Optical ID tags for automatic vehicle identification and authentication

Bahram Javidi[a], Elisabet Pérez-Cabré[b], María S. Millán[b]

[a]Electrical & Computer Engineering Dept., University of Connecticut, 371 Fairfield Road, Unit 2157, Storrs, CT 06269-2157, USA.

[b]Dept. Optica i Optometria, Universitat Politècnica de Catalunya, Terrassa (Barcelona), SPAIN.

ABSTRACT

We review the potential of optical techniques in security tasks and propose to combine some of them in the design of new optical ID tags for automatic vehicle identification and authentication. More specifically, we propose to combine visible and near infrared imaging, optical decryption, distortion-invariant ID tags, optoelectronic devices, coherent image processor, optical correlation, and multiple authenticators. A variety of images and signatures, including biometric and random sequences, can be combined in an optical ID tag for multifactor identification. Encryption of the information codified in the ID tag allows increasing security and deters from unauthorized usage of optical tags. A novel NIR ID tag is designed and built by using commonly available materials. The ID tag content cannot be visually perceived at naked eye; it cannot be copied, scanned, or captured by any conventional device. The identification process encompasses several steps such as detection, information decoding and verification which are all detailed in this work. Design of rotation and scale invariant ID tags is taken into account to achieve a correct authentication even if the ID tag is captured in different positions.

Keywords: Information security, optical ID tags, pattern recognition, multifactor validation, near infrared imaging

1. INTRODUCTION

Optics provides useful resources for remote, real-time, automatic and reliable signal verification as it has been reported by a large number of papers published in the last decades.[1-3] Complex operations such as authenticator selection, signature encoding, encryption, identity tags, remote readout, decryption, hybrid processors, pattern recognition, resistance to degradations, identification, (multifactor) validation, and authentication are involved in the broad area of security systems. New methods have been reported for information encryption and designing identification (ID) tags for object surveillance or tracking.

A method to encode a primary image into a white-noise-like distribution is proposed in Ref. [4] and it can be implemented either optically or electronically. It has been applied to identify objects by optical correlation[5] in a nonlinear joint-transform correlator (JTC).[6] In nonlinear (fully-phase) encoding, a phase-only version of the primary image is encoded.[7] The identity (ID) tags consist of an optical code containing complex valued encrypted information to increase security.[8] A distortion-invariant ID tag,[9] 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. Other optical techniques have been used in the field of security systems, for instance, to multiplex encrypted data by polarized light,[10] or to encrypt three-dimensional information with digital holography.[11] Some research papers have pointed out the need of encoding multiple primary images for increasing the reliability of the security system.[12, 13] Different categories of identity signals or factors are combined to produce a multifactor authentication that only gives positive verification when the whole set of signals are identified.

Optical identification (ID) tags[8] have been introduced for robust, real-time and remote identification to enable surveillance or tracking of moving objects, such as vehicles or parcels on a conveyor belt. From the development of the first proposal, specific designs for distortion-invariant ID tags were presented [9,14] to allow remote information readout under the effects of scale variations or/and in-plane rotations. A review of the ID tag design as well as the influence of different sources of noise can be found in Refs. 14,15. The system was made even more secure by synthesizing signatures from different spectral bands (VIS and NIR images).[16] A new scenario in securing techniques involving remote identification is suggested in a recent paper,[17] where we proposed a new combination of the multifactor encryption procedure and optical ID tags to take full advantage of both techniques. Moreover, the reliability of the security system was increased by using infrared techniques working together with the previous ones.

Optical Pattern Recognition XIX, edited by David P. Casasent, Tien-Hsin Chao,
Proc. of SPIE Vol. 6977, 697702, (2008) · 0277-786X/08/$18 · doi: 10.1117/12.785889

This paper is an overview of the technical work that we have performed and/or published on optical ID tags. Our compact technique for encryption-verification relates the following four elements: multifactor encryption, distortion-invariant ID tag, near infrared (NIR) readout, and optical processor. The designed (NIR) ID tag exhibits remarkable characteristics such as distortion-invariance, easy and economical tag building and increased robustness. The encrypted information included in the ID tag is verified by comparing the decoded signal with a reference signature. The comparison is carried out by optical correlation.

2. SELECTION OF AUTHENTICATORS

Optical security systems usually deal with a single primary image (an object, a signature, or a biometric signal) as authenticator. However, security can be reinforced by combining different authenticators. In such a case, a Boolean AND operation has to be performed for each factor's authentication results so all must be affirmative before final authentication is satisfied.[12] The selection of authenticators is a crucial step because the identification of an element is based on them. A possibility is to combine information coming from different spectral bands, for instance, the VIS and NIR bands. Infrared data have already been used for target detection in security systems.[18] Regarding the signals, biometric images such as fingerprints, face, hand, iris, and retina are more and more considered in authentication mechanisms because biometrics is based on something intrinsic to a person (something the person is) in contrast to other schemes based on either something a person knows (e.g. a password) or has (e.g. a metal key, an ID card).[12]

In this work we consider multiple signals to identify a person, an object (vehicle) or both. The information is combined using two different techniques: in the first technique, a single signature is synthesized from two signals in the VIS and NIR spectral bands.[16] Secondly, we use a multifactor encryption-authentication technique that reinforces optical security by allowing the simultaneous AND-verification of four primary images.[13]

2.1 Single signature synthesized from VIS and NIR images

We describe this technique using the images of Fig. 1 (Example 1). 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 synthesis of captured data from the VIS and NIR spectral bands. Fig. 1(a) displays the intensity distribution of the captured image, $f_{VIS}(x)$ in one-dimensional notation for simplicity, when the signature is illuminated by daylight and captured by a conventional camera sensitive to the visible spectral bandwidth (VIS-camera). Only the bottom part of the signature is retrieved. Fig. 1(b) shows the NIR-image, $f_{NIR}(x)$, captured by a camera sensitive to this spectral region (NIR-camera). In the NIR channel, only the upper half of the signature is reproduced. Binarized versions of both the VIS and the NIR images ($\overline{f}_{VIS}(x)$, $\overline{f}_{NIR}(x)$) can be combined by using the logical operation

$$f(x)=\left\{NOT\left[\overline{f}_{VIS}(x)\right]\right\}XOR\left\{\overline{f}_{NIR}(x)\right\}, \tag{1}$$

which is computed to obtain the whole numerical code acting as the signature (Fig. 1(c)). From the whole numerical code $f(x)$ of Fig. 1(c), the encrypted signal $\psi(x)$ is to be computed in Section 3.

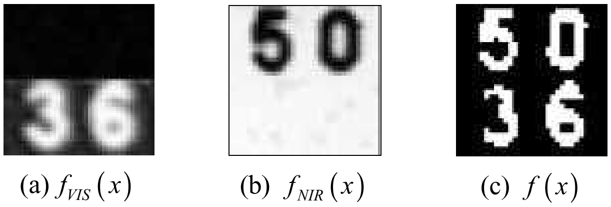
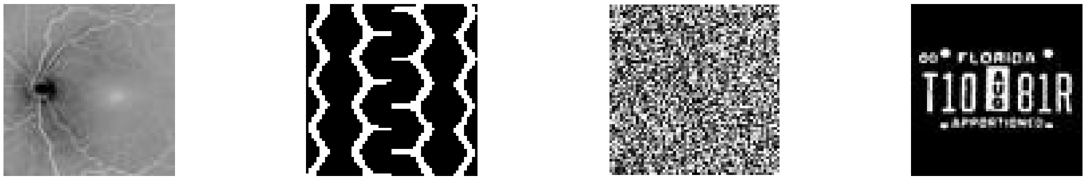

(a) $f_{VIS}(x)$ (b) $f_{NIR}(x)$ (c) $f(x)$

Fig. 1. Example 1: (a) VIS and (b) NIR images of the reference signature. (c) Synthesized signature after applying Eq. (1).

2.2 Biometrics and multifactor authenticators

The technique presented here is designed for four-factor authentication.[13,19] In Example 2 (Fig. 2) a combination of one biometric (to validate the authorised person), one alphanumeric sign and one pattern (to validate a vehicle) and one random phase sequence (to act as key code) are considered. The vessel distribution of a retina fundus image is used as biometric signal. The key phase code is known by the processor databases and is introduced as a degree of freedom to codify, for instance, the key of the day. These four reference primary images, double-phase encoded (see Section 3) and encrypted in an ID tag (see Section 4), are compared with the actual input images obtained *in situ* from the person and the vehicle whose authentication is wanted.



(a) Biometric $s(x)$ (b) Tyre pattern $r(x)$ (c) Key code $b(x)$ (d) Vehicle plate $n(x)$

Fig. 2. Example 2. Reference primary images considered as authenticators in the multifactor authentication technique.

3. COMPLEX-AMPLITUDE ENCRYPTED FUNCTION $\psi(x)$

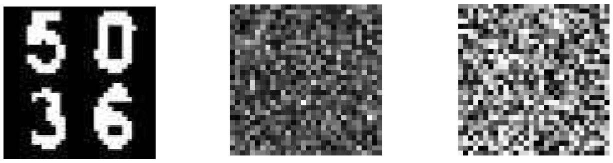
3.1 Fully-phase encrypted function $\psi^s(x)$ of a single signature

Let $f(x)$ be the signature to be encrypted that is a normalized positive function distributed in [0,1] and has a total amount of pixels N. This image can be phase-encoded to yield $t_f(x)$ that is generically defined by $t_f(x)=\exp\{j\pi f(x)\}$. The coordinates in the spatial and in the frequency domain are represented by (x) and (μ), respectively. Similarly to the double-phase encoding,[4] the fully-phase encryption technique[7] converts a primary image $f(x)$ 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 by computing $t_f(x)$. The range of variation of the phase encoding is $[0,\pi]$. Afterwards, the phase-encoded image is multiplied by the phase mask $t_{2p}(x)=\exp\{j2\pi p(x)\}$. Finally, this product is convolved by a function $h(x)$, which is the impulse response of a phase-only transfer function $H(\mu)=t_{2b}(\mu)=\exp\left[j2\pi b(\mu)\right]$. Thus, the fully phase encrypted function $\psi^s(x)$ is a complex valued function given by

$$\psi^s(x)=t_{f+2p}(x)*h(x). \tag{2}$$

Fig. 3 shows the magnitude and phase distributions of the encrypted function $\psi^s(x)$ corresponding to the synthesized signature of Example 1 (Fig.1(c)). Its dim appearance does not reveal the content of the original signature.

To decrypt the information included in the encrypted function $\psi^s(x)$, it will be necessary to firstly Fourier transform and multiply by the complex conjugate of the phase mask, or key 1, used in the encryption procedure, $t_{-2b}(\mu)$. The output $t_{f+2p}(x)$ is obtained. The original signature is retrieved in the space domain by using a second key, $t_{-2p}(x)$, extracting the phase of $t_f(x)$ and dividing by π.



(a) $f(x)$ (b) $|\psi^s(x)|$ (c) $\phi_{\psi^s}(x)$

Fig. 3. (a) Synthesized signature (Example 1, Fig.1c) (b) Magnitude and (c) phase of the $\psi^s(x)$ encrypted function.

3.2 Fully-phase encrypted function $\psi^{m}(x)$ of multifactor signatures

Let $r(x)$, $s(x)$, $b(x)$, and $n(x)$ be the multiple authenticators or reference primary images (for instance, those of Example 2 in Fig. 2), in one-dimensional notation for simplicity. As in the previous case (Section 3.1), all the four primary images $r(x)$, $s(x)$, $b(x)$ and $n(x)$ are normalized positive functions distributed in [0,1]. These images can be phase-encoded to yield $t_r(x)$, $t_s(x)$, $t_{2b}(x)$, $t_n(x)$ that are generically defined by $t_f(x)=\exp\{j\pi f(x)\}$. The fully-phase encrypted function containing the multifactor authenticators is given by the equation

$$\psi^{m}(x) = t_{r+2b}(x) * t_s(x) * \mathbb{F}^{-1}\left[t_n(x)\right], \tag{3}$$

where $t_{r+2b}(x) = t_r(x)\, \mathrm{t}_{2b}(x) = \exp\{j\pi\, r(x)\}\exp\{j2\pi\, b(x)\}$, $\mathbb{F}^{-1}$ indicates inverse Fourier transform, and $*$ the convolution operation. The encrypted function is complex-amplitude valued. It can be either optically generated by using an optical hardware equivalent to a JTC or computed and electronically implemented using conventional techniques for computer generated holograms.

Fig. 4 shows the magnitude and phase distributions of the encrypted function $\psi^{m}(x)$ obtained when Eq. (3) is applied to the set of reference primary images of Example 2 (Fig.2). Again, the appearance of the encrypted function is dim enough and does not reveal the content of any primary image of the set. The specific combination of information expressed by Eq. (3) is related to the automatic process of optical simultaneous recognition to validate the set of four authenticators.[13]

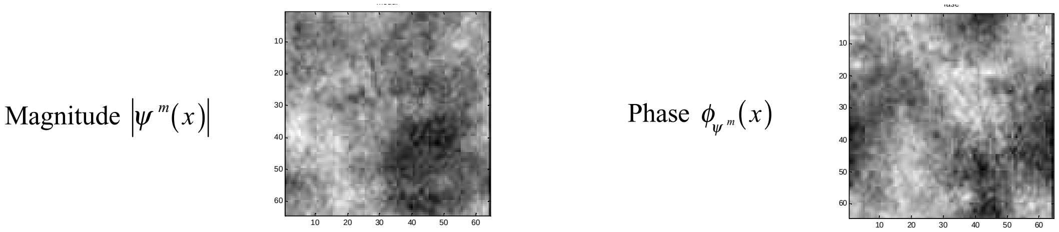


Fig. 4. Magnitude and phase of the encrypted function $\psi^{m}(x)$ corresponding to the set of images of Example 2 (Fig.2).

4. NIR ID TAG RESISTANT TO SCALE AND ROTATION DISTORTIONS

A robust ID tag must include the information of the encrypted function in a way that it can be read with invariance to certain distortions, in particular, to scale variations and rotations. If this property is shown, the receiver will be able to remotely capture the ID tag from an unexpected location and orientation and, within certain limits, to successfully process the information included in it. We follow the procedure described in Ref. 14. Distortion-invariance is achieved by both multiplexing the information included in the ID tag and taking advantage of the ID tag topology.

The complex valued encrypted function $\psi(x)$, which represents either $\psi^{s}(x)$ or $\psi^{m}(x)$ of Section 3 in general, is to be fully grayscale encoded. It is convenient to print the phase content of $\psi(x)$ in grayscale variations rather than in phase. Otherwise, the phase content of the encrypted distribution could be easily neutralized and the ID tag sabotaged if an adhesive transparent tape were stuck on it. For this reason it is useful to further encode the phase content of the signal in intensity variations. Thus, we consider encoding both the magnitude and phase in grayscale values.

Let us consider the $\psi(x)$ in array notation $\psi(t) = \left|\psi(t)\right| \exp\left\{i\phi_{\psi}(t)\right\}$ where t=1,2,...N, and N is the total number of pixels of the encrypted function. We build two vectors: the magnitude vector $\left|\psi(t)\right|$ and the phase vector $\phi_{\psi}(t)$, with t=1,2,...N. The information included in the ID tag is distributed in two circles. Fig. 5 shows a possible arrangement of both circles. One of the circles corresponds to the magnitude $\left|\psi(t)\right|$ of the encrypted signature (left circle in Fig. 5). The other contains the phase distribution $\phi_{\psi}(t)$ of the encrypted function (right circle in Fig. 5). 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. 5) includes either the magnitude or the phase distribution of the encrypted function 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. 5) contains either the magnitude or the phase distribution of the encrypted function written circularly and repeated in concentric rings. Therefore, the information of a given pixel of the encrypted function 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 examples given in Section 3, 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. 5, 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 one to know the orientation of the whole ID tag. Both, the magnitude $|\psi(t)|$ and the phase $\phi_\psi(t)$ are 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.[15] Fig. 6 shows the ID tag corresponding to the encrypted function of Fig. 3 (b,c).

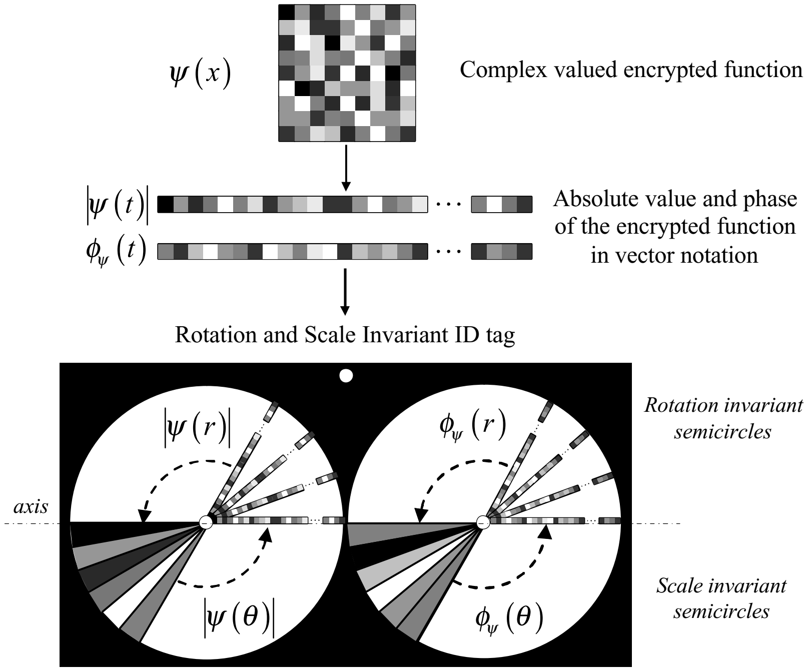

$\psi(x)$
Complex valued encrypted function
$|\psi(t)|$
$\phi_\psi(t)$
Absolute value and phase of the encrypted function in vector notation
Rotation and Scale Invariant ID tag
$|\psi(r)|$
$\phi_\psi(r)$
Rotation invariant semicircles
axis
$|\psi(\theta)|$
$\phi_\psi(\theta)$
Scale invariant semicircles

Fig. 5. Synthesis of a rotation and scale invariant ID tag from the encrypted function $\psi(x)$.

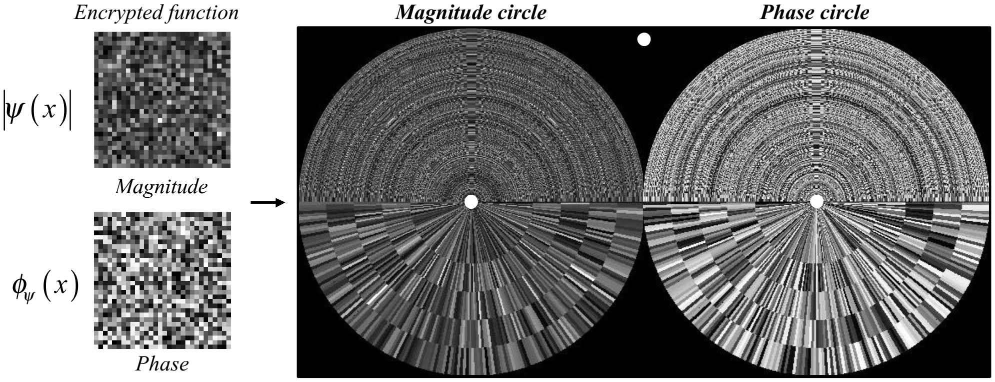


Fig. 6. Rotation and scale-invariant ID tag corresponding to the signature of Fig.3.

As an additional degree of security we increase the system robustness to counterfeiting by gathering the data of the ID tag from the NIR region of the spectrum.[17] In this way, data is no longer visible at naked eye and only by using the adequate sensor it is possible to grab the correct information. The NIR ID tag is built by printing the ID tag gray level distribution with a common laser printer on a black cardboard. In the visible spectrum, the whole information is completely hidden to either the naked eye or common cameras operating in the visible region of the spectrum. When looking at the ID tag, both the eye and the common camera would see just a black patch. Thus, it is not possible for them to know neither the kind of information included in the ID tag nor the exact position of this ID tag over the item under surveillance. Only NIR InGaAs cameras or conventional monochrome CCD cameras without the IR cut-off filter are able to detect the information necessary for verification.

Using the procedure described, the information is also redundantly written, so that an improved resistance to noise and other damages due to common handling (e.g. scratches) is obtained. [17] An auto-destruction mechanism of the ID tag has been proposed to invalidate the ID tag in case of having cuts or other damage produced by any attempt of tampering. [17] For example, a reservoir of black ink (black in terms of NIR illumination) under the ID tag. When the tag is cut, the ink is spread throughout it, the tag cannot be properly read, and the processor gives an alarm.

5. REMOTE READOUT, DECODIFICATION AND VERIFICATION

The ID tag can be captured in a situation similar to that represented in Fig. 7. The NIR ID tag is captured by a NIR sensitive device. The information contained in the ID tag stuck on the vehicle has to be compared with the input signals contained, for instance, in a card. In this way, it is possible to verify the identity of both the card holder and the vehicle. When the ID tag is captured, the encrypted information is decoded following a deciphering procedure that is the reverse of that described in Section 4. From one circle the magnitude is obtained and from the other, the phase distribution. Once the border between the rotation-invariant area and scale-invariant area is extracted (the axis in Fig. 8), the signature in vector notation $\psi(t)$ can be decoded either from the rotation or the scale-invariant region.

From the rotation-invariant region, the optical code can 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. 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 are written back into matrix notation prior to deciphering the signature $\psi(x)$. Following this procedure, the encrypted signature will be recovered whether the ID tag is captured in its original orientation or its rotated format. Similarly, $\psi(t)$ can be recovered by reading the ID tag in circular rings in the scale-invariant region. To reduce errors in the reading process, the median value of pixels located in neighbour rings is computed. The signature is then written in matrix notation $\psi(x)$ and decrypted. The optical code will be recovered even if the ID tag is scaled.

The processor that verifies the information of the single signature contained in the ID tag can be an optical correlator.[5] Fig. 7 shows the classical *4f* setup for optical correlation. The signature to be verified is imaged onto the input plane, and compared with the synthesized input image obtained from the VIS and NIR imaging of an identity card.

The multifactor authentication technique involves an optical processor that consists of a combined nonlinear JTC and a classical *4f*-correlator[5] for simultaneous AND authentications of multiple images as it is described in Ref. 13.

The set of input images deciphered from the ID tag is compared with the set of reference images by using nonlinear optical correlation.[20] The severity of the nonlinearity can be chosen according to characteristics of the recognition task.[21]

6. CONCLUSIONS

We have shown the potential of optical techniques in security tasks and have combined some of them for automatic authentication. We have used multiple signatures, NIR imaging, distortion-invariant ID tags, optoelectronic devices, coherent image processor, optical decryption, optical correlation, and multiple authenticators. The distortion-invariant NIR ID tag, which has a non visible signal, can be built by using commonly available materials so that it is only captured in the NIR spectral region. ID tag designing is smart: distortion-invariant, NIR ID tag printing on a black cardboard just using a laser printer, and increased robustness are the remarkable characteristics this kind of tag exhibits. Neither the encrypted functions nor the ID tags reveal their content in any case, which is an extreme difficulty in counterfeiting.

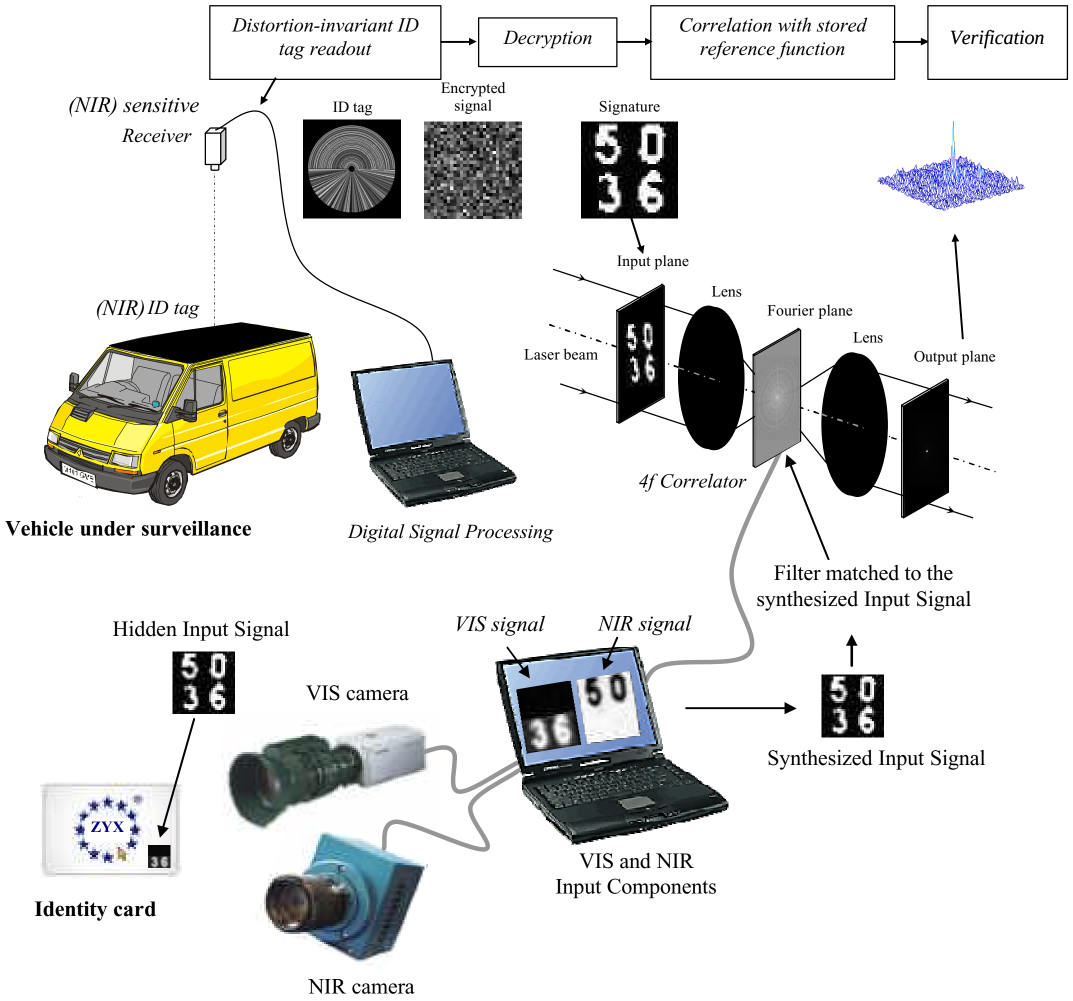


Fig. 7. ID tag readout, signature decryption and comparison with the input signal in an optical correlator for verification.

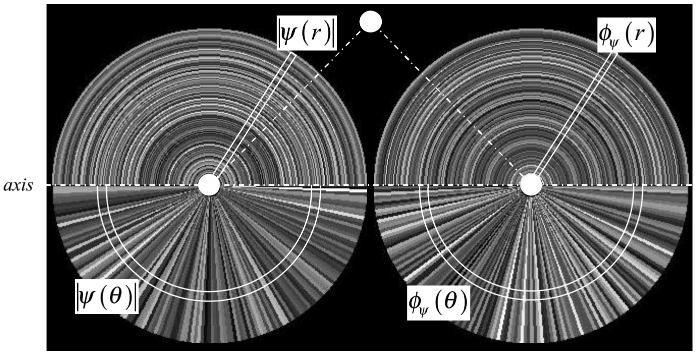


Fig. 8. Readout of the rotation and scale-invariant ID tag.

An intensity peak in the output plane of an optical processor will be used to decide whether an element (person or vehicle) is authenticated or not. Authentication is achieved even if the ID tag is captured in its original position, scaled or rotated. The techniques described in this work can be useful to control the access to restricted areas, where the highly secure identification of a person, a vehicle or both is required.

We have proposed a highly secure single signature synthesized from VIS and NIR images that increases the system robustness against counterfeiting. In another technique, we encrypt multifactor authenticators in a single complex-amplitude function that can be used in combination with rotation-scale invariant ID tags. This optical technique is attractive for high-security purposes that require multifactor authentication and real-time automatic verification.

ACKNOWLEDGEMENTS

To the financial support of Spanish Ministerio de Educación y Ciencia and FEDER (project DPI2006-05479).

REFERENCES

1. B. Javidi, J.L. Horner, "Optical pattern recognition for validation and security verification," *Opt. Eng.* 33(6), 1752-1756 (1994).
2. J.L. Horner, B. Javidi, Opt. Eng. 38, Special issue on Optical security, 1999.
3. B. Javidi, *Optical and Digital Techniques for Information Security*, Springer, New York, 2005.
4. P. Réfrégier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.* 20, 767-769 (1995).
5. J. W. Goodman, *Introduction to Fourier optics*, 2nd. Ed., McGraw Hill, New York, 1996.
6. B. Javidi, G. Zhang, J. Li, "Experimental demonstration of the random phase encoding technique for image encryption and security verification," *Opt. Eng.* 35, 2506-2512 (1996).
7. N. Towghi, B. Javidi, Z. Luo, "Fully phase encrypted image processor," *J. Opt. Soc. Am.* A 16, 1915-1927 (1999).
8. B. Javidi, "Real-time remote identification and verification of objects using optical ID tags," *Opt. Eng.* 42, 1-3 (2003).
9. 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).
10. J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, N. Bolognini, "Multiplexing encrypted data by using polarized light," *Opt. Commun.* 260, 109-112 (2006).
11. E. Tajahuerce, B. Javidi, "Encrypting three-dimensional information with digital holography," *Appl. Opt.* 39, 6595-6601 (2000).
12. L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proceedings of IEEE* 91, 2021-2040 (2003).
13. M. S. Millán, E. Pérez-Cabré, B. Javidi, "Multifactor authentication reinforces optical security," *Opt. Lett.* 31, 712-723 (2006).
14. E. Pérez-Cabré, M.S. Millán, B. Javidi, "Design of distortion-invariant optical ID tags for remote identification and verification of objects," in *Physics of the automatic target recognition*, F. Sadjadi and B. Javidi, eds., Springer Verlag, 2007, Chap.12.
15. 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).
16. E. Pérez-Cabré, M.S. Millán, B. Javidi, "Visible and NIR spectral band combination to produce high security ID tags for automatic identification," *Proc. SPIE* 6394, 63940I, (2006).
17. E. Pérez-Cabré, M.S. Millán, B. Javidi, "Near infrared multifactor identification tags," *Optics Express* 15, 15615-15627 (2007).
18. S. Der, A. Chan, N. Nasrabadi, H. Kwon, "Automated vehicle detection in forward-looking infrared imagery," *Appl. Opt.* 43 (2), 333-348 (2004).
19. M. S. Millán, E. Pérez-Cabré, B. Javidi, "High secure authentication by optical multifactor ID tags," *Proc. SPIE* 6394, 63940J, (2006).
20. B. Javidi, "Nonlinear joint power spectrum based optical correlation," *Appl. Opt.,* 28 (12), 2358-2367 (1989).
21. E. Pérez, M. S. Millán, K. Chalasinska-Macukow, "Optical pattern recognition with adjustable sensitivity to shape and texture," *Opt. Commun.,* 202, 239-255 (2002).
22. *ATR Definitions and Performance Measures*, Automatic Target Recognizers Working Group (ATRWG) Publications, no. 86-001, 1986.