Detection and authentication of objects by using distortion-invariant optical ID tags

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

ABSTRACT

Distortion-invariant identification (ID) tags are designed for remote identification and verification of objects. An optical code contained in an ID tag, placed in a visible part of an object, can be detected and verified by a remote receiver even if it captures a distorted version of the code due to in-plane rotations and variations in scale. In a general pattern recognition task, these distortions usually require to increase the level of complexity of the recognition system. We aim to use a less complex identification system that operates in real-time. Distortion-invariance is achieved by both multiplexing the information included in the ID tag and taking advantage of the topology of the tag.

For security purposes, double-phase encryption has already been shown as an appropriate technique to encode the information. By using double phase encryption, a signature is hidden in an encoded ID tag. Once the ID tag is captured by the receiver and is decrypted, a correlation-based processor verifies the decoded information with a previously stored reference signal.

The proposed system may have broad applications in transportation, in tasks such as the security control of authorized vehicles inside a restricted area, or in the control of objects for inventory purposes.

Keywords: Optical ID tags, distortion-invariant identification, double-phase encryption, object authentication

1. INTRODUCTION

Active and passive optical identification (ID) tags and readers were described to achieve real-time remote identification and verification of objects.[1]

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

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

Opto-Ireland 2005: Photonic Engineering, edited by B. W. Bowe, G. Byrne, A. J. Flanagan,
T. J. Glynn, J. Magee, G. M. O'Connor, R. F. O'Dowd, G. D. O'Sullivan, J. T. Sheridan, Proc.
of SPIE Vol. 5827 (SPIE, Bellingham, WA, 2005) · 0277-786X/05/$15 · doi: 10.1117/12.610224

identify the information included in the ID tag even when the optical code is captured rotated or from an unexpected location (Fig. 1).

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.

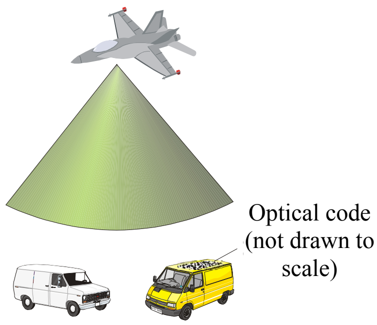
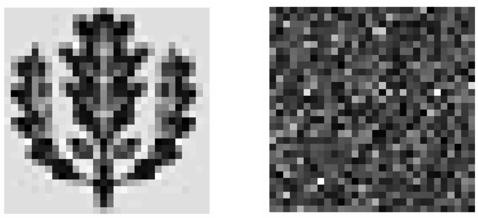


Fig. 1. Example of a distortion-invariant passive optical ID tag.

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. The codification process will follow a double phase encryption technique,[4] which allows us to encode a primary image into stationary white noise. One phase code is used in the input plane, and the second phase code 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. 2).



(a) (b)

Fig. 2. (a) Original signature $f(x,y)$; (b) Encoded information $\psi(x,y)$ by using the double-phase encryption technique.

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 phase code or encrypted signature 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.

Once the signature is captured by the receiver, it has to be decrypted. 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:

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

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. Another metric used in this work is the peak-to-correlation energy (PCE). This parameter usually indicates the sharpness and height of the output correlation peak. Thus, the higher the PCE value, the easier the detection of a given object.

3. DISTORTION-INVARIANT ID TAGS

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.

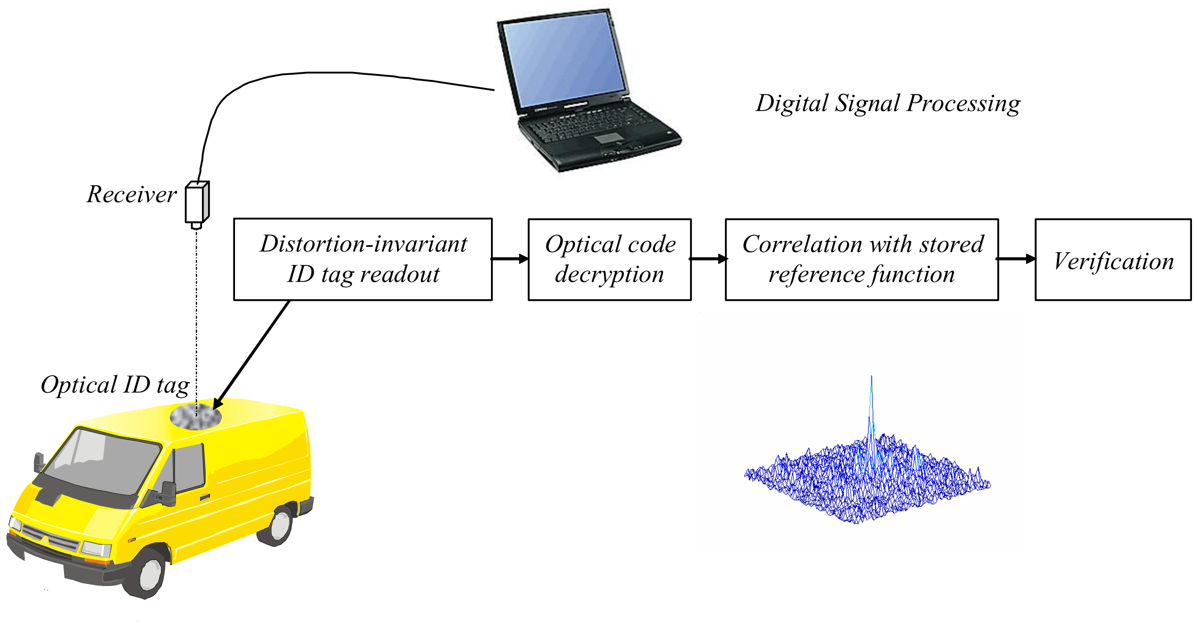


Fig. 3. Block-diagram of the remote identification system.

Let us describe the design of a rotation and scale-invariant ID tag. Similarly to a wedge ring detector, the information included in the ID tag is distributed in a circle in two ways. One region of the optical code will include the encrypted signature written in a radial direction and repeated angularly so that rotation-invariance could be achieved.[28] Another region of the optical code will correspond to the encrypted information written circularly and repeated in concentric semicircles. Therefore, in this second region 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.

More specifically, let us consider the encrypted signature $\psi(x,y)$ in vector notation $\psi(t)$ where t=1,2,...N, and N is the total number of pixels. Rotation invariance is achieved by writing $\psi(t)$ in the radial direction and repeating it angularly within one of the two semicircles of the optical code. For discrete matrices, we could write the Rotation-Scale Invariant ID tag function (C_{RSI}) as:[3]

$$C_{RSI}(m,n) = C_{RSI}\left(\left[\sqrt{(m-m_0)^2+(n-n_0)^2}\right]\right) = \psi(t) \qquad for\ (n-n_0)>0\,, \qquad (2)$$

where $[\cdot]$ denotes the nearest integer towards zero and (m_0,n_0) are the centre coordinates of $C_{RSI}(m,n)$.

The scale-invariant region of the ID tag is built by rearranging the information of the encrypted signature $\psi(t)$ written in vector notation, in sectors of a semicircle. In the case of discrete matrices, it will be:[3]

$$C_{RSI}(m,n) = C_{RSI}\left(\left[\frac{(N-1)}{2\pi}\left(\pi + arctg\left(\frac{n-n_0}{m-m_0}\right)\right)\right]\right) = \psi(t) \qquad for\ (n-n_0)\le 0\,. \qquad (3)$$

Figure 4 depicts the procedure followed to obtain this distortion-invariant ID tag.

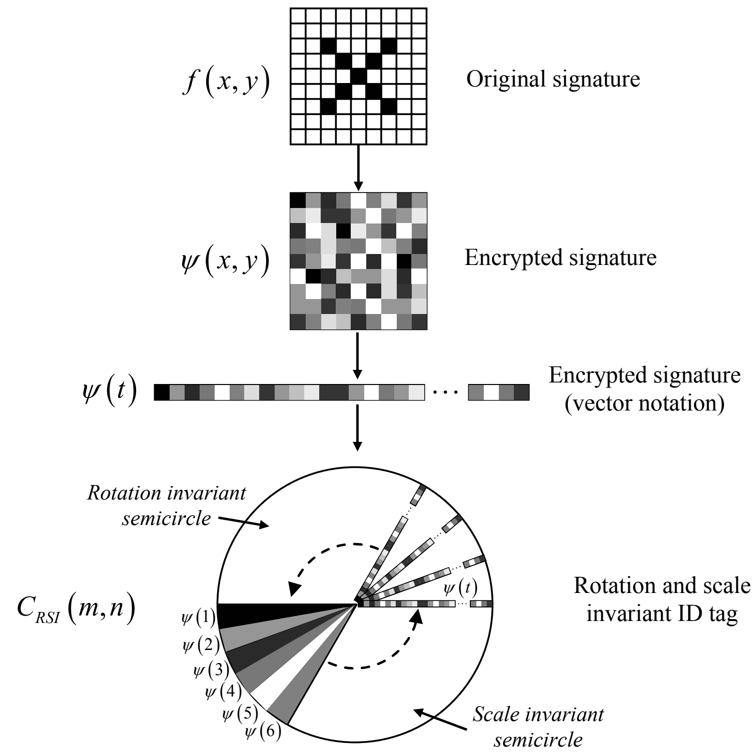


Fig. 4. Synthesis of a distortion (rotation and scale)-invariant ID tag.

Encrypted information is recovered by the following procedure.[3] First, it is necessary to detect the border between the rotation-invariant region and the scale-invariant region. This is achieved by computing the gradient over the radial direction of the ID tag for different angles. For the semicircle which includes the rotation-invariant tag, changes in the radial direction are noticeable, whereas, for the scale-invariant tag, the gradient is ideally null in the radial direction. Gradient differences permit the determination of the angle for which the ID tag changes from a rotation-invariant region to a scale-invariant region.

Once the border between the rotation-invariant area and scale-invariant area is detected, the signature in vector notation $\psi(t)$ can be decoded by reading out the information of the optical code either from the rotation-invariant region or the scale-invariant region.

From the rotation-invariant region, the optical code could be read out in any radial direction, from the center to the exterior of the code. Not only is a single code read along a unique radial direction for decoding, but a mean 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 scale-invariant region, the encrypted signature in vector notation $\psi(t)$ is recovered by reading out the pixels of the ID tag in circular sectors. To minimize errors in the reading process, not only is one pixel taken into account for each circular sector, but a mean value of pixels located in the same sector in the radial direction. Afterwards, the signature is written in matrix notation $\psi(x,y)$ and decrypted. Then, the optical code will be recovered even if the ID tag is captured in its original size or scaled.

For encrypted signatures with a large number of pixels, information of the scale-invariant ID tag could be distributed by using different concentric semicircles to assure a minimum number of pixels for each sector to recover the information properly. Consequently, the tolerance to scale variation is affected in accordance to the number of concentric circles used in the ID tag. The procedure to recover the encrypted signature would be the same except for we should take into account the size of the concentric circles. When various semicircles are used in the code, the gradient procedure to detect the border between the rotation invariant and the scale invariant region is applied only to the most external concentric semicircle.

If we consider a real image (for instance, the signature of Fig. 2a and its encrypted version shown in Fig. 2b), the distortion-invariant ID tag synthesized following the described procedure is shown in Fig. 5.

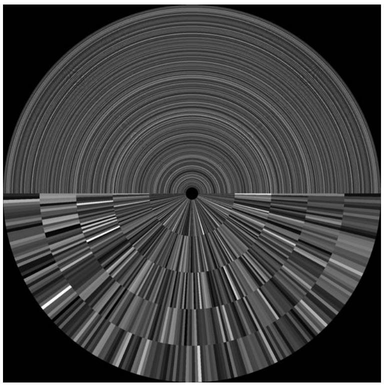


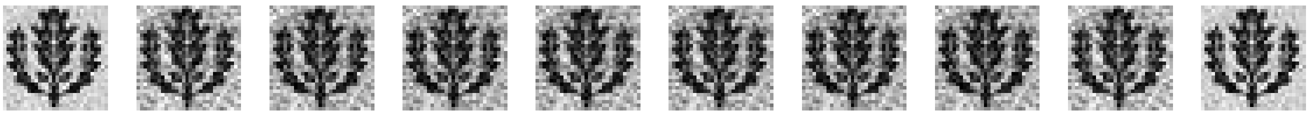
Fig. 5. Example of distortion (rotation and scale)-invariant ID tag built from the encoded signature of Fig. 2b. The information of the optical code is distributed similarly to a wedge ring detector.

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. 2a and its encrypted image, computed by using the double phase encoding technique, is shown in Fig. 2b. The rotation and scale-invariant ID tag (Fig. 5) is synthesized from this encoded information by following the procedure described in section 3.

4.1 Rotation-invariant detection

First, we test the rotation invariance of the verification system that detects the ID tag shown in Fig. 5. 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 semicircle 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. 6.



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

Fig. 6 Decoded signatures for rotated versions of the distortion-invariant ID tag shown in Fig. 5.

Signatures are correctly decoded in all the cases even though some noise is overlapping with the recovered images. To verify whether the object is an authorized signal, the recovered signatures must be compared with a previously stored reference signal (Fig. 2a). The recognition results obtained using a correlation-based processor are plotted in Fig. 7. The *cc*/*ac* ratio is displayed versus the rotation angle of the captured ID tag. Different degrees of nonlinearity are applied to compare their corresponding recognition results. Value of $k = 1$ stands for linear correlation, which corresponds to a more distortion-tolerant system. Thus, *cc*/*ac* remains nearly constant and close to unity for different rotation angles of the ID tag (solid line in Fig. 7).

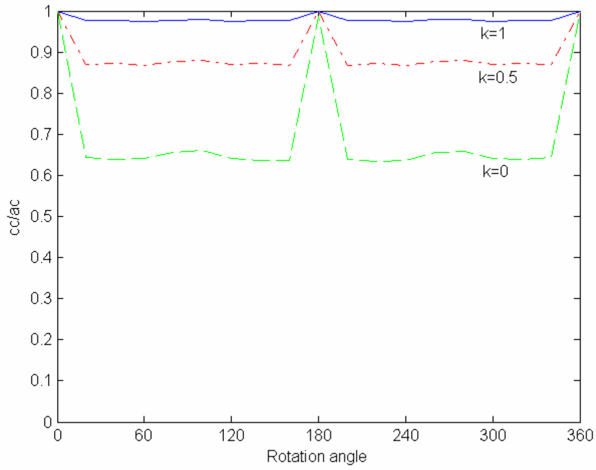


Fig. 7. *cc/ac* versus rotation angle for the rotation and scale-invariant ID tag (Fig. 5).

Value of $k = 0$ corresponds to a recognition system with a high discrimination capability because small changes in the analyzed image are detected and this implies that the *cc*/*ac* ratio decreases rapidly (dashed line in Fig. 7). Nevertheless, the intensity of the correlation peak is high enough to identify the signature and to discriminate it from a different object. Finally, intermediate values of k, such as $k = 0.5$, are tested. In this case, the system has an intermediate behavior between the two aforementioned extreme cases (dash-dot line in Fig. 7).

It is necessary to remark that for all the nonlinearities tested, the ratio *cc*/*ac* has its maximum values for rotation angles of 0º and 180º. This is due to the fact that for these angles, interpolation algorithms are not needed to digitally rotate an image.

Figure 8 plots *PCE* values versus rotation angle for the same degrees of nonlinearity considered before. *PCE* values obtained for k=0 are significantly higher than those obtained for the other nonlinearities. From the graphs plotted in Fig. 8, we conclude that the correlation peak sharpness increases for lower values of k, and/or the output noise floor decreases.

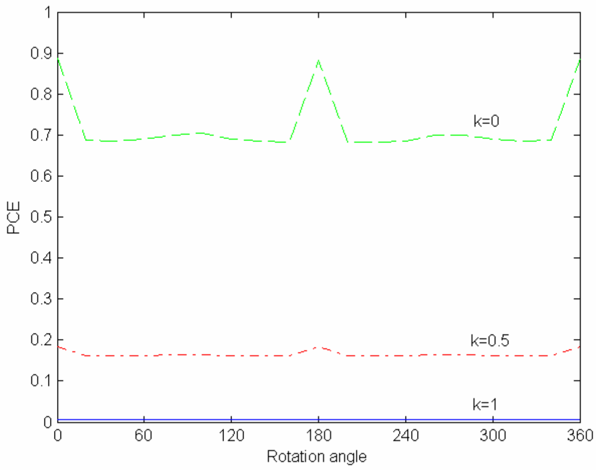


Fig. 8. PCE versus rotation angle for the rotation and scale-invariant ID tag (Fig. 5).

If both results, *cc/ac* and PCE, are taken into account (Figs. 7 and 8) it is necessary to achieve a compromise between distortion-tolerance and peak sharpness. Thus, intermediate values of *k* lead to obtain a trade off.

4.2 Scale-invariant detection

Invariance to scale variations is tested by using the distortion-invariant ID tag shown in Fig. 5. 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. When the ID tag is captured from a long distance (that is, if small scale factors lower than 0.6 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.

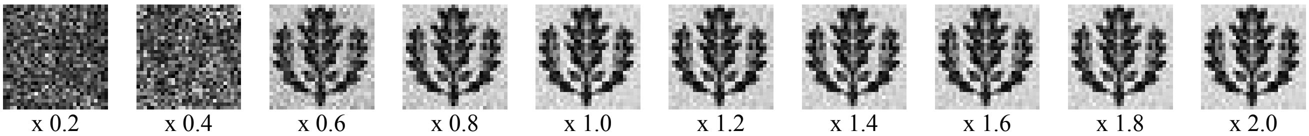


Fig. 9. Decoded images for scaled versions of the distortion-invariant ID tag shown in Fig. 5.

Nonlinear correlation of decoded images with the stored reference signal (Fig. 2a) is used to evaluate the image quality of the recovered signatures. Fig. 10 shows the variation of the *cc*/*ac* ratio versus the scale factor of the ID tag for different nonlinearities. As in the rotation-invariant case, the degree of tolerance of the receiver against scale variations can be adjusted by tuning the parameter *k*. Value of *k*=1 corresponds to the most tolerant system, for which the ratio *cc*/*ac* remains nearly constant for all the scale factors. It decreases for smaller scale factors (<0.6), which correspond to signatures not properly recovered.

On the contrary, for *k*=0 a highly discriminant processor is obtained and *cc*/*ac* values decrease rapidly when the ID tag is captured from a large distance (scale factor ≤0.6). Intermediate values for parameter *k* permits tunable behavior.

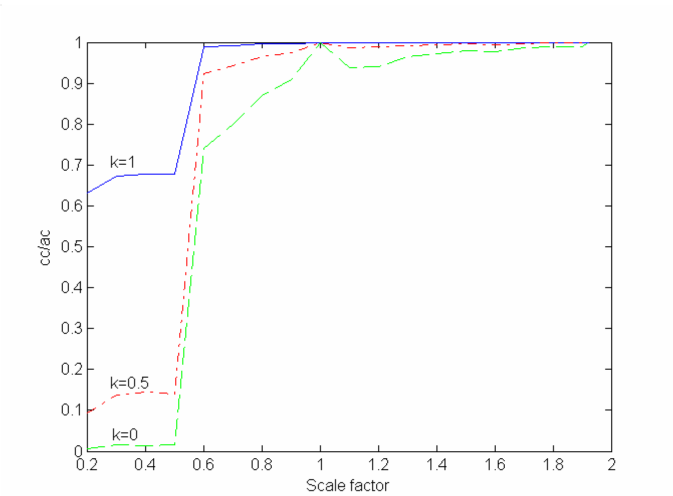


Fig. 10. *cc/ac* versus scale factor for the rotation and scale-invariant ID tag (Fig. 5).

Figure 11 shows the variation of *PCE* for different scale factors and nonlinearity strengths. High *PCE* values are obtained for *k*=0 and scale factor above 0.6 and they differ significantly from the results obtained for the other nonlinearities (*k*=0.5 and *k*=1).

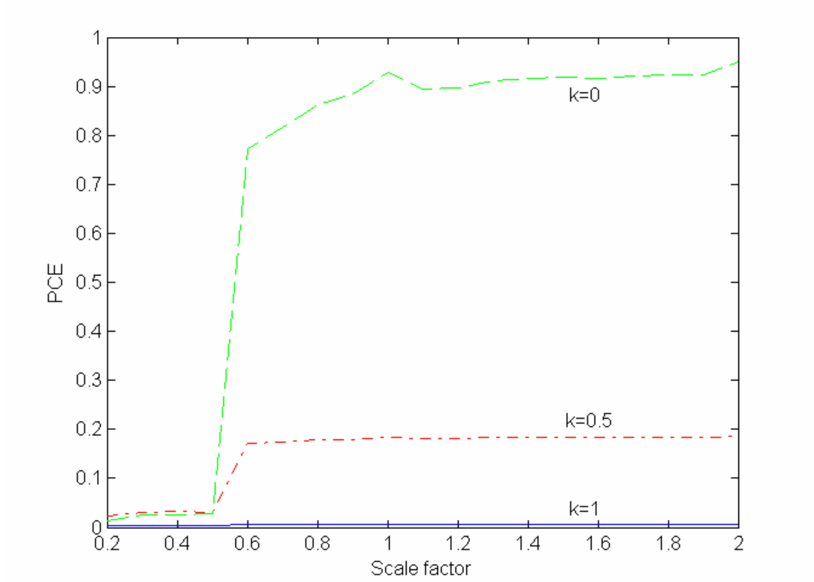


Fig. 11. PCE versus scale factor for the rotation and scale-invariant ID tag (Fig. 5).

From the analysis carried out and presented in Figs. 10-11, an intermediate value of *k* (such as *k*=0.5) seems to be a good compromise to achieve a well balanced processor.

4.3 Integrated rotation and scale-invariant

Finally, the identification system is tested against rotation and scale distortion appearing simultaneously in the captured ID tag. Figure 12 displays the output plane of the recognition system along with the decoded signature obtained for a rotated (80 degrees) and scaled version (scale factor 0.7) of the ID tag shown in Fig. 5. The signature has been correctly decoded and identified by using *k*=0.5 for correlation.

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 (0.8 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. 13).

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 14 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. 2a) used in the previous experiments.

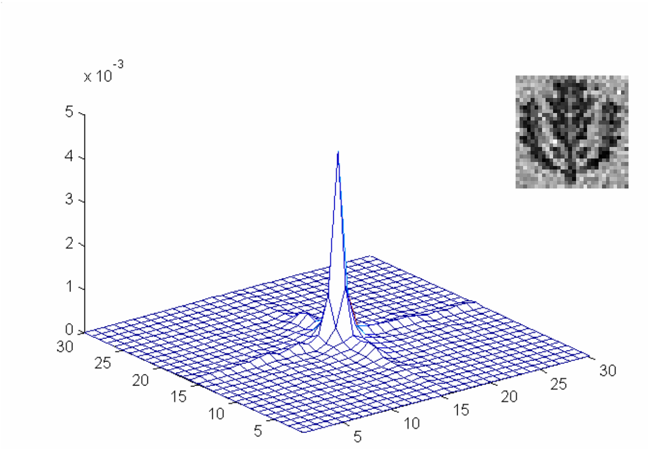


Fig. 12. Decoded signature and correlation output (k=0.5) for a simultaneously rotated and scaled version of the ID tag shown in Fig. 5. Scale factor: x 0.7 and rotation angle: 80º.

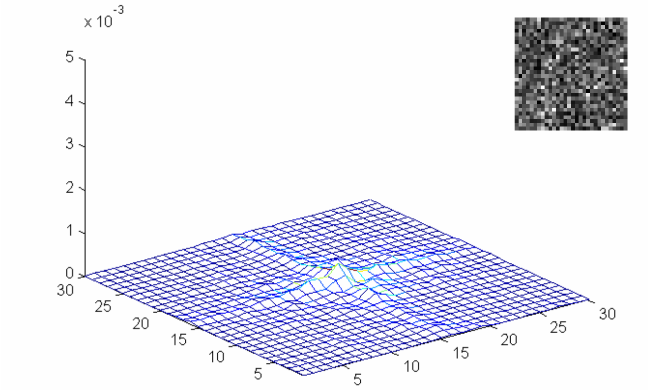


Fig. 13. Decoded image by using a false key and correlation output for k=0.5. The ID tag was rotated 40 degrees and scaled by a factor of 0.8.

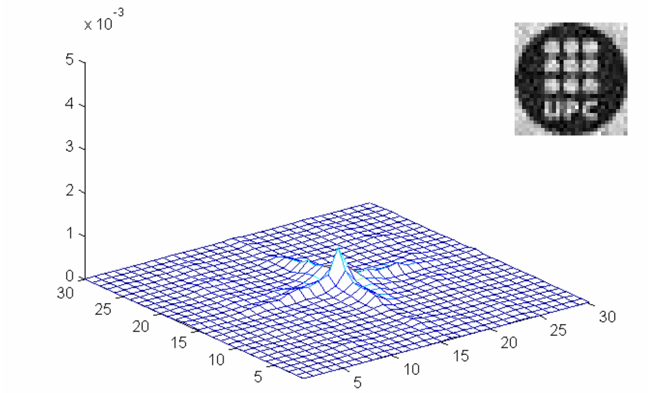


Fig. 14. Decoding a different signature with the correct phase key. The ID tag was rotated 40 degrees and scaled by a factor of 0.8. Correlation output for k=0.5 when the decoded image is compared with the stored reference image (Fig. 2a).

5. CONCLUSIONS

We have presented a method to encode an encrypted signature into an ID tag to provide distortion invariance. 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.

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.

Other distortion-tolerant techniques can be studied. However, the main advantage of the proposed method is its simplicity. Further work should analyze the influence of noise, cluttered background and the effect of atmospheric turbulences during the capturing process of the receiver.

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, 2005. (Accepted for publication).
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.