ACCESS CONTROL SYSTEM WITH HAND GEOMETRY
VERIFICATION AND SMART CARDS

Raul Sanchez-Reillo, Ana Gonzalez-Marcos
E-mail: reillo@ifo.upm.es
E.T.S.I. Telecomunicacion - Dpt. Tecnologia Fotonica
Ciudad Universitaria, s/n; E-28040 - Madrid; SPAIN

Abstract - The authors define here an access control system that includes the uniqueness of biometric verification, as well as the storage security and processing capabilities of smart cards. The biometric technique chosen has been hand geometry, which is considered as low/medium security (there are other much more secure, as fingerprint, iris or retina), easy usage, users' high acceptance, fast processing and medium cost. Also, the small template size needed is positive for the storage and processing capabilities required. But the innovation in the system proposed is that the smart card not only stores the user's template, but also performs the whole verification process with the features set by the terminal to the card. With this improvement, the security of the system has been risen because the template is never extracted from the card, avoiding duplication of such a sensible data. The specifications for the enrollment process will be also presented as well as the applications where this new system is recommended.

I. INTRODUCTION
Most of the access control systems implanted nowadays are based in PIN (Personal Identification Number) presentation and/or Magnetic Stripe Cards. These solutions, although secure enough for most of the applications, could not be valid for some high security environments. This lack of security is led by the possibility of forgetting or saying the PIN and/or losing or duplicating the card. The industry is solving this problem by applying new technologies like smart cards and biometric recognition. Smart cards solve the duplication problem and ease the management of lost cards, but the user must remember a PIN in order to be verified by the system. This means that if a user have more than one card, he must remember so many different PINs as cards owned, which leads to the common practice of applying the same PIN to all cards, with the lost of security that this practice can achieve. Biometric recognition solves the problem of remembering several PINs, as this number is transformed in biological features of the user.

But before designing or selecting a biometric access control system, two aspects must be defined: the biometric technique used and the configuration of the system. The selection of the biometric technique is not at all trivial. There are several techniques (fingerprint, voice, face, iris, retina, hand, signature, etc.), and its selection should be made by means of security level, cost, environment, user interaction, user acceptance and verification time. The configuration of the system can be as an identification system (comparing the features extracted with the templates of all users stored in a database), or as a verification system (comparing the features extracted to the template of the user who claims his identity). An identification system requires a central database, and communication of all the POAs (Point of Access) with that database. A verification system, can avoid the need of such a database and connections, by using a portable storage media, where the user's template is recorded.

II. FEATURES EXTRACTION
From the biometric techniques existing nowadays, hand geometry has been selected. Hand geometry is considered a low/medium security technique, what can lead to take it out of consideration, compared to much more secure techniques such as fingerprint, iris or retina. But hand geometry have several advantages which are interesting for developing an access control system. This advantages are:
- Medium cost (only a low/medium resolution CCD camera is needed).
- Fast computation (low computational cost and immediate result obtained).
- Low template size (the lowest of all techniques known nowadays).
- Very easy to use and attractive to users.
- Easy to clean and maintain.
- Lack relation to police, justice and criminal records.
All this characteristics makes this technique attractive for systems integrators, due to its low overall cost, and as well very quickly accepted by users who do not see any inconvenience in using the system.

After that, a simplified volumetric image processing is performed with the photograph. Several measurements are taken, including finger widths at several points, width of the palm, deviation of the fingers from the straight line, location of the inter-finger points, angles between them, palm height, etc.

From all those features extracted, a set of them is selected for verification purposes. This selection has been performed through inter-class/intra-class deviation ratio. Once the features with the highest ratio are detected, a principal component analysis has been performed to reduce the dimension of the feature vector. The structure of the feature vector obtained through this analysis, is applied to all the users and, therefore, the feature vector for each user sample is represented by 13 bytes.

III. VERIFICATION

Several methods for the verification process have been studied. From those methods three of them are presented here as being the most representative:

- **Euclidean Distance**: Verification is performed calculating the Euclidean distance between the template of the user and the sample taken, and comparing it with a threshold value. The template is obtained as the mean value of the first 5 photographs taken from that user in the enrollment process.

- **Hamming Distance**: The number of features out of the mean, plus/minus a factor of the standard deviation, is counted and compared to a threshold. The template is obtained as the mean and standard deviation of the 5 first photographs taken from the user in the enrollment process.

- **Gaussian Mixture Modelling (GMM)**: The user’s sample is entered in the GMM and the likelihood probability is obtained. The GMM of each user is composed by a set of means, variances and weights, tuned with the enrollment samples (5 of them).

Among the other methods studied, a neural network approach through Radial Basis Functions was tried. It showed really good results in classification, i.e. having a central database with all users enrolled in the system. But in order to use this approach in verification, a set of others users should be used in the enrollment process. This fact goes against the philosophy of this paper, as the existence of a central database is avoided. The success of the verification scheme is obtained by two ratios: False Acceptance Ratio (FAR) and False...
Rejection Ratio (FRR). These two ratios are complementary, in the sense that if a reduction in FAR is needed, then an increase in FRR is obtained. Results obtained are presented in the following table targeting a FRR near to 10%. 20 users and at least 10 samples of each user participated in the calculation of the ratios.

<table>
<thead>
<tr>
<th></th>
<th>FAR</th>
<th>FRR</th>
<th>Template size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Euclidean</td>
<td>23%</td>
<td>19%</td>
<td>13 bytes</td>
</tr>
<tr>
<td>Hamming</td>
<td>16%</td>
<td>9%</td>
<td>26 bytes</td>
</tr>
<tr>
<td>GMM</td>
<td>6.6%</td>
<td>9%</td>
<td>153 bytes</td>
</tr>
</tbody>
</table>

IV. SMART CARDS

Biometric Authentication Systems based in hand geometry or other techniques are available, even commercially and with great success. But this kind of systems present a lack of security due to the way of storing the template and verifying the user’s sample. Not considering the systems based in a central database where the users’ templates are stored, other systems use a portable storage media to keep and transmit the template. Examples of this media could any memory based one, such as magnetic stripe cards, laser cards or integrated circuit cards. With this system configuration the verification is performed in the terminal, therefore needing the terminal to extract the user’s template from the card.

The solution presented by the authors is analog to the advance that smart cards meant about PIN verification, compared to magnetic stripe cards. In smart cards, the PIN is verified inside the card, not being able never to read the PIN from the card, avoiding duplication of the user’s template. The system proposed compares the user’s sample with the template stored, inside the card. To achieve this goal a new data structure must be present in the card, as well as new commands for writing and updating the template, and verifying it. JavaCards have been used to develop the prototype in order to test the technology and after a successful pilot project, to manufacture in hard masking.

The three verification methods selected have been tested, obtaining the following figures:

<table>
<thead>
<tr>
<th></th>
<th>Verification Time</th>
<th>Code Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Euclidean</td>
<td>0.3 seconds</td>
<td>372 bytes</td>
</tr>
<tr>
<td>Hamming</td>
<td>0.2 seconds</td>
<td>428 bytes</td>
</tr>
<tr>
<td>GMM</td>
<td>2.1 seconds</td>
<td>3873 bytes</td>
</tr>
</tbody>
</table>

With these results and the ones showed in the verification analysis, it seems that the Hamming Distance gives the best performance ratio, between Failures (FAR and FRR), code size and verification time.

REFERENCES