Remote object authentication using distortion-invariant ID tags

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

A number of applications in security or inventory control may benefit from an authentication system able to identify a remote object viewed from different perspectives or distances. Object identification can be accomplished by using optical ID tags, which include relevant information of the target and are located on a visible part of the object under surveillance. Encryption of the information codified in the ID tag allows increasing security and deters from unauthorized usage of optical tags. The identification process encompasses several steps such as detection, information decoding and verification which are all detailed in this work. Design of distortion-invariant ID tags has to be taken into account to achieve a correct object authentication even if the ID tag is detected and captured at different distances (i.e. different scales) or from different views (i.e. rotated versions of the original ID tag). Description of diverse distortion-invariant ID tags and authentication results using the proposed ID tags are provided. We show that distortion-tolerance is achieved by the described identification system. Information encrypted on the tested ID tags is correctly decoded and verified even if variations in scale and rotations are considered. The effects of environmental degradation are taken into account in the recognition process.

Keywords: Object authentication, optical ID tags, double-phase encryption, distortion-invariance recognition.

1. INTRODUCTION

Active and passive optical identification (ID) tags and readers were described in Ref. 1 to achieve real-time remote identification and verification of objects. As an active imaging system, a tunable laser was used to generate a specific sequence of optical waveforms according to an electronic code assigned to authenticate a particular remote object.[1] A photo-detector array detected the wavelength hopped spread spectrum sequence as a function of time and afterwards, a correlator[2] verified the authenticity of the code as a function of its spectral and temporal contents.

On the other hand, an optical code manufactured with retro-reflective materials was proposed to be used as a passive ID tag.[1] The optical code was inspected by a reader to verify the authenticity of the object. An identification number, a vehicle image, or other type of information could be stored in the optical code. The verification system that reads the encoded identification tag could be also a correlator,[2] which compares the information included in the optical tag with a previously stored reference function.

Active or passive ID tags can provide different benefits depending on the task where they are going to be used. Moreover, if necessary, active imaging systems could be used in tandem with the passive optical tags to increase system flexibility and reliability. The good properties of data storage of optically encoded materials and the free space identification possibilities of active imaging systems constitute an attractive combination for remote security, identification, verification and location of objects.

Our aim in this work is to design a novel distortion-invariant passive ID tag,[3] which could be detected under the effects of distortions such as variations in scale or/and in-plane rotations. The verification system should be able to detect and identify the information included in the ID tag even when the optical code is captured rotated or from an unexpected location (Fig. 1).

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

Optical Information Systems III, edited by Bahram Javidi, Demetri Psaltis, Proceedings of SPIE Vol. 5908
(SPIE, Bellingham, WA, 2005) · 0277-786X/05/$15 · doi: 10.1117/12.615006

In the first part of this work, we focus our attention on the description of the verification system. A double-phase encryption technique is introduced as a tool to increase the security of the procedure. Verification of the information embedded in the ID tag is carry out by correlation. For this reason, a correlation-based system is briefly described. Secondly, as the main point of this work, the design of a distortion-invariant ID tag is provided. The distortions to be considered are variations in scale and in-plane rotations. Numerical results will show the validity of the proposal.

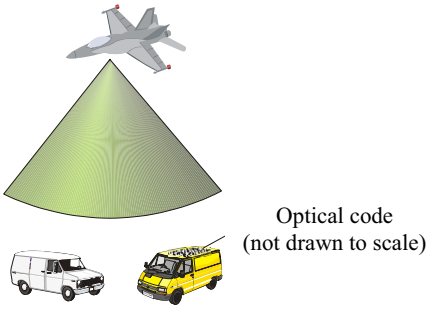


Fig. 1. Example of a distortion-invariant passive optical ID tag.

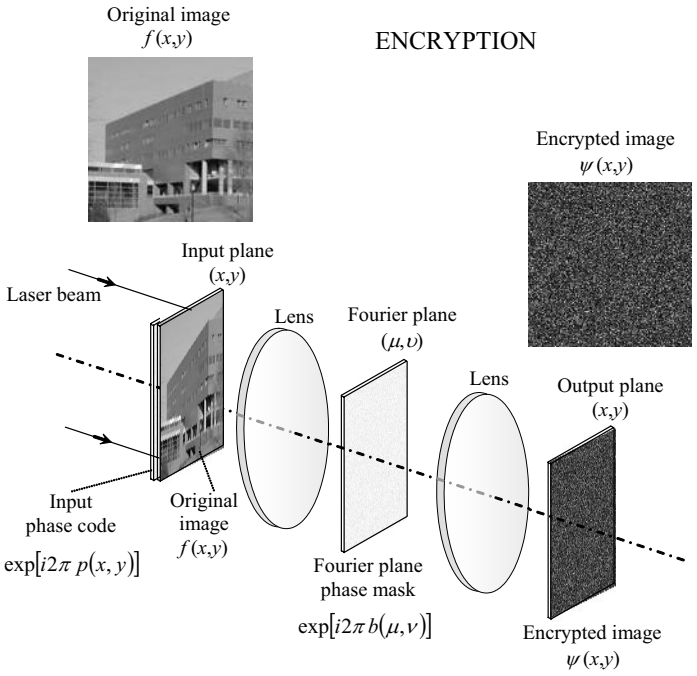
2. SECURITY AND VERIFICATION OF ID TAGS

2.1. Double-phase encryption

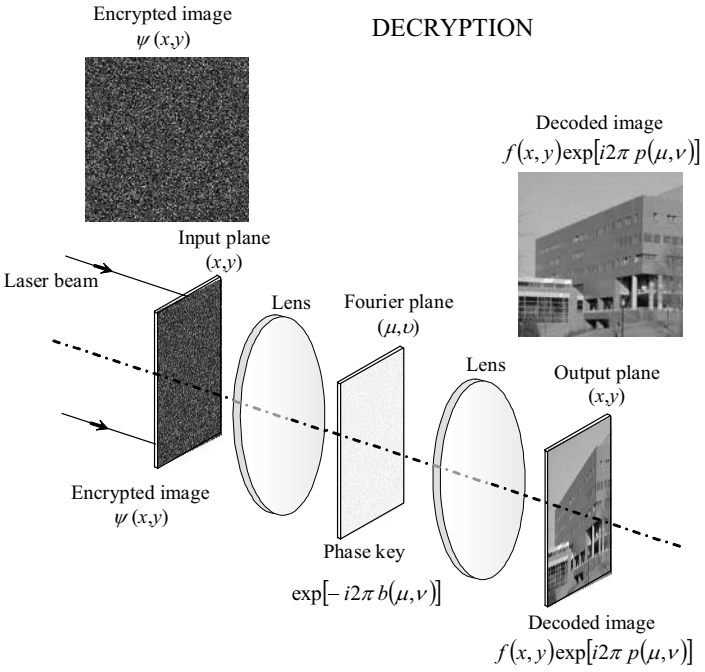
In order to increase security, the designed ID tag will consist of an encrypted signature. An identification number, an object image or other kinds of information may be used as a signature $f(x,y)$ to identify a given object. Commonly, $f(x,y)$ is a real function. The codification process will follow a double phase encryption technique,[4] which allows us to encode a primary image into stationary white noise (Fig. 2a). One phase code, $\exp\left[i2\pi p\left(x,y\right)\right]$, is used in the input plane, and the second phase code, $\exp\left[i2\pi b\left(\mu,\nu\right)\right]$, is used in the frequency domain (Fourier plane).[4] By using double phase encryption, the signature will be hidden in an encoded ID tag $\psi(x,y)$ not recognizable at human sight (Fig. 2a). In general, $\psi(x,y)$ is a complex valued function that needs to be encoded in both its absolute value and phase or, alternatively, in its real and imaginary parts.

Double phase encryption provides robustness against different types of ID tag degradation such as noise, occlusion, scratches, etc.[5-6] Therefore, we choose this encoding technique among other encryption techniques such as the standard private key system. Double phase encryption permits to appropriately cipher gray-scale images for optical tags without conversion to binary signatures which is the case for XOR encryption with a stream of pseudo random key.[5]

The encrypted signature $\psi(x,y)$ can be fabricated by micro-optics or embossing techniques, or, for high-security applications, made of a volume-recording material such as a photopolymer that is more difficult to duplicate due to the Bragg effect.[7] The encrypted signature will be placed in a visible part of the object to be detected. This way of generating an ID tag that reproduces both the magnitude and phase values of function $\psi(x,y)$ at each point of the tag is particularly appropriate for remote identification and verification in environmental conditions under control, such as conveying belts or indoor storage.



(a)



(b)

Fig. 2. Optical setup for double phase: a) encryption and b) decryption.

When remote identification and verification of objects has to be made outdoors, a large number of environmental conditions may affect the information contained in the ID tag as they introduce noise or even invalidate the captured signal. For instance, shading effects or non-uniform illumination affect mainly the signal magnitude, air turbulences or rain affect the signal phase. Moreover, the phase content of the signature can be easily neutralized and the ID tag sabotaged if an adhesive transparent tape is stuck on it. For all these reasons, it appears to be convenient to further encode the phase content of the signal in intensity variations. Thus, process can be made more robust by encoding both the magnitude and phase of function $\psi(x,y)$ in grayscale values.

Once the signature is captured by the receiver, it has to be decrypted (Fig. 2b). Only the Fourier plane phase mask, referred to as the key, is necessary for decryption provided the signature is a real and positive function.[4]

2.2. Signature verification based on correlation

The final step for the ID tag receiver will be the verification of the captured information in order to identify a given object. A correlation-based processor[2,8] will compare the decoded information with a previously stored reference signal. Comparison of these two functions would be based on a nonlinear correlator.[9]

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:

$$c(x,y) = IFT\left\{\left|F(\mu,\nu)R(\mu,\nu)\right|^k \exp\left[i\left(\phi_F(\mu,\nu)-\phi_R(\mu,\nu)\right)\right]\right\}. \qquad (1)$$

In a k'th-law nonlinear processor,[9] 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.[9-11] Optimum nonlinear transformations can be obtained to enhance the detection process by optimizing a performance metric.[12] 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.[13-16] 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 if the *cc*/*ac* ratio approaches the value of unity.

3. GRAYSCALE ENCODED TAGS FOR DISTORTION-INVARIANT IDENTIFICATION

Different contributions can be found in the literature that deal with scale and rotation invariant systems for a wide variety of purposes.[17-27] In general, sophisticated methods are needed to achieve enough tolerance to different distortions simultaneously. Information of several distorted views of a given target could 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.

A complete diagram of the proposed remote authentication system is depicted in Fig. 3. First, an optical code is built and placed on the object to be detected. Then, a distortion-invariant ID tag readout is carried out by a receiver. And finally, the signature is decrypted and verified by correlation.

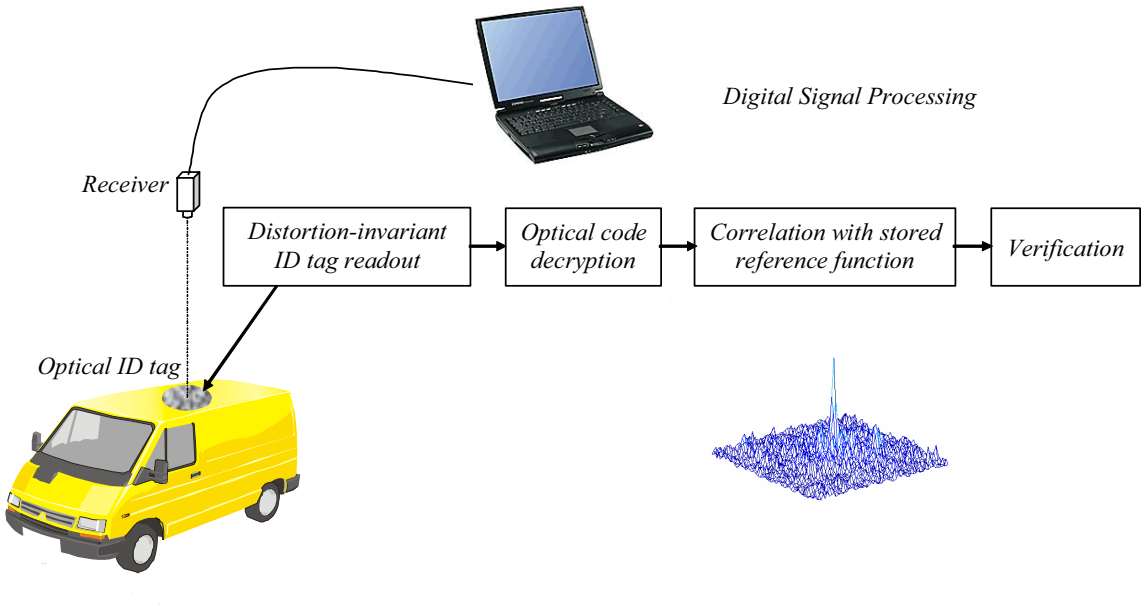


Fig. 3. Block-diagram of the remote identification system.

Let us describe the design of a rotation and scale-invariant ID tags whose complex valued function $\psi(x,y)$ is fully grayscale encoded. Let us consider the encrypted signature $\psi(x,y)$ in array notation $\psi(t)=|\psi(t)|\exp\{j\phi_\psi(t)\}$ where t=1,2,...N, and N is the total number of pixels of the encrypted signature (Fig. 4). We build two vectors: the magnitude vector $|\psi(t)|$ 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 $\psi(t)=\{|\psi(t)|,\phi_\psi(t)\}$ written in a radial direction and repeated angularly so that rotation-invariance could be achieved.[28] The other circle (scale-invariant ID tag) contains the encrypted signature $\psi(t)=\{|\psi(t)|,\phi_\psi(t)\}$ 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 a sector of a circle in the optical code. Thus, the readout of the ciphered information will be tolerant to variations in scale. Figure 4 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. 4) and the triangle vertex defines the semiplane (upper semiplane in Fig. 4) 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.

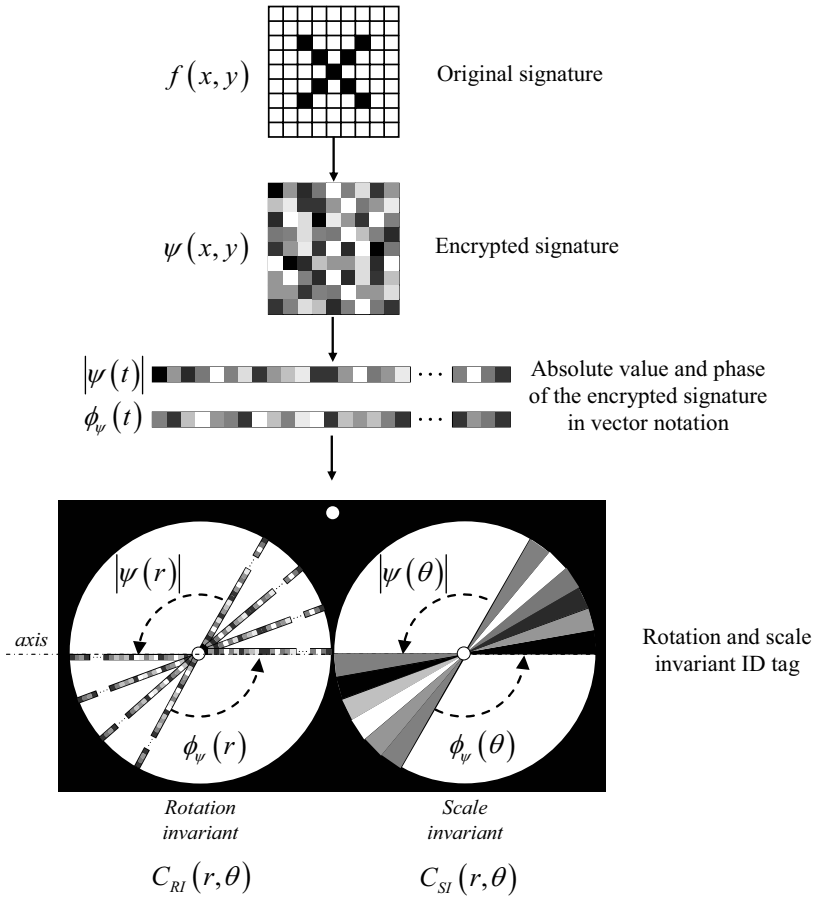


Fig. 4. Synthesis of a distortion (rotation and scale)-invariant ID tag.

Rotation invariance is achieved in one circle (on the left in Fig.4) by writing $\psi(t) = \{|\psi(t)|, \phi_\psi(t)\}$ 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. 4).

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

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

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. (2), 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.4) by writing $\psi(t) = \left\{ \left|\psi(t)\right|, \phi_\psi(t) \right\}$ in the angular direction: magnitude vector $\left|\psi(t)\right|$ 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. 4).

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

$$C_{SI}(r,\theta) = \begin{cases} \left|\psi(\theta)\right|, & for\ \theta = (1...N)\left(\frac{\pi}{N}\right), \forall r \in (R_0, R_L] \\ \phi_\psi(\theta), & for\ \theta = (N+1...2N)\left(\frac{\pi}{N}\right), \forall r \in (R_0, R_L]. \\ V_{\max}, & for\ r \le R_0 \quad (white\ central\ dot) \end{cases} \tag{3}$$

In Eq. (3), 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. (2) and (3). 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 4 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 $\left|\psi(t)\right|$ 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. 3. 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 (Fig. 5). In each circle, the border between the regions where $\left|\psi(t)\right|$ 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 $\left|\psi(t)\right|$ is written (upper semiplane). The other semiplane corresponds to function $\phi_\psi(t)$ (bottom semiplane). The 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, 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 $\left|\psi(t)\right|$, 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 prior to decoding the signature $\psi(x,y)$ by using the decryption technique.[4] Following this procedure, the encrypted signature will be recovered whether the ID tag is captured in its original orientation or its rotated format.

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. 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 signature is written in matrix notation and complex valued function $\psi(x,y)$ and decrypted. Then, the optical code will be recovered even if the ID tag is captured in its original size or scaled.

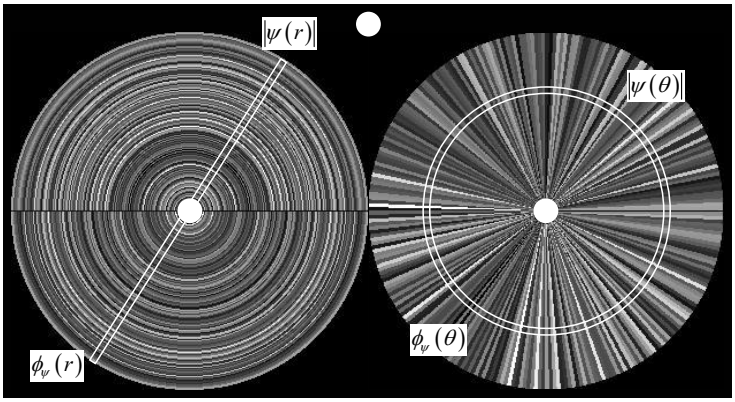
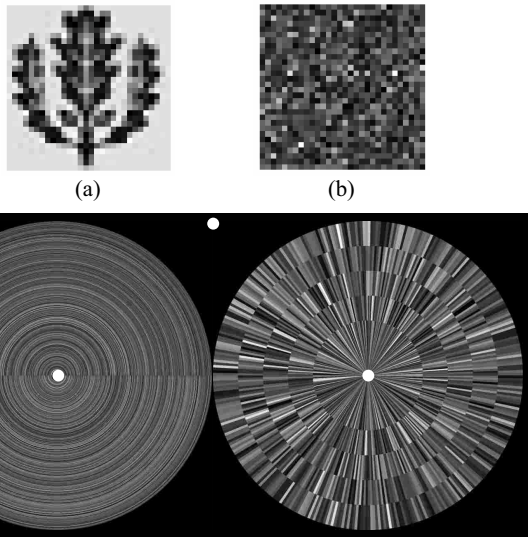


Fig. 5. Rotation and scale invariant recovering the encrypted signature from the optical code of the ID tags of Fig.4.

For encrypted signatures with a large number of pixels, 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. 6). 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.



(a) (b)

(c)

Fig. 6. Example of distortion-invariant ID tag built from an encrypted signature with a large number of pixels. (a) Original signature $f(x,y)$; (b) Encrypted signature ψ(x,y); and (c) Distortion-invariant ID tags. The information of the optical code in the scale-invariant tag is distributed in concentric circles.

4. AUTHENTICATION RESULTS

In this section, numerical results are obtained to demonstrate the feasibility of the proposed distortion-invariant ID tag. The signature used to verify the identification system is shown in Fig. 6a and its encrypted image, computed by using the double phase encoding technique, is shown in Fig. 6b. 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 (Fig. 6c).

4.1 Rotation-invariant detection

First, we test the rotation invariance of the verification system that detects the ID tag shown in Fig. 6c. 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 are obtained by using the double phase decryption technique.[4] Some of these decrypted signatures are depicted in Fig. 7.

Fig. 7 Decoded signatures from rotated versions of the distortion-invariant ID tag shown in Fig. 6c.

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, instead of the mean value as in previous papers,[3,28,29] 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. 6a), by using a correlation-based processor. An example of identification results is plotted in Fig. 8. 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 compromise between distortion-tolerance and peak sharpness. The ration *cc/ac* is also displayed in Fig. 8. The high and sharp peak indicates the authentication of the signature.

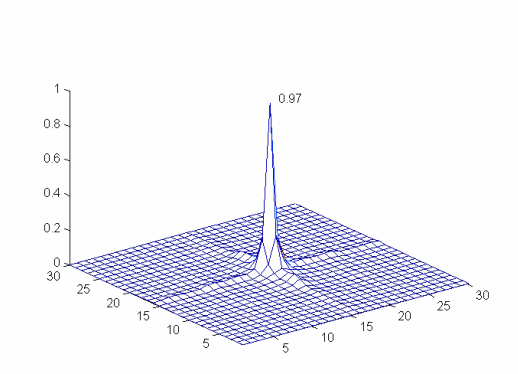


Fig. 8. Normalized output plane for the decoded signature obtained from a rotated version (80 degrees) of the ID tag (Fig. 6c). Parameter k=0.5 is used.

4.2 Scale-invariant detection

Invariance to scale variations is tested by using the other circle of the distortion-invariant ID tag shown in Fig. 6c. 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. 9. The quality of the recovered signature is visually acceptable in nearly all 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 small scale factors lower than 0.3 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.

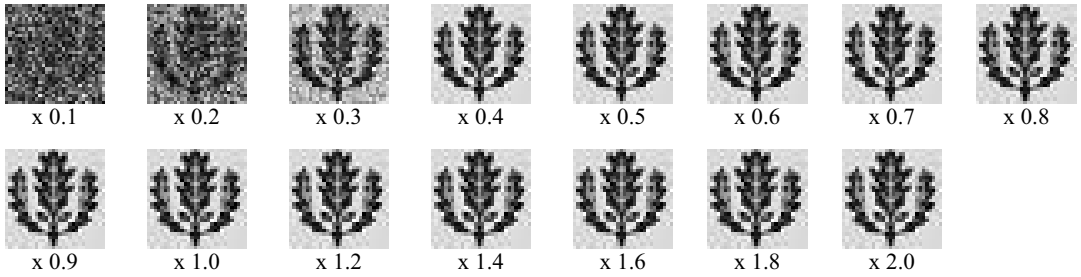
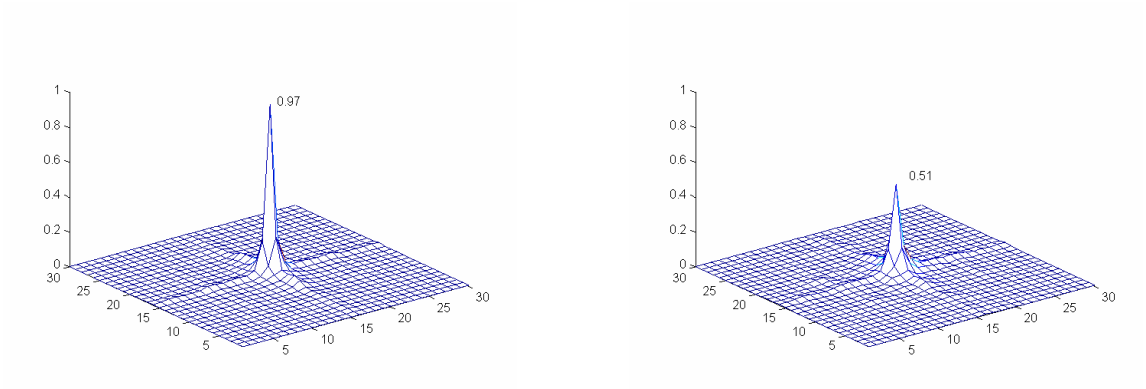


Fig. 9. Decoded images for scaled versions of the distortion-invariant ID tag shown in Fig. 6c.

Nonlinear correlation of the decoded images with the stored reference signal (Fig. 6a) is used to evaluate the image quality of the recovered signatures. Fig. 10 shows the normalized output planes for two decoded images obtained from scaled versions (scale factors 0.4 and 0.2, respectively) of the ID tag of Fig. 6c. 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 scale by a factor 0.4 (Fig.10a). For a scale factor of 0.2 (Fig. 10b), a lager amount of noise occurs and this fact is responsible for the decrease of the ratio *cc/ac*. However, a sharp peak projects over the flat background and permits the identification.

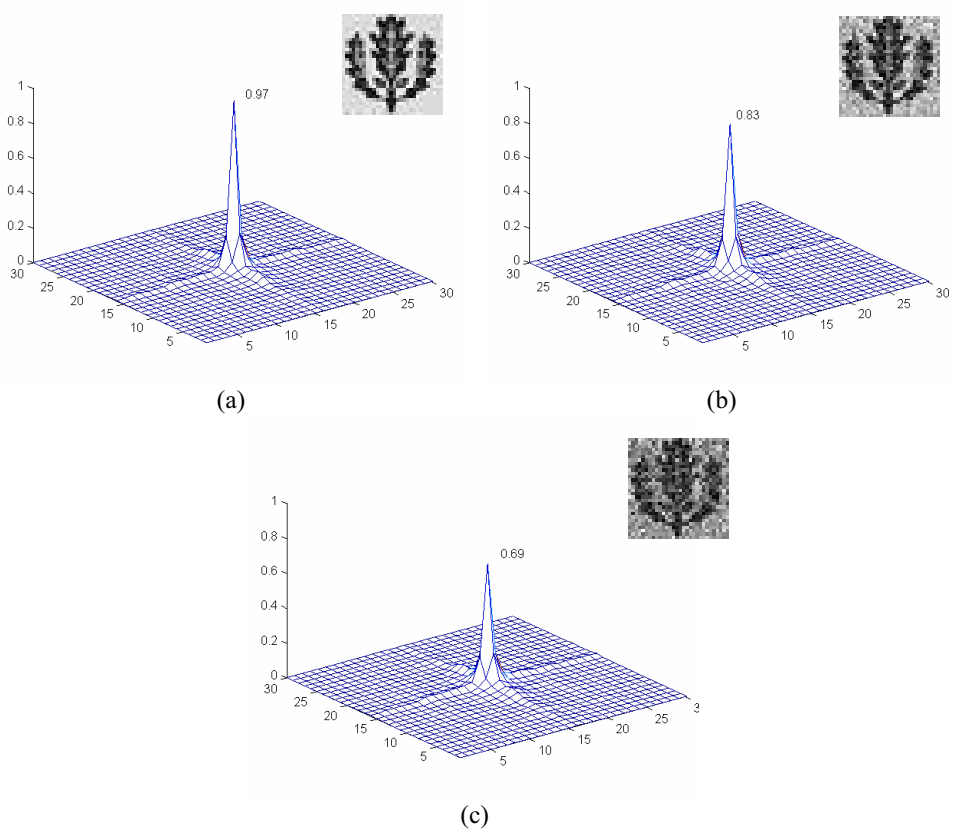


(a) (b)

Fig. 10. Normalized output planes for the decoded signatures obtained from rotated version of the ID tag (Fig. 6c). Parameter k=0.5 is used. The ID tag was scaled by a factor (a) 0.4, and (b) 0.2.

4.3 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 11 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. 6c. 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 distortion.



(a) (b)

(c)

Fig. 11. Decoded signatures and correlation outputs (k=0.5) for simultaneously rotated and scaled versions of the ID tag shown in Fig. 6c. (a) Scale factor: x 0.6 and rotation angle: 40º; (b) Scale factor: x 0.5 and rotation angle: 60º; (c) Scale factor: x 0.4 and rotation angle: 70º.

To demonstrate the robustness of the ID tags for verification and identification, let us recover the decrypted information from a rotated (40 degrees) and scaled (0.6 scale factor) ID tag, and let us decrypt the encoded information by using a false phase key. As a result, we obtain a noisy image where no signature can be recognized (Fig. 12).

It is also important to demonstrate that a different signature, even if it is correctly decrypted with the appropriated phase key, will not be recognized as the reference image. Figure 13 presents the decoded signature corresponding to a different logo, and the corresponding correlation output with a low peak which is below the threshold. Thus, the decoded signature is discriminated from the authentic one (Fig. 6a) used in the previous experiments.

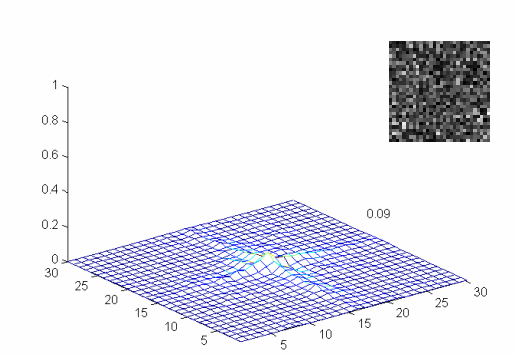


Fig. 12. Decoded image by using a false key and correlation output for k=0.5. The ID tag was rotated 40 degrees and scaled by a factor of 0.6.

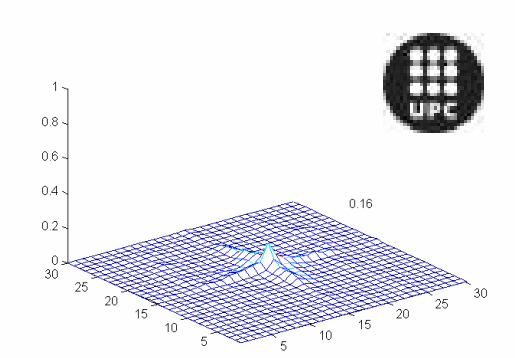


Fig. 13. Decoding a different signature with the correct phase key. The ID tag was rotated 40 degrees and scaled by a factor of 0.6. Correlation output for k=0.5 when the decoded image is compared with the stored reference image (Fig. 6a).

5. 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 double phase 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.)

The designed ID tag can be located on a given object, and is captured by a receiver, which will decode and verify the information. The signature is a characteristic image that allows identification of the object. 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 if the ID tag is rotated, scaled, or both rotated and scaled simultaneously. The method used for encrypting the signature has been shown to be robust against using a different key for the decryption technique. Also, the receiver is able to discriminate between a reference signature and a different image by using correlation.

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. J. W. Goodman, *Introduction to Fourier optics*, 2nd. Ed., McGraw Hill, New York, 1996.
3. E. Pérez-Cabré, B. Javidi, *Scale and rotation-invariant ID tags for automatic vehicle identification and authentication*, IEEE Trans. on Vehicular Technology, Vol. 54, n. 4, 2005.
4. 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.
5. 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.
6. 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.
7. O. Matoba, B. Javidi, B., *Encrypted optical memory systems based on multidimensional keys for secure data storage and communications*, IEEE Circuits and Devices Magazine, vol. 16,, no. 5, pp. 8-15, 2000.
8. J. L. Turin, *An introduction to matched filters*, IRE Transactions on Information Theory, vol. IT-6, pp. 311-329, 1960.
9. B. Javidi, *Nonlinear joint power spectrum based optical correlation*, Appl. Opt., vol. 28, no. 12, pp. 2358-2367, 1989.
10. 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.
11. 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.
12. S. H. Hong, B. Javidi, *Optimum nonlinear composite filter for distortion-tolerant pattern recognition*, Appl. Opt., vol. 41, no. 11, pp. 2172-2178, 2003.
13. B. Javidi, J. L. Horner, *Real-time Optical Information Processing*, Academic Press, Boston, 1994.
14. *ATR Definitions and Performance Measures*, Automatic Target Recognizers Working Group (ATRWG) Publications, no. 86-001, 1986.
15. J. L. Horner, *Metrics for assessing pattern-recognition performance*, Appl. Opt., vol. 31, no. 2, pp.165-166, 1992.
16. B. V. K. Vijaya Kumar, L. Hassebrook, *Performance measures for correlation filters*, Appl. Opt., vol. 29, no. 20, pp. 2997-3006, 1990.
17. 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.
18. IEEE Trans. on Image Processing. Special issue on *Automatic Target Detection and Recognition*, vol. 6, no. 1. 1997.
19. B. Javidi, ed. *Smart imaging systems*, SPIE Press, SPIE, Bellingham, WA, 2001.
20. B. Javidi, ed., *Image recognition and classification: Algorithms, systems and applications*, Marcel Dekker, New York, 2002.
21. C. F. Hester, D. Casasent, *Multivariant technique for multiclass pattern recognition*, Appl. Opt., vol. 19, no. 11, pp. 1758-1761, 1980.
22. H. J. Caulfield, *Linear combinations of filters for character recognition: a unified treatment*, Appl. Opt., vol. 19, pp. 3877-3879, 1980.
23. 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.
24. 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.
25. B. Javidi, D. Painchaud, *Distortion-invariant pattern recognition with Fourier-plane nonlinear filters*, Appl. Opt., vol. 35, no. 2, pp. 318-331, 1996.
26. 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.
27. 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.
28. E. Pérez-Cabré, B. Javidi, *Distortion-invariant ID tags for object identification*, Proc. SPIE, vol. 5611, pp. 33-41, 2004.
29. 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.