. A. Nelleri, J. Joseph, and K. Singh, "Lensless complex data encoding for digital holographic whole information security," Opt. Eng. **47**, 115801 (2008).
14. E. Rueda, J. F. Barrera, R. Henao, and R. Torroba, "Lateral shift multiplexing with a modified random mask in a joint transform correlator encrypting architecture," Opt. Eng. **48**, 027006 (2009).
15. R. Henao, E. Rueda, J. F. Barrera, and R. Torroba, "Noise-free recovery of optodigital encrypted and multiplexed images," Opt. Lett. **35**, 333–335 (2010).
16. C. L. Chen, L. C. Lin, and C. J. Cheng, "Design and implementation of an optical joint transform encryption system using complex-encoded key mask," Opt. Eng. **47**, 068201 (2008).
17. E. Rueda, C. Ríos, J. F. Barrera, R. Henao, and R. Torroba, "Experimental multiplexing approach via code key rotations under a joint transform correlator scheme," Opt. Commun. **284**, 2500–2504 (2011).
18. J. F. Barrera, E. Rueda, C. Ríos, M. Tebaldi, N. Bolognini, and R. Torroba, "Experimental opto-digital synthesis of encrypted sub-samples of an image to improve its decoded quality," Opt. Commun. **284**, 4350–4355 (2011).
19. G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption system that uses phase conjugation in a photorefractive crystal," Appl. Opt. **37**, 8181–8186 (1998).