Secure verification by multifactor optical validation

María S. Millán*a, Elisabet Pérez-Cabréa, Bahram Javidib

*aDept. Optica i Optometria, Universitat Politècnica de Catalunya, Violinista Vellsolà 37 08222 Terrassa, Spain;
bElectrical & Computer Engineering Dept., University of Connecticut, 371 Fairfield Road, Unit 2157, Storrs, CT 06269-2157, USA.

ABSTRACT

We propose a novel multifactor encryption-authentication technique that reinforces optical security by allowing the simultaneous AND-verification of more than one primary image. We describe a method to obtain four-factor authentication. The authenticators are: two different primary images containing signatures or biometric information and two different white random sequences that act as key codes. So far, optical security techniques deal with a single primary image (an object, a signature, or a biometric signal), not combined primary images. Our method involves double random-phase encoding, fully phase-based encryption and a combined nonlinear JTC and a classical 4f-correlator for simultaneous recognition and authentication of multiple images. There is no a priori constraint about the type of primary images to encode. Two reference images, double-phase encoded and encrypted in an ID tag (or card) are compared with the actual input images obtained in situ from the person whose authentication is wanted. The two key phase codes are known by the authentication processor. The complex-amplitude encoded image of the ID tag has a dim appearance that does not reveal the content of any primary reference image nor the key codes. The encoded image function fullfills the general requirements of invisible content, extreme difficulty in counterfeiting and real-time automatic verification. The possibility of introducing nonlinearities in the Fourier plane of the optical processor will be exploited to improve the system performance. This optical technique is attractive for high-security purposes that require multifactor reliable authentication.

Keywords: Information security, optical encryption, optical recognition, Fourier optics, optical signal processing, nonlinear correlation

1. INTRODUCTION

Optical security technology [1] is based on complex information processes 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 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 Ref. [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 [8]. 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 noise robustness [8,9]. In the presence of additive noise, and using the mean-squared-error metric, Ref. [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].

* millan@oo.upc.edu; phone 34 93 7398339; fax 34 93 7398301; www.goapi.upc.edu
Regarding the signals, biometric images such as fingerprints, face, hand, iris, and retina are more and more considered in authentication mechanisms because biometrics is based on something intrinsic to a person (something the person is) in contrast to other schemes based on either something a person knows (e.g., a password) or has (e.g., a metal key an ID card) [11]. 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 [11].

In this work we propose a novel multifactor encryption-authentication technique that reinforces optical security by allowing the simultaneous AND-verification of more than one primary image [12]. This optical technique is attractive for high-security purposes that require multifactor reliable authentication. We describe both the encoded information contained in the ID tag 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 logotypes, bar codes, alphanumerical signs, signatures or biometric information, and a number of white random sequences that constitute key codes. So far, optical security techniques deal with a single primary image (an object, a signature, or a biometric signal), not combined primary images. The proposed method involves double random-phase encoding, full phase-based encryption and a combined nonlinear JTC and a classical 4f-correlator [13] for simultaneous AND authentications of multiple images. The possibility of introducing nonlinearities in the Fourier plane of the optical processor will be exploited to improve the system performance.

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 this work, we consider a combination of two biometric signals and two random phase sequences acting as key codes. Two reference images, double-phase encoded and encrypted in an ID tag (or card), are compared with the actual input images obtained in situ from the person whose authentication is wanted. Retina images, which are stable, accurate, and very effective for authentication, are used as biometric signals. The two key phase codes are known by the databases of the authentication processor.

2. MULTIFACTOR OPTICAL VERIFICATION

First, we describe the principles and the mathematics of the method for a four-factor authentication. Let \( r(x) \) and \( s(x) \) be the reference primary images (for instance, biometric images), in one-dimensional notation for simplicity, and let \( b(x) \) and \( n(x) \) be two independent random white sequences used to mask and encrypt the information in the ID tag. All the four, \( r(x) \), \( s(x) \), \( b(x) \) and \( n(x) \) are normalized positive functions distributed in \([0,1]\). These images can be phase-encoded to yield \( t_r(x) \), \( t_s(x) \), \( t_b(x) \), \( t_n(x) \) that are generically defined by \( t_s(x) = \exp\{j\pi f(x)\} \). The complex-amplitude encoded function \( \psi(x) \) containing the multifactor authenticators is given by the equation:

\[
\psi(x) = t_{r+b}(x) * t_s(x) * F^{-1}[t_{n+x}]
\]  

where \( t_{r+b}(x) = t_r(x) t_b(x) = \exp\{j\pi r(x)\} \exp\{j2\pi b(x)\} \), \( F^{-1} \) 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 \( p(x) \) and \( q(x) \) denote the positive and normalized input images to compare with the reference images \( r(x) \) and \( s(x) \), respectively. A possible realization of the optical processor combines a nonlinear JTC and a classical 4f-correlator [12] (Fig. 1).

In the first step, the ID-tag \( \psi(x-a) \) 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.
In a first approach, let us assume that $t_{2b}(x)$ and $t_{2a}(x)$ are key phase codes known by the processor. The phase mask $t_{2b}(x + a) = \exp\{j2\pi b(x + a)\}$ is placed against the screen where the input $t_{p}(x + a)$ is displayed. Consequently, the amplitude distribution in the input plane is $\psi(x - a) + t_{p,2b}(x + a)$.

A CCD sensor placed in the Fourier plane of the JTC captures the intensity distribution $I(u)$ of the joint power spectrum,

$$I(u) = \mathcal{F}\left[\psi(x - a) + t_{p,2b}(x + a)\right]^2.$$  \hspace{1cm} (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:**

$$\mathcal{F}\left[\psi(x)\right] \mathcal{F}\left[t_{p,2a}(x)\right] \exp\{j2au\} = T_{r,2a}(u) T_{r^*,2a}(u) T_{p,2b}(u) \exp\{j2au\},$$  \hspace{1cm} (3)

**Term 2:**

$$\mathcal{F}\left[\psi(x)\right] \mathcal{F}\left[t_{p,2b}(x)\right] \exp\{-j2au\} = T_{r,2b}(u) T_{r^*,2b}(u) T_{p,2b}(u) \exp\{-j2au\},$$

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 [14-16] 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

$$NL_k \left[I(u)\right] = I(u) \left[I(u)\right]^{k-1},$$  \hspace{1cm} (4)

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 ($k = 0$) [16] also called pure phase correlation (PPC) [14]. The resultant nonlinearity modified joint power spectrum (Eq. 4) is displayed on the Fourier plane of a 4f-classical correlator (Fig. 1). There, a transparency
with the random phase mask $t_{2n} (u)$ is placed against the screen. The second 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) are converted into:

$$
\text{Term 1:} \begin{bmatrix} T_q (u)T_s (u) \end{bmatrix}^{k-1} \begin{bmatrix} T_{r+2b} (u) \end{bmatrix}^{k-1} \begin{bmatrix} T_{r+2b} (u)T_{r+2b} (v) \end{bmatrix}^{k-1} \begin{bmatrix} T_{r+2b} (u)T_{r+2b} (w) \end{bmatrix}^{k-1} \begin{bmatrix} t_{2n} (u) \end{bmatrix} \exp \{ 2jau \},
$$

$$
\text{Term 2:} \begin{bmatrix} T_q (u)T_s (u) \end{bmatrix}^{k-1} \begin{bmatrix} T_{r+2b} (u) \end{bmatrix}^{k-1} \begin{bmatrix} T_{r+2b} (u)T_{r+2b} (v) \end{bmatrix}^{k-1} \begin{bmatrix} T_{r+2b} (u)T_{r+2b} (w) \end{bmatrix}^{k-1} \begin{bmatrix} t_{2n} (u) \end{bmatrix} \exp \{ -2jau \}. \tag{5}
$$

If the information contained in the ID tag corresponds to a positive validation, then the AND condition $r(x) = p(x)$ AND $s(x) = q(x)$ 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. (5) simplifies into $T_q (u) \exp \{ j2au \}$, which represents a wavefront with all its curvature cancelled [13] that focuses on a sharp multifactor autocorrelation peak centered in $x = -2a$ of the output plane (Fig. 1). From Eq. (5), the output intensity distribution corresponding to Term 1 is the cross-correlation of autocorrelation signals given by

$$
\left| AC_{POF} [t_1 (x)] \right| \left| AC_{CMF}^* [t_{r+2b} (x)] \right| \left| AC_{CMF}^* [t_{2n} (x)] \right| \delta (x + 2a) \right|^2, \tag{6}
$$

where $\star$ 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 condition $r(x) = p(x)$ AND $s(x) = q(x)$ is fulfilled, and the phase extraction $k = 0$ is considered, Term 2 of Eq. (5) becomes $T_q (u) \exp \{ -j2au \}$, which does not yield an interesting result for recognition purposes. If $p(x) \neq r(x)$ or $q(x) \neq s(x)$, Term 1 contains a cross correlation signal that is, in general, broader and less intense than the multifactor autocorrelation peak of Eq. (6). Furthermore, the key codes known by the processor, $t_{2b} (x)$ and $t_{2n} (x)$, play an important role in optical security as additional authenticators with the properties described in Refs. [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) would be introduced in the Fourier plane of the 4f-correlator. Again, if the information contained in the ID tag corresponds to a positive validation [i.e., $r(x) = p(x)$ AND $s(x) = q(x)$ is true], the output intensity distribution of Term 1 is the cross-correlation of autocorrelation signals given by

$$
\left| AC_{CMF} [t_1 (x)] \right| \left| AC_{CMF}^* [t_{r+2b} (x)] \right| \left| AC_{CMF}^* [t_{2n} (x)] \right| \delta (x + 2a) \right|^2, \tag{7}
$$

that is centered in $x = -2a$ of the output plane. In comparison with the result of Eq. (6), all the autocorrelation signals contained in Eq. (7) are of the same type (CMF).

Intermediate cases between the aforementioned 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. 5) will lead to the cross-correlation of multiple autocorrelation signals resulting from the intermediate nonlinearities. Features, such as peak intensity and sharpness, discrimination capability and noise robustness of the validation system can be modified by changing parameter $k$ according to the identification requirements [15, 17-20].
3. NUMERICAL EXPERIMENTS AND RESULTS

The method is illustrated here with numerical simulations. We consider the biometric retina images of Fig. 2(a,b) (188 x 188 pixels) as primary reference images: (a) $s(x)$ and (b) $r(x)$, though the signals used in the process are those of Figure 2(a,b) but with reverse contrast, for which veins appear more intense than the background.

Fig. 2. Retina images: (a) right eye, (b) left eye (they are used with reverse contrast in the primary reference images $s(x)$, $r(x)$); (c) key code $b(x)$, (d) key code $n(x)$; (e) magnitude and (f) phase of the encoded image $\varphi(x)$ of the ID tag.
The phase masks $b(x)$ and $n(x)$ are two different random white sequences [Figure 2(c,d)]. Figures 2(e,f) show the magnitude and phase of the complex-amplitude encoded image $\psi(x)$ of Eq. (1), respectively. Their dim appearance does not reveal the content of any primary reference image. In the following subsections, we analyze the effects of applying different nonlinearities in the Fourier plane by varying parameter $k$ on the validation system response.

### 3.1 Linear processor

When the input images coincide with reference images $r(x) = p(x)$ and $s(x) = q(x)$ and the key codes $b(x)$ and $n(x)$ are properly used, that is, when all four factor’s authentication results are satisfied, the output intensity distributions for Terms 1 and 2 of the linear processor with $k = 1$ (Eq. 5) are plotted in Figure 3.

![Intensity output distribution for (a) Term 1 and (b) Term 2 of Eq. (5) corresponding to the response of a linear processor ($k = 1$) when all four factors are validated.](image)

Figure 3(a) shows a small peak on an intense background that accounts for the cross correlation of the three CMF autocorrelation signals of Eq. (7). The characteristics of both the CMF filtering technique and the sort of images chosen as factors for validation can explain the broad output. This result is unsatisfactory because the peak does not show good enough properties of sharpness to be detected. Figure 3(b) shows the intensity distribution corresponding to Term 2 of Eq. (5) with $k = 1$. In this case, the intensity level is very high, but insignificant.

Table 1 provides a signal comparison of multifactor validation for different cases: when every signal is correct and when any mismatch occurs among the four signals verified by the processor. The maximum value of the output intensity of Term 1 given by the linear processor (Eq. 7) is analyzed in a variety of wrong situations: both signals $p(x)$ and $q(x)$ differ from $r(x)$ and $s(x)$, respectively; either the key phase code $b(x)$ or $n(x)$ is false, and both key codes are false simultaneously. The first case $[r(x) \neq p(x) \text{ and } s(x) \neq q(x)]$ corresponds to the situation for which a non-authorized person is compared with the authorized person whose information is contained in the ID tag of Figure 2. Note that both retina images change from one person to another. In our comparison, the retina images of the non-authorized person are shown in Figure 4. As it can be seen in Table 1, there are some cases that reach very high values in their maximum correlation intensities, thus producing false alarms. These situations show that the authentication results provided by a linear processor are not reliable. For this reason, nonlinearities are to be taken into account in the following experiments.
Table 1. Signal comparison for multifactor validation. Maximum value of the output intensity of Term 1 in the linear processor ($k = 1$ in Eq. 5). The ID tag contains the information shown in Figure 2. The input images $p(x)$ and $q(x)$, which are $q(x) \neq s(x)$ and $p(x) \neq r(x)$, are represented in Figure 4.

<table>
<thead>
<tr>
<th>$q$</th>
<th>$p$</th>
<th>Key $b$</th>
<th>Key $n$</th>
<th>Norm. peak</th>
<th>Authorized</th>
</tr>
</thead>
<tbody>
<tr>
<td>$s$</td>
<td>$r$</td>
<td>Right</td>
<td>Right</td>
<td>1.0</td>
<td>YES</td>
</tr>
<tr>
<td>$q \neq s$</td>
<td>$p \neq r$</td>
<td>Right</td>
<td>Right</td>
<td>0.76</td>
<td>YES (False alarm)</td>
</tr>
<tr>
<td>$s$</td>
<td>$r$</td>
<td>False</td>
<td>Right</td>
<td>0.05</td>
<td>NO</td>
</tr>
<tr>
<td>$s$</td>
<td>$r$</td>
<td>Right</td>
<td>False</td>
<td>0.92</td>
<td>YES (False alarm)</td>
</tr>
<tr>
<td>$s$</td>
<td>$r$</td>
<td>False</td>
<td>False</td>
<td>0.05</td>
<td>NO</td>
</tr>
</tbody>
</table>

Fig. 4. Input images: (a) $q(x)$ and (b) $p(x)$ to compare with the primary reference images of Figure 2(a,b). Note that both retina images change from one person to another ($q(x) \neq s(x)$ and $p(x) \neq r(x)$).

### 3.2 Nonlinear processor

Let us now consider parameter $k = 0$ in Terms 1 and 2 of Eq. (5) corresponding to a nonlinear processor based on a phase extraction of the joint power spectrum. When all four factor’s authentication results are satisfied, that is, $[r(x) = p(x) \text{ and } s(x) = q(x)]$ and the key codes $b(x)$ and $n(x)$ are properly used, the output intensity distributions for Terms 1 and 2 are plotted in Figure 5. Now, Term 1 shows a high and sharp multifactor autocorrelation peak that accounts for the final authentication, whereas Term 2 shows a low non-interesting signal.

Any mismatching between the four signals $r(x), s(x), b(x), n(x)$ involved in the encoded image $\psi(x)$ and the second set of four signals consisting of $p(x), q(x)$ and the two key codes known by the processor, leads to a decrease of the output correlation peak of Term 1 (Table 2). Figure 6(a) shows the output distribution corresponding to Term 1 when another person is analyzed by the processor ($q(x) \neq s(x)$ and $p(x) \neq r(x)$, see Fig. 4). Figure 6(b) corresponds to the case when the person is right but false key phase codes are used.
Fig. 5. Intensity output distributions corresponding to (a) Term 1 and (b) Term 2 of the nonlinear processor based on phase extraction ($k = 0$). Term 1 shows a sharp peak of intensity produced by the cross-correlation of the three auto-correlation signals (Eq. 6).

Table 2. Signal comparison for multifactor validation. Maximum value of the output intensity of Term 1 in the nonlinear processor (Eq. 5). The ID tag contains the information shown in Figure 2. The input images $p(x)$ and $q(x)$, which are $q(x) \neq s(x)$ and $p(x) \neq r(x)$, are represented in Figure 4.

<table>
<thead>
<tr>
<th>$q$</th>
<th>$p$</th>
<th>Key $b$</th>
<th>Key $n$</th>
<th>Norm. peak</th>
<th>Authorized</th>
</tr>
</thead>
<tbody>
<tr>
<td>$s$</td>
<td>$r$</td>
<td>Right</td>
<td>Right</td>
<td>1.0</td>
<td>YES</td>
</tr>
<tr>
<td>$q \neq s$</td>
<td>$p \neq r$</td>
<td>Right</td>
<td>Right</td>
<td>0.01</td>
<td>NO</td>
</tr>
<tr>
<td>$s$</td>
<td>$r$</td>
<td>False</td>
<td>Right</td>
<td>0.006</td>
<td>NO</td>
</tr>
<tr>
<td>$s$</td>
<td>$r$</td>
<td>Right</td>
<td>False</td>
<td>0.005</td>
<td>NO</td>
</tr>
<tr>
<td>$s$</td>
<td>$r$</td>
<td>False</td>
<td>False</td>
<td>0.005</td>
<td>NO</td>
</tr>
</tbody>
</table>

Fig. 6. Intensity output distributions corresponding to Term 1 of a nonlinear processor based on phase extraction ($k = 0$). (a) Another person, with $q(x) \neq s(x)$ and $p(x) \neq r(x)$, is analyzed; (b) the person is right but false key phase codes are used.
3.3 Intermediate nonlinearities

We now explore the possibilities of adjusting the applied nonlinearity in order to change the validation results according to the requirements of a given identification task. It is well-known that nonlinearities can be introduced in order to control the processor performance in terms of intensity peak profile, discrimination capability, signal-to-noise ratio or noise robustness [13-20].

Figure 7 shows the intensity output distributions corresponding to Term 1 for intermediate applied nonlinearities, when a four multifactor is satisfied \((q(x) = s(x)\) and \(p(x) = r(x)\) and the right phase key codes \(b(x)\) and \(n(x)\) are used).

On the one hand, small values of parameter \(k\), close to zero or equivalently to the phase extraction-based processor, provide sharper and higher output intensity peaks on low background (Fig. 7c) which allow an easier detection during the validation process. On the other hand, values of parameter \(k\) close to unity, or equivalently to the linear processor, give slightly wider peaks on a more energetic background (Fig. 7a) that permit a greater tolerance in case of the presence of noise, but usually imply a decrease in the discrimination capability of the validation system. Differences between the output planes for intermediate nonlinearities can be clearly appreciated in Fig. 7.

![Fig. 7. Intensity output distributions corresponding to Term 1 for a four correct multifactor validation \((q(x) = s(x), p(x) = r(x), b(x)\) and \(n(x)\) are used) when intermediate nonlinearities are applied in the Fourier plane: (a) \(k = 0.75\); (b) \(k = 0.5\) and (c) \(k = 0.25\).](image-url)
The discrimination capability of the validation system is analyzed by comparing the results obtained for non-authorized (i.e., \( q(x) \neq s(x) \) and \( p(x) \neq r(x) \)) to authorized (i.e., \( q(x) = s(x) \) and \( p(x) = r(x) \)) people. The correct phase key codes are properly used in the multifactor validation process. Figure 8 plots the maximum normalized intensity peak of Term 1 in the output plane for a non-authorized person versus the applied nonlinearity defined by parameter \( k \). Numerical results are normalized by taking into account the maximum peak value for an authorized person. From Fig. 8, we notice that values of parameter \( k \) below 0.5 provide small normalized maximum intensity values so that a good discrimination capability for the multifactor validation system is achieved. However, values of parameter \( k \) larger than 0.6, lead to higher normalized maximum intensity peak values that permit a greater system tolerance to variations in the input signals. This characteristic may allow the validation of an authorized person by using retina scans under slightly different conditions (lighting, aging, etc.) that may contribute to the system robustness and it will be studied further in the future.

![Fig. 8. Maximum normalized intensity peak value for the output of Term 1 versus the applied nonlinearity defined by parameter \( k \) (Eq. 5). Another person, with \( q(x) \neq s(x) \) and \( p(x) \neq r(x) \) is analyzed. Both key codes are correct.](image)

**4. CONCLUSIONS**

We have proposed a method to encode multifactor authenticators in a single complex-amplitude image function that can be used for an ID tag. A number of other multiplexing techniques are possible including Fresnel domain encoding to increase the degrees of freedom of the system [21]. The encoded image fulfills 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. The optical processor that performs linearly leads to an output correlation peak that could be insufficient in most of practical cases. It is advantageous to introduce a nonlinearity 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. Intermediate performances can be achieved by adjusting parameter \( k \) that defines the applied nonlinearity. We have presented the results obtained by using a combination of biometric images (retina scanning) and key codes consisting of random white sequences. In the studied cases for the nonlinear processor, 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 and the person was rejected. Adjustment of the discrimination capability and intensity peak profile of the validation system can be carried out by choosing intermediate \( k \) values from the linear case to the phase extraction-based processor.
ACKNOWLEDGEMENTS

Authors thank the Spanish Ministerio de Educación y Ciencia and FEDER for financial support (project DPI2003-03931).

REFERENCES