Visible and NIR spectral band combination to produce high security ID tags for automatic identification

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

ABSTRACT

Verification of a piece of information and/or authentication of a given object or person are common operations carried out by automatic security systems that can be applied, for instance, to control the entrance to restricted areas, access to public buildings, identification of cardholders, etc. Vulnerability of such security systems may depend on the ease of counterfeiting the information used as a piece of identification for verification and authentication. To protect data against tampering, the signature that identifies an object is usually encrypted to avoid an easy recognition at human sight and an easy reproduction using conventional devices for imaging or scanning. To make counterfeiting even more difficult, we propose to combine data from visible and near infrared (NIR) spectral bands. By doing this, neither the visible content nor the NIR data by theirselves are sufficient to allow the signature recognition and thus, the identification of a given object. Only the appropriate combination of both signals permits a satisfactory authentication. In addition, the resulting signature is encrypted following a fully-phase encryption technique and the obtained complex-amplitude distribution is encoded on an ID tag. Spatial multiplexing of the encrypted signature allows us to build a distortion-invariant ID tag, so that remote authentication can be achieved even if the tag is captured under rotation or at different distances. We also explore the possibility of using partial information of the encrypted signature to simplify the ID tag design.

Keywords: Automatic security systems, Identification, Optical ID tags, Phase encryption, Distortion-invariant recognition, Visible and NIR spectral bands.

1. INTRODUCTION

Optical identification (ID) tags can be used for real-time remote identification and authentication of objects which have diverse applications in transportation and homeland security.[1] The ID tags consist of an optical code containing complex valued encrypted information to increase security. A distortion-invariant ID tag,[2-6] was designed so that the verification system was able to detect and identify the information included in the tag even when the optical code was captured rotated or at a varying distance. Both the magnitude and the phase of the encrypted signature were codified in grayscale to improve robustness against phase distortions produced by outdoors environmental conditions (rain, air turbulences, etc.).[5] Verification of the signature embedded in the ID tag was carried out by correlation.[7] To increase security, the information included in the ID tag was encrypted by following either the double-phase encryption procedure,[8] or the fully-phase encryption technique.[9] The latter has been shown as an encryption method that permits to increase the noise resistance of the processor in the presence of additive Gaussian noise.[6,10-11]

In this work, we want to further increase the system robustness against counterfeiting by combining data from visible and near infrared (NIR) spectral bands. The encrypted information included in the distortion-invariant ID tag is verified by comparing the decoded signal with a reference signature, which would be carried by the tag holder, and it should be read in both, the visible and the NIR spectral bands. Only the appropriate combination of both signals permits a satisfactory authentication of the signature that identifies the sought object. Moreover, the distortion-invariant ID tag itself is built in such a way that it is only detected in the NIR band and its encrypted information is additionally hidden

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

Unmanned/Unattended Sensors and Sensor Networks III, edited by Edward M. Carapezza,
Proc. of SPIE Vol. 6394, 63940I, (2006) · 0277-786X/06/$15 · doi: 10.1117/12.689871

from human sight. This proposal is especially attractive for cases where the identity of a person, a vehicle or another object has to be validated (see examples in Fig. 1).

Fig. 1. Airport customs, control of a vehicle fleet or parking entrance, attendance to an event of masses, are examples where the proposal of this work can be applied to control the access to restricted areas.

2. OPTICAL ID TAG REVIEW

Verification of information at a distance generally requires that the receiver should be able to capture an ID tag from an unexpected location and/or orientation and, within certain limits, to process the information included in it. Recent proposals[2-5] have described in detail a possible procedure to include the information of a signature in an distortion-invariant ID tag, which is invariant to scale variations and rotations. In addition, to increase security it is convenient that, prior to be included in the ID tag, the signature itself is encrypted. Several encryption procedures are available and two of them, the double phase[8] and the fully-phase[9] encryption techniques have been compared to improve noise resistance of the distortion-invariant ID tags.[6] In this section, we briefly introduce both, the fully-phase encryption technique, which is to be used in this work, and the procedure to build a distortion-invariant ID tag.

2.1. Fully-phase encryption

An identification number, an alphanumeric code, an object image or other kinds of information can be used as signatures to identify a given object. Commonly, this information consists of an intensity image. Let $f(x,y)$ be the signature to be encrypted that is normalized ($0 \le f(x,y) \le 1$) 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. Similarly to the double-phase encoding,[8] the fully-phase encryption technique[9] converts a primary image $f(x,y)$ into stationary white noise, so that the encrypted function does not reveal the appearance of the signature to the naked eye. The signature to be encoded is represented as a phase-only function[12] by computing $\exp\left[i\pi f(x,y)\right]$. The range of variation of the phase encoding is $[0,\pi]$. Afterwards, the phase-encoded image is multiplied by the phase mask $\exp\left[i2\pi p(x,y)\right]$. Finally, this product is convolved by a function $h(x,y)$, which is the impulse response of a phase-only transfer function $H(\mu,\nu)=\exp\left[i2\pi b(\mu,\nu)\right]$. Thus, the fully phase encrypted signature, $\psi(x,y)$, is a complex valued function given by

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

Figure 2 shows an original signature and the corresponding fully-phase encoded function prior to be encrypted in a distortion-invariant ID tag.

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

2.2. Distortion-invariant tags

We aim to include the information of the encrypted signature in an ID tag invariant to different distortions, in particular to scale variations and rotations. If we do so, the receiver will be able to capture the ID tag from an unexpected location and orientation and, within certain limits, to process the information included in it. We follow the procedure described in Refs. [2-6]. Distortion-invariance is achieved by both multiplexing the information included in the ID tag and taking advantage of the ID tag topology. In comparison to multiple contributions that have been done in the field of distortion-invariant recognition,[13-23] the used procedure permits to obtain a relevant degree of distortion-invariance with a certain reduction of the system complexity.

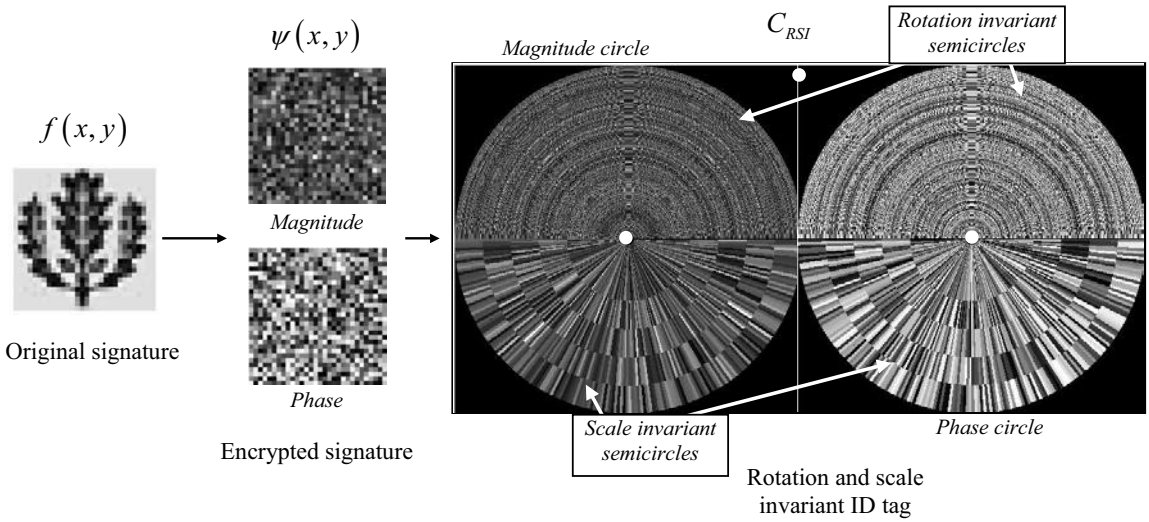


Fig. 2. Synthesis of a distortion (rotation and scale)-invariant ID tag.

The complex valued function $\psi(x,y)$ obtained from Eq. (1) is to be fully grayscale encoded. Let us consider the encrypted signature $\psi(x,y)$ in array notation $\psi(t)=|\psi(t)|\exp\{i\phi_\psi(t)\}$ where t=1,2,...N, and N is the total number of pixels of the encrypted signature. 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. Figure 2 shows a possible arrangement of both circles. One of them corresponds to the magnitude of the encrypted signature (left circle in Fig. 2). The other contains the phase distribution of the encrypted function (right circle in Fig. 2). In both circles, the information is distributed similarly to the structure of a wedge-ring detector. One half of each circle (upper semicircles in Fig. 2) includes either the magnitude $|\psi(x,y)|$ or the phase distribution $\phi_\psi(x,y)$ of the encrypted signature written in a radial direction and repeated angularly so that rotation-invariance can be achieved. The other semicircle of both circles (bottom semicircles in Fig. 2) contains either the magnitude $|\psi(x,y)|$ or the phase $\phi_\psi(x,y)$ of the encrypted signature written circularly and repeated in concentric rings. Therefore, the information of a given pixel of the encrypted signature

will correspond to an angular sector in the optical code. Thus, the readout of the ciphered information will be tolerant to variations in scale. For encrypted signatures with a large number of pixels, such as the example given in Fig. 2, information of the scale-invariant ID tag have to 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 will be affected in accordance to the number of concentric circles used in the ID tag.

As it is shown in Fig. 2, the centers of both circles are white dots that, along with a third white dot in the upper part, build a reference triangular shaped pattern that allows to know the orientation of the whole ID tag. Both, the magnitude $|\psi(t)|$ and the phase $\phi_{\psi}(t)$ will be encoded in grayscale in the left and right circles, respectively.

Other possibilities can be considered to rearrange the information contained in the two circles of the ID tags.[2-6] 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.[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, by using a linear array detector placed in any radius of the semicircle, from the center to the exterior of the code. From one circle the magnitude is obtained and from the other, the phase distribution. Not only is a single code read along a unique radial direction for decoding, but a median value from several radial codes is computed to increase robustness against noise. Pixels should be written back into matrix notation prior to decoding the signature $\psi(x,y)$ by using the decryption technique.[9] 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 rings. To minimize errors in the reading process, not only is one pixel taken into account for each circular ring, but a median value of pixels located in neighbour concentric rings in the radial direction. Magnitude and phase are obtained repeating the procedure for both circles of the ID tag. 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.

If several concentric circles are used for signatures with a large number of pixels, 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.

2.3. Correlation-based authentication

The final step for the ID tag receiver will be the verification of the captured information in order to authenticate a given object. A correlation-based processor[7,24] will compare the decoded information with a reference signal. Comparison of these two functions would be based on a nonlinear correlator.[25] The reference signal can be either previously stored or,

to avoid large databases, it can be enbodied in a different tag either carried by the tag holder or stuck on the sidewall of a vehicle.

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:

$$c(x,y) = IFT\left\{\left|F(\mu,\nu)R(\mu,\nu)\right|^k \exp\left[i\left(\phi_F(\mu,\nu)-\phi_R(\mu,\nu)\right)\right]\right\} . \quad (2)$$

In a *k*'th-law nonlinear processor,[25] 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.[25-27] Optimum nonlinear transformations can be obtained to enhance the detection process by optimizing a performance metric.[28] We use *k*'th-law nonlinearity for computational efficiency.

A threshold operation, applied to the correlation output, finally determines the identity of the object. Correlation-based detection is feasible when an output peak above background level is obtained. The processor performance must be evaluated using different metrics. The metrics that are taken into account in this sort of works are well-known parameters described in the literature.[29-32] We consider, as a measure of the system discrimination capability, the cc/ac metric which is the ratio between the maximum peak value of the correlation output, cc, and the maximum autocorrelation value, ac, for the reference signature. Similarity between the decoded information and the reference signature will be greater as the cc/ac ratio approaches the value of unity.

3. COMBINATION OF VISIBLE AND NIR SPECTRAL BANDS

In this section, we explore the possibility of combining information coming from different spectral bands to increase the system security. We consider visible and near infrared (NIR) bands. Infrared data have already been used for target detection in security systems.[33-34] Our aim is to take advantage of the different spectral reflectance of objects when they are illuminated by light sources emitting in different bandwidths.

For instance, as reference signature we consider a numerical code reproduced by printing a sheet of paper by using two different types of ink, commonly used in commercially available printers. The sheet has a white part and a black part. The complete signature results from the combination of captured data from the visible and NIR spectral bands as it is shown in Fig. 3. Figure 3(a) displays the intensity distribution of the captured image, $f_{VIS}(x,y)$, when the signature is illuminated by a D65 daylight simulator and captured by a colour Sony DX-9100P 3CCD camera. Only information at the bottom part of the signature is recognizable from the visible image. Figure 3(b) shows the corresponding captured image, $f_{NIR}(x,y)$, when the signature is illuminated by a set of LEDs emitting in the near infrared region (950 nm) and captured by a Xenics XEVA-FPA-640 NIR camera. In the NIR channel, only the upper half of the signature is reproduced. Both the visible and the NIR images are first binarized ($\overline{f}_{VIS}(x,y)$, $\overline{f}_{NIR}(x,y)$) by applying a threshold level, and afterwards, the logical operation

$$f(x,y) = \left\{NOT\left[\overline{f}_{VIS}(x,y)\right]\right\} XOR\left\{\overline{f}_{NIR}(x,y)\right\} \quad (3)$$

is computed to obtain the whole numerical code acting as the signature (Fig. 3c). In order to avoid large databases storing all reference signatures, this information is given to the distortion-invariant ID tag holder. This fact permits to simultaneously verify the information of the ID tag and the two-spectral band reference signature (Fig. 4).

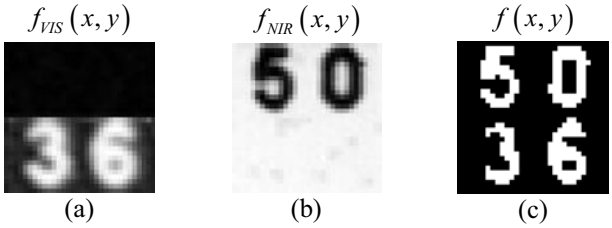


Fig. 3. (a) Visible and (b) NIR spectral components of the reference signature. (c) Complete signature that results from the logical operation of Eq. (3) applied to the visible and NIR binarized components.

From the whole numerical code $f(x,y)$ shown in Fig. 3(c), the fully-phase encrypted signal ($\psi(x,y)$ in Eq. 1) is computed. The resulting ciphered information is used to build the distortion-invariant ID tag following the procedure described in Sec. 2.

It is also possible to increase security in the identification system by taking advantage of the NIR spectral band. Moreover, similarly to other encoding techniques,[35-36] we will explore the possibility of simplifying the ID tag design by using partial information of the encrypted signature. By including only the phase distribution, $\phi_{\psi}(x,y)$, of the encrypted function in the distortion-invariant ID tag, the original signature $f(x,y)$ can be decrypted with an reasonable image quality, as it will be shown in the numerical results provided in Sec. 4. Thus, only one circle is necessary to obtain a distortion-invariant ID tag, C_{RSI} (Fig. 5) which will be equivalent to the right circle of the ID tag displayed in Fig. 2. The only-phase distortion-invariant ID tag is grayscale encoded so that it is only detected in the NIR spectral band. The visible spectral component does not reveal the information embedded on the ID tag (Fig. 4).

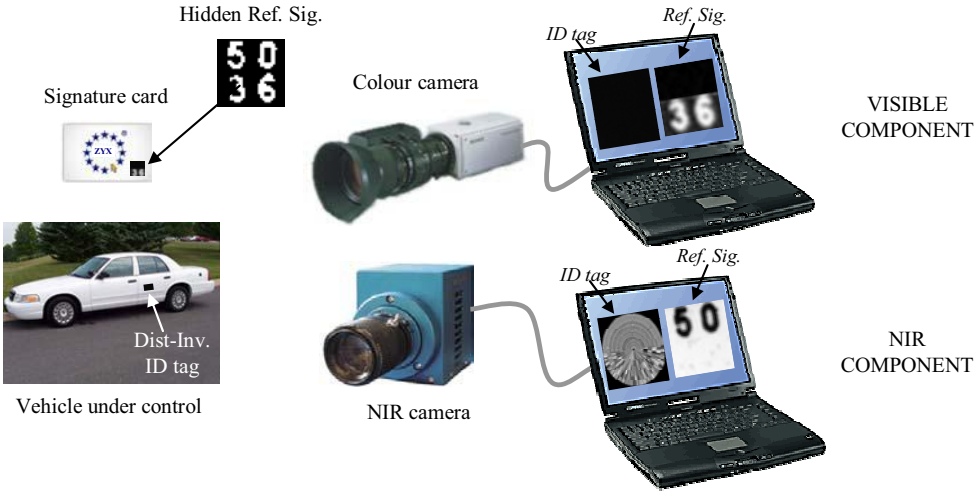


Fig. 4. Example of the two-spectral proposal. The distortion invariant ID tag, which is built from the phase-only encrypted signature, is located on a sidewall of a vehicle. On the one hand, the grayscale encoded information is only noticeable in the NIR spectral band but not in the visible component. On the other hand, both visible and NIR components of the image on the card permit to obtain the whole reference signature.

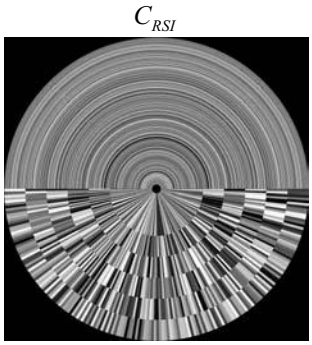


Fig. 5. Distortion invariant ID tag built from the phase-only encrypted signature. The grayscale encoded information is only noticeable in the NIR spectral band.

When the ID tag is captured, the encrypted information is decoded following the deciphering procedure described in Sec. 2, and afterwards, it is compared to the two spectral band reference signature by nonlinear correlation ($k = 0$ in Eq. 2). The following section provides some verification results in a number of situations.

4. VERIFICATION RESULTS

Firstly, let us suppose that the whole complex-amplitude encrypted function $\psi(x, y)$ is used to build the distortion-invariant ID tag in an equivalent way to that shown in the synthesis of the ID tag of Fig. 2. The receiver captures the NIR spectral component of the ID tag, which should ideally contain two circles, one for the magnitude and the other for the phase to have the whole complex-amplitude of the encrypted function. Afterwards, the encrypted signature is correctly deciphered and this information is compared with the reference signature obtained from the combination of the visible and NIR spectral components as it is computed by Eq. (3). The output signal of the processor has its maximum intensity value (ac), which is normalized to unity (Fig. 6), and a positive identification is achieved.

(a) (b) (c)

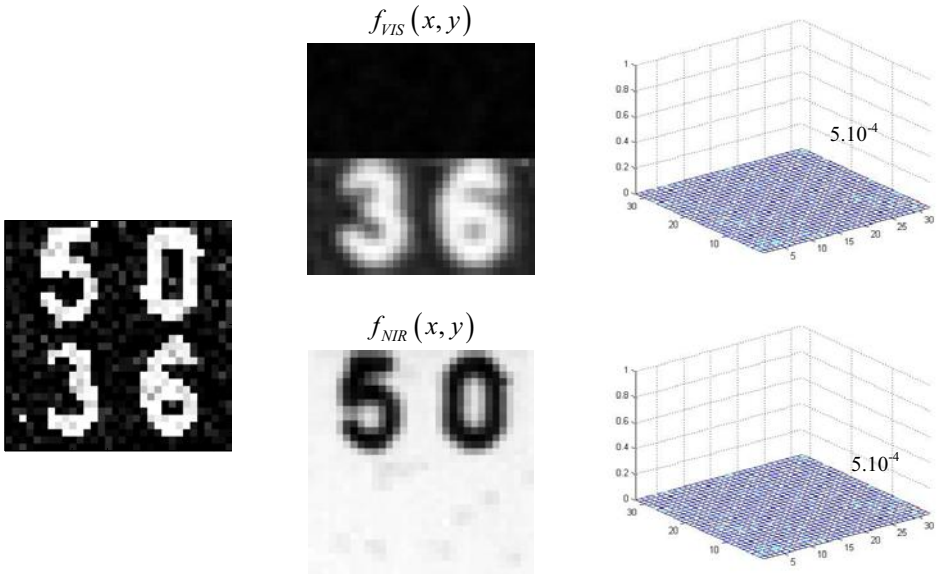
Fig. 6. (a) Signature retrieved from the distortion-invariant ID tag. (b) Reference signature $f(x, y)$ obtained from the appropriate combination of the visible and NIR components (Eq. 3). (c) Output (ac) of the verification system that leads to a positive identification.

Secondly, we consider the distortion-invariant ID tag shown in Fig. 5 containing just the phase distribution of the encrypted signature, $\phi_\psi(x,y)$. When the receiver captures its NIR spectral component, the signature can be recovered and compared to the reference signature $f(x,y)$. The fact that only the phase distribution is used makes the output peak intensity (cc) to decrease slightly but a positive and correct verification is still achieved (Fig. 7).

(a) (b) (c)

Fig. 7. (a) Signature retrieved from the phase-only distortion-invariant ID tag of Fig. 5. (b) Reference signature $f(x,y)$ obtained from the appropriate combination of the visible and NIR channels (Eq. 3). (c) Output (cc/ac) of the verification system that leads to a positive identification.

If the reference signature is only partially recovered by capturing a single spectral band (either the visible or the NIR component), the system output is nearly null corresponding to a negative verification of the information (Fig. 8) assuring a high secure identification system.



(a) (b) (c)

Fig. 8. (a) Signature retrieved from the phase-only distortion-invariant ID tag of Fig. 5. (b) Reference signature obtained from one single spectral channel, either the visible (top) or the NIR (bottom) spectral band. (c) Outputs (cc/ac) of the verification system that lead to a negative result for the visible (top) and NIR (bottom) components.

Even though the information of a single channel is binarized and written with the correct contrast (i.e. white numbers on a black background), the output intensity peak decreases significantly so that the identification system detects that is not the sought person or object (Fig. 9).

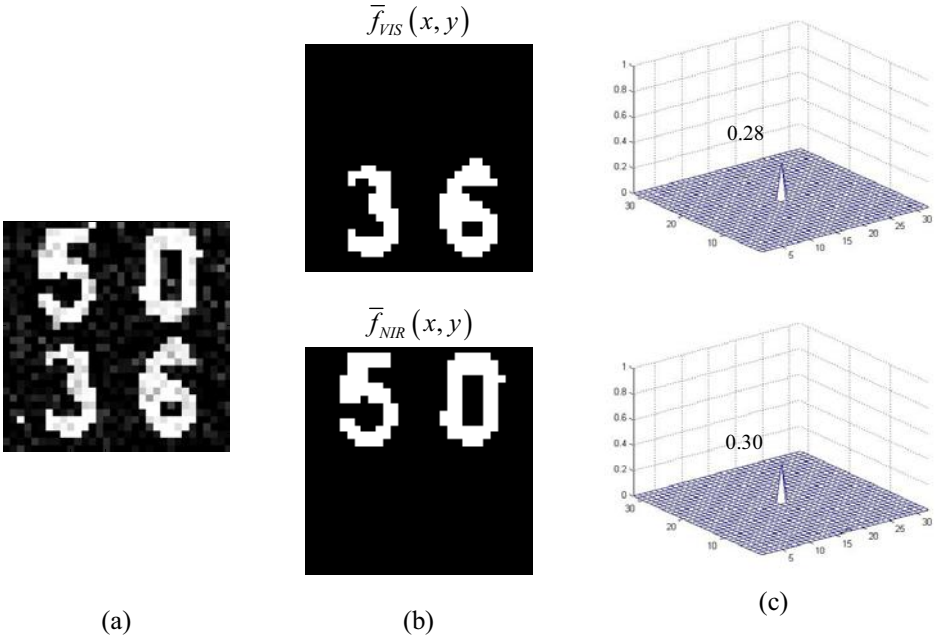


Fig. 9. (a) Signature retrieved from the phase-only distortion-invariant ID tag of Fig. 5. (b) Reference binarized signatures obtained from one single spectral channel, either the visible (top) or the NIR (bottom) spectral bands after being processed to obtain a binary image. (c) Outputs (cc/ac) of the verification system that leads to a negative result for the visible (top) and NIR (bottom) components.

Finally, we tested the tolerance of the built ID tag against rotation and variations of scale. Fig. 10 shows the results when the ID tag is captured under rotation of 60º degrees and scaled by a factor x0.5. Only when the complete reference signature is obtained from the visible and NIR components (top of Fig. 10 (b) and (c)), the intensity output peak reaches a high intensity value (over 0.5) that indicates that the verification of the information is positively achieved. Either when using the visible (central images of Fig. 10(b) and (c)) or the NIR (bottom of Fig. 10 (b) and (c)) component alone, the intensity output of the processor strongly decreases to indicate that the identification is not achieved.

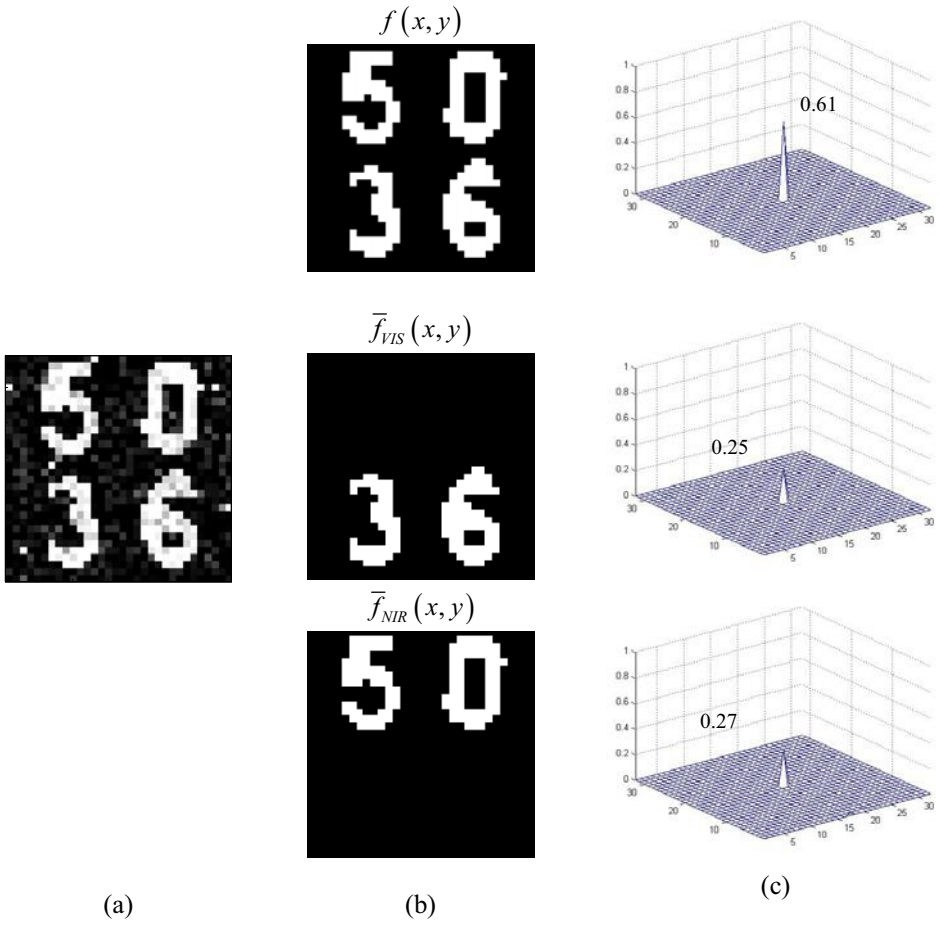


Fig. 10. (a) Signature retrieved from rotated (60 degrees) and scaled (x0.5) phase-only ID tag. (b) Reference binarized signatures obtained from the combination of visible and NIR channels of Eq. (3) (top), only the visible (center) and only the NIR channel (bottom) after being processed to obtain a binary image. (c) Verification system outputs (cc/ac) that only leads to a positive identification for the complete signature (top), and gives a negative result for partial spectral data (center and bottom).

CONCLUSIONS

We have proposed a highly secure distortion-invariant ID tag by combining visible and NIR spectral bands to increase the system robustness against counterfeiting. On the one hand, the reference signature that identifies the sought object is stored in such a way that only by computing the appropriate combination of two spectral image components, the whole signature is retrieved. On the other hand, the distortion-invariant ID tag that contains the encrypted signature is grayscale encoded and reproduced to be detected only in the NIR spectral band. The visible component of the ID tag does not reveal the information included in the ID tag. This feature is possible by using only partial information of the encrypted signature. Only the phase distribution of the encrypted signal is used to build the distortion invariant ID tag. Once the encrypted signature is deciphered from the ID tag, it is compared with the reference signature. Results provided in this work show that only the combination of the visible and NIR data of the signature provides a positive verification. Neither the visible content nor the NIR content by themselves can produce a positive identification. Tolerance to rotation and variation in scale of the ID tag has been checked and verification results have been shown.

The proposed combination of visible and NIR spectral bands applied to the design of optical ID tags can be useful to control the access to restricted areas, where the highly secure identification of a person, an object or vehicle is required.

ACKNOWLEDGEMENTS

The authors would like to thank the Spanish Ministerio de Educación y Ciencia and FEDER for financial support (project DPI2003-03931).

REFERENCES

1. B. Javidi, *Real-time remote identification and verification of objects using optical ID tags*, Opt. Eng., 42, 1-3 (2003).
2. E. Pérez-Cabré, B. Javidi, *Scale and rotation-invariant ID tags for automatic vehicle identification and authentication*, IEEE Trans. on Vehicular Technology, 54 (4), 1295-1303 (2005).
3. E. Pérez-Cabré, B. Javidi, *Distortion-invariant ID tags for object identification*, Proc. SPIE, 5611, 33-41 (2004).
4. E. Pérez-Cabré, B. Javidi, M. S. Millán, *Detection and authentication of objects by using distortion-invariant optical ID tags*, Proc. SPIE, 5827, 69-80 (2005).
5. E. Pérez-Cabré, M. S. Millán, B. Javidi, *Remote object authentication using distortion-invariant ID tags*, Proc. SPIE, 5908, 164-176 (2005).
6. E. Pérez-Cabré, M. S. Millán, B. Javidi, *Remote optical ID tag recognition and verification using fully spatial phase multiplexing*, Proc. SPIE, 5986, 598602 (2005).
7. J. W. Goodman, *Introduction to Fourier optics*, 2nd. Ed., McGraw Hill, New York, 1996.
8. Ph. Réfrégier, B. Javidi, *Optical image encryption based on input plane and Fourier plane random encoding*, Opt. Let., 20 (7), 767-769 (1995).
9. N. Towghi, B. Javidi, Z. Luo, *Fully phase encrypted image processor*, JOSA A., 16 (8), 1915-1927 (1999).
10. B. Javidi, L. Bernard, and N. Towghi, *Noise performance of double-phase encryption compared with XOR encryption*, Opt. Eng., 38, 9-19 (1999).
11. F. Goudail, F. Bollaro, P. Refregier, and B. Javidi, *Influence of perturbation in a double phase encoding system*, JOSA A, 15, 2629-2638 (1998).
12. B. Javidi, A. Sergent, *Fully phase encoded key and biometrics for security verification*, Opt. Eng., 36 (3), 935-942 (1997).
13. 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., CR 65, 240-260 (1996).
14. IEEE Trans. on Image Processing. Special issue on *Automatic Target Detection and Recognition*, 6 (1), (1997).
15. B. Javidi, ed. *Smart imaging systems*, SPIE Press, SPIE, Bellingham, WA (2001).
16. B. Javidi, ed., *Image recognition and classification: Algorithms, systems and applications*, Marcel Dekker, New York, 2002.
17. C. F. Hester, D. Casasent, *Multivariant technique for multiclass pattern recognition*, Appl. Opt., 19 (11), 1758-1761 (1980).
18. H. J. Caulfield, *Linear combinations of filters for character recognition: a unified treatment*, Appl. Opt., 19, 3877-3879 (1980).
19. H. Y. S. Li, Y. Qiao, D. Psaltis, *Optical network for real-time face recognition*, Appl. Opt., 32 (26), 5026-5035 (1993).
20. 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., 34 (11), 1885-1890 (1995).
21. B. Javidi, D. Painchaud, *Distortion-invariant pattern recognition with Fourier-plane nonlinear filters*, Appl. Opt., 35 (2), 318-331 (1996).
22. 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, 7 (8), 1113-1121 (1998).
23. E. Pérez, B. Javidi, *Nonlinear distortion-tolerant filters for detection of road signs in background noise*, IEEE Trans. on Vehicular Technology, 51 (3), 567 –576 (2002).
24. J. L. Turin, *An introduction to matched filters*, IRE Transactions on Information Theory, IT-6, 311-329 (1960).
25. B. Javidi, *Nonlinear joint power spectrum based optical correlation*, Appl. Opt., 28 (12), 2358-2367 (1989).

26. M. S. Millán, E. Pérez, K. Chalasinska-Macukow, *Pattern recognition with variable discrimination capability by dual non-linear optical correlation*, Opt. Commun., 161, 115-122 (1999).
27. E. Pérez, M. S. Millán, K. Chalasinska-Macukow, *Optical pattern recognition with adjustable sensitivity to shape and texture*, Opt. Commun., 202, 239-255 (2002).
28. S. H. Hong, B. Javidi, *Optimum nonlinear composite filter for distortion-tolerant pattern recognition*, Appl. Opt., 41 (11), 2172-2178 (2003).
29. B. Javidi, J. L. Horner, *Real-time Optical Information Processing*, Academic Press, Boston, 1994.
30. *ATR Definitions and Performance Measures*, Automatic Target Recognizers Working Group (ATRWG) Publications, no. 86-001, 1986.
31. J. L. Horner, *Metrics for assessing pattern-recognition performance*, Appl. Opt., 31 (2), 165-166 (1992).
32. B. V. K. Vijaya Kumar, L. Hassebrook, *Performance measures for correlation filters*, Appl. Opt., 29 (20), 2997-3006 (1990).
33. S. Der, A. Chan, N. Nasrabadi, H. Kwon, *Automated vehicle detection in forward-looking infrared imagery*, Appl. Opt., 43 (2), 333-348 (2004).
34. J. F. Khan, M. S. Alam, *Target detection in cluttered forward-looking infrared imagery*, Opt. Eng., 44 (7), 076404 (2005).
35. B. Javidi, A. Sergent, E. Ahouzi, *Performance of double phase encoding encryption technique using binarized encrypted images*, Opt. Eng., 37 (2), 565-569 (1998).
36. B. Javidi, E. Ahouzi, *Optical security system with Fourier plane encoding*, Appl. Opt., 37 (26), 6247-6255 (1998).