Optics Communications 281 (2008) 5750–5755

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Synchronized chaotic phase masks for encrypting and decrypting images

Edgar Rueda [a,*], Carlos A. Vera [a], Boris Rodríguez [a], Roberto Torroba [b]

[a] Instituto de Física, Universidad de Antioquia, A.A. 1226, Medellín, Colombia
[b] Centro de Investigaciones Ópticas (CONICET-CIC) and UID OPTIMO, Facultad Ingeniería, Universidad Nacional de La Plata, La Plata, Argentina

ARTICLE INFO

Article history:
Received 3 April 2008
Received in revised form 25 July 2008
Accepted 1 September 2008

PACS:
42.30.–d
05.45.Gg

Keywords:
Optical encryption
Chaotic phase generation
Synchronization system

ABSTRACT

This paper presents an alternative to secure exchange of encrypted information through public open channels. Chaotic encryption introduces a security improvement by an efficient masking of the message with a chaotic signal. Message extraction by an authorized end user is done using a synchronization procedure, thus allowing a continuous change of the encrypting and decrypting keys.

And optical implementation with a 4f optical encrypting architecture is suggested. Digital simulations, including the effects of missing data, corrupted data and noise addition are shown. These results proof the consistency of the proposal, and demonstrate a practical way to operate with it.

1. Introduction

In recent literature, authors proposed several methods for the encryption of 2D information using linear optical systems [1–3]. Optical security technology is based in complex information processes where the signals are first hidden from human perception (to keep them secret). Besides, images should be extremely difficult to be reproduced with the same properties (to avoid counterfeiting). Optical security techniques involve tasks such as encoding, encryption, recognition, secure identification and/or verification. We paid much attention to the double random phase encoding (DRPE) system [1]. This is a method to encode a primary image into a white-noise-like distribution. The method uses two random phase key codes on each of the input and Fourier planes and it can be implemented either optically or electronically in both the encryption and the decryption stages. In linear (amplitude-based) encoding, the primary image, which is commonly assumed to be real and positive, is encoded in magnitude in the encrypted image. In nonlinear (full-phase) encoding, a phase-only version of the primary image is encoded. With amplitude-based encoding the first phase mask is not needed to decode the encrypted image, whereas this mask has to be known with full-phase encoding. Both possibilities have been analyzed in the presence of perturbation of the encrypted image, and the results show their good properties regarding noise robustness [4,5]. In the presence of additive noise, and using the mean-square error metric, Ref. [4] shows that full-phase encoding performs better than amplitude-based encoding.

Regarding high transfer rates, holographic data storage [6,7] offers terabyte capacity. Optical multiplexing encryption systems [8–11] were used to improve the performance of these systems. This improvement is attributed to the suppression of cross talk between adjacent images. While the original data is recovered with the correct random phase key, the overlapping reconstructed images from neighboring orders remain white-noise-like images because an incorrect random phase key has been used.

Recently, concern about the vulnerability of the encryption systems based on DRPE has arose. Several authors [12–14] have used different attacks in order to access the encrypted information and have been able to recover the keys (phase masks) of the system in cases where the attacker has access to a few plaintexts and its corresponding cyphertexts. To overcome this system flaw authors have proposed the use of frequency spectral analysis and Fresnel domain or Fractional Fourier Transform schemes instead of the Fourier Transform scheme.

Summarizing, there are several attempts to overcome the crucial shortcomings derived from eavesdroppers' attacks, designing a highly reliable security protocol.

With this in mind, now we find in chaotic encryption an alternative candidate for security improvement of optical telecommunication systems. Chaotic systems are dynamical systems that defy synchronization. Two identical autonomous chaotic systems

* Corresponding author. Tel.: +574 2196556.
E-mail address: earueda@barlai.udea.edu.co (E. Rueda).

0030-4018/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.optcom.2008.09.002

started at nearly the same initial points in phase space have trajectories which quickly become uncorrelated, even though each maps out the same attractor in phase space. It is thus a practical impossibility to construct identical, independent, chaotic, synchronized systems in the laboratory.

The development of synchronized chaotic systems has been greatly motivated by the possibility of encoding information within a chaotic carrier. This possibility was explored in electronic circuits whereby a small analog signal (the message) was added to a chaotic voltage and transmitted to a receiver that is a replica of the electronic circuit that generates the chaotic carrier. The receiver synchronizes with the chaotic carrier itself, and a subtraction of the synchronized signal from the transmitted signal (carrier + message) results in the recovery of the message.

The security of data encryption using chaos methods relies upon two important points: the unpredictability of the carrier signal, and the sensitivity exhibited by the dynamics of chaotic systems under parameter mismatch. Due to the second point, only a system very similar to the chaotic transmitter can be used to decode the message in an efficient way.

Summarizing, the operation principle behind chaotic encryption relies on the efficient masking of the message within a chaotic signal and the extraction of the message at the receiver's side through a synchronization process that allows a continuous change of the encrypting and decrypting keys. We find the experimental proof for different configurations involving semiconductor laser emitters that operate in the telecommunication wavelengths and that exhibit chaotic dynamics of high complexity [15–17]. Among all possible schemes, optical feedback is one of the most extensive configurations used to generate a high-dimensional chaotic laser output [16].

In this contribution, we use a DRPE system in a 4f encryption architecture, where the random masks of the DRPE are obtained using a non-linear system in chaotic regime. The great innovation is obtaining the right decrypting mask, which allows modifying the encrypting mask indefinitely without sending the correct decrypting mask to the authorized user. Another advantage is the transmission of both the encrypted image and the key construction data (driving message) through public open channels without any risk. Encryption is performed using Fourier transforms.

Additionally, we address the results of losing information, corrupting information and adding noise to the data needed to reconstruct the decryption key. This technique enhances the overall security and exploits in the best way the characteristics of the chaotic behavior of dynamical systems.

2. Chaotic phase mask generation for image encryption

Phase masks for the encryption procedure are generated from the y state of the *chaotic web map* [18], $X_{n+1} = F(X_n)$, $X_n = (x_n, y_n)$

$$\begin{aligned} x_{n+1} &= x_n \cos\alpha - (y_n + k\sin x_n)\sin\alpha, \\ y_{n+1} &= x_n \sin\alpha + (y_n + k\sin x_n)\cos\alpha. \end{aligned} \tag{1}$$

Which is an area preserving map, moreover, it is a symplectic one:

$$\widetilde{\partial F}\,\Omega\,\partial F = \Omega, \tag{2}$$

where Ω is the symplectic matrix. Thus there is not a transient regime in the dynamics, ensuring that the values y for the phase mask are chaotic from the beginning of the iteration. We choose the operation point in the parameter space to be $\alpha = 1.366$ and $k = 3$ where the maximum exponent is positive (Fig. 1), at this point the phase space exhibits irregular zones and stability islands as it is typical for symplectic dynamics.

3. Chaotic system synchronization for image decryption

Consider two chaotic systems operating with different initial conditions; the states for this systems will be denoted by X_n and $\tilde{X}_n$, the former being described by (1) and the latter by

$$\begin{aligned} \tilde{x}_{n+1} &= \tilde{x}_n \cos\tilde{\alpha} - (\tilde{y}_n + \tilde{k}\sin\tilde{x}_n)\sin\tilde{\alpha} + u(X_n, \tilde{X}_n), \\ \tilde{y}_{n+1} &= \tilde{x}_n \sin\tilde{\alpha} + (\tilde{y}_n + \tilde{k}\sin\tilde{x}_n)\cos\tilde{\alpha}, \end{aligned} \tag{3}$$

for the sake of simplicity let us consider the case $\tilde{\alpha} = \alpha$ and $\tilde{k} = k$. The term u is included to compensate the difference between the systems states in order to reach synchronization between them (see Eq. 4). Now, let suppose the state x_n of the first system is measured and sent to the second one, in such a way that $\tilde{x}_n = x_n$. With this two considerations it is a direct task to compute the error between this systems, that is the difference of the states $X'_n = \tilde{X}_n - X_n$, whose dynamics is described by

$$\begin{aligned} x'_{n+1} &\equiv \tilde{x}_{n+1} - x_{n+1} = -y'_n \sin\alpha + u(X_n, \tilde{X}_n), \\ y'_{n+1} &\equiv \tilde{y}_{n+1} - y_{n+1} = y'_n \cos\alpha, \end{aligned} \tag{4}$$

since a measure of x_n is available for all n, is straightforward to set the dependence of the input function u only on this state, that is $u = u(x_n, \tilde{x}_n)$, moreover, let choose a specific form for u based in feedback control theory [19]

$$u(x_n, \tilde{x}_n) = -\beta(\tilde{x}_n - x_n), \quad 0 < \beta < 1. \tag{5}$$

Here is important to note that in Eq. (5) $\tilde{x}_n$ has the value obtained with Eq. (3) for the n step and with $\tilde{x}_{n-1} = x_{n-1}$, thus it is not equal to the value x_n obtained with Eq. (1) for the same step unless the systems are synchronized, since Eqs. (1) and (3) have a dependency on y and $\tilde{y}$, respectively. With this election the error dynamics becomes linear

$$X'_{n+1} = AX'_n, \tag{6}$$

with A having eigenvalues at $\{-\beta, \cos\alpha\}$, both with module smaller than unity, thus the error goes asymptotically to zero with the spent

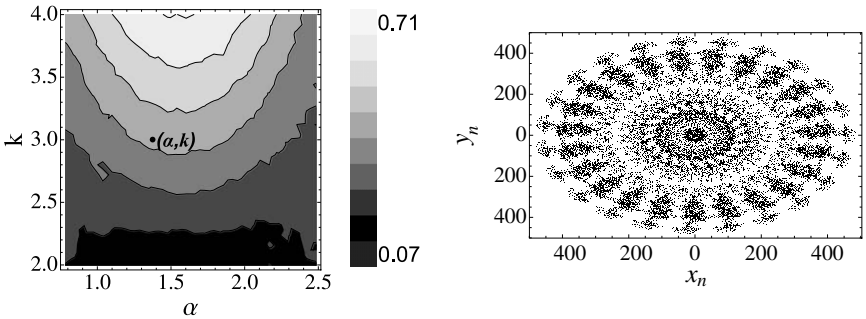

Fig. 1. Maximum Lyapunov exponent, the coordinate corresponds to $(\alpha, k) = (1.366, 3)$ (left panel), Phase space for the operation point (right panel).

time in the transient dynamics depending on β: the lower β, the smaller spent time. Note that by sending only the x_n state, systems X_n and $\tilde{X}_n$ are quickly synchronized (fig. 2) and therefore both dynamical states reach the same numerical values after few iterations, allowing a continuous change of the encrypting masks (see Eq. 7). In order to synchronize both systems, system $\tilde{X}_n$ must know the parameters k and α and the whole time series x_n (it does not matter initial conditions), however only k and α have to be secret while x_n can be sent using a public channel. Although the encryption algorithm is public it does not make it vulnerable to brute force attacks, for example, suppose the actual values of α and k are irrational and are chosen such the system is operated in a chaotic regime, small variations around these values leave the system still operating in a chaotic regime (see Fig. 1), making impossible to choose the correct values of the parameters by following a brute force attack, since brute force attacks only enables rational values of the parameters α and k.

A scheme of the whole communication system is shown in Fig. 3. The phase masks are generated from the relation

$$\frac{\phi_n}{2\pi} = 2y_n \mathrm{mod} 1. \tag{7}$$

The map $2y_n$mod1 has an invariant measurement constant [20] so that phases look like having a random origin, which is a wrong prediction since the true origin is a chaotic dynamics. This chaotic origin ensures a high sensibility to initial conditions, i.e. slightly different initial conditions lead to completely uncorrelated encrypting chaotic phase masks, and thus generating a dynamical encrypting process where the encrypting and decrypting masks can be change continuously.

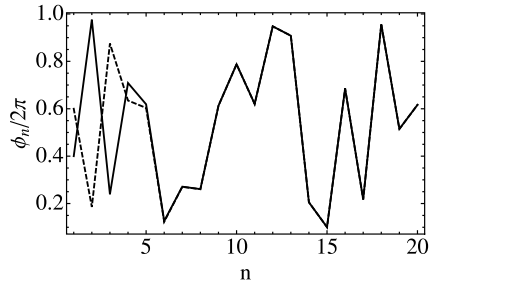

Fig. 2. Phase mask synchronization for $\beta = 0.5$.

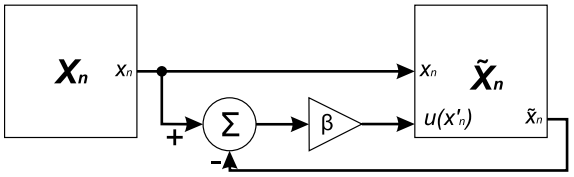

Fig. 3. System scheme.

4. Optical implementation and performance simulations

Optical implementation is a key factor in the development of this information security techniques. Two main architectures: 4f (Fig. 4) and Joint Transform Correlator (JTC) [21,22], together with: Spatial Light Modulators (SLMs), photorefractive crystals and holographic or digital holographic techniques [23–26], are commonly used. With this in mind a suitable optical implementation for the proposed security system is presented in Fig. 5. In the encrypting step a computer generates the chaotic phase masks and addresses two SLMs in a 4f optical architecture (SLM1 displays the original image and the first phase mask in plane O, SLM2 displays the encrypting phase mask in plane K, as seen in Figs. 4 and 5). The computer, through a CCD (in plane E, Fig. 4), stores the hologram of the encrypted image and uses a digital holographic technique to send the complex-value encrypted image through a public channel together with the driving message. In the decrypting step, another computer, by means of the driving message, generates the decrypting chaotic phase mask and addresses two SLMs in a 4f optical architecture (SLM3 displays the inverted complex-value encrypted image, SLM4 displays the decrypting phase mask in plane K, as seen in Figs. 4 and 5). The computer, through a CCD (in plane E, Fig. 4), stores the decrypted image.

In order to study the performance of the system a 4f architecture is simulated for the image encryption and decryption with chaotic phase masks (Fig. 4). For the encryption process the chaotic phase mask and the amplitude image to be encrypted are placed in plane O. In plane K the Fourier transform of the phase mask and amplitude image is obtained by means of lens L_1, and then multiplied by the encrypting chaotic phase mask. Finally, using lens L_2 the amplitude in plane K is Fourier transformed to plane E, obtaining the desired encrypted image.

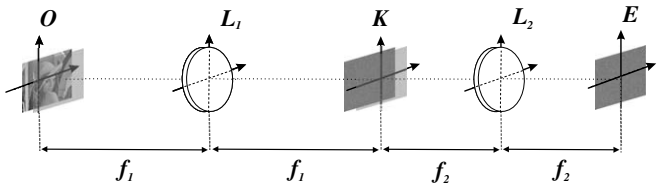

Fig. 4. 4f optical setup. In plane K lens L_1 performs the Fourier Transform of objects in plane O. In plane E lens L_2 performs the Fourier Transform of objects in plane K. f_1 and f_2 are the focal length of lens L_1 and L_2, respectively.

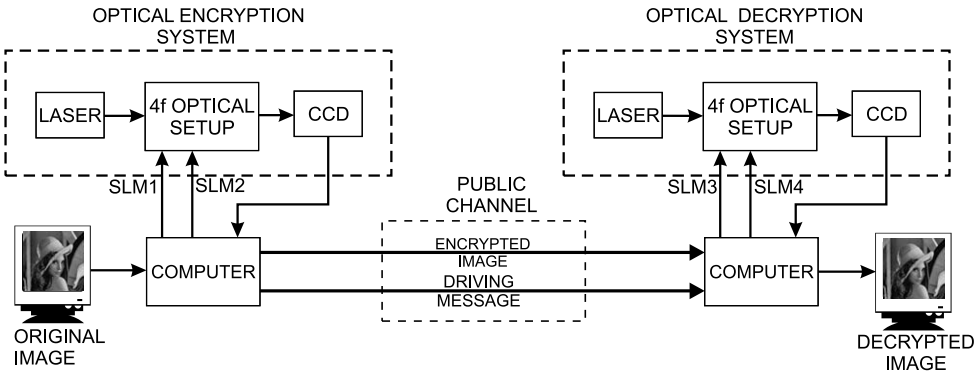

Fig. 5. Suggested optical implementation.

For the decryption process the encrypted image is placed inverted in plane O, Fourier transformed into the plane K, multiplied by the complex conjugate of the decrypting chaotic phase mask obtained by means of the proposed synchronization method and Fourier transformed into the plane E, where the intensity stored by the recording media will correspond to: the correct decrypted image if the right decrypting mask is used, or white-noise-like image if a wrong mask is used.

In order to show the invulnerability of the proposed system an image encrypted with it is then decrypted using: (i) a random generated phase decrypting mask, (ii) an old decrypting mask generated with the true security parameters but different initial conditions in the encoding step, and (iii) a decrypting mask generated with security parameters *very similar* to the true ones. Results are compared with the decrypted image obtained with the true security parameters. Simulations were performed on the gray scale image of Fig. 6 with a 512×512 pixels size.

The security parameters and initial conditions are: for the authorized encoder $k = 3$, $\alpha = 1.366$, $x_0 = -3.6$ and $y_0 = 1.3$. For the authorized decoder $k = 3$, $\alpha = 1.366$, $\tilde{x}_0 = 2.6$ and $\tilde{y}_0 = 2.8$. For (ii) $k = 3$, $\alpha = 1.366$, $x_0 = -6.5$ and $y_0 = 4.0$, and for (iii) $k = 3$, $\alpha = 1.364$, $\tilde{x}_0 = -5.1$ and $\tilde{y}_0 = 2.4$.

Figs. 7a and b show the encrypting mask and the encrypted image, respectively. The decrypted images are presented in: Fig. 7c using the true security parameters, Fig. 7d using a random generated decrypting mask (i), Fig. 7e using an old generated decrypting mask (ii), and Fig. 7f using a decrypting mask generated with security parameters very similar to the true ones (iii). This system can be improved if in addition to the two security parameters, another security parameter is added in the form of the fractional Fourier order when the $4f$ setup is replace by the $4f$ optical fractional Fourier setup [27,28].

Fig. 6. Gray scale image with 512×512 pixels for the simulations.

5. Communication losses and additive noise

The idea with the optical processing is to use its parallel information processing ability and its high processing speed (the speed of light), specially in the usually time-consuming encryption step. But in a real situation this encrypted 2D information must be transmitted using the common digital channels of communication and so the encrypted information has to be codified for the transmission and decodified for the decryption step (5). This procedure will inevitably introduce additive noise and cause the loss and corruption of some information, thus affecting the quality of the image. In particular, this technique requires the transmission of both, the encrypted information and the driving message (x_n). Ref. [4] address the results of adding noise to the encrypted image using an MSE metric. In this work a new metric is going to be use to address the results of losing and corrupting information, and adding noise in the driving message data. Thus simulations of losing, corrupting and addition of noise to the driving message data have been performed. The new metric is defined in order to facili-

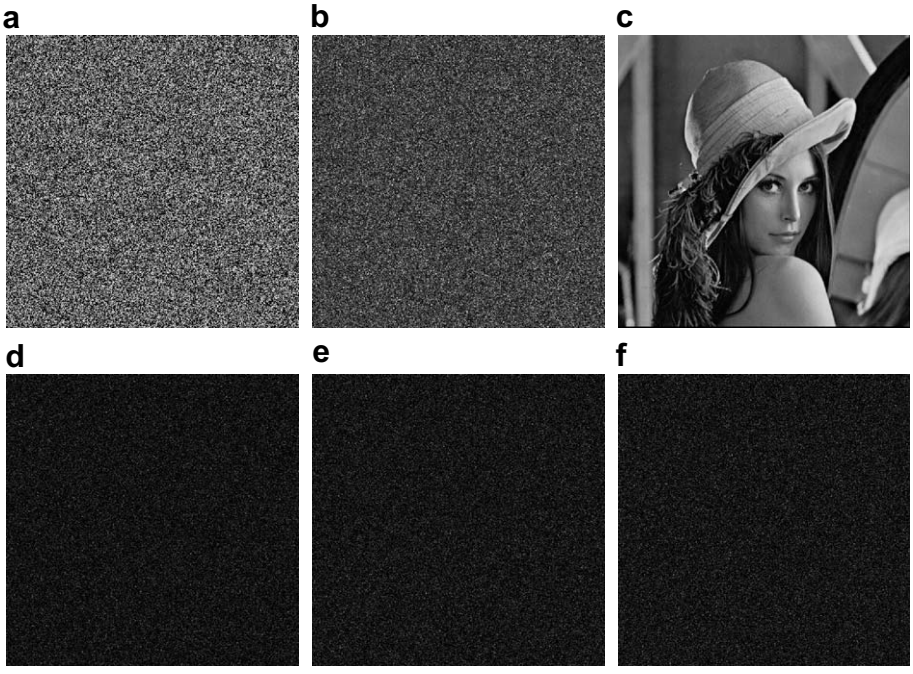

Fig. 7. (a) Encrypting phase mask obtained with the proposed system, (b) encrypted image, (c) decrypted image using the true security parameters of the authorized user, (d) decrypted image using a random generated decrypting mask *(i)*, (e) decrypted image using an old generated decrypting mask *(ii)*, (f) decrypted image using a decrypting mask generated with security parameters very similar to the true ones *(iii)*.

tate the comparison of the results as can be seen in Fig. 8, comparison that can not be done with the unbounded MSE metric. The new metric is simply the well known MSE divided by the MSE obtained when the decrypted image corresponds to a completely random white-noise-like image. This has the property that all possible values are between 0 (perfectly decrypted image) and 1 (white-noise-like decrypted image). NMSE stands by Normalized Mean Square Error and is defined as

$$\mathrm{NMSE}(I_0, I) = \frac{1}{K}\sum_{i,j}^{N} |I(i,j) - I_0(i,j)|^2, \tag{8}$$

where I_0 and I denote the input and output image intensity at the pixel (i,j), respectively. The image has a total of $N \times N$ pixels, and K (Eq. 9) is the MSE between I_0 and a white-noise-like image I_w

$$K = \sum_{i,j}^{N} |I_w(i,j) - I_0(i,j)|^2. \tag{9}$$

In the first case the driving message is subjected to data loss, corresponding to changing the value of a randomly selected pixel to a null value. Fig. 9 shows the result NMSE for the driving message. The second case corresponds to a data corruption where a randomly selected pixel randomly changes its value. Fig. 10 shows the NMSE for the driving message. The third case takes into account an additive noise. This additive noise was applied

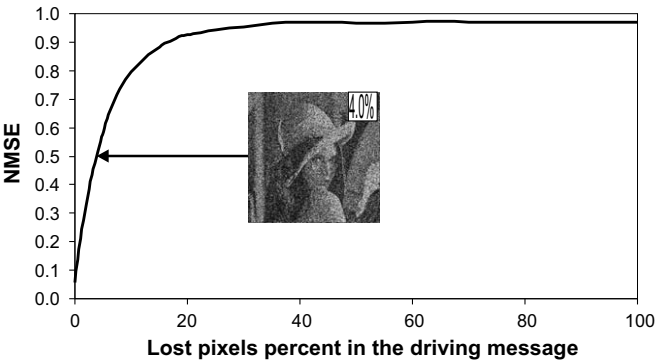

Fig. 9. NMSE as a function of the data loss percent in the driving message.

to all the driving message time series and corresponds to a percentage of the mean absolute value of such time series. Fig. 11 shows the NMSE for the driving message. Figs. 9–11 show that the decryption process is more sensible to additive noise than to loss or corruption of information in the driving message. This difference exists because additive noise always affects all the pixels of the image, thus each time the system is synchronized the additive noise change the correct value and so the synchronization process has to "start" again, problem that only occurs in

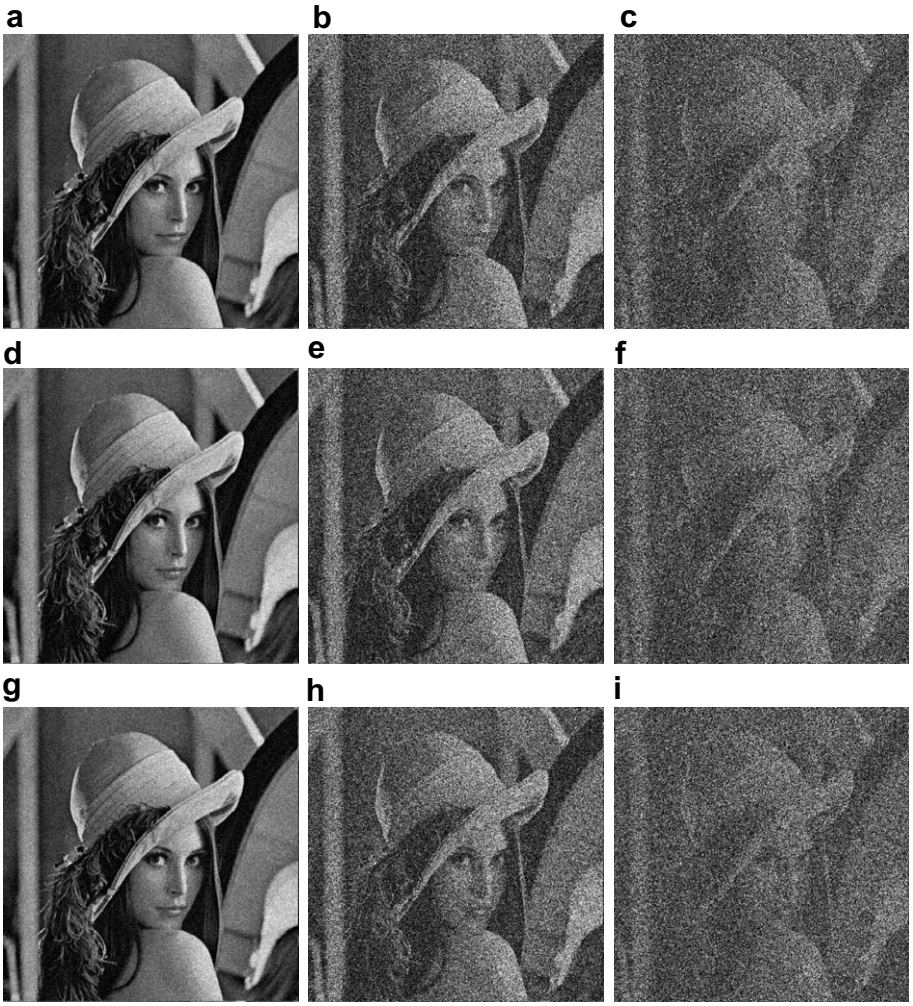

Fig. 8. Results of the image decryption with: data loss for (a) NMSE = 0.1, (b) NMSE = 0.5, (c) NMSE = 0.8, data corruption for (d) NMSE = 0.1, (e) NMSE = 0.5, (f) NMSE = 0.8, and noise addition for (g) NMSE = 0.1, (h) NMSE = 0.5, (i) NMSE = 0.8.

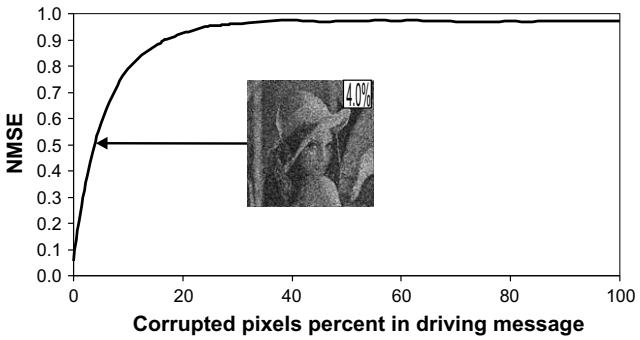

Fig. 10. NMSE as a function of the data corruption percent in the driving message.

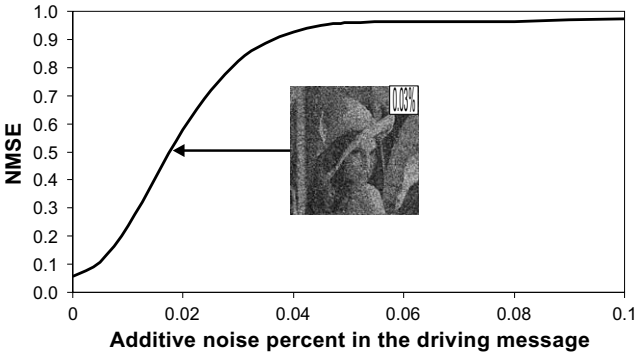

Fig. 11. NMSE as a function of the additive noise percent in the driving message.

the other cases when the number of lost and corrupted pixels becomes important. Finally, if a recognizable image in the decryption process is considered the limit of the acceptable noise, loss or corruption, a NMSE = 0.8 will be the value of maximum tolerance as can be seen in Fig. 8.

When thinking in the practical implementation of our proposal, we have to focus on the SLM performance. The condition for full-range complex modulation is that the SLM must provide a 2π-range phase modulation. In that sense, look-up table encoding methods permits the compensation of phase-amplitude coupling and nonlinearity in the SLM modulations.

Experimental techniques for determining the SLM-device parameters, for maximizing the phase-mostly modulation range and the amplitude-mostly modulation contrast, and for testing the complex-amplitude modulation were developed in the literature, therefore for the sake of brevity we do not discuss them here [29–31]. We have to mention also that the commercially available devices are generally produced under proprietary conditions. Every single SLM unit may show significant differences in its optical behavior from other units of even the same trademark and model. Consequently, knowledge of the Jones matrix for these devices helps to evaluate their performance in optical processing systems.

It is clear that the quality and effectiveness of the optical component addressed to the SLM strongly depends on the knowledge of the device response. In fact, the signal must be modified before addressing it to the SLM to compensate for the distortions internally introduced by the device and hence, to eventually reproduce the optical signal with the desired performance. It is important to obtain good enough dynamic ranges and try to correct for the nonlinear mapping of digital gray-level (voltage) to phase modulation. Nevertheless, once calibration operation is performed, we can overcome these issues and work correctly with currently commercially available devices.

6. Conclusions

This paper introduces an alternative approach to the field of optical encryption. Using tools from non-linear systems operated in chaotic regime and a synchronization process, it is possible to generate phase masks to be used in a 4f optical encrypting-decrypting architecture, preserving the conditions found in optically generated phase masks and achieving an increase in security by allowing the use of public open channels and a continuous change of encrypting and decrypting masks without risks. We profit from the fact that the chaotic regime dynamics origin of the masks leads to a high sensitivity to the initial conditions. In this way, slight differences in these conditions produce completely uncorrelated encrypting chaotic phase masks.

We also successfully addressed the effects of losing and corrupting information, and noise addition into the data needed to get the right decryption key. In analyzing the introduction of alterations in the transmitted information, we define a new metric, the NMSE. Clearly, with NMSE we make easier result comparisons.

Along the proposal, results show the potential, versatility and security improvement obtained with our method. We also foresee additional improvements using encrypting optical architectures working in the fractional Fourier domain, thus offering extra security parameters (fractional order). We emphasize that this new encryption-decryption alternative is a promising one, specially when actual message transmission through open channels is of concern.

Acknowledgements

The Grants from COLCIENCIAS (Colombia) and CODI-Universidad de Antioquia (Colombia) are gratefully acknowledged. R. Torroba thanks the Grants: CONICET No. 5995 (Argentina), ANCYT PICT 12564 (Argentina), and Facultad de Ingeniería, Universidad Nacional de La Plata No. 11/I105 (Argentina).

References

[1] P. Refregier, B. Javidi, Opt. Lett. 20 (1995) 767.
[2] B. Hennelly, J. Sheridan, Opt. Lett. 28 (2003) 269.
[3] B. Hennelly, J. Sheridan, Optik 114 (2003) 251.
[4] N. Towghi, B. Javidi, Z. Luo, J. Opt. Soc. Am. A 16 (1999) 1915.
[5] F. Goudail, F. Bollaro, B. Javidi, P. Réfrégier, J. Opt. Soc. Am. A 15 (1998) 2629.
[6] H. Caulfield, D. Psaltis, G. Sincerbox, Holographic Data Storage, Springer-Verlag, 2000.
[7] L. Hesselink, S. Orlov, M. Bashaw, Proc. IEEE 92 (2004) 1231.
[8] J. Barrera, R. Henao, M. Tebaldi, R. Torroba, N. Bolognini, Opt. Comm. 261 (2006) 29.
[9] J. Barrera, R. Henao, M. Tebaldi, R. Torroba, N. Bolognini, Opt. Comm. 260 (2006) 109.
[10] J. Barrera, R. Henao, M. Tebaldi, R. Torroba, N. Bolognini, Opt. Comm. 276 (2007) 231.
[11] J. Barrera, R. Henao, M. Tebaldi, R. Torroba, N. Bolognini, Optik 119 (2008) 139.
[12] A. Carnicer, M. Montes-Usategui, S. Arcos, I. Juvells, Opt. Lett. 13 (2005) 1644.
[13] X. Peng, P. Zhang, H. Wei, B. Yu, Opt. Lett. 31 (2006) 1044.
[14] Y. Frauel, A. Castro, T. Naughton, B. Javidi, Opt. Exp. 31 (2006) 1044.
[15] G. Van Wiggeren, R. Roy, Science 279 (1998) 1198.
[16] J. Ohtsubo, IEEE J. Quantum Electron. 38 (2002) 1141.
[17] N. Gastaud, S. Poinsot, L. Larger, J. Merolla, M. Hanna, J. Goedgebuer, F. Malassenet, Electron. Lett. 40 (2004) 898.
[18] J. Sprott, Chaos and Time-Series Analysis (physics), first ed., Oxford, 2003.
[19] K. Ogata, Discrete-Time Control System, second ed., Prentice Hall, 1994.
[20] E. Ott, Chaos in Dynamical Systems, second ed., Cambrigde, Berlin, 2002.
[21] B. Javidi, G. Zhang, J. Li, Opt. Eng. 35 (1996) 2506.
[22] T. Nomura, B. Javidi, Opt. Eng. 39 (2000) 2031.
[23] L. Neto, Y. Sheng, Opt. Eng. 35 (1996) 2459.
[24] T. Nomura, B. Javidi, Apl. Opt. 39 (2000) 4783.
[25] G. Unnikrishnan, J. Joseph, K. Singh, Apl. Opt. 37 (1998) 8181.
[26] B. Javidi, T. Nomura, Opt. Lett. 25 (2000) 28.
[27] A. Lohmann, J. Opt. Soc. Am. A 10 (1993) 2181.
[28] M. Singh, A. Sinha, Opt. Lasers Eng. 46 (2008) 117.
[29] C. Soutar, K. Lu, Opt. Eng. 33 (1994) 2704.
[30] L. Neto, D. Roberge, Y. Sheng, Apl. Opt. 35 (1996) 4567.
[31] J. Otón, P. Ambs, M. Millán, E. Pérez-Cabré, Apl. Opt. 46 (2007) 5667.