Distortion-invariant ID tags for object identification

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

ABSTRACT

Active and passive optical identification (ID) tags and readers for remote identification and verification of objects are described. We focus our attention on the design of passive ID tags to achieve distortion-invariant authentication of the information included in the optical tag. A passive ID tag will consist of an optical phase code which can be placed in a visible part of an object for remote detection. We aim to authenticate the object even if the reader captures a distorted version of the code due to in-plane rotations. Distortion-invariance is achieved by both multiplexing the information included in the ID tag and the topology of the tag. For security purposes, double-phase encryption has already been shown as an appropriate technique to encode information. By using double-phase encryption, a signature is hidden in a phase-encoded ID tag not visible by visual inspection. Once the ID tag is captured by the reader 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, homeland security, and inventory control.

Keywords: ID tags, remote object identification, distortion-invariance recognition, double-phase encryption, correlation

1. ACTIVE AND PASSIVE IDENTIFICATION TAGS

Optical identification (ID) tags has been introduced to achieve real-time remote identification and verification of objects.[1] Active and passive optical ID tags and readers were described. As an active imaging system, a wavelength-hopped laser encoding and decoding system (Fig. 1) was proposed.[1] A commercially available high speed wavelength tunable laser may be used to generate an optical code by varying the transmitted wavelength. An electronic code assigned to authenticate a particular remote object can be used to produce a specific sequence of output optical waveforms with a unique set of different wavelengths. The tunable laser coupled with a flexible and thin single mode fiber can broadcast the beam. Multiple fiber optic links can be used to guide the light to the different areas of the object (for instance, vehicle identification by aircraft or land transportation inspection). By using a collimating GRIN lens attached at the end of the fiber, it is possible to uniformly illuminate the receiver. The transmitted optical waveforms are focused onto a fiber by a lens such as GRIN. The fiber is connected to a wavelength sensitive optical component such as a diffraction grating to deflect the received optical beam according to its wavelength sequence. A photo-detector array detects the diffracted light to reproduce the wavelength hopped spread spectrum sequence as a function of time. A correlator[2] will verify the authenticity of the code as a function of its spectral and temporal contents.

A different option is the use of passive retro-reflective optical ID tags.[1] An optical phase code manufactured with retro-reflective materials can be inspected with a reader to verify the authenticity of the object (Fig. 2). Not only can be a identification number stored in the phase tag but also a vehicle image, type, category, model, year, etc. The verification system that reads the phase-encoded identification tag can be a correlator.[2] The optical tag to be verified is imaged onto the input plane, and compared with a stored reference function. An intensity peak in the output plane will be used to decide whether the object is authenticated or not. Active imaging optics may be used for compensating environmental degradations, such as variations in scale, rotations, changes in illumination, noise/clutter suppression, etc. These effects can be taken into account in the recognition process.[3]

Active or passive ID tags can provide different benefits depending on the task for which 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. Combining the high level of data storage of optically encoded materials with the free space

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

(SPIE, Bellingham, WA, 2004)0277-786X/04/$15 · doi: 10.1117/12.582093

identification possibilities of active imaging systems offers an attractive solution for remote security, identification, verification and location of objects.

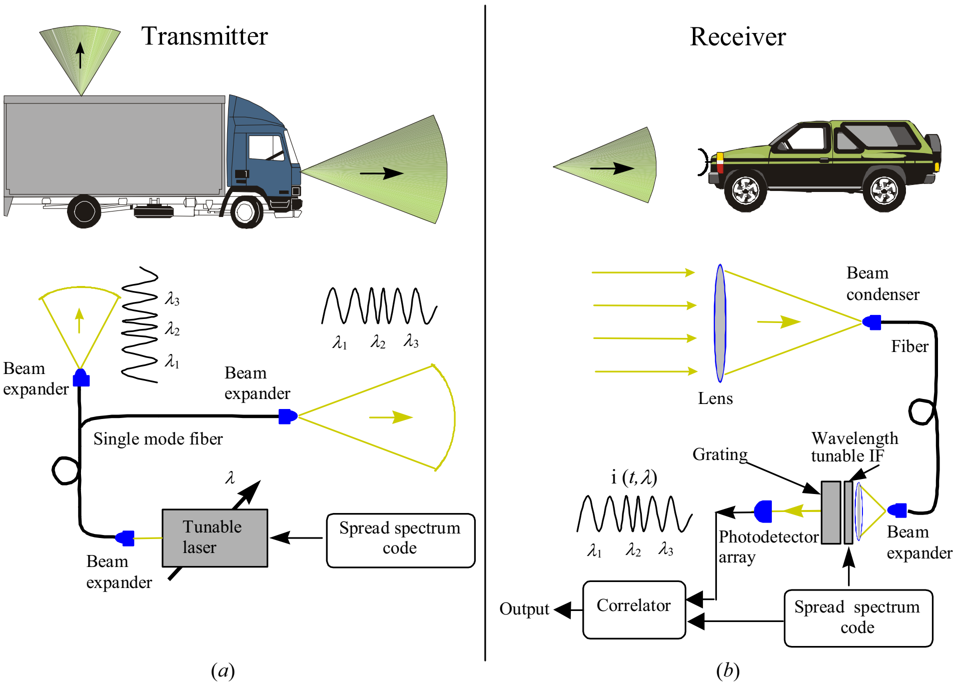

Fig. 1. Active imaging system. Laser tagging based on wavelength division multiplexing. (a) Code generation by tuning the emitted wavelength and its transmission. (b) Code verification by the receiver.

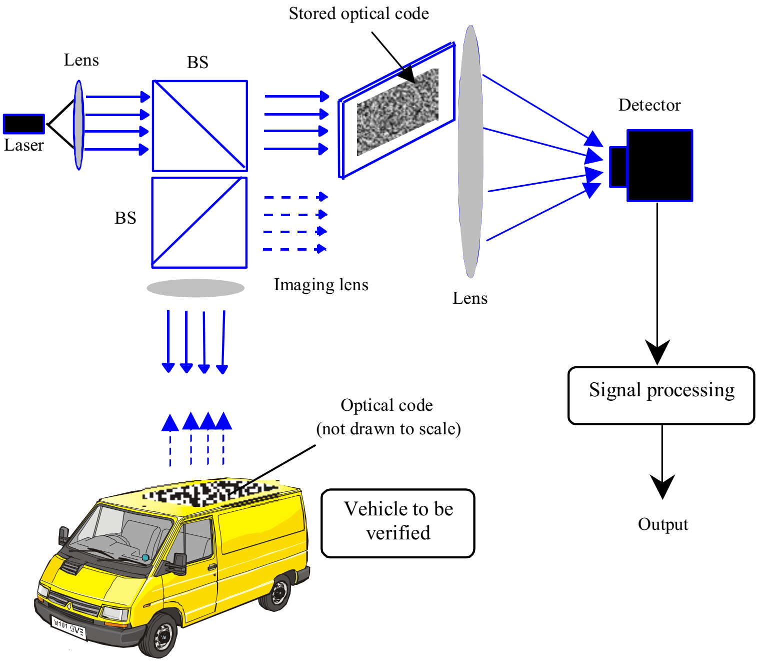

Fig. 2. Passive optical ID tag. Tagging based on retro-reflective optical phase code. Verification by using a correlator.

In this work, we focus our attention on passive optical tags. Description of the complete processor is provided. The effects of in-plane rotation are taking into account in order to achieve the verification of an object even though its optical ID tag is captured under this type of distortion.

2. SECURITY AND VERIFICATION OF PASSIVE 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 to identify a given object. The codification process will follow a double phase encryption technique,[4] which allows encoding a primary image into stationary white noise (Fig. 3). By using double phase encryption, the signature will be hidden in a phase-encoded ID tag not visible by visual inspection.

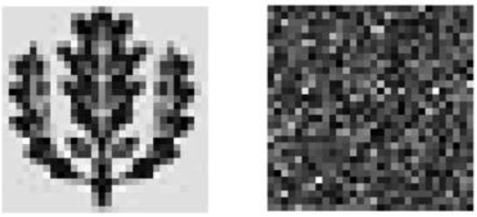

Fig. 3. (a) Original signature *f*(*x*,*y*); (b) Encoded information $\psi(x,y)$ (amplitude) by using the double-phase encryption technique.

Image encryption is achieved by using two random phase codes that 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 *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. 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 $exp[i2\pi p(x,y)]$. Then, this product is convolved by the impulse response *h(x,y)* which has a phase-only transfer function, $H(\mu,\nu) = exp[i2\pi b(\mu,\nu)]$, denoted as Fourier plane phase mask. Thus, the encrypted information, $\psi(x,y)$, is given by the following equation:

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

where * denotes the convolution operation. The encoding method can be implemented optically or electronically. In either case, the complex-amplitude encoded image, $\psi(x,y)$, must be represented with both amplitude and phase.

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

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

Finally, multiplication by the phase mask $exp[-i2\pi p(x,y)]$ will recover *f(x,y)*. Alternatively, because *f(x,y)* is real and positive, the signature may be recovered by computing the magnitude of $f(x,y)\ exp[i2\pi p(x,y)]$ 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 $exp[i2\pi b(\mu,\nu)]$, referred to as key, is used for the decryption.

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 cipher gray-scale images appropriate for optical tags without conversion to binary signatures which is the case for XOR encryption with a stream of pseudo random key.

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.

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 $f(x,y)$ with a previously stored reference signal $r(x,y)$. Comparison of these two functions is 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. Correlation plane 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 $\phi_F(\mu, \nu)$ and $\phi_R(\mu, \nu)$ denote their phase distribution in the frequency domain. According to this notation, nonlinear correlation is obtained by using the equation:

$$c(x,y) = IFT\left\{\left|F(\mu,\nu)R(\mu,\nu)\right|^k \exp\left[i\left(\phi_F(\mu,\nu)-\phi_R(\mu,\nu)\right)\right]\right\}. \qquad (3)$$

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. Optimum nonlinear transformations can be obtained to enhance the detection process by optimizing a performance metric.[10] We use k'th-law nonlinearity for computational efficiency.

Correlation-based detection is feasible when an output peak above a noise floor is obtained. Performance of the processor should be evaluated by using different metrics. The metrics that are taken into account in this work are well-known parameters described in the literature.[11-14] 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 is, the easier the detection of a given object becomes.

3. DISTORTION-INVARIANT ID TAGS

Different contributions can be found in the literature that deals with distortion invariant systems for a wide variety of purposes.[15-24] In general, sophisticated methods are needed to achieve tolerance to different distortions simultaneously. Information of several distorted views of a given target could be included in the filter design to obtain a distortion-tolerant system. Number of considered distortions usually increases the level of complexity of the recognition system. In this work, distortion-invariance is achieved by both multiplexing the information included in the ID tag and the topology of the ID tag. This procedure permits to reduce the system complexity.

We aim to design a novel passive optical ID tag which will be detected and verified even if the receiver captures a distorted version of the code. As an example, we consider a vehicle identification task. Let us suppose that there is a camera placed over a road intersection, so that the phase code can be always captured from the same distance but vehicles may approach from different angles. In such a situation, the ID tag will be distorted only by in-plane rotations.

Apart from introducing a novel design of the passive ID tag, the identification system keeps the encryption of the signature to increase security and the correlation-based processor to verify the information. Thus, a complete diagram of the proposed remote authentication system is depicted in Fig. 4. 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.

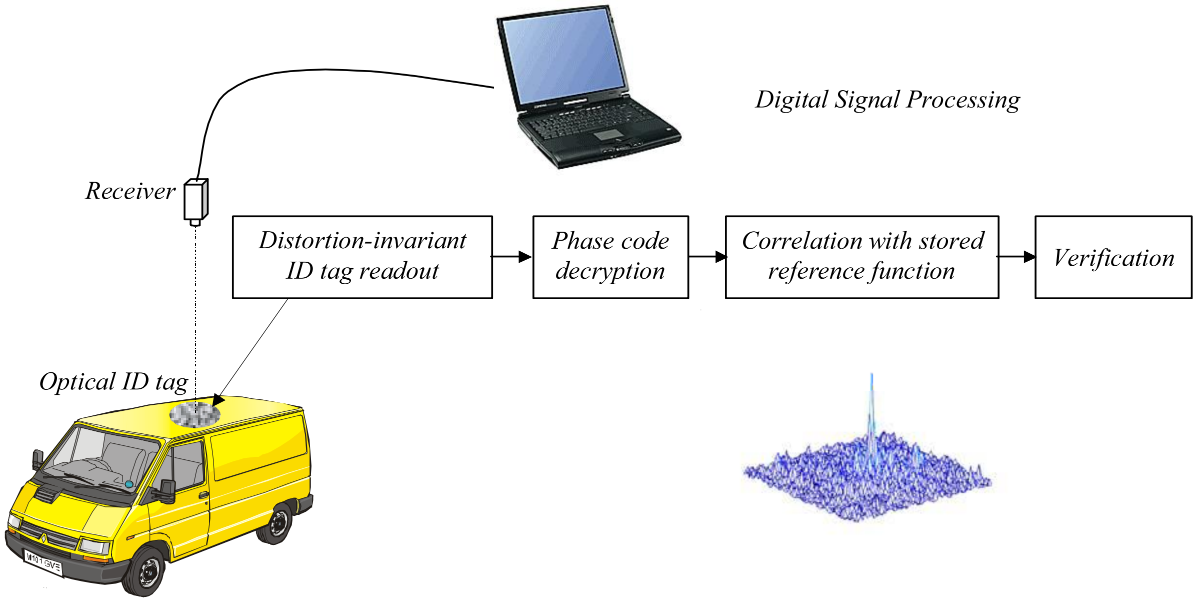
Digital Signal Processing
Receiver
Distortion-invariant ID tag readout
Phase code decryption
Correlation with stored reference function
Verification
Optical ID tag

Fig. 4. Block-diagram of the remote identification system.

3.1. Design of a rotation-invariant ID tag

Let us suppose that the receiver is fixed in a given position (e.g. receiver above a road intersection) and captures the codes located at the roofs of the vehicles coming from different directions. In this situation, the phase codes are always going to be captured at the same scale but distorted by in-plane rotations. Thus, the ID tag needs to be rotation-invariant.

The encrypted signature $\psi(x,y)$ is considered 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. Figure 5 displays an example of C_{RI} as a rotation-invariant ID tag.

Once the receiver captures this ID tag from a given distance, the signature in vector notation $\psi(t)$ can be decoded by reading out the information of the phase code in any radial direction, from the center to the exterior of the code. Not only is a single radius taken into account for decoding, but a mean value from several radii 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. Following this procedure, the encrypted signature will be recovered whether the ID tag is captured in its original orientation or its rotated format.

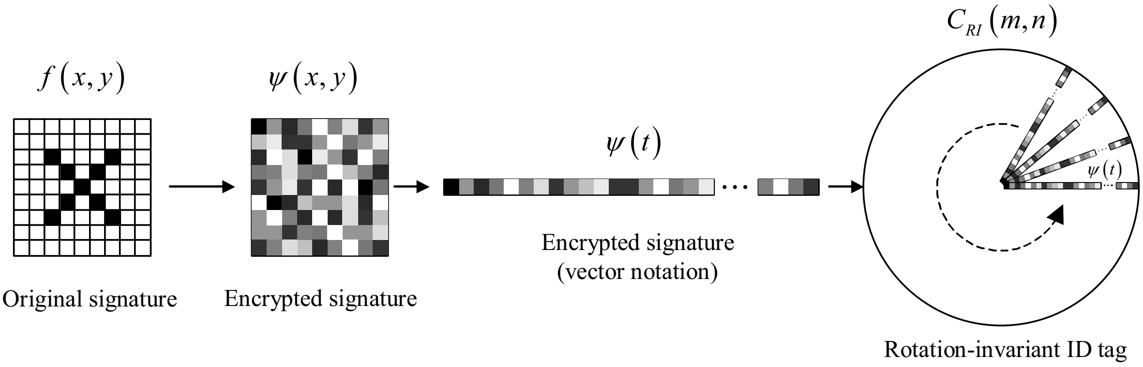

Fig. 5. Synthesis of a rotation-invariant ID tag.

4. AUTHENTICATION RESULTS

Numerical results are carried out to demonstrate the feasibility of the proposed distortion-invariant ID tag. The signature used to verify the identification system is shown in Fig. 3a and its encrypted image, computed by using the double phase encoding technique, is shown in Fig. 3b. A rotation-invariant ID tag (Fig. 6) is synthesized from this encoded information by following the procedure described in section 3.

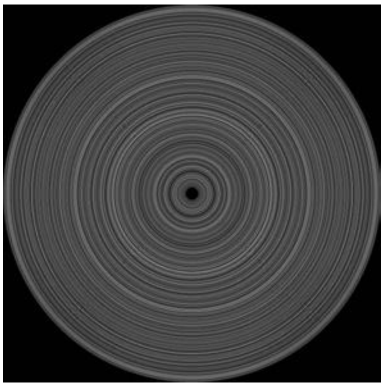

Fig. 6. Rotation-invariant ID tag built from the encoded signature of Fig. 3b.

4.1 Rotation-invariant detection

We test the rotation invariance of a verification system that deals with the ID tag shown in Fig. 6, which is designed to achieve rotation invariance. 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 following the procedure described in section 3, and decrypted signatures are obtained by using the double phase decryption technique. The decrypted signatures are depicted in Fig. 7.

Signatures are correctly decoded in all the cases even though some noise is overlapping with the recovered images. To verify whether the vehicle is an authorized signal, recovered signatures should be compared with a previously stored reference signal (Fig. 3a). Recognition results using a correlation-based processor are plotted in Fig. 8. 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. 8).

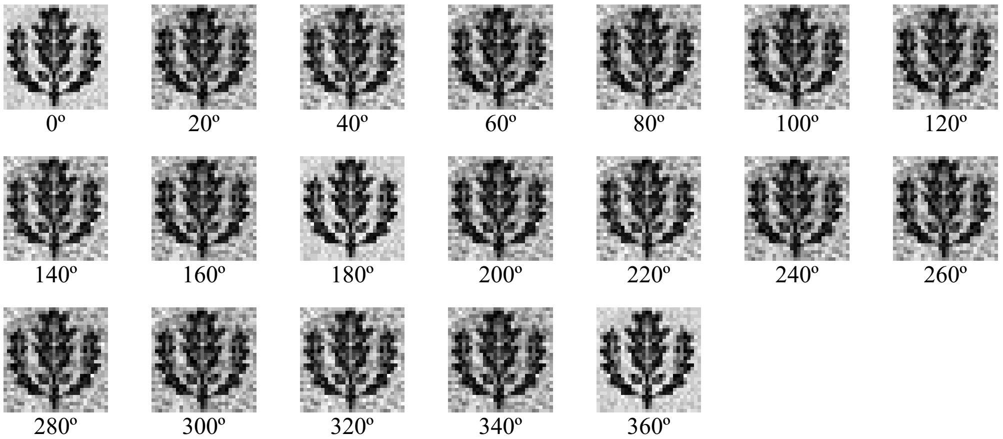

Fig. 7. Decrypted signatures from rotated version of the rotation-invariant ID tag shown in Fig. 6.

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. 8). 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. 8).

It is necessary to remark that for all the nonlinearities tested, the parameter *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 9 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 for the other applied nonlinearities. From graphs plotted in Fig. 9, we can conclude that sharpness of correlation peak increases for lower values of *k*, and/or the output noise floor is decreased. If both results are taken into account (Figs. 8 and 9) it is necessary to achieve a compromise between distortion-tolerance and peak sharpness. Thus, intermediate values of *k* can produce a trade off.

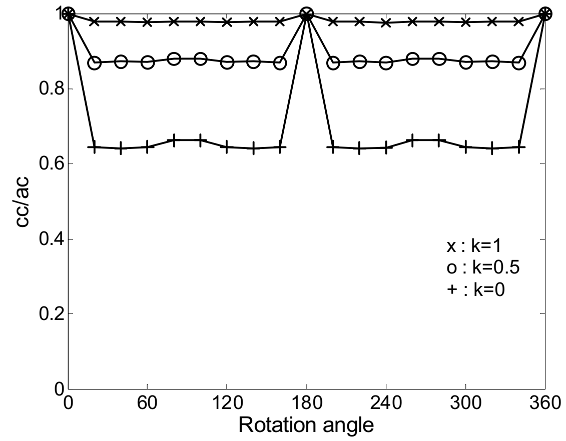

Fig. 8. cc/ac ratio versus rotation angle for the rotation-invariant ID tag (Fig. 6).

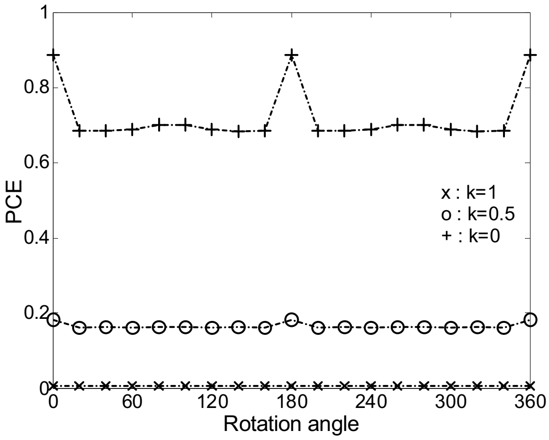

Fig. 9. PCE versus rotation angle for the rotation-invariant ID tag (Fig. 6).

5. CONCLUSIONS

We have presented a method to obtain rotation-invariant ID tags. The ID 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 a phase code containing double phase encrypted information to increase security. The encrypted signature is encoded in the ID tag to provide the desired distortion invariance.

The designed ID tags can be located on an object, and are captured by a receiver, which will decode and verify the information included in the tag. Signature may be 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 objects.

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. 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 given signature used as a reference image and a different image by using correlation.

Other distortion-tolerant techniques may be studied. However, the main advantage of the proposed method is its simplicity. Further work should introduce other distortions such as scale variations, and 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. B. Javidi, ed., *Image recognition and classification: Algorithms, systems and applications*, Marcel Dekker, New York, 2002.
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. S. H. Hong, B. Javidi, *Optimum nonlinear composite filter for distortion-tolerant pattern recognition*, Appl. Opt., vol. 41, no. 11, pp. 2172-2178, 2003.
11. B. Javidi, J. L. Horner, *Real-time Optical Information Processing*, Academic Press, Boston, 1994.
12. *ATR Definitions and Performance Measures*, Automatic Target Recognizers Working Group (ATRWG) Publications, no. 86-001, 1986.
13. J. L. Horner, *Metrics for assessing pattern-recognition performance*, Appl. Opt., vol. 31, no. 2, pp.165-166, 1992.
14. B. V. K. Vijaya Kumar, L. Hassebrook, *Performance measures for correlation filters*, Appl. Opt., vol. 29, no. 20, pp. 2997-3006, 1990.
15. 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.
16. IEEE Trans. on Image Processing. Special issue on *Automatic Target Detection and Recognition*, vol. 6, no. 1. 1997.
17. B. Javidi, ed. *Smart imaging systems*, SPIE Press, SPIE, Bellingham, WA, 2001.
18. C. F. Hester, D. Casasent, *Multivariant technique for multiclass pattern recognition*, Appl. Opt., vol. 19, no. 11, pp. 1758-1761, 1980.
19. H. J. Caulfield, *Linear combinations of filters for character recognition: a unified treatment*, Appl. Opt., vol. 19, pp. 3877-3879, 1980.
20. 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.
21. 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.
22. B. Javidi, D. Painchaud, *Distortion-invariant pattern recognition with Fourier-plane nonlinear filters*, Appl. Opt., vol. 35, no. 2, pp. 318-331, 1996.
23. 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.
24. 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.