Hand-Based Multimodal Identification System with Secure Biometric Template Storage

M.B. Ramalho[1], P.L. Correia[1,2] and L.D. Soares[1,3]

[1]Instituto de Telecomunicações, [2]Instituto Superior Técnico, [3]ISCTE - Instituto Universitário de Lisboa

Torre Norte - Piso 10, Av. Rovisco Pais, 1, 1049-001, Lisboa, Portugal

Phone: +(351)218418461, fax: +(351)218418472

E-mail: {mar, plc, lds}@lx.it.pt

Abstract

This paper proposes a biometric system for personal recognition (identification) based on three biometric characteristics from a single body part: the hand. Features are extracted from the palmprint, finger surface and hand geometry, in order to create a single template. A protection scheme is applied to guarantee the template's revocability, security and diversity amongst different biometric systems. An error-correcting code (ECC), a cryptographic hash function (CHF) and a binarization module are the core of the template protection scheme. Since the ECC and CHF operate on binary data, an additional feature binarization step is required.

This paper proposes: (1) a novel identification architecture that uses hand geometry as a soft biometric to accelerate the identification process and ensure the system's scalability; and (2) a new feature binarization technique that guarantees that the Hamming distance between transformed binary features is proportional to the difference between their real values.

The proposed system achieves promising recognition performance and speed on two publicly available hand image databases.

1 Introduction

Biometrics are an attractive and convenient solution for private data protection, time and attendance control, controlling the access to restricted areas, online banking or identity authentication. Traditionally, this is solved using something a person knows (e.g., password) or possesses (e.g., identifying document, smart card). However, these methods present some serious disadvantages, becoming less reliable in a world where security threats are escalating (e.g., identity theft).

The idea behind biometric systems is to recognize individuals, using pattern recognition algorithms on one or more biometric traits, being the latter called multimodal biometrics. Such systems can operate in verification or identification modes. In verification mode, the person presents the biometric to a sensor and claims an identity (via, e.g., a password); a one-to-one comparison with the stored template is performed to decide if the person is who she claims to be. In identification mode, the biometric presented to the sensor is tested by comparing the acquired template with all registered templates and the person is authenticated if a match is found.

Identification can be extremely time-consuming as many comparisons may be required, unless some criteria are used to reduce the search space. The first steps in biometric sample classification were given by Ratha et al. [1], who proposed a method to reduce the search space when performing fingerprint identification, by assigning a fingerprint sample to a specific class according to its texture. A probe biometric sample is then categorized into the corresponding class and only the templates in the same class are used for matching. A similar classification technique has been applied to iris and palmprint identification [2,3] using, in the latter, the number of principal lines as a classification criterion.

An alternative to the above classification schemes is database indexing, where an index value is assigned to every biometric template in the database. In indexing systems, the identities whose indices are similar to the index value of the probe sample are retrieved. The probe sample is only matched against the retrieved identities, reducing the identification time and, potentially, the identification error rate. An iris database indexing method has been proposed in [4], where a hash is generated from a specific region of the template and used as an index value.

The above mentioned techniques either extract values from the biometric template for database indexing or use implicit features in the biometric sample to divide the database into categories.

This paper proposes the usage of the hand's geometry as a soft biometric to sort the list of identification candidates according to the similarity scores and use this sorted list to index the template database. The hand's geometry is not known to be very distinctive between individuals [5] and the issue of its uniqueness is still somewhat controversial [6]. Recent research studies [7,8,9] have shown high recognition rates, but the datasets used in these studies were acquired in highly controlled environments. Thus, even if the hand's geometry is unique amongst a large population, it might not be feasible to extract accurate features in a rather unconstrained environment [6]. Nevertheless, it is suitable to perform a coarse first approach to the main problem faced by a biometric identification system – "who can this person be?" – and let the most likely candidates in the database be compared to in the first place.

In the proposed system, the final identification decision is taken based on palmprint (PP) and finger surface (FS) matching, which are two well studied modalities. Several PP verification/identification systems have been proposed, using different feature extraction techniques, such as 2-D Gabor filters [10,11,12,13,14], 2-D Gaussian filters [15], finite Radon transform [16] and Discrete Cosine Transform (DCT) [17,18]. Subspace-based approaches are also commonly employed to perform feature extraction through Principal Component Analysis (PCA) [19,20,21], Linear Discriminant Analysis (LDA) [13,20,22,23] and Independent Component Analysis (ICA) [20,24,25]. Although FS recognition systems are not commonly found in the literature, this biometric trait is usually associated with PP in multimodal systems [14,19,22].

Besides the risk of authenticating an impostor, biometric systems present other potential vulnerabilities. The need to store a biometric template on a database is considered to be the main vulnerability amongst biometric systems because, unlike other authentication methods, a person cannot change a biometric if it is compromised due to a security breach in the recognition system. Jain et al. [26] mentioned that one of the most potentially damaging attacks on a biometric system is against the template database. A secure template storage scheme should be employed in order to protect users' identities and guarantee their privacy. This scheme must, however, deal with the acquisition noise, also called intra-user sample variability [27], which may be caused by: environmental variability (e.g., non-uniform illumination), sample presentation variability (e.g., placing the hand at a different angle), intrinsic biological variability (e.g., elastic skin deformation) or acquisition losses/errors introduced by the sensor.

Several schemes that provide secure template storage and deal with sample variability have been proposed, typically using ECC to handle the intra-user variations. Juels and Wattenberg [28] proposed the fuzzy commitment scheme, where a hash function is used to ensure the privacy of the biometric data together with an ECC to deal with intra-user variability. Juels and Sudan [29], proposed the fuzzy vault scheme, which consists in securing a secret κ under a set $A = \{a_1, a_2, ..., a_t\}$, where $a_1, a_2, ..., a_t$ are the features of a biometric template. A single variable polynomial *p(x)* is selected such that its coefficients have the secret κ embedded in some way. Treating the elements of *A* as *x*-values, the values of $p(a_1), p(a_2), ..., p(a_t)$ are computed. This method relies on polynomial reconstruction using a Reed-Solomon ECC. More recently, Vetro et al. [30] proposed a technique that allows secure template storage based on a Low-Density Parity-Check (LDPC) code and a CHF.

In this work, the adopted secure template storage technique is similar to the one proposed in [30], but with a different approach concerning the ECC, a different architecture (identification instead of verification) and a novel binarization technique to convert real-valued features into binary strings.

Despite resulting in a more complex and challenging architecture, identification is chosen over the verification mode because one of the main advantages of biometrics is to allow personal recognition without any additional information that can be forgotten or lost.

The remainder of the paper is organized as follows: Section 2 provides an overview of the system's architecture and details of the pre-processing (Section 2.1) and feature extraction (Section 2.2) modules. Section 3 presents the proposed secure template storage scheme. Details about the template binarization module and the Log-Likelihood Ratio (LLR) initialization method in the LDPC decoder are presented in Sections 3.1 and 3.2, respectively. The enrolment and identification procedures are explained in Sections 3.3 and 3.4. Section 4 presents the test conditions and experimental results. Finally, conclusions and future work are discussed in Section 5.

2 System Overview

The proposed system architecture is illustrated in Figure 1 and Figure 2, for the enrolment and identification stages, respectively. In both cases, the acquired sample undergoes the same processing until the template binarization module.

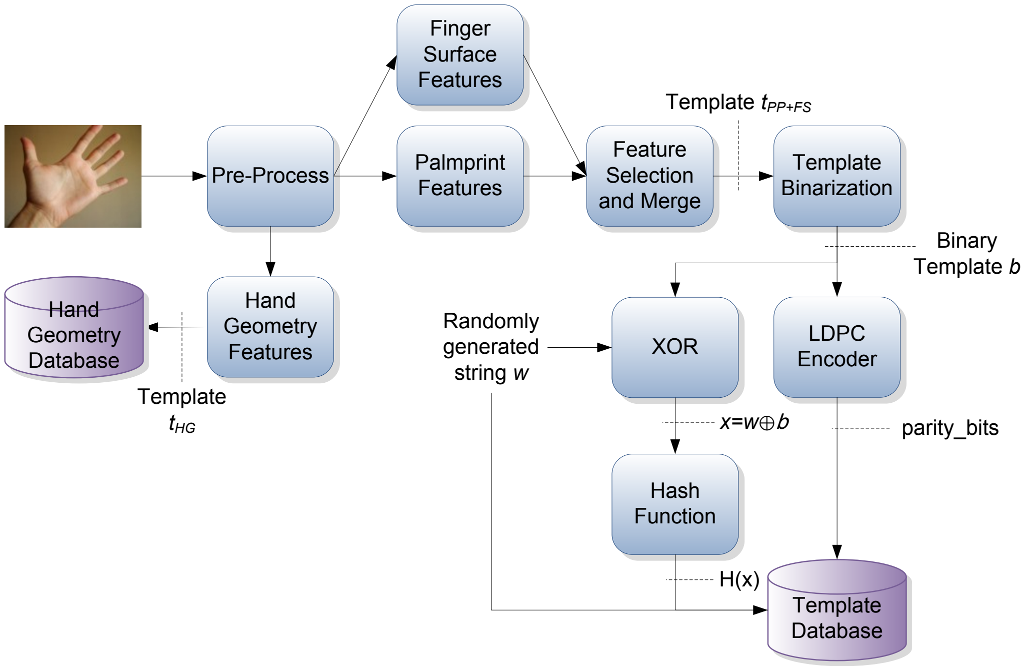


Figure 1 – Proposed system architecture: enrolment stage.

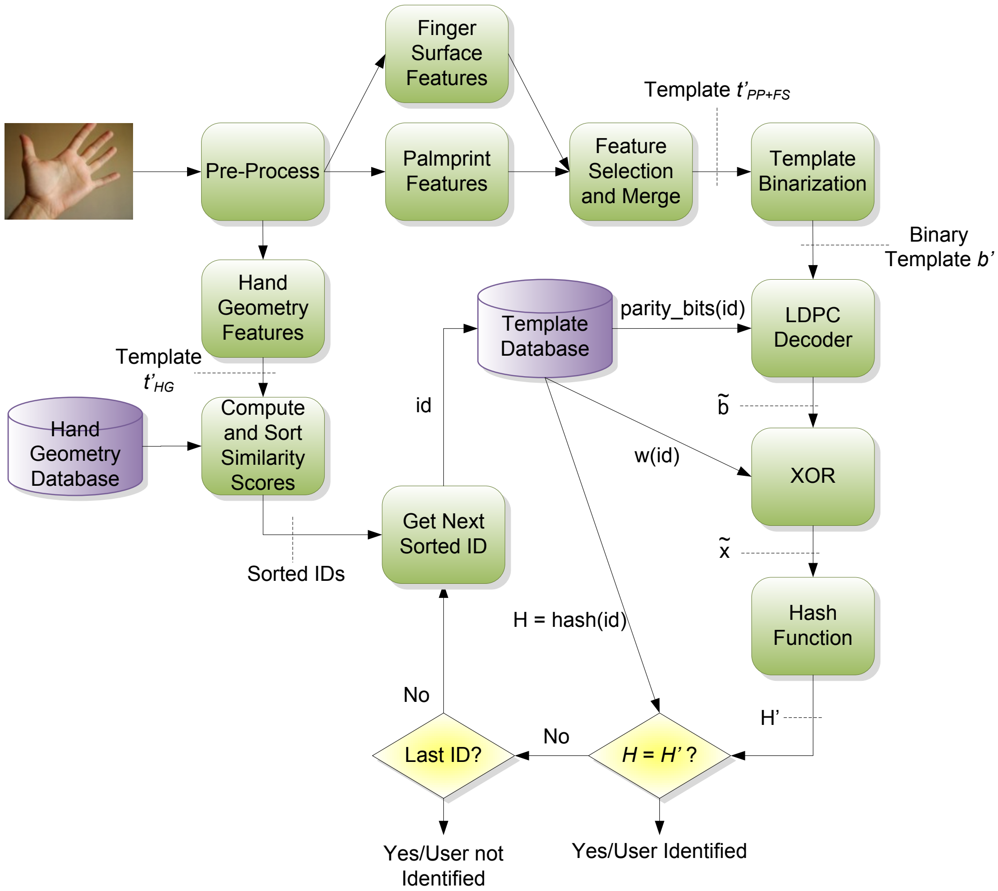


Figure 2 – Proposed system architecture: identification stage.

Although score-level fusion is the most commonly used fusion technique [31], the proposed system combines PP and FS at feature-level. This is because score-level fusion cannot be applied to the proposed architecture, where only an encrypted (and non-invertible) version of the template is stored in the database, for which it is meaningless to compute matching scores.

2.1 Pre-processing

The pre-processing module computes the hand's contour and the regions of interest (ROI), which are the palm and the index, middle, ring and little finger regions. The thumb is discarded because its texture is typically not completely visible in the acquired images due to its sideways positioning.

The major pre-processing steps are illustrated in Figure 3. In the first place, the input image is converted to greyscale and resized to a lower dimension in order to reduce the computational burden in further processing. The resized image is binarized using Otsu's method [32] and the contour is traced. Then, the fingertips $\left(ft_1,...,ft_5\right)$ and finger-webs $\left(fw_1,...,fw_4\right)$ are detected using a combination of two commonly used techniques: radial distance to a reference point and contour curvegram [7]. Let ft_1 always correspond to the little finger's tip and fw_1 to the finger-web between the little and ring fingers and so on. In order to segment the ROIs from the input image, two reference points, rp_1 and rp_2, are also computed. These points are determined by discovering, for the little and index fingers, which contour point, p, satisfies the following conditions:

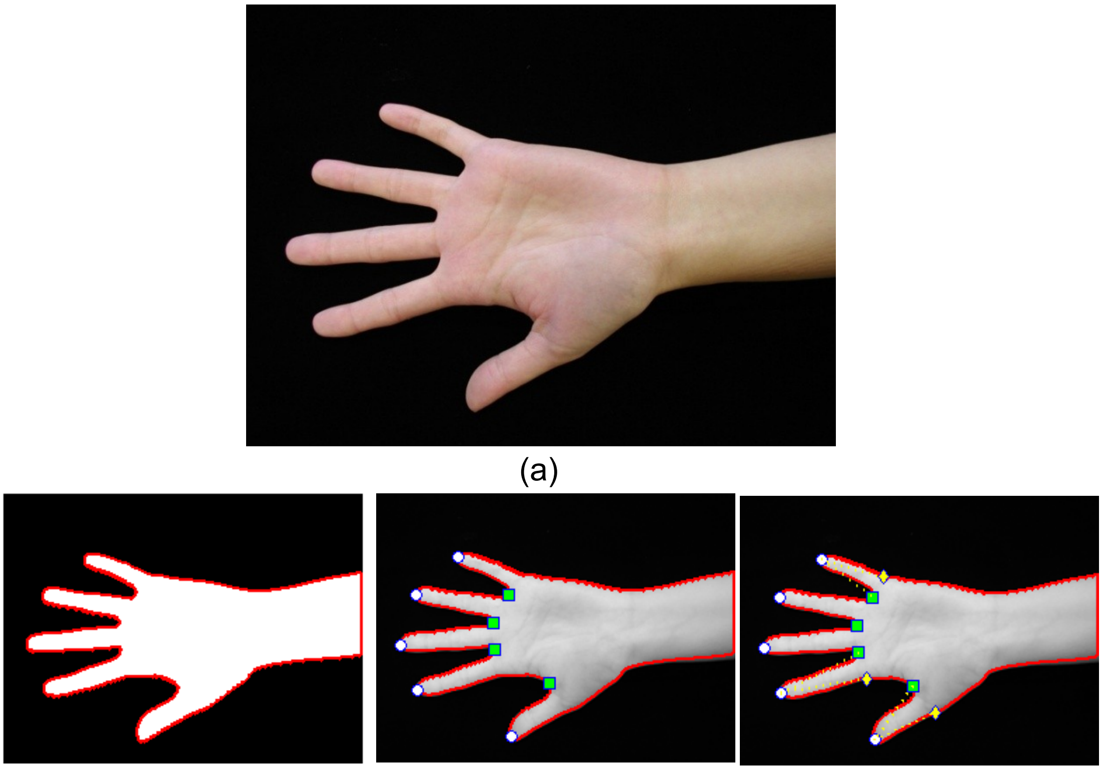
$$\begin{aligned} rp_1 &= \left\{p : d\left(ft_1, fw_1\right) = d\left(ft_1, p\right)\right\}, \\ rp_2 &= \left\{p : d\left(ft_4, fw_3\right) = d\left(ft_4, p\right)\right\}, \end{aligned} \tag{1}$$

where d denotes the Euclidean distance. Since there may be multiple contour points that satisfy these conditions, the search for rp_1 and rp_2 should begin in the fingertips and follow the contour until the target distance has been found. The obtained point should be matched against the already known finger-webs to check if the contour tracking was done in the correct direction. For hand geometry feature extraction purposes, an additional reference point for the thumb, rp_3, is computed in the same manner.

Finally, the ROIs are detected and segmented using the previously calculated points and are then resized to a standard size. The palm area is defined as a square region where two of the vertices, v_1 and v_2, are computed as

$$v_1 = \frac{fw_1 + rp_1}{2}, v_2 = \frac{fw_3 + rp_2}{2}. \tag{2}$$

The remaining vertices are derived from v_1 and v_2 by selecting the square that lies inside the contour. The fingers' areas are defined as the largest rectangles that lie inside the finger contours, which are the contour segments delimited by the fw and rp points, depending on the finger.



(a)

(b)

(c)

(d)

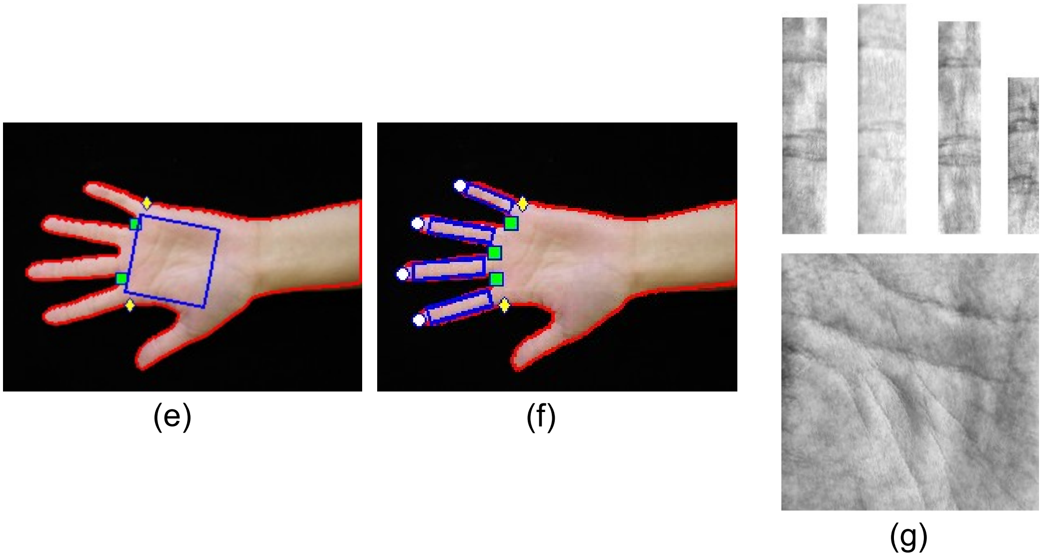


Figure 3 – Major pre-processing steps: (a) – input image; (b) – binarization and contour tracing; (c) – fingertip (circles) and finger-web (squares) detection; (d) – additional reference points computation (diamonds); (e) – palm segmentation; (f) – finger segmentation; (g) – extracted ROIs.

Before feature extraction, the palm and finger ROIs are resized to 16x16 and 32x8 pixels, respectively.

2.2 Feature Extraction

Palmprint and finger surface features are extracted using LDA, which projects the ROI vectors into a subspace where the between-class variations are maximized and the within-class variations are minimized [23]. This property is very useful for the proposed binarization scheme (see Section 3.1) which, in turn, has good properties for the initialization procedure in the LDPC decoder (see Section 3.2). A total of 64 features are extracted from the PP and from each finger, out of which, only the features with smaller intra-class variations are selected and merged into a final template. The merged template contains 140 features: 40 PP features and 100 FS features (20 for each finger).

Besides improving the recognition performance, limiting the number of features is also a way of assigning weights to each biometric characteristic, i.e., the more discriminative it is, the more features are used to represent it in the template.

Hand geometry features are measures, in pixels, computed from the hand contour, namely: twenty finger widths (four from each finger), five finger lengths, five finger perimeters and five intra-palm distances (see Figure 4).

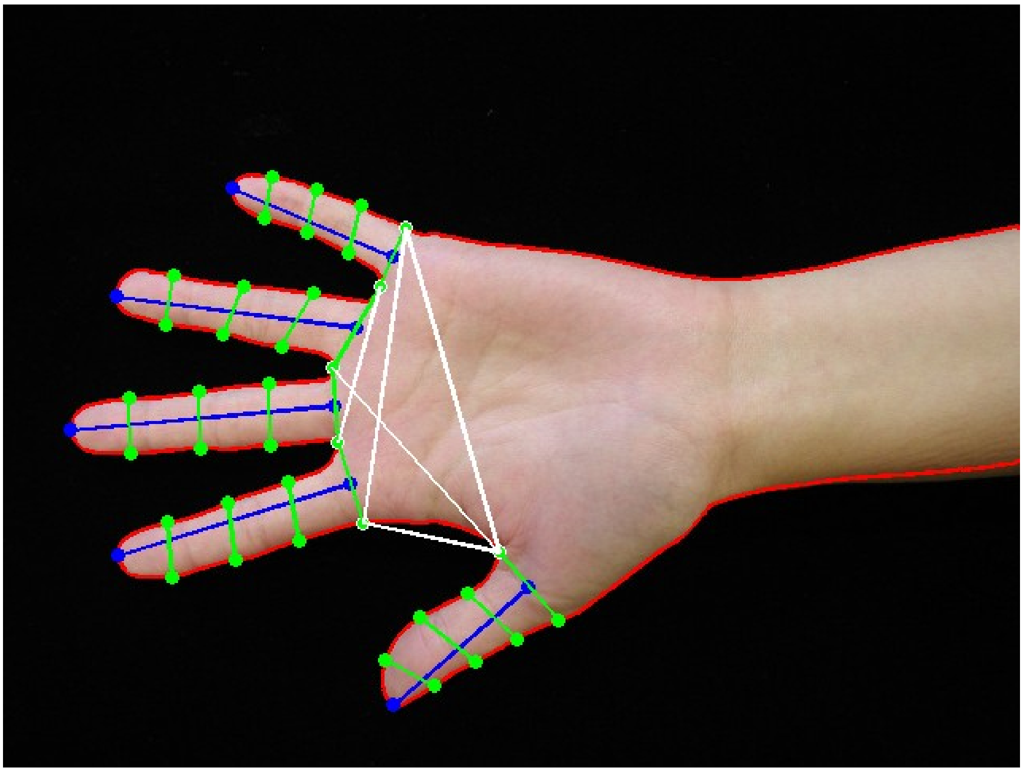


Figure 4 – Hand geometry features.

3 Secure Template Storage

A CHF is an effective way to encrypt data for it is a non-invertible transform. However, due to its dispersive nature, it has completely different outputs for similar inputs. This is a major disadvantage when dealing with biometric data, because two measurements of the same user are never exactly equal and so will not be the encrypted data, transformed by the CHF. This is different from what happens in password-based systems. To deal with this issue, an LDPC code is used, which cancels the acquisition noise by correcting the errors in biometric templates. When a user attempts to be recognized, the errors (i.e., differences) in the newly acquired template will be corrected (up to a certain extent) to match the template that was acquired when the user was registered in the biometric system.

To use ECC and CHF, these secure template storage schemes require a fixed-length binary representation of the biometric sample, referred to as a binary feature vector [33] or binary template.

3.1 Template Binarization

The binarization module transforms the features in the real-valued template *t* into binary strings, which are then concatenated to form the binary template *b*. Each real-valued feature has its own feature space, which is an interval $\left[c,d\right]$, where *c* and *d* are the minimum and maximum observed values of that feature in the training set (defined in Section 4). A quantizer is then applied to each feature space, dividing it into *N* equiprobable intervals to guarantee that the probability of a feature falling in any interval is the same and equal to $1/N$. According to Chen et al. [34], having the same probability mass in all intervals is beneficial for the users' privacy, as it yields independent output bits. Each interval is then associated with a binary string that is used to code a feature if its value is comprehended between the interval's boundaries. This process is illustrated in Figure 5, where a histogram containing the frequency of the observed values for a given feature is represented, as well as a fitted Gaussian curve for a clearer perception of the equiprobable intervals.

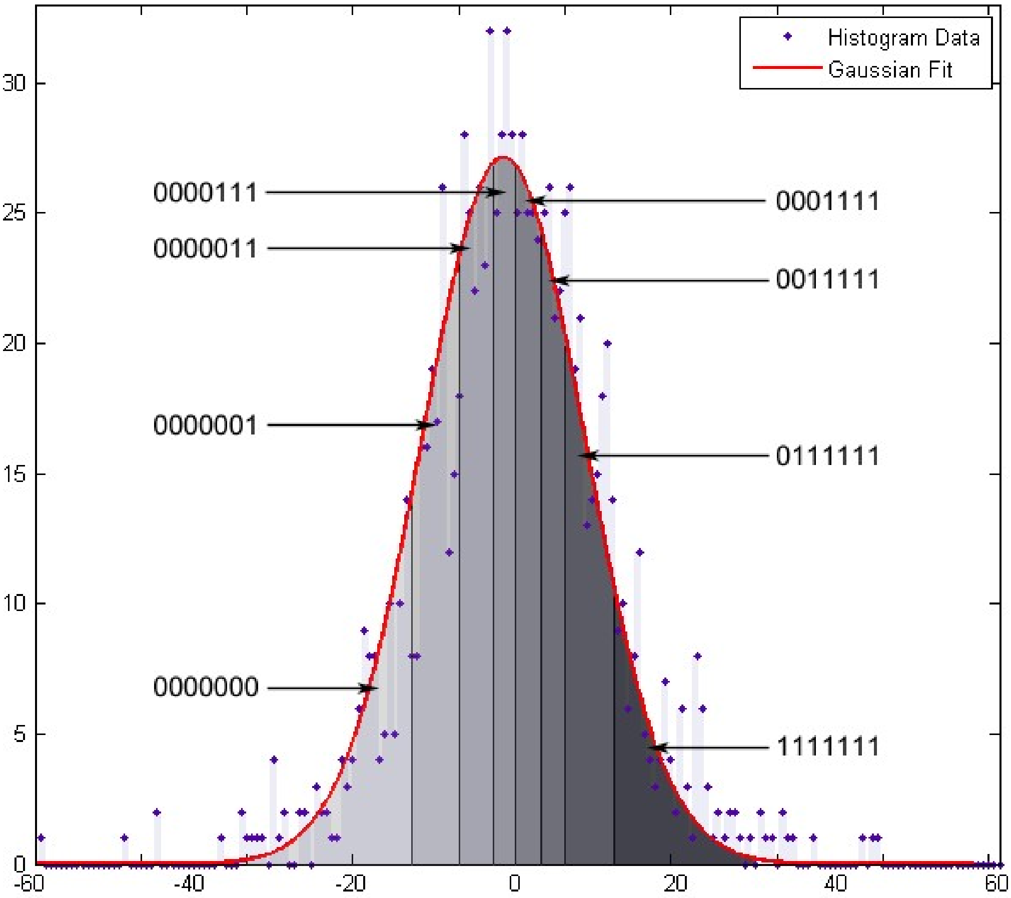


Figure 5 – Equiprobable interval division of feature space, for *N*=8.

The binary coding of each feature space uses *N* binary strings of length $N-1$, that are generated by the following algorithm:

```
for i=1;i<N;i++ {
      b[i] = 1;
}
binary_coding[1] = b;
for i=2;i<=N;i++ {
      b = b >> 1; /* Bitwise shift right by 1 position */
      binary_coding[i] = b;
```

}

Let $\Delta = \{\delta_i : i = 1,2,...,N\}$ represent the set of binary strings used to code the intervals. For $N = 8$, the resulting binary coding is $\Delta =${0000000, 0000001, 0000011, 0000111, 0001111, 0011111, 0111111, 1111111}. The equiprobable intervals are coded in this manner to satisfy the following condition:

$$HD(\delta_i, \delta_{i+j}) = |j|, \tag{3}$$

where *HD* is the Hamming distance between the two binary strings. This condition maintains larger Hamming distances between binary strings used to encode further apart intervals, which guarantees that the distance between two real-valued features is reflected in the Hamming distance computed on the transformed binary features.

The above proposed template binarization scheme produces fixed-length binary templates with $T = num_{features} \times (N - 1)$ bits.

3.2 LDPC Decoder

The LDPC codes were first introduced by Gallager in 1962 [35], but remained unused for 30 years due to the high computational requirements. It was only with the appearance of turbo codes, in 1993, that the application of LDPC codes was made technologically possible and popularized [36].

The LDPC code is suitable for biometric systems due to its granularity and correcting power, i.e., by varying the number of parity bits used, the correcting capacity can be very finely adjusted while maintaining a steep slope curve. This is of high importance because when used in a biometric system, the objective of an ECC is not to correct all bit errors (to avoid correcting impostor templates), but to correct binary strings with, at most, a determined bit error rate (BER). In this work, BER is defined as the bit error rate measured between two binary templates at the decoder's input side rather than the output side.

The LDPC decoding process is iterative and done by belief propagation [35]. In the proposed system, the number of iterations is limited to 20 because experiments revealed that a larger number of iterations degraded the recognition speed while not bringing significant improvements on the correcting capacity. The decoder’s inputs are not the binary template and parity bits, but their associated LLR instead, which is given by:

$$LLR(b_i \mid b_i') = \log\left(\frac{P(b_i = 0 \mid b_i')}{P(b_i = 1 \mid b_i')}\right) = \log\left(\frac{1 - P(b_i = 1 \mid b_i')}{P(b_i = 1 \mid b_i')}\right), \qquad (4)$$

where $P(b_i = 1 \mid b_i')$ is the probability of the *i*-th bit in *b* being 1, given the observed value in b_i'. Since there is no model for the intra-user sample variability, an easy but less effective way to deal with this issue would be to set the initial LLR to a random or fixed value, for example, $\alpha < 0$ if the bit is 1 and $\alpha > 0$ if the bit is 0. However, this would be a poor choice of the initial LLR values as it would not give any information to the decoder about the certainty of the bit's value.

In the proposed system, these probabilities can easily be estimated due to the interval coding used in the proposed template binarization module. To do this, the first step is to divide the probe binary template into strings with length $N-1$, to treat each feature separately. The next step is to match the feature’s value in the coding table, as illustrated in Table 1. Assuming that the feature's value corresponds to δ_i, the binary strings in the range $[\delta_{i-\varepsilon}, \delta_{i+\varepsilon}]$ are selected and the probabilities for each bit are estimated based on the observed frequencies. In the proposed system, ε is set to 2.

Interval	Coding ($b_1b_2b_3b_4b_5b_6b_7$)	
1	$\delta_1 = 0000000$	$P(b_1 = 1) = 0/5 = 0$
2	$\delta_2 = 0000001$	$P(b_2 = 1) = 1/5 = 0.2$
3	$\delta_3 = 0000011$	$P(b_3 = 1) = 2/5 = 0.4$
4	$\delta_4 = 0000111$	$P(b_4 = 1) = 3/5 = 0.6$
→ 5	$\delta_5 = 0001111$	$P(b_5 = 1) = 4/5 = 0.8$
6	$\delta_6 = 0011111$	$P(b_6 = 1) = 5/5 = 1$
7	$\delta_7 = 0111111$	$P(b_7 = 1) = 5/5 = 1$
8	$\delta_8 = 1111111$	

Table 1 – Probability estimation for interval 5 with $N = 8$ and $\varepsilon = 2$.

If $P(b_i = 1 | b') = 1$ or $P(b_i = 1 | b') = 0$, the corresponding LLR would be $-\infty$ or $+\infty$, which would prevent the decoder from correcting that bit, as happens with b_1, b_6 and b_7 in Table 1. For this reason and because the probabilities are only an estimate, the value 1 is changed to 0.95 and the value 0 is changed to 0.05. As for the parity bits, they are not affected by the acquisition noise and are assumed to be uncorrupted, so the LLR is $-\infty$ or $+\infty$ if the parity bit is 1 or 0, respectively.

3.3 Enrolment

In the enrolment stage (see Figure 1), the binary template, b, is processed by the LDPC encoder, which computes a set of parity bits, p, that are stored in the template database; b is also processed by a XOR module, which computes the bitwise exclusive disjunction between b and a randomly generated binary string, w, to output a result x. This is done for two reasons: i) to guarantee that two templates from the same person are different in distinct biometric systems and ii) to ensure that if a template is compromised, a new one can be issued just by changing w.

Since w is stored in the database, it would be trivial to recover b from x and w, so x is transformed by a CHF to guarantee its privacy. The result, $H(x)$, is also stored in the database. The user's template is stored as the triplet (p,w,H) and is associated with an ID, which is an automatically generated number. The same ID is associated with the template t_{HG}, which is stored in the hand geometry database.

3.4 Identification

The goal is to determine whether a probe binary template, b', belongs to a registered user or not (see Figure 2). First, the probe template t'_{HG} is compared to all registered templates in the hand geometry database and the similarity scores are computed using the Euclidean distance and then sorted. Let id_1 be the ID with the highest similarity score. The data associated with id_1in the template database,(p,w,H), is retrieved and the parity bits, p, extracted from b are used in the LDPC decoder to correct b'. If the number of bits in b' differing from b is less than the correcting power of the LDPC code, then $\tilde{b} = b \Leftrightarrow H' = H$ and the user is authenticated. Otherwise, the identification algorithm takes the next ID in the sorted list, retrieves the respective stored data and the process is repeated. If no more IDs are available, the user is not authenticated.

4 Experimental Results

The proposed system operates in a semi-constrained environment. The distance between the acquisition device and the user's hand must be approximately constant. Also, the background must be of a colour that contrasts with the skin. However, the user can place his hand freely within the sensor's field of view.

Recognition performance tests were carried out on two publicly available hand image databases that satisfy the abovementioned requirements: the UST [37] and GPDS [38] hand image databases. Although [37] and [38] report a database size of 100 and 109 users, their latest versions, [39] and [40], contain 287 and 150 users, respectively. The well-known PolyU palmprint database [10] is not suitable to test the proposed system because its images do not include the fingers.

The UST database is composed of 5740 images, captured with a digital camera, from both left and right hands of 287 users (10 images per hand). For recognition performance tests, each hand is treated as a different user. Therefore, a total of 574 identities is considered. The GPDS database contains 1500 images, acquired with a desk scanner, of 150 users' right hands (10 images per user).

For both databases, training and test sets were built. The training set contains five randomly chosen templates from every user, which are registered in the database, and the test set contains the remaining five templates.

Recognition performance tests consist in comparing each template in the test set with all the templates in the training set to generate a matching score (in this case, the Hamming distance is used). Therefore, each test template generates 5 genuine and $(num\_users - 1) \times 5$ impostor Hamming distances. The number of genuine and impostor comparisons are presented in Table 2.

	Genuine	Impostor
UST	14,350	1,644,510
GPDS	3,750	111,750

Table 2 – Number of genuine and impostor comparisons in the UST and GPDS databases.

Recognition results can be depicted in the form of receiver operating characteristic (ROC) curves, as illustrated in Figure 6, where the results for PP, ring, middle and index fingers, as well as the four finger surfaces' feature-level fusion (FSF) and PP+FSF fusion are presented. It is clear that the recognition accuracy of the multimodal fusion is better than any of the biometric characteristics, when used separately. Another form of presenting the recognition results is through genuine and impostor distributions (see Figure 7) and the most common measure to evaluate these distributions is the decidability index [41]. It reflects how well separated the two distributions are and is given by:

$$d' = \frac{|\mu_g - \mu_i|}{\sqrt{\frac{(\sigma_g^2 + \sigma_i^2)}{2}}}, \tag{5}$$

Where μ_g, μ_i, σ_g and σ_i are the means and standard deviations of the genuine and impostor distributions, respectively.

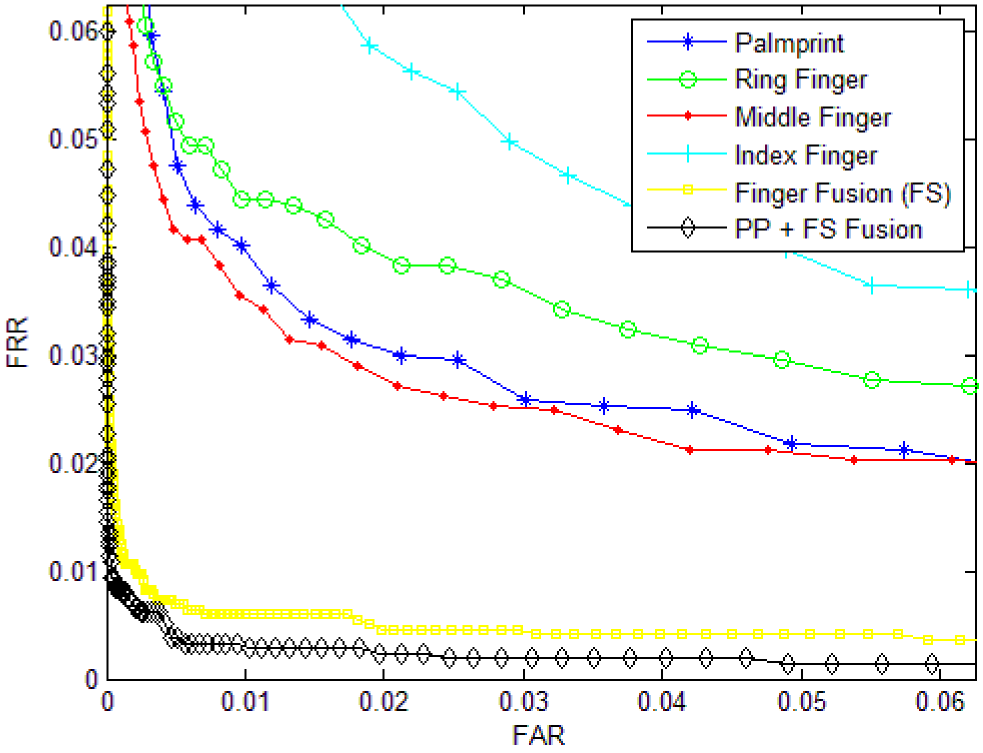
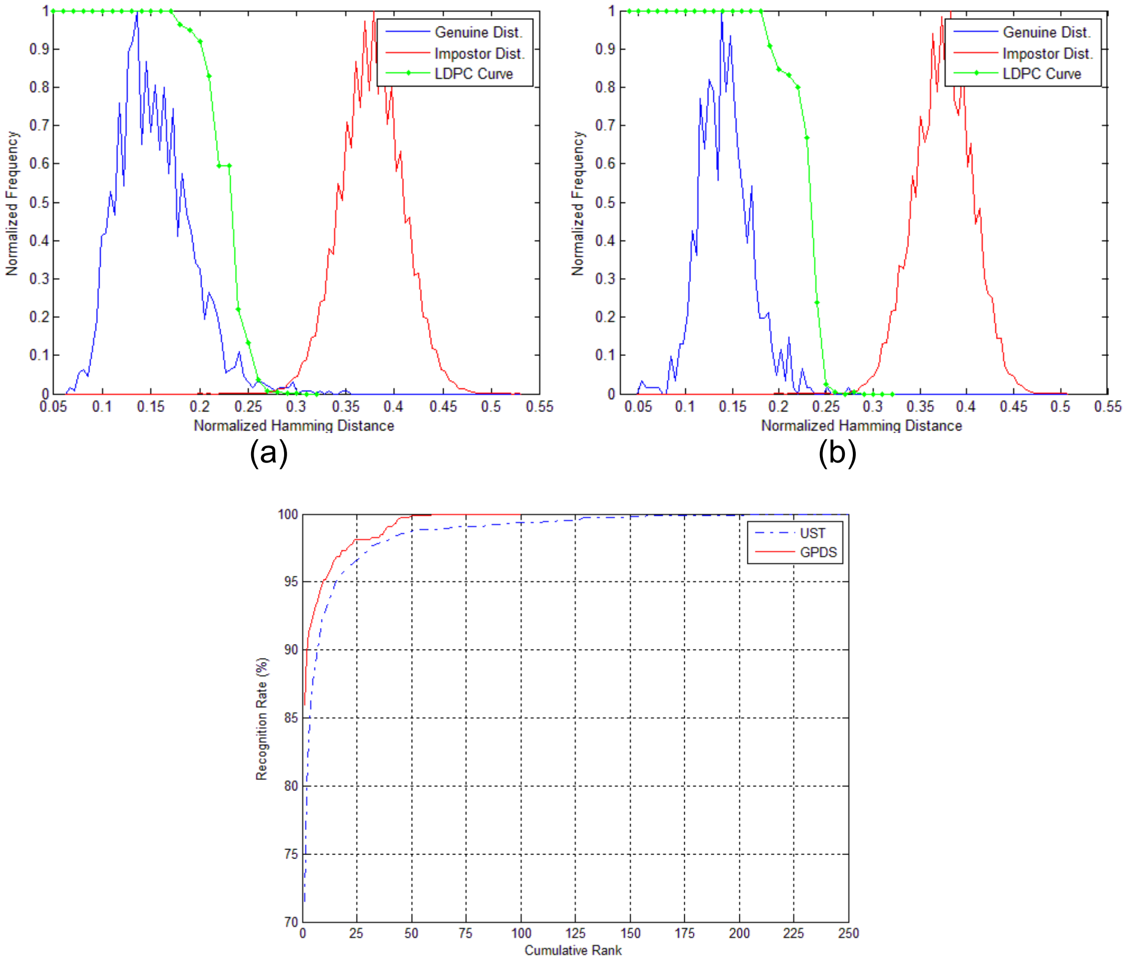


Figure 6 – Recognition results for PP, Ring, Middle and Index Fingers, FSF and PP+FSF fusion on the UST database.

The number of intervals used in the binarization module is $N = 8$, as it was found to yield the best recognition results. This leads to a template length of $T = num_{features} \times (N-1) = 140 \times 7 = 980$ bits.

Since the two databases have slightly different correcting capacity requirements, two LDPC codes were used: a (980,880) code and (980,890) code, which will be referred to as code 1 and code 2, respectively, from now on. These LDPC codes were designed to correct templates with a BER of, at most, 26% and 27%, respectively. The parity-check matrices have a fixed number of 3 ones per column and a variable number of ones per row: $\rho_{1,4} = 0.6966$, $\rho_{1,5} = 0.3034$, $\rho_{2,4} = 0.6591$ and $\rho_{2,5} = 0.3409$ represent the ratio of rows that contain 4 and 5 ones in code 1 and code 2, respectively. As expected, the LDPC codes have a filtering effect on the genuine/impostor distributions, as illustrated in Figure 7 (a) and (b).



(a)

(b)

(c)

Figure 7 – Recognition performance results: genuine (left) and impostor (right) distributions overlaid with the LDPC correction curve on (a) UST database

and (b) GPDS database; (c) hand geometry cumulative rank curve on both databases.

The resulting Equal Error Rates (EER) are 0.43% and 0.047% and the decidability index values are 6.36 and 7.89 for the UST and GPDS databases, respectively. The extent to which the LDPC decoder corrects the probe templates is what defines the system's operating point, in terms of False Acceptance Rate (FAR) and False Rejection Rate (FRR). Since a secure biometric system is proposed, a low FAR is chosen over a low FRR to prevent impostor access. Using code 1 and code 2, the results are a 0.01% FAR and 2.63% FRR on the UST database and a 0% FAR and 0.95% FRR on the GPDS database.

In Figure 7 (c), a hand geometry cumulative rank curve is presented. As expected, the smaller population in the GPDS allows better recognition results and the images also produce more reliable hand geometry features because they were acquired using a desk scanner, so the hand is placed on a stable, fixed surface. As a result, the genuine user is sorted out in the first place 85.95% of the times, against the 71.51% in the UST database. Using the hand's geometry as a soft biometric in the proposed system proves to be advantageous because it reduces the number of LDPC decoding attempts, which is a costly process. A comparison is presented in Table 3.

	Without Soft Biometrics		**With Soft Biometrics**	
	UST	GPDS	UST	GPDS
Pre-process and Feature Extraction	40 ms	40 ms	40 ms	40 ms
Template Binarization	1 ms	1 ms	1 ms	1 ms
Similarity Score Computation	N/A	N/A	4 ms	1 ms
LDPC Decoding	1.56 s	614 ms	29ms	17ms
Total Identification Time	1.601 s	655 ms	74ms	59ms

Table 3 – Comparison of average identification time with and without using soft biometrics. The LDPC decoding time is computed as the average time until a positive match is found (see Figure 2).

The probability estimation scheme, presented in Section 3.2, allows an LDPC decoder to achieve greater correction capability with the same amount of parity bits. In other words, an LDPC decoder requires a smaller amount of parity bits to achieve the same correction capacity as an LDPC decoder with no knowledge about the probabilities (see Figure 8).

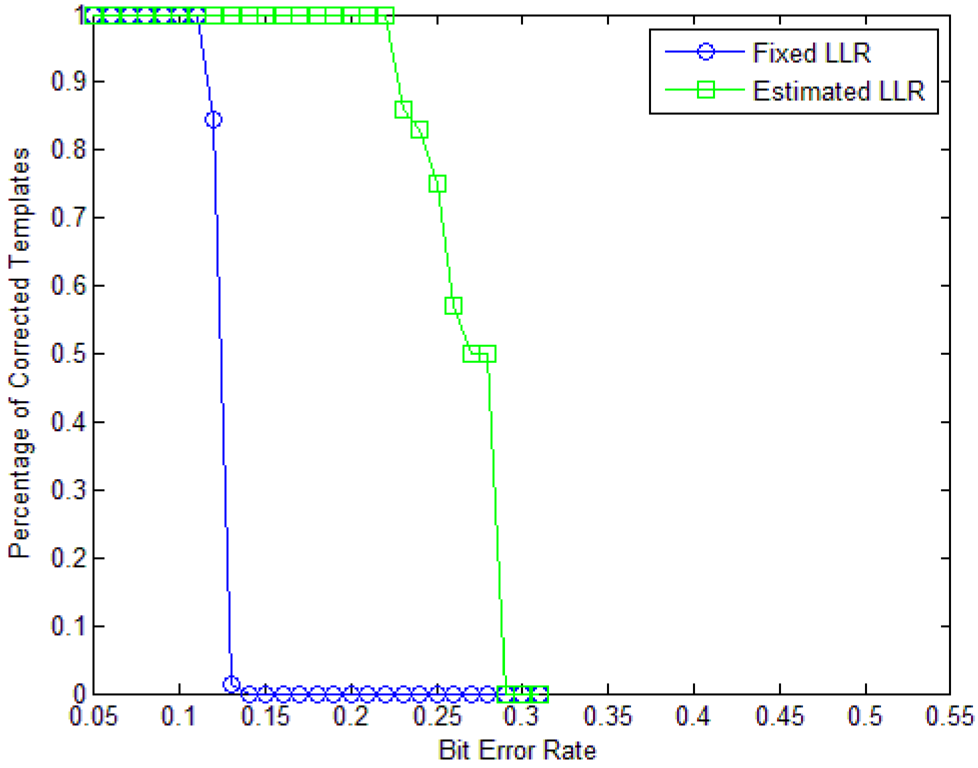


Figure 8 – Correcting performance of an LDPC code using fixed and estimated LLR values.

Parity bits are the result of the linear modulo-2 equation: $p = H_{LDPC} \cdot b$, where H_{LDPC} is the parity-check matrix and b is the binary template. If b has length T and p length k, there are k equations and T unknowns, $T > k$. Operating on a binary field, there are 2^{T-k} possible solutions [42]. According to [30], the security metric in an ECC-based secure biometric system is the number of security bits, given by $T - k$.

Summarizing, the proposed LLR initialization method provides the system with more security, measured with the metric described above.

5 Conclusions and Future Work

This paper proposes a fast multimodal identification system that achieves good recognition accuracy while securing the stored data.

Feature-level fusion is used because, as mentioned in Section 2, score-level fusion is not feasible. Another commonly used fusion strategy, at the decision level, was not used in the proposed system because the recognition based on each finger is not very accurate, as shown in Figure 6. Using decision-level fusion on PP and FSF would also not be very wise, since there would be an even number of decisions. Other levels of fusion (e.g., rank- or sensor-level) are also not applicable to the proposed system [31].

The proposed database indexing technique presents some advantages over previously proposed classification and indexing methods. Unlike classification techniques, no errors are introduced in the system due to misclassification of the input image and unlike the previous indexing techniques, no candidates are excluded. If only a given number of top candidates were considered, the hand's geometry would limit the recognition accuracy. Thus, the proposed system is able to perform faster without affecting the FAR and FRR. Also, the usage of hand geometry as a soft biometric makes the system scalable because the computation of similarity scores is a fast process and, since the similarity scores are sorted, the average number of decoding attempts can be considered independent of the number of registered users.

The downside of storing hand geometry templates in the clear for fast comparisons is that it exposes some information about the user. This does not affect the proposed system because the final decision does not rely on hand geometry; however, it may compromise other biometric systems where this trait is used. In the future, this problem will be addressed.

The proposed binarization technique is a high-level and general method that can be applied to other biometric traits (e.g., face). The interval coding was specifically designed to provide a good estimate of the initial LLR value, which improves the system's security by reducing the number of parity bits that need to be stored along with the hashed version of the template.

6 Acknowledgements

The authors acknowledge the support of Fundação para a Ciência e Tecnologia (FCT), under the project BioSec - PTDC/EEATEL/098755/2008.

7 References

[1] N K Ratha, K Karu, S Chen, and A K Jain, "A Real-Time Matching System for Large Fingerprint Databases," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 18, no. 8, pp. 799-813, August 1996.

[2] L Yu, D Zhang, K Wang, and W Yang, "Coarse Iris Classification Using Box-counting to Estimate Fractal Dimensions," *Pattern Recognition*, vol. 38, no. 11, pp. 1791-1798, November 2005.

[3] X Wu, D Zhang, K Wang, and B Huang, "Palmprint Classification Using Principal Lines," *Pattern Recognition*, vol. 37, no. 10, pp. 1987-1998, October 2004.

[4] C Rathgeb and A Uhl, "Iris-Biometric Hash Generation for Biometric

Database Indexing," in *20th International Conference on Pattern Recognition (ICPR)*, Instanbul, Turkey, 2010, pp. 2848-2851.

[5] A Ross and A K Jain, "Human Recognition Using Biometrics: An Overview," *Annals of Telecommunications*, vol. 62, no. 1, pp. 11-35, January 2007.

[6] N Duta, "A Survey of Biometric Technology Based on Hand Shape," *Pattern Recognition*, vol. 42, no. 11, pp. 2797-2806, November 2009.

[7] E Yörük, E KonukoGlu, B Sankur, and J Darbon, "Shape-Based Hand Recognition," *IEEE Transactions on Image Processing*, vol. 15, no. 7, pp. 1803-1815, July 2006.

[8] H Dutagaci, B Sankur, and E Yoruk, "A Comparative Analysis of Global Hand Appearance-based Person Recognition," *Journal of Electronic Imaging*, vol. 17, no. 1, pp. 011018/1-011018/19, January 2008.

[9] G Amayeh, G Bebis, A Erol, and M Nicolescu, "Peg-Free Hand Shape Verification Using High Order Zernike Moments," in *Conference on Computer Vision and Pattern Recognition Workshop*, 2006, pp. 40-47.

[10] D Zhang, W-K Kong, J You, and M Wong, "Online Palmprint Identification," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 9, pp. 1041-1050, September 2003.

[11] Wai Kin Kong, David Zhang, and Wenxin Li, "Palmprint Feature Extraction Using 2-D Gabor Filters," *Pattern Recognition Journal*, vol. 36, no. 10, pp. 2339-2347, October 2003.

[12] A W-K Kong and D Zhang, "Competitive Coding Scheme for Palmprint Verification," in *17th International Conference on Pattern Recognition*,

2004, pp. 520-523.

[13] V Struc and N Pavesic, "Phase Congruency Features for Palm-print," *IET Signal Processing*, vol. 3, no. 4, pp. 258-268, July 2009.

[14] M A Ferrer, A Morales, C M Travieso, and J B Alonso, "Combining Hand Biometric Traits for Personal Identification," in *43rd Annual International Carnahan Conference on Security Technology*, Zurich, Switzerland, 2009, pp. 155-159.

[15] Z Sun, T Tan, Y Wang, and S Z Li, "Ordinal Palmprint Representation for Personal Identification," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR)*, San Diego, CA, USA, 2005, pp. 279-284.

[16] D S Huang, W Jia, and D Zhang, "Palmprint Verification Based on Principal Lines," *Pattern Recognition*, vol. 41, no. 4, pp. 1316-1328, April 2008.

[17] X-Y Jing and D Zhang, "A Face and Palmprint Recognition Approach Based on Discriminant DCT Feature Extraction," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, vol. 34, no. 6, pp. 2405-2415, December 2004.

[18] A Kumar and D Zhang, "Personal Recognition Using Hand Shape and Texture," *IEEE Transactions on Image Processing*, vol. 15, no. 8, pp. 2454-2461, August 2006.

[19] S Ribaric and I Fratric, "A Biometric Identification System Based on Eigenpalm and Eigenfinger Features," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 27, no. 11, pp. 1698-1709,

November 2005.

[20] T Connie, A T B Jin, M G K Ong, and D N C Ling, "An Automated Palmprint Recognition System," *Image and Vision Computing*, vol. 23, no. 5, pp. 501-515, May 2005.

[21] G Lu, D Zhang, and K Wang, "Palmprint Recognition Using Eigenpalms Features," *Pattern Recognition Letters*, vol. 24, no. 9-10, pp. 1463-1467, June 2003.

[22] T Savic and N Pavesic, "Personal Recognition Based on an Image of the Palmar Surface of the Hand," *Pattern Recognition*, vol. 40, no. 11, pp. 3152-3163, November 2007.

[23] X Wu, D Zhang, and K Wang, "Fisherpalms Based Palmprint Recognition," *Pattern Recognition Letters*, vol. 24, no. 15, pp. 2829-2838, November 2003.

[24] G-M Lu, K-Q Wang, and D Zhang, "Wavelet based independent component analysis for palmprint identification," in *Proceedings of International Conference on Machine Learning and Cybernetics*, Shanghai, China, 2004, pp. 3547-3550 vol.6.

[25] L Shang, D-S Huang, J-X Du, and C-H Zheng, "Palmprint Recognition Using FastICA Algorithm and Radial Basis Probabilistic Neural Network," *Neurocomputing*, vol. 69, no. 13-15, pp. 1782-1786, August 2006.

[26] Anil K Jain, Karthik Nandakumar, and Abhishek Nagar, "Biometric Template Security," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, January 2008.

[27] S Z Li and A K Jain, *Encyclopedia of Biometrics, Volume 2*.: Springer, p.

97.

[28] A Juels and M Wattenberg, "A Fuzzy Commitment Scheme," in *Proceedings of Sixth ACM Conference on Computer and Communications Security*, Singapore, 1999, pp. 28-36.

[29] A Juels and M Sudan, "A Fuzzy Vault Scheme," in *Proceedings of IEEE International Symposium on Information Theory*, Lausanne, Switzerland, 2002, p. 408.

[30] A Vetro, S Draper, S Rane, and J Yedidia, "Securing Biometric Data," in *Distributed Source Coding*.: Academic Press, 2009, ch. 11, pp. 293-324.

[31] A Ross, K Nandakumar, and A K Jain, *Handbook of Multibiometrics*, 1st ed. New York, USA: Springer, 2006.

[32] N Otsu, "A Threshold Selection Method from Gray-Level Histograms," *IEEE Transactions os Systems, Man and Cybernetics*, vol. 9, no. 1, pp. 62-66, January 1979.

[33] E J C Kelkboom, G G Molina, T A M Kevenaar, R N J Veldhuis, and W Jonker, "Binary Biometrics: An Analytic Framework to Estimate the Bit Error Probability under Gaussian Assumption," in *2nd IEEE International Conference on Biometrics: Theory Applications and Systems*, Washington, USA, 2008, pp. 1-6.

[34] C Chen, R.N.J. Veldhuis, T.A.M. Kevenaar, and A.H.M. Akkermans, "Biometric Binary String Generation with Detection Rate Optimized Bit Allocation," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, Anchorage, Alaska, USA, 2008, pp. 1-7.

[35] R Gallager, "Low-Density Parity-Check Codes," *IRE Transactions on Information Theory*, vol. 8, no. 1, p. 21, January 1962.

[36] T Richardson and R Urbanke, "The capacity of low-density parity check codes under message-passing decoding," *IEEE Transactions on Information Theory*, vol. 47, pp. 599-618, 2001.

[37] A Kumar, D C M Wong, H C Shen, and A K Jain, "Personal Authentication Using Hand Images," *Pattern Recognition Letters*, vol. 27, no. 13, pp. 1478-1486, October 2006.

[38] Miguel Ferrer, Aythami Morales, Carlos Travieso, and Jesús Alonso, "Low Cost Multimodal Biometric identification System Based on Hand Geometry, Palm and Finger Print Texture," in *41st Annual IEEE International Carnahan Conference on Security Technology*, 2007, pp. 52-58.

[39] (2011, May) UST Hand Image Database. [Online]. http://www.comp.polyu.edu.hk/csajaykr/Database/palm/2dhand.htm

[40] (2011, May) GPDS Hand Image Database. [Online]. http://www.gpds.ulpgc.es/download/index.htm

[41] J Daugman, "How Iris Recognition Works," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 21-30, January 2004.

[42] A Stoianov, "Security of Error Correcting Code for Biometric Encryption," in *Eighth Annual International Conference on Privacy Security and Trust (PST)*, Ottawa, ON, Canada, 2010, p. 231.