Encryption and validation of multiple signals for optical identification systems

To cite this article: E Pérez-Cabré et al 2007 J. Phys.: Conf. Ser. 77 012008

View the article online for updates and enhancements.

Related content
- Optical Cryptosystems: Joint transform correlator-based schemes for security and authentication
  N K Nishchal
- Optical Cryptosystems: Digital techniques of data and image encryption
  N K Nishchal
- Optical identification system of three-dimensional random phase object by use of speckle patterns in propagation distances
  O Matoba, T Sawasaki, K Nakajima et al.
Encryption and validation of multiple signals for optical identification systems

Elisabet Pérez-Cabré¹, María S. Millán¹ and Bahram Javidi²

¹Universitat Politècnica de Catalunya, Dept. Optica i Optometria, Violinista Vellsolà 37, 08222 Terrassa, Spain
²University of Connecticut, Electrical & Computer Engineering Dept., 371 Fairfield Road, CT 06269 Storrs, USA
E-mail: elisabet.perez@upc.edu

Abstract. Multifactor encryption-authentication technique reinforces optical security by allowing the simultaneous AND-verification of more than one primary image. Instead of basing the identification on a unique signature or piece of information, our goal is to authenticate a given person, object, vehicle by the simultaneous recognition of several factors. Some of them are intrinsic to the person and object or vehicle under control. Other factors, act as keys of the authentication step. Such a system is proposed for situations such as the access control to restricted areas, where the demand of security is high. The multifactor identification method involves double random-phase encoding, fully phase-based encryption and a combined nonlinear joint transform correlator and a classical 4f-correlator for simultaneous recognition and authentication of multiple images. The encoded signal fulfills the general requirements of invisible content, extreme difficulty in counterfeiting and real-time automatic verification. Four reference double-phase encoded images are compared with the retrieved input images obtained in situ from the person or the vehicle whose authentication is wanted and from a database. A recognition step based on the correlation between the signatures and the stored references determines the authentication or rejection of the person and object under surveillance.

1. Introduction
The current demand of security has motivated the development of highly complex information processes for identification and authentication. Optical techniques have a great contribution to the field and now it is possible to carry out a process in which the signals are hidden from human perception or commonly accessible conversion into visible signals (to keep them secret), they are extremely difficult to be reproduced with the same properties (to avoid counterfeiting), and finally, they are automatically, real-time, robustly, and often remotely readable by compact processors that validate authorized signatures. Optical security techniques [1] involve tasks such as encoding, encryption, recognition, verification, use of biometric images, and optical keys [2]-[5]. A method to encode a primary image into a white-noise-like distribution is proposed in [2]. 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 decryption stages. It has been applied to identify objects by optical correlation in a nonlinear joint-transform correlator (JTC) [6, 7]. 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 [2]. In nonlinear (fully-phase) encoding, a phase-only version of the primary image is encoded...
With amplitude-based encoding [2] the first mask is not needed to decode the encrypted image, whereas this mask has to be known with fully-phase encoding [8]. Both possibilities have been analyzed in the presence of perturbation of the encrypted image, and the results show their good properties regarding robustness against noise [8, 9]. In the presence of additive noise, and using the mean-squared-error metric, [8] shows that fully-phase encoding performs better than amplitude-based encoding. Note that this result is different from that obtained in optical correlation when additive noise affects the very primary image [10]. Recently, reports on cryptanalysis [11]-[14] have shown certain vulnerability of double random phase based ciphering techniques to some given attacks due to the linearity of the encryption scheme. For this reason, thorough analysis of ciphering techniques and further development of encryption methods are required to consider a system to be secure. Security can be enhanced by combining different authenticators (multifactor authentication). In such a case, a Boolean AND operation has to be performed for each factor’s authentication result so all must be affirmative before final authentication is satisfied [15]. In this work we use a novel multifactor encryption-authentication technique that reinforces optical security by allowing the simultaneous AND-verification of more than one primary image [16]. This optical technique is attractive for high-security purposes that require multifactor reliable authentication. We describe both the complex-amplitude encoded function and the optoelectronic processor that validates an identity on a basis of multiple signal recognition. The multiple signals that act as authenticators can be a number of different primary images containing alphanumerical signs, signatures or biometric information, and a number of white random sequences that constitute key codes. The method presented here is designed to obtain four-factor authentication. There is no a priori constraint about the type of primary images to encode. In the example analysed in this work a combination of one biometric signal (to validate the authorised person), one alphanumeric sign and one pattern (to validate a vehicle) and one random phase sequence (to act as key code) are considered. The vessel distribution of a retina fundus image, which is stable, accurate, and very effective information for authentication, is used as biometric signal. The key phase code is known by the database of the authentication processor and is introduced as a degree of freedom to codify, for instance, the key of the day. These four reference primary images, double-phase encoded are compared with the actual input images obtained in situ from the person and the vehicle whose authentication is. Simulation results are presented and discussed.

2. Multifactor encryption technique and optical verification

First, we describe the principles and the mathematics of the method for a four-factor authentication [16]. Let the four \( r(x), s(x), b(x) \) and \( n(x) \), be the set of reference primary images, in one-dimensional notation for simplicity, to be encoded as the secret information for multifactor verification. At least one of them, preferably \( b(x) \), is a random phase sequence that acts as key code. All the four reference primary images are normalized positive functions distributed in \([0,1]\). These images can be phase-encoded to yield \( t_r(x), t_s(x), t_b(x) \) and \( t_n(x) \) that are generically defined by \( t_f(x) = \exp(j\pi f(x)) \). The complex-amplitude encoded function \( \psi(x) \) containing the multifactor authenticators is given by the equation:

\[
\psi(x) = t_{r+2b}(x) * t_s(x) * FT^{-1}[t_n(x)]
\]

where \( t_{r+2b}(x) = t_r(x) \cdot t_{2b}(x) = \exp(j\pi r(x)) \cdot \exp(j2\pi b(x)) \). \( FT^{-1} \) indicates inverse Fourier transform, and \(* \) the convolution operation. The encoded function can be either optically generated by using an optical hardware equivalent to a JTC or computed and electronically implemented using conventional techniques for computer generated holograms. Let \( p(x), q(x), d(x) \) and \( m(x) \), denote the positive and normalized input images to compare with the set of reference images, \( r(x), s(x), b(x) \) and \( n(x) \), respectively. A possible realization of the optical
processor combines a nonlinear joint transform correlator (JTC) and a classical 4f-correlator [17] (Fig. 1).

![Joint Fourier Transform and 4f-Classical Correlator Diagram]

**Figure 1.** Optical processor for multifactor authentication.

In the first step, the encrypted distribution \( \psi(x-a) \) and one phase encoded input image, for instance \( t_p(x+a) = \exp\{j\pi p(x+a)\} \), are displayed side-by-side a distance \( 2a \) apart on the input plane of the nonlinear JTC illuminated by coherent light. The phase distribution \( t_{2d}(x+a) = \exp\{j2\pi d(x+a)\} \) is placed against the screen where the input \( t_p(x+a) \) is displayed. Consequently, the amplitude distribution in the input plane is \( \psi(x-a) + t_p + 2d(x+a) \). A CCD sensor placed in the Fourier plane of the JTC captures the intensity distribution \( I(u) \) of the joint power spectrum,

\[
I(u) = |FT[\psi(x-a) + t_{p+2d}(x+a)]|^2 \tag{2}
\]

The development of Eq. (2) gives the classical four terms of which two are interesting because they convey the cross-correlation signals that lead to spatially separated distributions in the output plane. These two terms are:

Term 1:

\[
FT^*[\psi(x)]FT[t_{p+2d}(x)]e^{j2au} = T_{r+2h}(u)T_s^*(u)t_n^*(u)T_{p+2d}(u)e^{j2au} \tag{3}
\]

Term 2:

\[
FT[\psi(x)]FT^*[t_{p+2d}(x)]e^{-j2au} = T_{r+2h}(u)T_s(u)t_n(u)T_{p+2d}^*(u)e^{-j2au} \tag{4}
\]

where a function in capital letter indicates the Fourier transform of the function in small letter and \( u \) is the spatial frequency coordinate. Terms 1 and 2 of Eqs. (3) can be modified according to a variety of nonlinear techniques [18]-[20] that are useful to adjust the discrimination capability of a recognition system and to improve noise resistance, among other properties. In this work we consider nonlinear transformations of the joint power spectrum of the general form

\[
NL^k\{I(u)\} = I(u) \cdot |I(u)|^{k-1} \tag{5}
\]

where \( k \in [0, 1] \) defines the strength of the applied nonlinearity and it can vary from the linear case \((k = 1)\) to the phase extraction technique \((k = 0)\) [20] also called pure phase correlation (PPC) [18]. The resultant modified joint power spectrum (Eq. 5) is displayed on the Fourier
plane of a 4f-classical correlator (Fig. 1). There, a transparency with the phase distribution \( t_\text{m}(u) \) is placed against the screen. The input image \( q(x) \) is phase encoded and displayed on the input plane of the 4f-correlator. Behind the Fourier plane, Terms 1 and 2 of Eqs. (3) and (4) are respectively converted into:

\[
\text{Term 1} : \quad \left[ T_q(u) T_s^\ast(u) |T_s(u)|^{k-1} \right] \left[ T_{r+2b}(u) T_{p+2d}(u) |T_{r+2b}(u) T_{p+2d}(u)|^{k-1} \right] [t_s(u)] t_m(u) e^{j2\alpha u} \tag{6}
\]

\[
\text{Term 2} : \quad \left[ T_q(u) T_s(u) |T_s(u)|^{k-1} \right] \left[ T_{r+2b}(u) T_s^\ast(u) T_{r+2b}(u) T_{p+2d}(u)|T_{r+2b}(u) T_{p+2d}(u)|^{k-1} \right] [t_{n+m}(u)] e^{-j2\alpha u} \tag{7}
\]

If the information contained in the encrypted distribution corresponds to a positive validation, then the multiple AND condition \( r(x) = p(x) \text{ AND } s(x) = q(x) \text{ AND } b(x) = d(x) \text{ AND } n(x) = m(x) \) is fulfilled. In such a case, if the phase extraction is applied \( k = 0 \) and provided the system is free of noise and distortions, Term 1 of Eq. (6) simplifies into \( |T_s(u)| exp\{j2\alpha u\} \), which represents a wavefront with all its curvature cancelled [17] that focuses on a sharp multifactor autocorrelation peak centered in \( x = -2\alpha \) of the output plane (Fig. 1). From Eq. (6), the output intensity distribution corresponding to Term 1 is the cross-correlation of autocorrelation signals given by

\[
|AC_{POF} [t_s(x)] \otimes AC_{PC}^* [t_{r+2b}(u)] \otimes AC_{CMF}^* [T_n(x)] * \delta(x + 2\alpha)|^2 \tag{8}
\]

where \( \otimes \) denotes cross-correlation, and subindices CMF, POF, PPC indicate the sort of filter involved in the autocorrelation signal (CMF stands for classical matched filter, POF for phase-only filter, and PPC for pure phase correlation). Since autocorrelation peaks are usually sharp and narrow, particularly those for POF and PPC, we expect that the cross-correlation of such autocorrelation signals will be even sharper and narrower. Consequently, the information contained in Term 1, allows reinforced security verification by simultaneous multifactor authentication. On the other hand, when the multiple AND condition \( r(x) = p(x) \text{ AND } s(x) = q(x) \text{ AND } b(x) = d(x) \text{ AND } n(x) = m(x) \) is fulfilled, and the phase extraction \( k = 0 \) is considered, Term 2 of Eq. (7) becomes \( |T_s^2(u) |T_s(u)| t_{2b}(u) exp\{-j2\alpha u\} \), which does not yield any interesting result for recognition purposes. If \( r(x) \neq p(x) \text{ or } s(x) \neq q(x) \text{ or } b(x) \neq d(x) \text{ or } n(x) \neq m(x) \), Term 1 contains a cross correlation signal that is, in general, broader and less intense than the multifactor autocorrelation peak of Eq. (8). Furthermore, the key code known by the processor, \( t_{2b}(x) \), plays an important role in optical security as an additional authenticator with the properties described in [1]-[2], [8]-[9]. In case of having a linear system \( k = 1 \) in Eq. (5), only a linear replica of the joint power spectrum of Eq. (2) and, consequently, of Terms 1 and 2 of Eq. (3) and (4) would be introduced in the Fourier plane of the 4f-correlator. Again, if the information contained in the encrypted distribution correspond to a positive validation (i.e. \( r(x) = p(x) \text{ AND } s(x) = q(x) \text{ AND } b(x) = d(x) \text{ AND } n(x) = m(x) \) is true), the output intensity distribution of Term 1, the cross-correlation of autocorrelation signals given by

\[
|AC_{CMF} [t_s(x)] \otimes AC_{CMF}^* [t_{r+2b}(u)] \otimes AC_{CMF}^* [T_n(x)] * \delta(x + 2\alpha)|^2 \tag{9}
\]

that centered in \( x = -2\alpha \) of the output plane. All the autocorrelation signals contained in Eq. (9) are of the same type (CMF). Very often, this result of Eq. (9) is rather unsatisfactory because the peak does not show good properties of sharpness for detection [21]. Intermediate cases between the phase extraction and the linear system can be achieved by adjusting parameter \( k \) between the two extreme values \([0,1]\). In such cases, the output intensity distribution corresponding to Term 1 (Eq. 6) leads to the cross-correlation of multiple autocorrelation signals resulting from the intermediate nonlinearities. Features, such as peak intensity and sharpness, discrimination capability and robustness of the system can be modified by changing parameter \( k \) according to the identification requirements [19], [22]-[25].
3. Numerical experiments and results

The method is illustrated here with numerical simulations. We consider the set of reference primary images of Fig. 2a (64 × 64 pixels each): \( s(x) \) is a biometric image, more specifically, it shows the vessel distribution of the retina fundus (with reverse contrast) that can be obtained in situ from a person with a retinal camera, \( r(x) \) is the tyre pattern of a wheel vehicle, \( b(x) \) is a random key code, and \( n(x) \) is the vehicle plate code. The encoded function \( \psi(x) \) that contains the information of all these four reference images is computed using Eq. (1). The resulting complex-valued function is shown in Fig. 3. Its dim appearance does not reveal the content of any primary image. In the experiment, the set of input images can be equal to the reference set, partly different or totally different. Fig. 2b contains some input images, different from those reference primary images, that are to be considered in the simulated experiments.

| Reference primary images       | Other images to compare |
|-------------------------------|-------------------------|
| \( s(x) \) Biometric          | \( q(x) \neq s(x) \)    |
| \( r(x) \) Tyre pattern       | \( p(x) \neq r(x) \)    |
| \( b(x) \) Random key code    | \( d(x) \neq b(x) \)    |
| \( n(x) \) Vehicle plate code | \( m(x) \neq n(x) \)    |

(a) Reference primary images to encrypt. (b) The images to consider in the simulated experiments.

In the first part of the experiment, we compute the output intensity distribution corresponding to the Term 1 of the multifactor correlation with phase extraction \((k = 0)\). If the set of input images coincide with the set of reference primary images, then the result is given by Eq. (8). We compute and represent the normalised result in Fig. 4 (validation). It shows a sharp peak shaped distribution of intensity that allows a complete validation of the set of input images. In the following columns of Fig. 4 we represent the results obtained when the input set of images differs from the reference set in just one image (specified on the top). The last graph on Fig. 4 (none coincides) shows the result obtained when all the images of the input set are different from the respective reference images. All the results shown in Fig. 4 are very satisfactory: when the set of input images coincide with the reference set, a positive validation is obtained from the multicorrelation peak. However, when both sets are different, even for just
one image, the output multicorrelation signal decreases drastically and is not peak shaped in general.

Figure 3. Magnitude and phase of the encrypted multifactor distribution $\psi(x)$.

Figure 4. Output intensity distributions corresponding to the Term 1 of the multifactor correlation with phase extraction ($k = 0$). The images considered are shown in Fig. 2.

4. Conclusions
A method to encode multifactor authenticators in a single complex-amplitude encoded function is analysed. The encoded function fulfils the requirements of: invisible content, which is an extreme difficulty in counterfeiting, and real-time automatic verification. This optical technique is attractive for high-security purposes that require multifactor authentication. It is advantageous to introduce nonlinearities in the optical signal processing by extracting the phase of the joint
power spectrum. This modification leads to obtain sharp peaks of intensity in the output plane of the system that permit the multifactor authentication. We have presented simulated results that shows that only the AND verification of the complete set of four signals led to the positive validation. Otherwise, if any mismatch appeared, the result was negative.

Acknowledgements
The authors thank the Spanish Ministerio de Educacin y Ciencia and FEDER for financial support (project DPI2006-05479).

References
[1] Javidi B 2005 Optical and Digital Techniques for Information Security (New York: Springer)
[2] Réfrégier P and Javidi B 1995 Opt. Lett. 20 767
[3] Mahalanobis A 1996 Optoelectronic Devices and Systems for Processing (Bellingham: SPIE) 65 240
[4] Sadjadi F 2000 Automatic Target Recognition (Bellingham: SPIE) 6
[5] Ganesan B, Techkedath D, Young R, Chatwin C 2006 Opt. and Lasers in Eng. 44 1
[6] Javidi B, Zhang G, Li J 1996 Opt. Eng. 35 2506
[7] Pérez-CabrÉ E, Javidi B 2005 IEEE Trans. on Vehicular Technology 54 1295
[8] Towghi N, Javidi B, Luo Z 1999 J. Opt. Soc. Am. A 16 1915
[9] Goudail F, Bollaro F, Javidi B, Réfrégier P 1998 J. Opt. Soc. Am. A 15 2629
[10] Maze S and Réfrégier P 1992 Opt. Lett. 17 426
[11] Carnicer A, Montes-Usategui M, Arcos S, Juvels I 2005 Opt. Lett. 30 1644
[12] Peng X, Zhung P, Wei H, Yu B 2006 Opt. Lett. 31 1044
[13] Gopinathan U, Monaghan D S, Naughton T J, Sheridan J T (2006) Opt. Exp. 14 3181
[14] Peng X, Wei H, Zhang P 2006 Opt. Lett. 31 3261
[15] O’Gorman L 2003 Proceedings of IEEE 91 2021
[16] MillÁn M S, Pérez-CabrÉ E, Javidi B 2006 Opt. Lett. 31 712
[17] Goodman J W 1996 Introduction to Fourier Optics 2nd ed. (New York: McGraw-Hill)
[18] Pérez E, Chalasinska-Macukow K, Styczynski K, Kotynski R, MillÁn M S 1997 J. Mod. Opt. 44 1535
[19] Javidi B 1994 Nonlinear joint transform correlators in Real-time optical information processing, (San Diego: Academic Press) 115
[20] Kotzer T, Rosen J, Shamir J 1992 Appl. Opt. 31 1126
[21] MillÁn M S, Pérez-CabrÉ E, Javidi B 2006 Proc. 5th International Workshop on Information Optics (WIO’06) (New York: AIP) 63
[22] MillÁn M S, Pérez E, Chalasinska-Macukow K 1999 Opt. Commun. 161 115
[23] Pérez E, MillÁn M S, Chalasinska-Macukow K 2002 Opt. Commun. 202 239
[24] Chalasinska-Macukow K, Kotynski R, Pérez-CabrÉ E, MillÁn M S 2005 Opt. Pura Apl. 28 75
[25] MillÁn M S, Pérez-CabrÉ E, Chalasinska-Macukow K, Kotynski R 2005 Opt. Pura Apl. 28 85