Remote optical ID tag recognition and verification using fully spatial phase multiplexing

Elisabet Pérez-Cabré [a*], María S. Millán[a], Bahram Javidi[b]
[a]Department of Optics and Optometry, Technical University of Catalonia, Barcelona, SPAIN
[b]Electrical & Computer Engineering Department, University of Connecticut, Storrs, CT, USA

ABSTRACT

In this paper, we present a novel technique for automated remote optical ID tag recognition and verification. The design of distortion-invariant ID tags aims to achieve a correct object authentication even if the ID tag is detected and captured at different distances (i.e. scale variance) or from different views (i.e. rotation variance). Information included in the ID tag is encrypted in order to increase security. We use a fully phase encoded primary pattern and keys by spatial phase multiplexing. This encryption technique is compared with the amplitude-based encoding used in previous works. Experimental results and analysis are presented.

Keywords: Optical ID tags, distortion-invariant recognition, phase encryption.

1. INTRODUCTION

Distortion-invariant recognition and authentication of objects by using optical identification (ID) tags has been described in Ref. [1]. Identification tags can be used for real-time remote identification and authentication of objects which have diverse applications in transportation and homeland security. The ID tags consist of an optical code containing encrypted information to increase security. A novel distortion-invariant ID tag,[2-5] was designed so that the verification system was able to detect and identify the information included in the tag even when the optical code was captured rotated or from an unexpected location. Both the magnitude and the phase of the encrypted signature were codified in grayscale to improve robustness against phase distortions produced by outdoors environmental conditions (rain, air turbulences, etc.).[5] Verification of the information embedded in the ID tag was carried out by correlation.[6] To increase security, the information included in the ID tag was encrypted by following the double-phase encryption procedure,[7] which is an amplitude-based encoding. In this work, we want to increase the system robustness by modifying the encoding technique to the fully phase encryption method,[8] which performs better in terms of noise robustness.[8] than the amplitude-based encryption method.[9-10]

2. ENCRYPTION TECHNIQUES

In order to increase security, the designed ID tag consists of an encrypted signature. An identification number, an object image or other kinds of information may be used as a signature to identify a given object. Commonly, images to be encrypted are intensity representations. Let $f(x,y)$ be the signature to be encrypted that is normalized ($0 \leq f(x,y) \leq 1$) and sampled to have a total amount of pixels *N*. The coordinates in the spatial and in the frequency domain are (x,y) and (μ,ν), respectively. Two encoding techniques, the double phase or amplitude-based encryption[7] and the fully phase encryption[8] are considered and compared. Both methods convert a primary image $f(x,y)$ into stationary white noise, so that the encrypted function does not reveal the appearance of the signature at human sight. We briefly describe the two possibilities for encrypting the signature information.

[*] eperez@oo.upc.edu; phone: 34 93 739 83 39; fax: 34 93 739 83 01

Unmanned/Unattended Sensors and Sensor Networks II,
edited by Edward M. Carapezza, Proc. of SPIE Vol. 5986
598602, (2005) · 0277-786X/05/$15 · doi: 10.1117/12.630427

2.1. Double-phase or amplitude-based encryption[7]

Double-phase encoding technique uses two random phase codes to convert the input information into stationary noise. One phase code is used in the input plane, and the second phase code is used in the frequency domain (Fourier plane). Let $p(x,y)$ and $b(\mu,\nu)$ be two independent white sequences, uniformly distributed in the interval [0,1]. Two operations are performed to obtain the encrypted information. First, the signature $f(x,y)$ is multiplied by the input phase mask $\exp\left[i2\pi p(x,y)\right]$. Then, this product is convolved by the impulse response $h(x,y)$ which has a phase-only transfer function, $H(\mu,\nu)=\exp\left[i2\pi b(\mu,\nu)\right]$, denoted as Fourier plane phase mask. Thus, the double-phase or amplitude-based encrypted information, $\psi_A(x,y)$, is given by

$$\psi_A(x,y)=\left\{f(x,y)\exp\left[i2\pi\, p(x,y)\right]\right\}*h(x,y), \tag{1}$$

where * denotes the convolution operation.

Once the signature is captured by the receiver, it is decrypted. In order to decrypt the encoded signature, $\psi_A(x,y)$, its Fourier transform must be multiplied by the complex conjugated phase mask $\exp\left[-i2\pi b(\mu,\nu)\right]$ and then inverse Fourier transformed, which produces

$$f(x,y)\exp\left[i2\pi\, p(x,y)\right]=IFT\left\{FT\left[\psi_A(\mu,\nu)\right]\exp\left[-i2\pi b(\mu,\nu)\right]\right\}. \tag{2}$$

Finally, multiplication by the phase mask $\exp\left[-i2\pi p(x,y)\right]$ will recover $f(x,y)$. Alternatively, because $f(x,y)$ is real and positive, the signature may be recovered by computing the magnitude of $f(x,y)\exp\left[i2\pi p(x,y)\right]$ or by using an intensity sensitive device such as a video camera or CCD camera. Thus, the encoded signature can only be decrypted when the corresponding phase code $\exp\left[i2\pi b(\mu,\nu)\right]$, referred to as key, is known by the processor and used for the decryption.

2.2. Fully phase encryption[8]

If the fully phase encryption method[8] is applied, the images to be encoded are represented as phase-only functions[11] in the double-phase encryption technique.[7] The fully phase encryption of the input signature $f(x,y)$ is obtained by three operations. First the primary image $f(x,y)$ is phase encoded by computing $\exp\left[i\pi f(x,y)\right]$. The range of variation of the phase encoding is $\left[0,\pi\right]$. Second, the phase-encoded image is multiplied by the phase mask $\exp\left[i2\pi p(x,y)\right]$. Finally, this product is convolved by a function $h(x,y)$, which is the impulse response of a phase-only transfer function $H(\mu,\nu)=\exp\left[i2\pi b(\mu,\nu)\right]$. Thus, the fully phase encrypted signature, $\psi_P(x,y)$, is given by

$$\psi_P(x,y)=\left\{\exp\left[i\pi f(x,y)\right]\exp\left[i2\pi p(x,y)\right]\right\}*h(x,y). \tag{3}$$

To decrypt the information included in the encrypted function $\psi_P(x,y)$, it is firstly Fourier transformed and multiplied by the complex conjugate of the phase mask, or key 1, used in the encryption procedure, $\exp\left[-i2\pi b(\mu,\nu)\right]$. The output $\exp\left[i\pi f(x,y)\right]\exp\left[i2\pi p(x,y)\right]$ is obtained. The original signature is retrieved in the space domain by using a second key, $\exp\left[-i2\pi p(x,y)\right]$ (key 2), extracting the phase of $\exp\left[i\pi f(x,y)\right]$ and dividing by π.

Differently to the previous amplitude-based encryption method, two keys are needed to retrieve the signature when the fully phase encryption technique is applied. In that sense, system security is increased.

Both encoding methods, the amplitude-based and the fully phase encryption, can be implemented optically or electronically. In either case, the complex-amplitude encoded image $\psi\left(x,y\right)$ must be represented with both amplitude and phase. Figure 1 shows an example of signature (Fig. 1a), which is encoded by using the amplitude-based encryption (Fig. 1b,c) or the fully phase encryption (Fig. 1d,e).

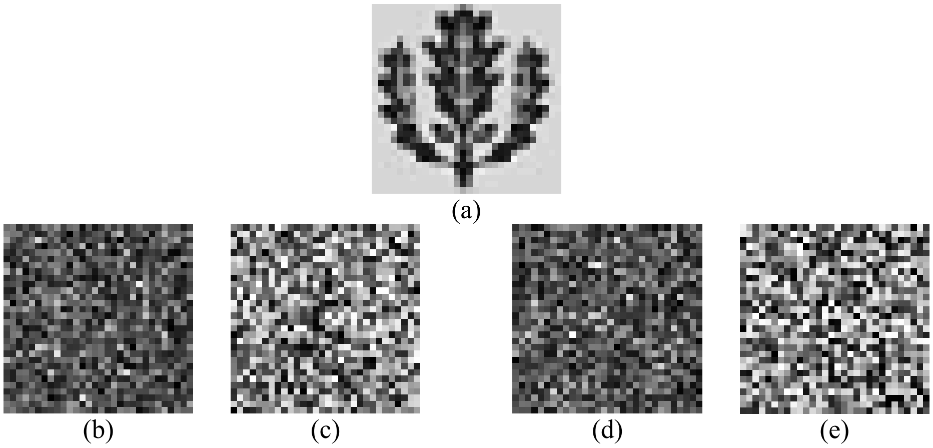


Fig. 1. (a) Signature $f\left(x,y\right)$; (b) Magnitude and (c) phase of the amplitude-based encrypted signature $\psi_A\left(x,y\right)$; (d) Magnitude and (e) phase of the fully phase encrypted signature $\psi_P\left(x,y\right)$.

3. DISTORTION-INVARIANT ID TAGS

We aim to include the information of the encrypted signature in an ID tag which should be invariant to different distortions, in particular to scale variations and rotations. If we do so, the receiver will be able to capture the ID tag from an unexpected location and orientation and, within certain limits, to process the information included in it.

Different contributions can be found in the literature that deal with scale and rotation invariant systems for a wide variety of purposes.[12-22] In general, sophisticated methods are needed to achieve enough tolerance to different distortions simultaneously. Information of several distorted views of a given target can be included in the design of a filter to obtain a distortion-tolerant system. When there are a number of considered distortions, the level of complexity of the recognition system usually increases notoriously. In this work, distortion-invariance is achieved by both multiplexing the information included in the ID tag and taking advantage of the ID tag topology. This procedure permits certain reduction of the system complexity.

Let us describe the design of a rotation and scale-invariant ID tags from an encrypted signature $\psi\left(x,y\right)$, which could be obtained either by using the amplitude-based[7] (Eq. 1) or the fully phase[8] (Eq. 3) encryption technique. The complex valued function $\psi\left(x,y\right)$ is fully grayscale encoded. Let us consider the encrypted signature $\psi\left(x,y\right)$ in array notation $\psi(t)=\left|\psi(t)\right|\exp\left\{i\phi_\psi(t)\right\}$ where t=1,2,...N, and N is the total number of pixels of the encrypted signature (Fig. 2). We build two vectors: the magnitude vector $\left|\psi(t)\right|$ and the phase vector $\phi_\psi(t)$, with t=1,2,...N. The information included in the ID tags is distributed in two circles. One of them (rotation-invariant ID tag) includes the encrypted signature $\psi(t)=\left\{\left|\psi(t)\right|,\phi_\psi(t)\right\}$ written in a radial direction and repeated angularly so that rotation-invariance can be achieved.[2]

The other circle (scale-invariant ID tag) contains the encrypted signature $\psi(t)=\left\{|\psi(t)|,\phi_\psi(t)\right\}$ written circularly and repeated in concentric rings. Therefore, in this second circle the information of a given pixel of the encrypted signature will correspond to an angular sector in the optical code. Thus, the readout of the ciphered information will be tolerant to variations in scale. Figure 2 shows a possible arrangement of both circles. Their centers are white dots that, along with a third white dot in the upper part, build a reference triangular shaped pattern. The triangle basis or longest side establishes an axis (the horizontal axis in Fig. 2) and the triangle vertex defines the semiplane (upper semiplane in Fig. 2) where the magnitude $|\psi(t)|$ will be encoded in grayscale in both circles. The phase $\phi_\psi(t)$ will be encoded also in grayscale in the bottom semiplane of both circles.

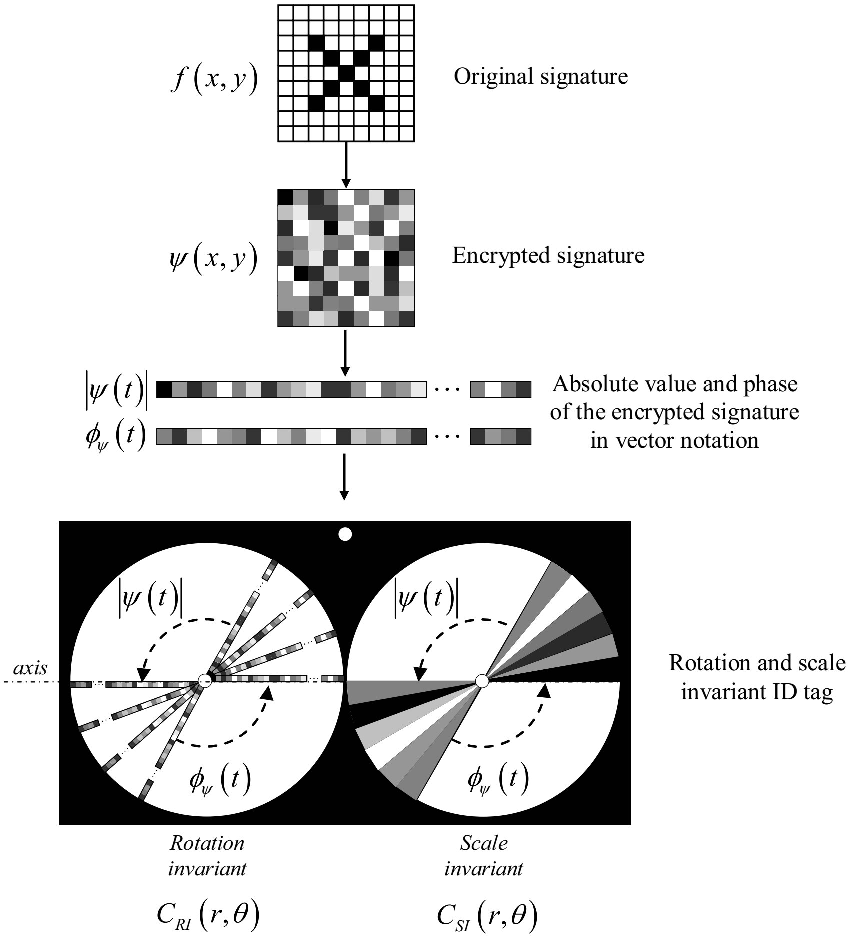


Fig. 2. Synthesis of a distortion (rotation and scale)-invariant ID tag.

Rotation invariance is achieved in one circle (on the left in Fig. 2) by writing $\psi(t)=\left\{|\psi(t)|,\phi_\psi(t)\right\}$ in the radial direction: magnitude vector $|\psi(t)|$ in the upper semiplane and, aligned along the same radial direction but in the bottom semiplane, the phase vector $\phi_\psi(t)$, and repeating it angularly within the circle (Fig. 2).

In polar coordinates, we can write the Rotation-Invariant ID tag function as:

$$C_{RI}(r,\theta)=\begin{cases}|\psi(r)|, & for\ r=(1...N)\left(\dfrac{R_L-R_0}{N}\right), \forall\theta\in(0,\pi] \\ \phi_\psi(r), & for\ r=(1...N)\left(\dfrac{R_L-R_0}{N}\right), \forall\theta\in(\pi,2\pi], \\ V_{\max}, & for\ r\le R_0 \quad (white\ central\ dot)\end{cases} \tag{4}$$

where functions $|\psi(t)|$ and $\phi_\psi(t)$ are discretized in 2^n values, and $V_{\max}=2^n$ is the maximum value of the grayscale (white). In our simulations, we will consider $n = 8$, that is, a 8-bit grayscale. In Eq. (4), R_L is the radius of the ID tag circle, R_0 is the radius of the white central dot. N indicates the radial partition, which is limited by the receiver resolution at the smallest pixels that surround the central dot.

Scale invariance is achieved in another circle (on the right in Fig. 2) by writing $\psi(t)=\{|\psi(t)|,\phi_\psi(t)\}$ in the angular direction: magnitude vector $|\psi(t)|$ in the upper semiplane and, at the same radial distance but in the bottom semiplane, the phase vector $\phi_\psi(t)$, and repeating it in concentric rings within the circle (Fig. 2).

In polar coordinates, we can write the Scale-Invariant ID tag function as:

$$C_{SI}(r,\theta)=\begin{cases}|\psi(\theta)|, & for\ \theta=(1...N)\left(\dfrac{\pi}{N}\right), \forall r\in(R_0,R_L] \\ \phi_\psi(\theta), & for\ \theta=(N+1...2N)\left(\dfrac{\pi}{N}\right), \forall r\in(R_0,R_L]. \\ V_{\max}, & for\ r\le R_0 \quad (white\ central\ dot)\end{cases} \tag{5}$$

In Eq. (5), N indicates the angular partition, which is limited by the receiver resolution at the smallest pixels that surround the central dot. Since the receiver resolution is not generally known *a priori*, the image of the triangular shaped pattern consisting of three white dots can be used as a reference to know if the receiver has enough resolution to read the encrypted information. For instance, the ID tags can be designed to ensure an appropriate readout for those receivers that measure a distance between the circle centers (or the triangle basis) greater than a certain value. The triangle pattern could give information about scale and rotation and, therefore one could think that there is no need to codify the encrypted signature $\psi(x,y)$ in the distortion invariant ID tags defined by Eqs. (4) and (5). But we must take into account that if the encrypted signature $\psi(x,y)$, written in a matrix array similar to the one shown in Fig. 2, is affected by rotation and/or scale variation, then it needs to be sampled again and rearranged into matrix form before decryption. This operation entails interpolations that can produce errors such as aliasing. For this reason, we consider that the distortion-invariant ID tags, provided they are correctly built, allow more accurate readouts of the encrypted information under rotation and/or scale variations. Figure 2 depicts the procedure followed to obtain these distortion-invariant ID tags.

Other possibilities can be considered to rearrange the information contained in the two circles of the ID tags. For example, one circle could contain the magnitude vector $|\psi(t)|$ and the other circle the phase vector $\phi_\psi(t)$. In this case, the upper semiplane of both circles could be the area for rotation invariant identification whereas the bottom semiplane could be the area for scale invariant identification, just following a distribution similar to that considered in Ref. [2]. The choice of a particular distribution of the signal information depends on practical considerations of a given problem.

Encrypted information is recovered by the following procedure. In each circle of Fig. 3, the border between the regions where $|\psi(t)|$ and $\phi_\psi(t)$ are respectively codified is determined by the axis defined by the two circle centers. Once this border is detected, the third white dot marks the semiplane where the $|\psi(t)|$ is written (upper semiplane). The other semiplane corresponds to function $\phi_\psi(t)$ (bottom semiplane). The encrypted signature in vector notation $\psi(t)$ can be decoded by reading out the information of the optical code either from the rotation-invariant or the scale-invariant ID tag.

From the circle corresponding to the rotation-invariant ID tag (Fig. 3, on the left), the optical code could be read out by using a linear array detector placed in any diameter of the circle. Half part of this linear sensor, from the center to the exterior of the code in the upper semiplane, is used to read $|\psi(t)|$, whereas the other half part in the bottom semiplane, is used to read $\phi_\psi(t)$. Not only is a single code read along a unique diameter, but the median value from several radial codes is computed to increase noise robustness. Pixels should be written back into matrix notation, $\psi(x,y)$, prior to decoding the signature $f(x,y)$ by using the decryption technique.[7-8] Following this procedure, the signature will be recovered whether the ID tag is captured in its original orientation or its rotated format.

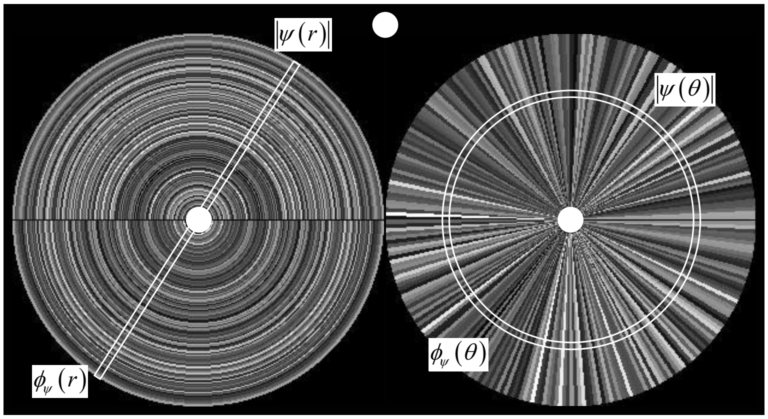


Fig. 3. Reading out process from the rotation and scale-invariant ID tags.

From the circle corresponding to the scale-invariant ID tag, the encrypted signature in vector notation $\psi(t)$ is recovered by reading out the pixels of the ID tag in circular rings (Fig. 3, on the right). Similarly to the previous case, the semicircle in the upper semiplane corresponds to the $|\psi(t)|$ vector, whereas the semicircle in the bottom semiplane corresponds to $\phi_\psi(t)$ vector. To minimize errors in the reading process, not only is one pixel taken into account for each circular ring, but the median value of pixels located in neighbor concentric rings in the radial direction. Afterwards, the encrypted signature is written in matrix notation and the complex valued function $\psi(x,y)$ is decrypted to obtain $f(x,y)$. Then, the optical code will be recovered even if the ID tag is captured in its original size or scaled.

For signatures with a large number of pixels (for instance, signature shown in Fig. 1a), information of the scale-invariant ID tag can be distributed using different concentric circles to assure a minimum number of pixels for each sector to properly recover the information (Fig. 4).[2] Consequently, the tolerance to scale variation is affected in accordance to the number of concentric circles used in the ID tag. In such a case, the procedure to recover the encrypted signature is basically the same, but the existence of concentric circles and their size must be taken into account in the readout.

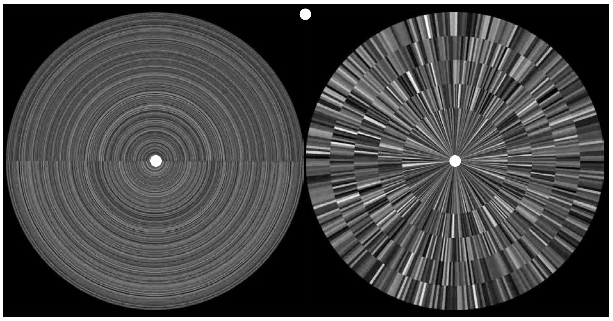


Fig. 4. Example of distortion-invariant ID tag built from an encrypted signature with a large number of pixels (Fig. 1). The information of the optical code in the scale-invariant tag (circle on the right) is distributed in concentric circles.

4. CORRELATION-BASED AUTHENTICATION

The final step for the ID tag receiver will be the verification of the captured information in order to authenticate a given object. A correlation-based processor[6,23] will compare the decoded information with a previously stored reference signal. Comparison of these two functions would be based on a nonlinear correlator.[24]

The decoded information $f(x,y)$ and the reference signature $r(x,y)$ are both Fourier transformed and nonlinearly modified. Both distributions are multiplied in the frequency domain. The correlation between the input and the reference signals is obtained by inverse Fourier transforming this product. Let $|F(\mu,\nu)|$ and $|R(\mu,\nu)|$ be the modulus of the Fourier transforms of $f(x,y)$ and $r(x,y)$, respectively, and let $\phi_F(\mu,\nu)$ and $\phi_R(\mu,\nu)$ denote their phase distributions in the frequency domain. According to this notation, nonlinear correlation is obtained by using the equation:

$$c(x,y) = IFT\left\{ \left| F(\mu,\nu) R(\mu,\nu) \right|^k \exp\left[i\left(\phi_F(\mu,\nu) - \phi_R(\mu,\nu) \right) \right] \right\} . \tag{6}$$

In a k'th-law nonlinear processor,[24] parameter k defines the strength of the applied nonlinearity. The nonlinearity will determine performance features of the processor, such as its discrimination capability, noise robustness, peak sharpness, etc. and it can be chosen according to the performance required for a given recognition task.[24-26] Optimum nonlinear transformations can be obtained to enhance the detection process by optimizing a performance metric.[27] We use k'th-law nonlinearity for computational efficiency.

A threshold operation, applied to the correlation output, determines the identity of the object. Correlation-based detection is feasible when an output peak above a noise floor is obtained. The processor performance must be evaluated using different metrics. The metrics that are taken into account in this work are well-known parameters described in the literature.[28-31] We consider, as a measure of the system discrimination capability, the cc/ac metric which is the ratio between the maximum peak value of the correlation output, cc, and the maximum autocorrelation value, ac, for the reference signature. Similarity between the decoded information and the reference signature will be greater as the cc/ac ratio approaches the value of unity.

5. AUTHENTICATION RESULTS

In this section, numerical results are obtained to demonstrate the feasibility of the proposed distortion-invariant ID tag. We focus our attention to the fully phase encryption technique,[8] and we finally compare its performance with the amplitude-based encryption in presence of noise. The signature used to verify the identification system is shown in Fig.

1a. The corresponding encrypted image, computed by using the fully phase encoding technique, is shown in Fig. 1d and Fig. 1e for its magnitude and phase distribution, respectively. The two circles of the rotation and scale-invariant ID tag are synthesized from this encoded information by following the procedure described in Section 3 and are shown in Fig. 4.

5.1 Rotation-invariant detection

First, we test the rotation invariance of the verification system that detects the ID tag shown in Fig. 4. We digitally rotate the ID tag from 0 to 360 degrees in steps of 20 degrees. For all the rotated ID tags, encrypted signatures in vector notation $\psi(t)$ are recovered from the rotation-invariant circle of the ID tag following the procedure described in Section 3, and decrypted signatures $f(x,y)$ are obtained by using the fully phase decryption technique.[8] Some of these decrypted signatures are depicted in Fig. 5.

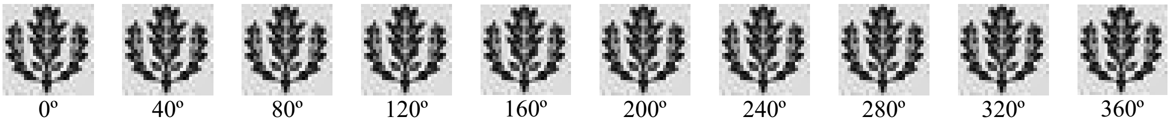

0º 40º 80º 120º 160º 200º 240º 280º 320º 360º

Fig. 5 Decoded signatures from rotated versions of the distortion-invariant ID tag shown in Fig. 4.

Signatures are correctly decoded in all the cases even though some noise is overlapping with the recovered images. It is worth to point out that the use of the median value of all the pixels corresponding to a particular value of $\psi(t)$ in the imaged ID tag,[5] instead of the mean value as in previous papers,[2-4] lead to improved results. To verify whether the object is an authorized signal, the recovered signatures must be compared with a previously stored reference signal (Fig. 1a), by using a correlation-based processor. An example of identification results is plotted in Fig. 6. The output plane of the recognition system is displayed. Parameter *k* of the nonlinear correlator was fixed to value 0.5 because this nonlinearity provides a good trade-off between distortion-tolerance and peak sharpness.[2] The ratio *cc/ac* is also displayed in Fig. 6. The high and sharp peak indicates the authentication of the signature.

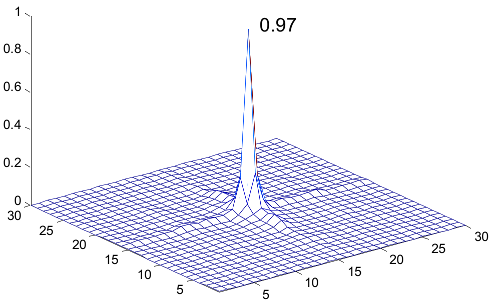


Fig. 6. Normalized output plane for the decoded signature obtained from a rotated version (80 degrees) of the ID tag (Fig. 4). Parameter *k*=0.5 is used.

5.2 Scale-invariant detection

Invariance to scale variations is tested by using the other circle of the distortion-invariant ID tag shown in Fig. 4. In this case, using simulation, the ID tag has been captured at different distances from the receiver. It is digitally scaled by a factor ranging from 0.2 to 2 in steps of 0.1. Some of the decrypted signatures obtained from this test are shown in Fig. 7. The quality of the recovered signature is visually acceptable in nearly all the cases. Also in this test, the use of the median -instead of the mean value- of all the pixels of a given sector of the imaged ID tag allows a significant improvement of the results. When the ID tag is captured from a long distance (that is, if scale factors lower than 0.2 are used), the noise level of the decoded images increases rapidly and the signature is not properly deciphered. In addition, we remind that the system tolerance to scale variations is limited due to the concentric semicircles used in the ID tag.

Nonlinear correlation of the decoded images with the stored reference signal (Fig. 1a) is used to evaluate the image quality of the recovered signatures. Fig. 8 shows the normalized output planes for two decoded images obtained from scaled versions (scale factors 0.2 and 0.1, respectively) of the ID tag of Fig. 4. Value of *k*=0.5 was used in both cases. A high and sharp correlation peak indicates the great similarity between the decoded image and the original signature when the ID tag was scaled by a factor 0.2 (Fig.8a). For a scale factor of 0.1 (Fig. 8b), a larger amount of noise occurs and this fact is responsible for the decrease of the ratio *cc/ac*. However, a peak projects over the flat background and may permit the identification.

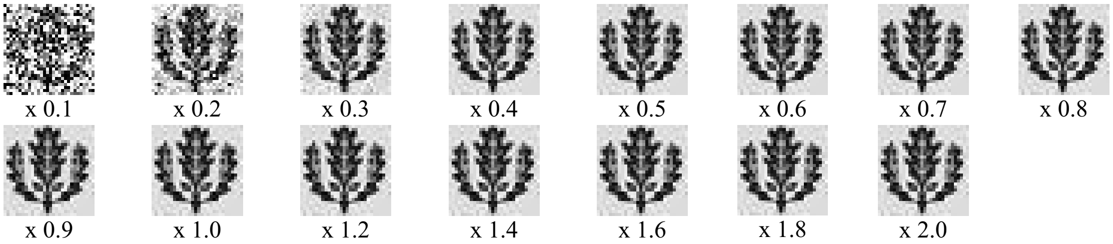


Fig. 7. Decoded images for scaled versions of the distortion-invariant ID tag shown in Fig. 4.

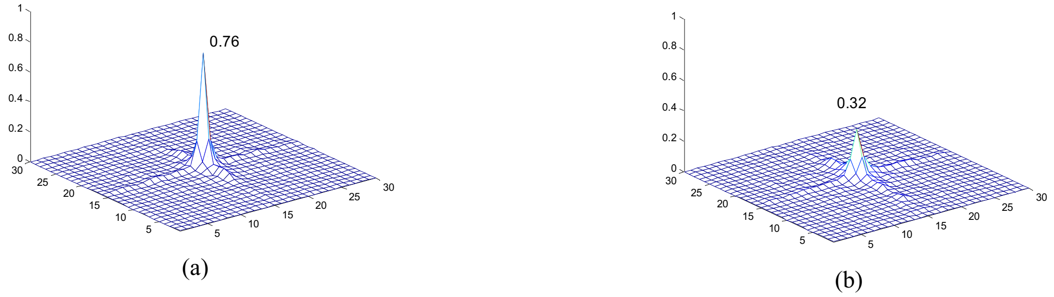


Fig. 8. Normalized output planes for the decoded signatures obtained from rotated version of the ID tag (Fig. 4). Parameter *k*=0.5 is used. The ID tag was scaled by a factor (a) 0.2, and (b) 0.1.

5.3 Integrated rotation and scale-invariant

Finally, the identification system is tested against rotation and scale distortion appearing simultaneously in the two circles of the captured ID tags. Figure 9 displays the output planes of the recognition system along with the decoded signatures obtained for simultaneously rotated and scaled version of the ID tag shown in Fig. 4. In all the cases, the signature has been correctly decoded and identified by using *k*=0.5 for correlation, even though the level of noise increases with the amount of distortion.

To demonstrate the robustness of the ID tags for verification and identification, let us recover the decrypted information from a rotated (60 degrees) and scaled (0.5 scale factor) ID tag, and let us decrypt the encoded information by using a false phase key. As we are applying the fully phase encryption technique,[8] two keys are needed in the decryption process. Figure 10 shows the results obtained when either one of the keys is not correct, or when both keys are false. In the three cases, we obtain a noisy image where no signature can be recognized (Fig. 10).

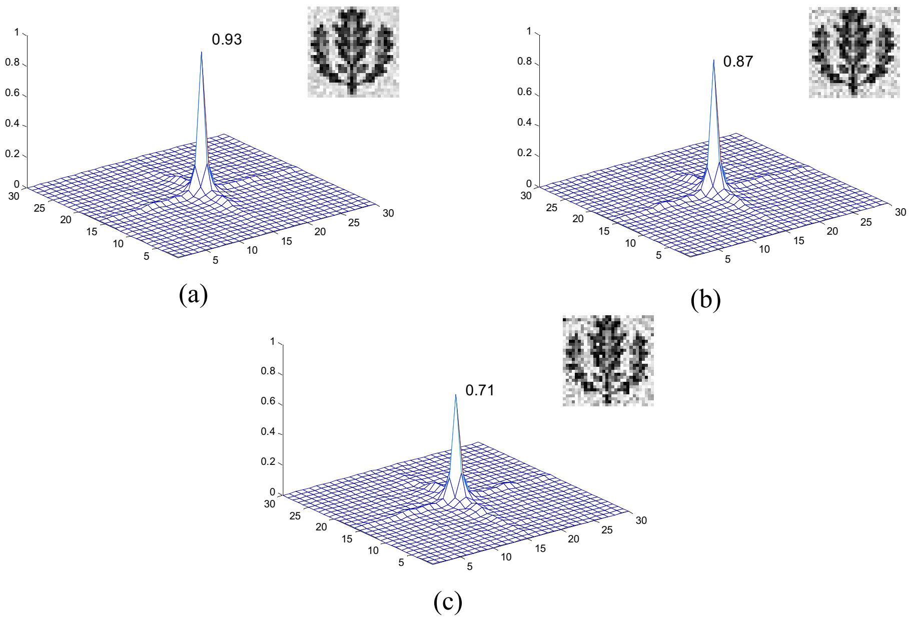


Fig. 9. Decoded signatures and correlation outputs (*k*=0.5) for simultaneously rotated and scaled versions of the ID tag shown in Fig. 4. (a) Scale factor: x 0.5 and rotation angle: 60º; (b) Scale factor: x 0.4 and rotation angle: 70º; (c) Scale factor: x 0.3 and rotation angle: 80º.

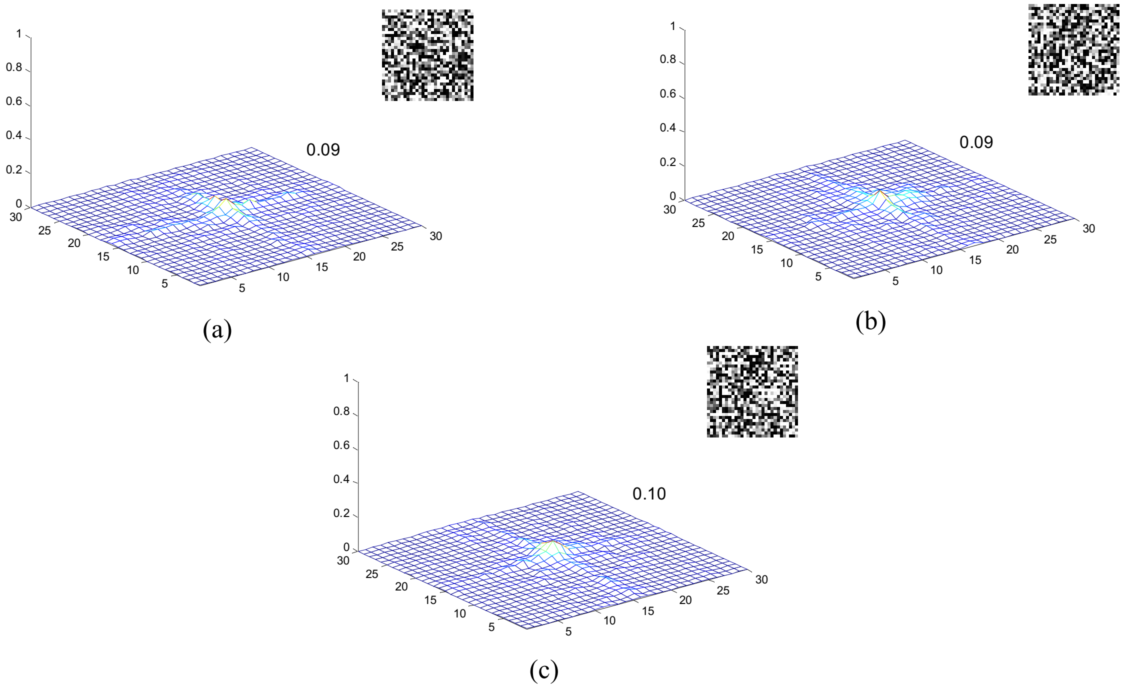


Fig. 10. Decoded image by using false keys and correlation output for *k*=0.5. The ID tag was rotated 60 degrees and scaled by a factor of 0.5. (a) Wrong key 1; (b) Wrong key 2; (c) Both key 1 and 2 are false.

5.4. Authentication in the presence of additive noise

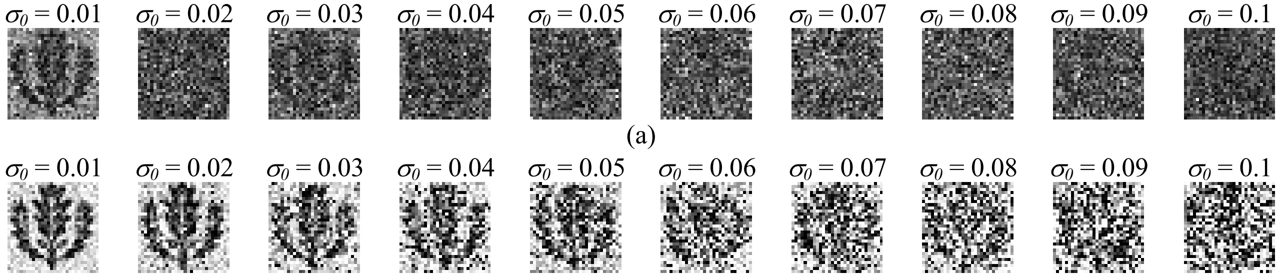
The motivation to introduce the fully phase encryption in the design of distortion-invariant ID tags was mainly due to its robustness in the presence of additive noise.[8] In the following experiment, we want to compare the performance of the proposed distortion-invariant ID tags, when they are built from an amplitude-based encrypted signature and from a fully phase encrypted signature, in the presence of additive Gaussian noise.

We consider that the captured ID tag is corrupted by a zero-mean white stationary Gaussian noise with variance σ_0. To evaluate the quality of the recovered image, $f_A(x,y)$ or $f_P(x,y)$ from the amplitude-based or the fully phase encryption methods respectively, the mean-squared-error (*mse*)[8] is used as a metric to compare the recovered image with the original input signature $f(x,y)$

$$mse\left[f_{A,P}(x,y)\right] = E\left\{\frac{1}{N}\sum_{x=0}^{N_x}\sum_{y=0}^{N_y}\left[\left|f_{A,P}(x,y) - f(x,y)\right|^2\right]\right\}, \quad \textbf{(7)}$$

where $N = N_x \cdot N_y$ is the total number of pixels of the original image, and $E\{\cdot\}$ is the expected value. This metric is considered because distortions due to additive noise affect the value of the pixel rather than its location. Therefore, a distance-measuring metric could be appropriate to evaluate and compare the performance of the two encryption methods.[8]

Figure 11a shows the recovered signatures from the amplitude-based encrypted images when the captured distortion-invariant ID tag is corrupted by an additive Gaussian noise of increasing variance σ_0. The same experiment is carried out with an ID tag built from a fully phase encrypted signature. The results obtained in this second case are shown in Fig. 11b.



(b)

Fig. 11. Decrypted signatures for distortion-invariant codes affected by additive zero-mean Gaussian noise of different variance σ_0. (a) Results for the amplitude-based and (b) fully phase encryption methods.

From results shown in Fig. 11, and in accordance to previous works,[8] we can state that fully phase encryption technique has a better performance than the amplitude-based encryption in the presence of additive Gaussian noise. The signature can be perceived for larger noise variance when the fully phase encryption is applied. From an amplitude-based encrypted signature, if the distortion-invariant ID tag is corrupted by a small amount of additive noise, the retrieved signature is embedded by noise and cannot be recognizable.

To make these results more evident, we computed the mean-squared-error between the original signature and the recovered image. Figure 12 plots the curves obtained for both encryption methods. The recovered image from the amplitude-based encryption method degrades quickly, and the *mse* increases with the level of noise. Signatures recovered from the fully phase encryption method degrades more gradually with the increase of variance of the additive noise.

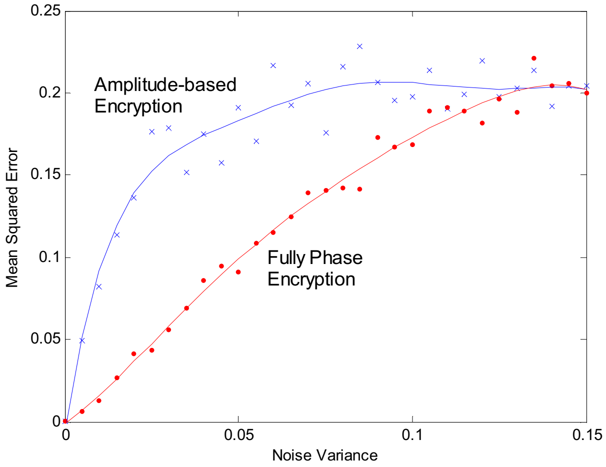


Fig. 12. Mean-squared-error for the decrypted signatures using amplitude-based encryption and fully phase encryption.

6. CONCLUSIONS

We have presented a method to encode an encrypted signature into an ID tag to provide invariance to rotation and scale distortions. Identification tags can be used for real-time remote identification and authentication of objects which have diverse applications in transportation and homeland security. The ID tags consist of an optical code containing encrypted information to increase security. Both the magnitude and the phase of the encrypted signature are codified in grayscale to improve robustness against phase distortions produced by outdoors environmental conditions (rain, air turbulences, etc.).[5]

The designed ID tag is located on a given object and captured by a receiver, which will decode and verify the information. The signature is a characteristic image that allows the identification of the object. The encrypting procedure is based on a fully phase encryption technique. This encoding technique has been shown as a robust encryption technique in the presence of Gaussian noise. Decryption and verification processes can be performed using PCs to assure real-time identification and authentication of vehicles.

Numerical results provided in this paper demonstrate that the proposed system is able to recover a given signature even when the ID tag is rotated, scaled, or both rotated and scaled simultaneously. In comparison to the amplitude-based encryption used in previous works, the fully phase encryption technique increases the noise robustness of the processor in the presence of additive Gaussian noise.

REFERENCES

1. B. Javidi, *Real-time remote identification and verification of objects using optical ID tags*, Opt. Eng., Vol. 42, pp. 1-3, 2003.
2. E. Pérez-Cabré, B. Javidi, *Scale and rotation-invariant ID tags for automatic vehicle identification and authentication*, IEEE Trans. on Vehicular Technology, Vol. 54, no. 4, pp.1295-1303, 2005.
3. E. Pérez-Cabré, B. Javidi, *Distortion-invariant ID tags for object identification*, Proc. SPIE, vol. 5611, pp. 33-41, 2004.
4. E. Pérez-Cabré, B. Javidi, M. S. Millán, *Detection and authentication of objects by using distortion-invariant optical ID tags*, Proc. SPIE, vol. 5827, pp. 69-80, 2005.
5. E. Pérez-Cabré, M. S. Millán, B. Javidi, *Remote object authentication using distortion-invariant ID tags*, Proc. SPIE, vol. 5908, pp. 164-176, 2005.
6. J. W. Goodman, *Introduction to Fourier optics*, 2nd. Ed., McGraw Hill, New York, 1996.

7. Ph. Réfrégier, B. Javidi, *Optical image encryption based on input plane and Fourier plane random encoding*, Opt. Let., vol. 20, no. 7, pp. 767-769, 1995.
8. N. Towghi, B. Javidi, Z. Luo, *Fully phase encrypted image processor*, JOSA A., vol. 16, no. 8, pp.1915-1927, 1999.
9. B. Javidi, L. Bernard, and N. Towghi, *Noise performance of double-phase encryption compared with XOR encryption*, Opt. Eng., vol. 38, pp. 9-19, 1999.
10. F. Goudail, F. Bollaro, P. Refregier, and B. Javidi, *Influence of perturbation in a double phase encoding system*, JOSA A, vol. 15, pp. 2629-2638, 1998.
11. B. Javidi, A. Sergent, *Fully phase encoded key and biometrics for security verification*, Opt. Eng., vol. 36, no. 3, pp. 935-942, 1997.
12. A. Mahalanobis, *A review of correlation filters and their application for scene matching*, in Optoelectronic Devices and Systems for Processing. Critical Review of Optical Science Technology, SPIE, Bellingham, WA., vol. CR 65, pp. 240-260, 1996.
13. IEEE Trans. on Image Processing. Special issue on *Automatic Target Detection and Recognition*, vol. 6, no. 1. 1997.
14. B. Javidi, ed. *Smart imaging systems*, SPIE Press, SPIE, Bellingham, WA, 2001.
15. B. Javidi, ed., *Image recognition and classification: Algorithms, systems and applications*, Marcel Dekker, New York, 2002.
16. C. F. Hester, D. Casasent, *Multivariant technique for multiclass pattern recognition*, Appl. Opt., vol. 19, no. 11, pp. 1758-1761, 1980.
17. H. J. Caulfield, *Linear combinations of filters for character recognition: a unified treatment*, Appl. Opt., vol. 19, pp. 3877-3879, 1980.
18. H. Y. S. Li, Y. Qiao, D. Psaltis, *Optical network for real-time face recognition*, Appl. Opt., vol. 32, no. 26, pp. 5026-5035, 1993.
19. T. D. Wilkinson, Y. Perillot, R. J. Mears, J. L. Bougrenet de la Tocnaye, *Scale-invariant optical correlators using ferroelectric liquid-crystal spatial light modulators*, Appl. Opt., vol. 34, no. 11, pp. 1885-1890, 1995.
20. B. Javidi, D. Painchaud, *Distortion-invariant pattern recognition with Fourier-plane nonlinear filters*, Appl. Opt., vol. 35, no. 2, pp. 318-331, 1996.
21. L. C. Wang, S. Z. Der, N. M. Nasrabadi, *Automatic target recognition using feature-decomposition and data-decomposition modular neural networks*, IEEE Trans. on Image Processing, vol. 7, no. 8, pp. 1113-1121, 1998.
22. E. Pérez, B. Javidi, *Nonlinear distortion-tolerant filters for detection of road signs in background noise*, IEEE Trans. on Vehicular Technology, vol. 51, no. 3, pp. 567 –576, 2002.
23. J. L. Turin, *An introduction to matched filters*, IRE Transactions on Information Theory, vol. IT-6, pp. 311-329, 1960.
24. B. Javidi, *Nonlinear joint power spectrum based optical correlation*, Appl. Opt., vol. 28, no. 12, pp. 2358-2367, 1989.
25. M. S. Millán, E. Pérez, K. Chalasinska-Macukow, *Pattern recognition with variable discrimination capability by dual non-linear optical correlation*, Opt. Commun., vol. 161, pp.115-122, 1999.
26. E. Pérez, M. S. Millán, K. Chalasinska-Macukow, *Optical pattern recognition with adjustable sensitivity to shape and texture*, Opt. Commun., vol. 202, pp. 239-255, 2002.
27. S. H. Hong, B. Javidi, *Optimum nonlinear composite filter for distortion-tolerant pattern recognition*, Appl. Opt., vol. 41, no. 11, pp. 2172-2178, 2003.
28. B. Javidi, J. L. Horner, *Real-time Optical Information Processing*, Academic Press, Boston, 1994.
29. *ATR Definitions and Performance Measures*, Automatic Target Recognizers Working Group (ATRWG) Publications, no. 86-001, 1986.
30. J. L. Horner, *Metrics for assessing pattern-recognition performance*, Appl. Opt., vol. 31, no. 2, pp.165-166, 1992.
31. B. V. K. Vijaya Kumar, L. Hassebrook, *Performance measures for correlation filters*, Appl. Opt., vol. 29, no. 20, pp. 2997-3006, 1990.