Improved design of optical ID tags for remote validation

S. Horrillo[*a], E. Pérez-Cabré[a], M. S. Millán[a], B. Javidi[b]
[a]Dept. Òptica i Optometria, Universitat Politècnica de Catalunya, Violinista Vellsolà 37, 08222 Terrassa (Spain)
[b]Dept. Electrical & Computer Engineering, University of Connecticut, 371 Fairfield Road, Storrs, CT 06268 (US)

ABSTRACT

Optical ID tags have been shown as a useful tool for surveillance by detection and verification of a signature. Previous work on the topic made ID tags robust to rotations and scale variations by spatially multiplexing the information on the tag. To achieve this goal, however, a large amount of pixels had to be encoded on the final tag. To overcome this drawback an improved design is presented. The information distribution on the ID tag has been modified to optimize the area occupied by the tag. Moreover, a set of reference points has been introduced to achieve resistance against distortions that can affect the tag in remote acquisition. We pay special attention to affine and projective (rotation, scale, shear, perspective) transformations as well as to distortion (barrel, pincushion) caused by the imaging system.
In comparison to prior designs, the novel optical ID tag has two additional advantages: it permits a significant reduction of the tag size, even if the verification is remote and affected by the aforementioned distortions. Verification results are presented for a number of practical situations.

Keywords: ID tags, distortion invariance, remote detection, authentication, identification

1. INTRODUCTION

Optical identification (ID) tags were introduced for remote identification and verification of objects [1-3]. A given ID tag usually contains the information of an image (signature) representative of the object under surveillance. As an additional level of security, the signature can be encrypted using different methods such as the double random phase encryption (DRPE) [4], the fully-phase encryption (FPE) [5], or the multifactor encryption [6]. Once the ID tag is generated, it can be stuck on the object under surveillance. When the tag is illuminated, a remote receiver reads the tag, decodes the signature and identifies the object. This identification can be achieved in nearly real-time by means of optical devices and computer aid.
In previous works, we proposed a design of an ID tag, which could be decrypted even if the receiver captured a distorted version of the tag. The distortions considered were rotations and/or scale variations [2-3,7-8]. Tolerance to such distortions was achieved by a special topologic design of the tag. However, this ID tag was highly redundant and needed much more resolution than the original image.
Along with the development of the ID tags, other authors have tested the resistance of the encryption methods to some attacks. In particularly, they have shown the vulnerability of the DRPE to known-plaintext attacks [9-11].
In this work we present an improved design of an optical ID tag, so that detection and identification of an object will be carried out even if the captured ID tag is affected by strong deformations, such as perspective and/or distortion caused by the relative location of the remote receiver and the optical imaging system. In addition to this, the size of the ID tag will be significantly reduced in comparison to our previous designs. The proposed design has a topology similar to a previous scale invariant tag [2]. Fifteen external reference circles have been additionally introduced to test the image distortion in the capturing process. The novel design permits to read and decrypt correctly the information of the ID tag and achieves a remarkable reduction of the tag.

*shorrillo@gmail.com, phone 34 937398339; fax 34 937398301; www.goapi.edu

Optics and Photonics for Information Processing III, edited by Khan M. Iftekharuddin, Abdul Ahad Sami Awwal,
Proc. of SPIE Vol. 7442, 74421D · © 2009 SPIE · CCC code: 0277-786X/09/$18 · doi: 10.1117/12.828649

2. ID TAG DESIGN

Figure 1 depicts the generation process of a given ID tag. Firstly, the information used to identify the object under surveillance is encrypted to keep the piece of identity in secret. Secondly, the encrypted function is distributed on the ID tag following the appropriate topology to achieve invariance to a number of possible distortions. A set of selected circles are located on the ID tag to permit identification when different deformations modify the captured tag. In this section, both steps, the encryption procedure and the generation of the ID tag, are described in more detail.

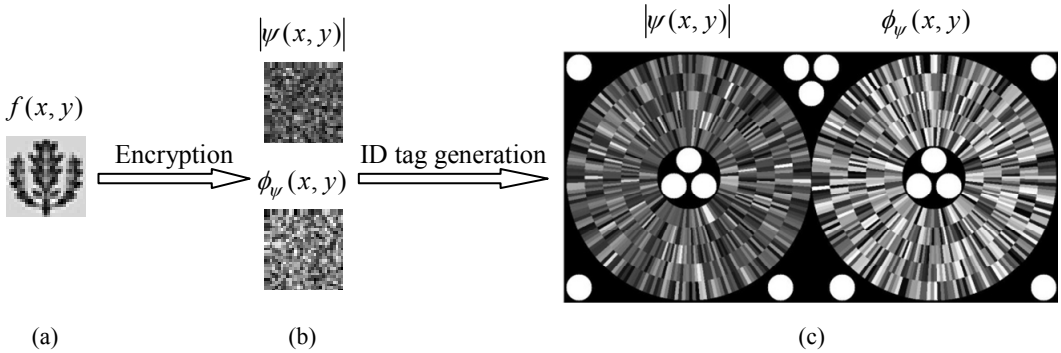


Fig.1. Generation of an optical ID tag: (a) signature; (b) amplitude and phase distribution of the encrypted signature by using the FPE technique and (c) optical ID tag.

2.1 Fully-phase encryption (FPE) method

The fully-phase encryption (FPE) method is used to codify the information that identifies a given object [5]. Similar to other encryption methods, the FPE converts a primary image $f(x,y)$ (Fig. 1(a)) into stationary white noise (Fig. 1(b)), so that the complex encryption function does not reveal the appearance of the signature at human sight.

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,η), respectively. The FPE is obtained by three operations. First, the signature $f(x,y)$ is phase encoded by computing $\exp\left[i2\pi f(x,y)\right]$. The range of variation of the phase encoding is $[0,\pi]$. Second, 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 $H(\mu,\eta)=\exp\left[i2\pi b(\mu,\eta)\right]$. Thus, the fully-phase encrypted signature, $\psi(x,y)$, is given by:

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

To decrypt the information included in the encrypted function $\psi(x,y)$, it is firstly Fourier transformed and multiplied by the complex conjugate of the phase mask, or key 1, used in the encryption procedure, $\exp\left[-i2\pi b(x,y)\right]$. Then, the result is inverse Fourier transformed to produce the output $\exp\left[i\pi f(x,y)\right]\exp\left[i2\pi p(x,y)\right]$. The original signature is retrieved in the spatial domain by using a second phase mask, $\exp\left[-i2\pi p(x,y)\right]$ (key 2), extracting the phase of $\exp\left[i\pi f(x,y)\right]$ and dividing it by π.

Differently from the double random phase encoding (DRPE) [4], two keys are needed to retrieve the signature when the fully-phase encryption technique is applied. In that sense, system security is increased.

2.2 ID tag generation

A robust ID tag must include the information of the encrypted function in a way that it can be read with resistance to certain distortions, in particular, deformations caused by perspective or distortions introduced by the optical imaging system. 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. In this work, we present an improved procedure in comparison to other previous analysis, where only invariance to rotations and scale variations were taken into account.

2.2.1 Distribution of the encrypted information on the ID tag

Figure 2 depicts the synthesis of an ID tag. The complex valued encrypted function $\psi(x,y)$ of Eq. (1) is fully grayscale encoded. Let us consider $\psi(x,y)$ in vector 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 function. We build two vectors: the magnitude vector $|\psi(t)|$ and the phase vector $\phi_\psi(t)$. The information included in the ID tag is distributed in two circles as it is shown in Fig. 2. The circle on the left of the ID tag corresponds to the magnitude $|\psi(t)|$ of the encrypted signature. The circle on the right contains the phase distribution $\phi_\psi(t)$ of the encrypted function. In both circles, the information is distributed in a similar way, so that the information of a given pixel will correspond to an angular sector in the optical code. Thus, the readout of the ciphered information will be, to a certain extend, tolerant to variations in scale.

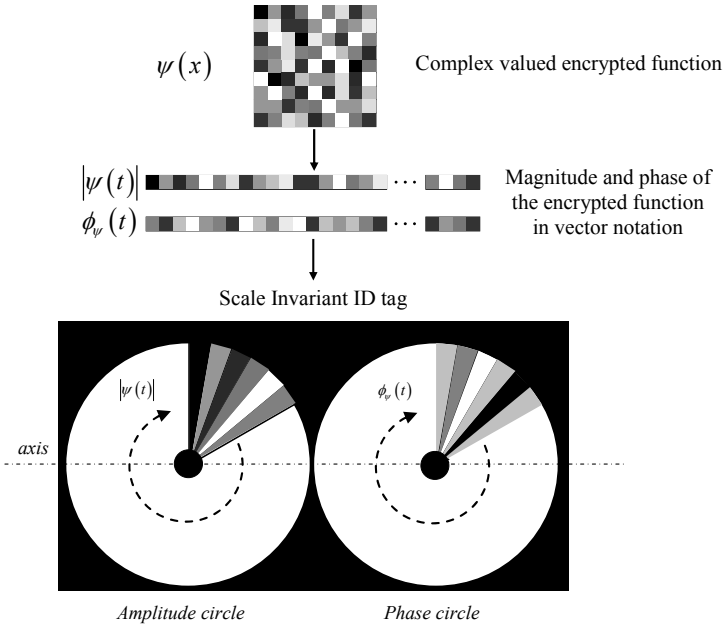


Fig. 2. Distribution of the encrypted information on the ID tag.

For encrypted signatures with a large number of pixels, such as the example shown in Fig. 1(c), the information of the scale-invariant ID tag has to be distributed by using different concentric circles to assure a minimum number of pixels in each sector. Consequently, the tolerance to scale variation will be affected in accordance to the number of concentric circles used in the ID tag. Figure 3 shows the procedure followed in case of using multiple concentric circles. The radius of the concentric circles increases always the same amount, ΔR, while the width of the angular sectors, ω_i, decreases

from a given circle to the following one in order to keep the number of pixels constant. Values of parameters ΔR and ω_i will be chosen according to a particular application and its tolerance requirements.

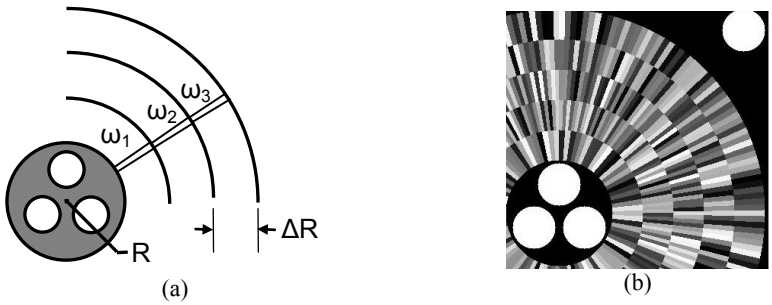


Fig. 3. Information distribution in angular sectors of the ID tag when using multiple concentric circles. (a) Diagram of the procedure; (b) detail of the corresponding ID tag.

As shown in the example of Fig. 3, the central circle of radius R of both, the amplitude and phase distributions of the encrypted signature is not divided into angular sectors. This is because it has not enough resolution to distinguish between different sectors.

Using the procedure described, the information is redundantly written, so that an improved resistance to noise and other damages due to common handling (e.g. scratches) is obtained.

Differently to our previous proposals, the topology of both circles is designed to obtain tolerance to scale variations. In the past, only half of the circle of the magnitude and half of the phase distribution were written for such a purpose. The other semicircles were used to obtain rotation-invariance by writing both vector $|\psi(t)|$ and vector $\phi_\psi(t)$ in the radial direction and repeating them angularly [2-3,7-8]. The rotation-invariant region of the ID tag was responsible for having many repetitions of the encrypted function and, therefore to have a bigger size than the original size of the signature. To optimize the dimensions of the ID tag, our current proposal does not include these rotation-invariant semicircles. We introduced instead a set of reference white circles.

2.2.2 Location of the selected reference circles to achieved distortion-invariance

We distribute fifteen white reference circles (see Fig. 4) in the rectangular ID tag. Four circles are located at the corners of the ID tag (numbered 1, 2, 14 and 15 in Fig. 4). Nine circles, grouped in sets of three spots, are placed in the central area of the scale-invariant distributions (groups named a and c of Fig. 4) and in the upper central part of the ID tag (group b in Fig. 4). Finally, two more circles are located at the bottom central part of the tag (group d in Fig. 4). It is necessary to introduce an asymmetry in the location of the reference circles (different number of circles in b and d groups) in order to establish a bijective function between the reference white circles of the original ID tag and the set of circles of the remotely captured ID tag. All fifteen reference circles have the maximum grey level to make their detection easy.

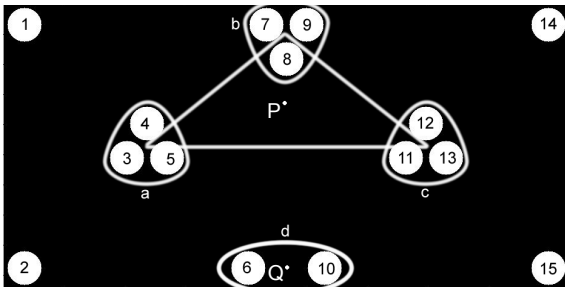


Fig. 4. Set of white circles used as a reference to determine the deformation of the captured ID tag. Not only are the circles themselves used to compensate for the deformation, but also the way their position and distribution on the ID tag. The center of mass of the reference circles as well as their distribution on the ID tag will permit us to determine the rotation angle and the transformation function that would compensate the possible deformations and distortions that the ID tag could have suffered in the remote acquisition by the receiver.

3. ID TAG READOUT AND DECRYPTION

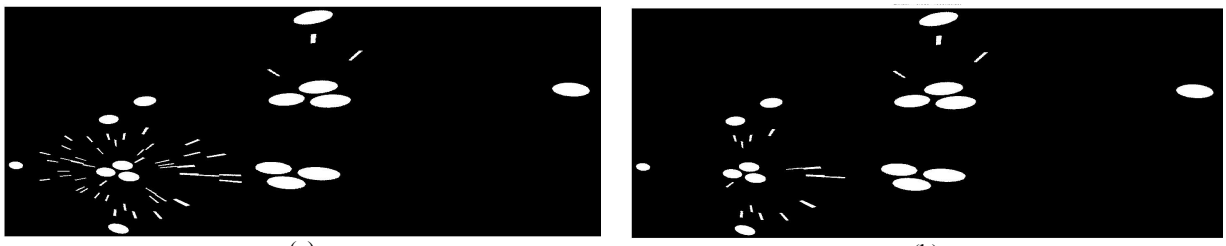
Once the ID tag is synthesized and located on an accessible part of the object under surveillance, the receiver remotely captures the tag, reads it out and decrypts its information to authenticate the object. In the capturing process deformations due to rotations, scale variations, shearing, perspective, distortion of the optical system and so on can severely modify the geometry of the ID tag. In order to satisfactorily retrieve the final decrypted information, it is important to assure that the magnitude and phase values of the encrypted function $\psi(x,y)$ are correctly readout without additional alterations.

For this reason, instead of digitally transforming the captured ID tag to compensate for deformations, which implies digital interpolations, we opt for building what we call a reading mask (Fig. 6 of Sect. 3.3) and modify it accordingly to the deformation detected in the capturing process. The reading mask would have a distribution similar to the original ID tag, but without containing secret information. It will be used to read the appropriate angular sector of the captured ID tag knowing to which pixel of the encrypted function $\psi(x,y)$ it corresponds.

In this section, we give details about the process, from the ID tag readout to the decrypted signature retrieval. Several steps have to be mentioned and described:
Firstly, the detection and identification of the white reference circles of the captured ID tag (Sect. 3.1).
Secondly, the determination of the deformation that the ID tag has suffered in the capturing process, by using the location and distribution of the reference circles. Afterwards, a transformation matrix $\mathbf{T}$ is obtained, which establishes a bijective function between the original ID tag and the deformed captured tag (Sect. 3.2).
Thirdly, synthesis of the reading mask and transformation of the mask by using matrix $\mathbf{T}$. In this way the mask is adapted to the captured ID tag and allows us to read the information of the ID tag (Sect. 3.3).
Finally, decryption of the obtained information by using the FPE technique is described in Sect. 2.1.

3.1 Detection and identification of the reference circles

It is assumed that the receiver has a complete knowledge of the tag topology and the geometry of the information distributed in it. Apart from deformations, we also consider the optical inversion done by the imaging system of the receiver. All fifteen reference circles have the maximum grey level corresponding to white. As a first approach, we apply a threshold level of 85% of the maximum grey level of the captured ID tag that permits to roughly detect the reference circles (see Fig. 5(a)). Afterwards, holes of the remaining binary objects are filled and an erosion operation with a circular structural element is carried out. Only the objects that remain in the eroded image are considered and they are reconstructed as they were before erosion. Finally, a threshold level taking into account the size of the objects is applied to eliminate small objects of the binary image. Figure 5(b) shows an example of a binary image obtained after the whole process.



(a) (b)

Fig. 5. Different sequences to detect the reference white circles of the captured ID tag with strong deformation in comparison with the original ID tag (Fig. 1(c)). Inversion of the optical imaging system has been taken into account. (a) Result after just applying a threshold level corresponding to 85% of the maximum grey level; (b) Result after applying the intensity threshold, erosion, reconstruction and a size threshold.

We can see that not only are the reference circles detected in the final binary image, but also some circular sectors. Due to deformations in the capturing process, both reference circles and circular sectors appear with different shapes. At this point, it is necessary to establish a criterion to discriminate between them. The proposed criterion must be robust against the strong deformations that may occur in the capturing process.
As usually circles are transformed to ellipses, the criterion to distinguish between circles and sectors is to compare the area (number of pixels) of a given object of the processed image with the area of a hypothetical ellipse that has the same length of the major and minor axes of the object. Only objects that obtain ratios over 0.99 are selected as the reference circles of the ID tag.
Once the reference circles are detected, it is necessary to identify them in order to determine their correspondance with each circle of the original ID tag. We use the information about their location along with their non-uniform distribution to achieve this purpose.
The position of the center of mass of each circle allows us to discriminate groups a, b and c (see Fig. 4) from the rest of circles by looking for the closest distances between circles. The barycenter of each group is computed and from them, point P is determined as the barycenter of the triangle formed by the former three barycenters.
Considering the other detected circles, we then identify group d and the middle point between both circles of the group (point Q in Fig. 4). Points P and Q are used to calculate an approximate angle of rotation of the deformed ID tag, so that the binary image with the detected circles can be rotated to orientate it with its upper and lower parts in the right position. Finally, circles will be numbered according to their relative positions (Fig. 4) and its relation with circles of an ideal non-rotated ID tag will be established.

3.2 Determination of the ID tag deformation during the capturing process

The identification of the fifteen circles on the captured ID tag is a necessary step to determine the deformation suffered by the tag and, therefore, to calculate the transformation matrix $\mathbf{T}$ that links the original and the captured ID tag. According to [12], the transformation introduced by a camera can be modelled by a polynomial transformation. In order to cover a wide range of deformations due to perspective and distortion of the optical imaging system, and from our preliminar studies, second order polynomials do not fulfil the desired outcome in case of severe deformations. However, third order polynomials achieve a good approximation between the original and the deformed patterns in the vast majority of cases. Thus, we choose this approximation to obtain a bijective transformation.
For a third order polynomial approximation, the transformation is defined by a matrix $\mathbf{T}$ that satisfies

$$\begin{bmatrix} u & v \end{bmatrix} = \begin{bmatrix} 1 & x & y & x \cdot y & x^2 & y^2 & y \cdot x^2 & x \cdot y^2 & x^3 & y^3 \end{bmatrix} \cdot \mathbf{T} \quad , \tag{1}$$

where (x, y) and (u, v) are the coordinates of the initial and the final spaces, respectively and matrix $\mathbf{T}$ has ten pairs of coefficients. Theoretically, a minimum of ten reference points are needed to solve the system and know the coefficients of the transformation matrix $\mathbf{T}$. As aforementioned, we have added fifteen white reference circles on the ID tag to assure that the minimum number of reference points would be covered even if the deformation of the tag were severe or if some circles were not registered due to non-optimal capturing conditions.
The centre coordinates of the white reference circles (usually, fifteen of them) detected and identify as described in section 3.1 will be used to determine the transformation matrix $\mathbf{T}$. Once this matrix is known, the bijective function described by Eq. (1) can be applied to transform a given image from one space to another [13].

3.3 Synthesis of a reading mask

Once the deformation of the captured ID tag is known, the following step is to read the information contained in the tag according to its acquired geometry. To avoid additional alteration of the information of the tag, we do not transform the captured ID tag to its original geometry because this process will imply interpolation of the pixel values. We propose instead to synthesise a reading mask that will adapt its shape to the distorted ID tag. Fig. 6 shows an example of a reading mask. It shows a structure similar to a scale-invariant ID tag (Sect. 2.2). It contains two circles divided into concentric circles and each concentric circle is subdivided in turn into small circular sectors.
The bijective transformation computed previously (Eq. (1)), is applied to the reading mask so that it adapts its geometry to the captured ID tag. The result of this operation can be seen on the example of Fig. 7. The reading mask of Fig. 7(b) has the same deformation as the captured ID tag shown in Fig. 7(a). Therefore, direct readout of the magnitude and phase

values can be achieved. The fact that the circular sectors of the reading mask are smaller than the ones on the ID tag is intended to increase the reliability of the reading process especially when strong deformations occur. In such a case, overlapping between lateral sectors may happen giving rise to errors in the reading process. The area for the reading circular sectors is approximately 50% of the corresponding circular sector of the ID tag. It accounts for the number of pixels we want to take into account for a reliable retrieval of values of the magnitude and phase of the pixels. The final value for each pixel of function $\psi(x,y)$ is obtained by computing the median value of the set of read pixels. On the other hand, the size of the reading sectors will affect the tolerance of the authentication system, for instance in the presence of noise. Depending on the application, this parameter could be optimized according to the conditions given in practice.

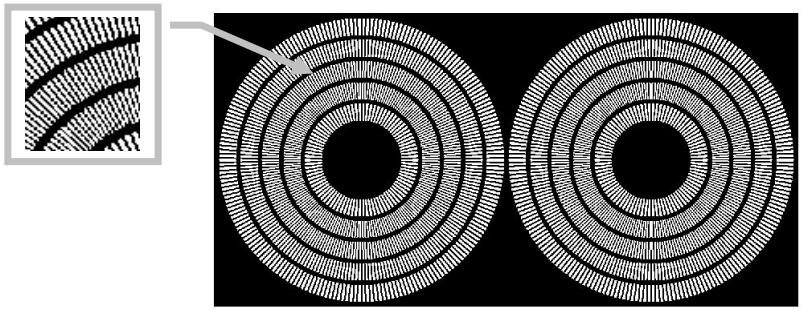
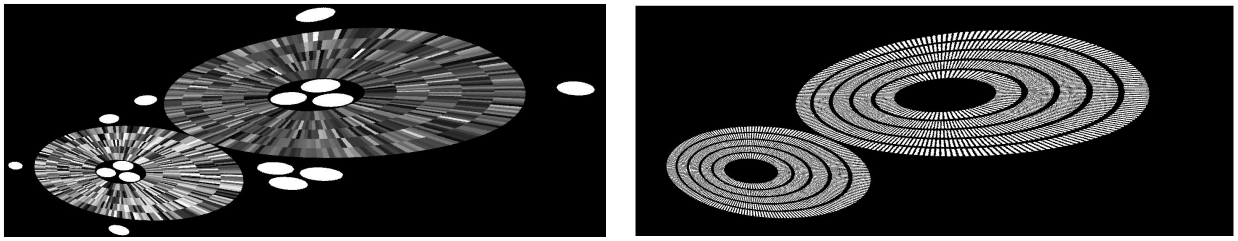


Fig. 6 Example of reading mask and detail on the left upper corner.



(a) (b)

Fig. 7. (a) Captured ID tag under deformation of perspective. (b) Reading masks transformed using Eq. (1) with matrix **T** determined from the reference white circles of Fig. 7(a).

Finally, we obtain the magnitude $|\psi(t)|$ and phase $\phi_{\psi}(t)$ values corresponding to the encrypted distribution from the reading process. Retrieved vectors $|\psi(t)|$ and $\phi_{\psi}(t)$ are rearranged in matrix notation to obtain the encrypted function $\psi(x,y)$. Then, the FPE method is applied to function $\psi(x,y)$ to decrypt the signature hidden on the ID tag. This procedure can be performed either optically or digitally as described in Section 2.1 provided one has the correct phase masks or keys.

Authentication of the obtained signature will be positive if a comparison to a previously stored reference signature satisfies a given degree of similarity. The comparison of two images can be achieved by different procedures. For instance, by computing the root-mean-square error between them [13].

4. SIMULATED RESULTS

In this section, we show simulation results to prove the reliability of the proposed ID tag. We test its novel design under a variety of situations corresponding to the expected deformations that could be introduced in the capturing process by a remote receiver. To summarize the experiences we have analyzed, we only show some of the most interesting results, to show the limits of the system and at the same time, to present results when the ID tag has suffered strong deformations, even stronger than what one can expect from a common capturing system.

In all the cases, the parameter chosen to evaluate the system performance is the root-mean-square error (e_{rms}), defined for a MxN image as [13]:

$$e_{rms} = \left[\frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \left[\hat{f}(x,y) - f(x,y) \right]^2 \right]^{1/2}, \quad (3)$$

where $f(x,y)$ is the reference signature and $\hat{f}(x,y)$ is the decrypted signature from the captured ID tag.

4.1 Scale variations

We analyzed the behaviour of the proposed ID tag when scale variations occur, so that for a given size of the circular sectors of the ID tag, and for a fixed size of the circular sectors of the reading mask, tolerance to scale variations can be established.

Table 1 shows the results obtained when the ID tag is captured from different distances and always perpendicularly to the tag plane. The designed ID tag has, on average, circular sectors of 260 pixels. The synthesized reading mask for the readout consists of circular sectors with areas approximately 50% of the tag sectors. From the results of Table 1, we can see that the signature is retrieved with good quality for the majority of analysed cases. Only when the variations in scale are stronger than 25%, the signature is retrived with an important level of noise. So, we can conclude that, under these conditions, the system is tolerant to scale variations until 25%.

If the proposed ID tags are to be used in an application where some constraints are fixed, for instance, they are used to control vehicles entering a restricted area, or to control parcels on a conveyor belt, the receiver can be positioned on a fixed location over the objects under control, and it can be assured that deformations of the captured ID tag will be caused by different heights of the vehicles or parcels, or by in-plane rotations. In such situations, the parameters of the ID tag can be optimized to extend the tolerance of the system to meet the requirements of the application.

Table 1. Retrieved signatures for scaled captured ID tags. RMS values are obtained by comparing $\hat{f}(x,y)$ with the original signature $f(x,y)$ (Fig. 1(a)).

Scale ratio	2x	0.8x	0.6x	0.4x	0.3x	0.25x	0.2x
Retrieved signature $\hat{f}(x,y)$							
e_{rms}	$6.3 \cdot 10^{-4}$	$6.3 \cdot 10^{-4}$	$6.3 \cdot 10^{-4}$	$7.7 \cdot 10^{-4}$	$6.3 \cdot 10^{-4}$	$1.2 \cdot 10^{-3}$	$8.6 \cdot 10^{-3}$

4.2 Deformations concerning perspective

In a general situation, the relative position of the receiver and the object under surveillance determines the perspective of the captured ID tag. To simulate this situation and evaluate the performance of our proposal, we have modelled the deformation introduced for a flat object, such the ID tag [12]. Fig.8 depicts the angles considered to obtain a deformed ID tag by perspective.

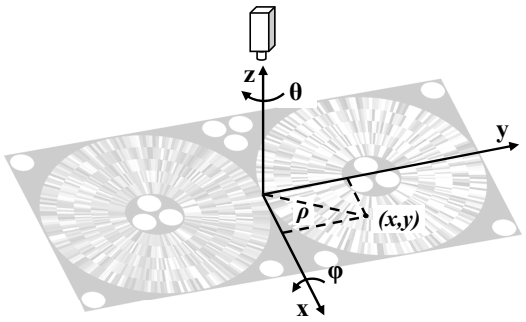
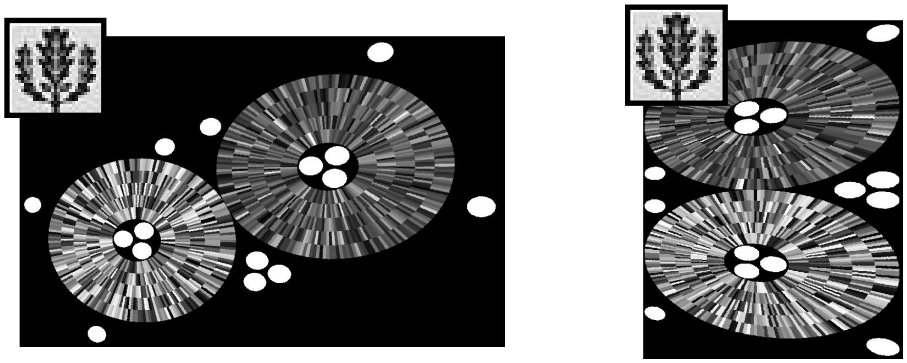


Fig. 8. Angles θ and φ used to model deformations caused by perspective. Distances ρ and (x,y) considered for distortions of the optical imaging system.

Figure 9 shows two examples of the captured ID tag viewed from different points so that they are deformed differently due to perspective. The inversion caused by the imaging system has been considered to depict images in Fig. 9. Fig. 9(a) shows an ID tag corresponding to angles θ=25º y φ =25º and fig. 9(b) corresponds to θ=90º y φ =40º. Both examples achieved a fairly good decryption of the signature as it is shown in the upper left corner of each ID tag.



(a) (b)

Fig. 9. Captured ID tags when they are mainly deformed by perspective. In the upper left corner the retrieved signature is shown. (a) θ=25º and φ =25º e_{rms} =6.3·10^{-4}; (b) θ=90º and φ =40º e_{rms} =6.4·10^{-4}.

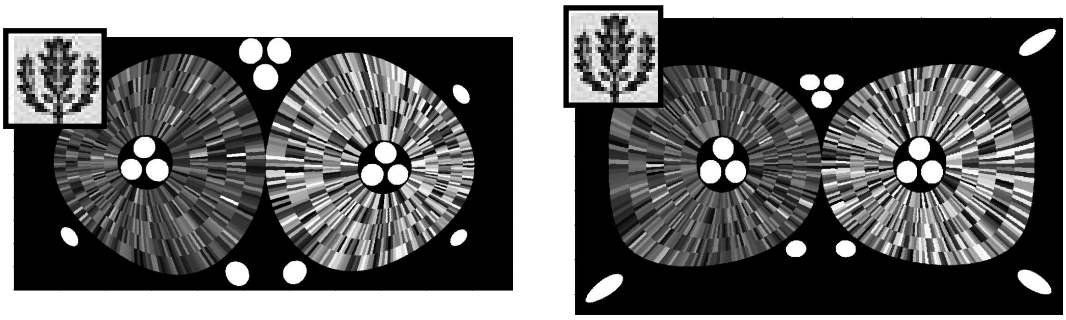
4.3 Distortion introduce by the camera

An optical system of a camera may introduce distortion for wide fields of view. We simulate this optical aberration in order to consider a more realistic approach. Both, barrel and pincushion distortion can be modelled by the following mathematical expression [14]:

$$\begin{cases} x = x + a \cdot \rho^3 & if\ x \geq 0 \\ x = x - a \cdot \rho^3 & if\ x < 0 \end{cases} \quad \begin{cases} y = y + a \cdot \rho^3 & if\ y \geq 0 \\ y = y - a \cdot \rho^3 & if\ y < 0 \end{cases}, \tag{4}$$

where $a < 0$ corresponds to barrel distortion and $a > 0$ to pincushion, and ρ corresponds to the polar coordinates of (x, y) (see Fig. 8).

By using Eq. (4), we have simulated an ID tag affected by both types of distortion. Fig. 10 shows two examples of this situation. In both cases, the captured ID tag suffers from severe distortion, stronger than what one could expect from a common optical camera system. The ID tag shown in Fig. 10(a) is affected by barrel distortion, while the ID tag in Fig. 10(b) is distorted by pincushion. Both examples obtained fairly good results when retrieving the hidden signature as it can be noticed from the signatures placed on the upper left corner of the ID tags.



(a) (b)

Fig. 10. ID tags modified by distortion of the optical system of the receiver: (a) barrel distortion e_{rms} =6.8·10^{-4}and (b) pincushion e_{rms} =6.3·10^{-4}. On the upper left corner of the ID tag, the retrieved signature is displayed.

5. CONCLUSIONS

A novel design for distortion-invariant optical ID tags has been presented. It is based on previous designs resistant to scale variations and a new approach to control the deformation of the captured ID tag by a remote receiver. The main novelty can be found in two aspects: first, the use of a set of reference circles located on free areas of the tag and grouped so that their distribution can account for the deformation suffered for the ID tag; and second, and the use of a reading mask to avoid additional modifications on the ID tag information by digital interpolations. A detailed description of the whole procedure is provided in this work.

The proposed ID tags have several advantages in comparison to prior designs. The size of the novel ID tag corresponds approximately to 30% of the previous tag for a given signature even if the verification is done remotely and outdoors. Moreover, it can deal with a great variety of deformations that may affect the ID tag on a more realistic environment. For instance, apart from rotations and scale variations, the information of the ID tag can be retrieved even if there is a strong change due to perspective or distortion of the optical imaging system. We have provided results in this work that confirm its robustness.

It is also remarkable that our proposal is flexible in a sense that for a given verification task with particular constraints (for instance, control of vehicles entering in a restricted area, or confiscated parcels inspected on a conveyor belt) the ID tag can be optimized by reducing its size without significantly affecting to its distortion-invariance.

ACKNOWLEDGMENTS

This research was supported by the Spanish Ministerio de Educación y Ciencia and FEDER funds (DPI2006-05479).

REFERENCES

1. Javidi, B. “Real-time remote identification and verification of objects using optical ID tags,” Opt. Eng. 42 (8), 2346-2348 (2003).
2. Pérez-Cabré, E., Javidi, B. “Scale and rotation invariant optical ID tags for automatic vehicle identification and authentication,”, IEEE Trans. Veh. Techn. 54 (4), 1295-1303 (2005).
3. Pérez-Cabré, E., Millán, M. S., Javidi, B. “Design of distortion-invariant optical ID tags for remote identification and verification of objects,” in Physics of automatic target recognition, Sadjadi, F. and Javidi B. Eds., Springer, NY, USA (2007).
4. Réfrégier, P., Javidi, B, “Optical image encryption based on input plane and Fourier plane random encoding,” Opt. Lett., 20 (7), 767-769 (1995).
5. Towghi, N., Javidi, B., Luo, Z., “Fully phase encrypted image processor,” J. Opt. Soc. Am A, 16 (8), 1915-1927 (1999).
6. Millán, M.S., Pérez-Cabré, E., Javidi, B. “Multifactor authentication reinforces optical security,” Opt. Lett., 31 (6), 721-723 (2006).
7. Javidi, B., Pérez-Cabré, E., Millán, M. S. “Optical ID tags for automatic vehicle identification and authenticatio,” Proc. SPIE, 6977, 697702 (2008).
8. Matoba, O., Nomura, T., Pérez-Cabré, E., Millán, M. S., Javidi, B. “Optical techniques for information security,” Proc. of the IEEE, 97 (6), 1128-1148 (2009).
9. Carnicer, A., Montes-Usategui, M., Arcos, S. Juvells, I. “Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys,” Opt. Lett., 30 (13), 1644-1646 (2005).
10. Frauel, Y., Castro, A., Naughton, T. J., Javidi, B. “Security analysis of optical encryption,” Proc. SPIE, 5986, 598603 (2005).
11. Gopinathan, U., Monaghan, D. S., Naughton, T. J., Sheridan, J. T. “A known-plaintext heuristic attack on the Fourier plane encryption algorithm,” Opt. Expr. 14 (8), 3181-3186 (2006).
12. Pratt, W. K. “Digital image processing”, 2nd Ed. John Wiley & Sons, Inc., NY, USA (1991).
13. Gonzalez, R. C., Woods, R. E., Eddins, S. L. “Digital image processing using matlab,” Pearson, Prentice Hall, NJ, USA (2004).
14. Mahajan, V. N. “Aberration theory made simple”, SPIE Opt. Eng. Press, Bellingham, Wa. (1991).