SECURE MULTI-SPECTRAL HAND RECOGNITION SYSTEM

Maurício Ramalho[1], Sanchit Singh[1], Paulo Lobato Correia[1,2] and Luís Ducla Soares[1,3]

[1]Instituto de Telecomunicações, [2]Instituto Superior Técnico, [3]Instituto Universitário de Lisboa (ISCTE-IUL)
Torre Norte - Piso 10, Av. Rovisco Pais, 1, 1049-001, Lisboa, Portugal
phone: + (351) 218418461, fax: + (351) 218418472, email: {mar, sanchit, plc, lds}@lx.it.pt

ABSTRACT

This paper proposes a secure multimodal biometric recognition system with a multi-level fusion architecture. A multi-spectral camera is used to capture hand images in the visible and in the near-infrared (NIR) bands of the spectrum. The system uses four biometric traits from the user's hands: palmprint (PP), finger surface (FS), hand geometry (HG) and palm veins (PV), being the latter captured in the near-infrared band. In the feature extraction stage, three different techniques (i.e., Orthogonal Line Ordinal Features, Competitive Code and PalmCode) are implemented to extract features from the palmprint, finger surface and palm veins. The resulting features are then converted to binary in order to apply a secure template storage scheme, consisting of a cryptographic hash function combined with an error-correcting code. In the proposed system architecture, the hand geometry is used as a database indexing trait to reduce the search time needed for identification. Recognition results, obtained using a proprietary database that was built for that purpose, are presented for different combinations of the feature extraction techniques on the various biometric traits, as well as for different fusion methods.

1. INTRODUCTION

The concept of combining multiple information sources to perform recognition is not something new. In fact, the human visual system relies on more than one sensory information processing module, which is why it is rarely fooled. However, illusions can still occur if the assumptions used by the visual system are wrong [1].

The goal of using this concept in biometric systems is the same: make the system more robust and less vulnerable to fraud. It has been used in the early 90s to combine multiple classifiers in handwriting recognition [2], to fuse voice and face classifiers into a personal recognition system [3] and, in the late 90s, to combine face and fingerprints for personal identification [4]. The results presented by these early studies showed that the biometric system's recognition performance was indeed improved when multiple classifiers or multiple biometric traits were combined and this was empirically demonstrated by Jain et al. in [5].

According to [6], multibiometric systems can be further classified into six categories: multi-algorithm, multi-sensor, multi-instance, multi-sample, multimodal and hybrid. In these systems, data fusion can performed at sensor-, feature-, score-, rank- or decision-level.

Recent research on hand-based multibiometric systems shows mostly multimodal [7,8,9] or multi-algorithm [10,11] systems.

In this paper, results will be presented considering different feature extraction techniques on the three biometric traits (PP, FS and PV) but, ultimately, the best feature extraction technique for each biometric trait is chosen, so the proposed system can be considered multimodal. In this paper, a multi-level fusion architecture is used, where the four fingers' features are fused at feature-level and then are fused with palmprint and palm vein features at decision-level. Only the index, middle, ring and little fingers are used, since the thumb's texture is typically not visible in the acquired images due to its sideways positioning.

A novelty presented in this paper is that four biometric traits are extracted from the hand's palmar surface, being one of them, the hand's geometry, used as a database indexing trait to accelerate the identification process. These biometric traits were chosen because (i) they can be easily acquired from a single body part; (ii) they do not require a high resolution imaging system and (iii) palm veins have inherent liveness detection.

After image acquisition, biometric data is usually stored in a database for future comparisons in identification attempts. Biometric systems should preserve their users' privacy by storing data in a non-invertible way because a person cannot change a biometric trait if it is somehow compromised. In what concerns template security in multimodal systems, not much work has been reported. However, in this research, a secure template storage technique is applied to the biometric templates. It is based on the scheme proposed by Vetro et al. [12] and consists of storing the result of a Cryptographic Hash Function (CHF) and the parity bits of a systematic Error Correcting Code (ECC). The CHF is assumed non-invertible and guarantees, with a very high probability, that $H(x) = H(x') \Leftrightarrow x = x'$, . However, if $x' \approx x$ then $H(x)$ will be completely different from $H(x')$. This is what usually happens in biometric systems: the enrolled and probe templates are not exactly the same due to intra-user variations. To handle this problem, a Low-Density Parity-Check (LDPC) code is used. It is particularly suitable for biometric systems because its correcting capacity can be very finely adjusted by varying the number of parity bits. In a biometric system, the objective of an ECC is not to correct all bit errors, to avoid correcting impostor templates. In order to improve the correcting capacity of the LDPC code, a novel Log-Likelihood Ratio initialization method for the LDPC decoder is proposed.

The last contribution of this paper is a multispectral hand database which consists of visible and near-infrared images of 35 users' left and right hands.

The remainder of the paper is organized as follows. Firstly, the proposed system architecture is presented in Section 2, which also includes the image acquisition system, pre-processing and feature extraction details. Section 3 describes the secure template storage and matching. In Section 4, experimental results are presented and finally, conclusions and future work are discussed in Section 5.

2. PROPOSED SYSTEM ARCHITECTURE

The proposed system architecture for enrolment and identification phases is illustrated in Figure 1 and Figure 2, respectively. In the enrolment phase, five samples from the user’s hand are acquired in order to capture most of the intra-user variations. After feature extraction, PP, PV and the fused FS templates are securely stored. Hand geometry templates are stored in the clear for quick matching score computation. Each template is stored with an associated user ID. In the identification phase, five samples of the user’s hand are

© EURASIP, 2011 - ISSN 2076-1465

also acquired, to account for small intra-user variations (e.g., slight finger movement or hand rotation). A secure template matching procedure is then employed. The matching results are binary decisions, one for each biometric trait, and the final decision is then taken by majority voting. The secure template storage and matching techniques will be further described in section 3.

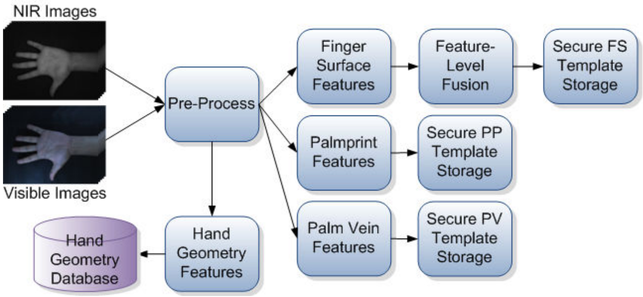


Figure 1 - Block diagram for enrolment phase.

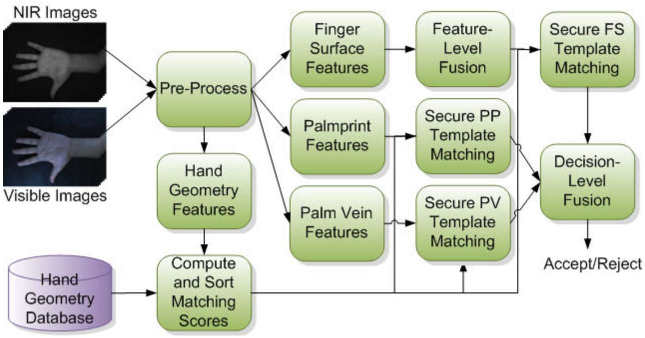
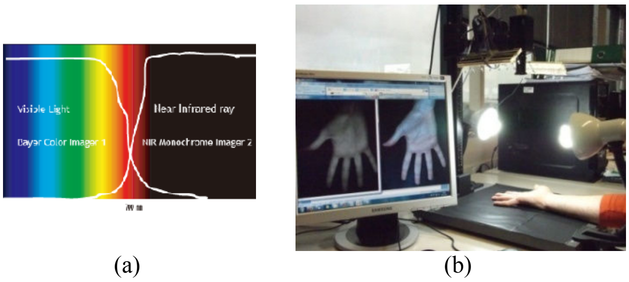


Figure 2 - Block diagram for identification phase.

2.1. Image Acquisition System

In this research, a JAI AD-080GE camera [13] was used to capture visible and NIR hand images. The camera contains two 1/3" progressive scan Charge-Coupled Devices (CCD) with 1024x768 active pixels. One of the CCDs is used to capture visible light images (400 to 700 nm) and the other captures light in the NIR band of the spectrum (700 to 1000 nm), as illustrated in Figure 3 (a).



(a) (b)

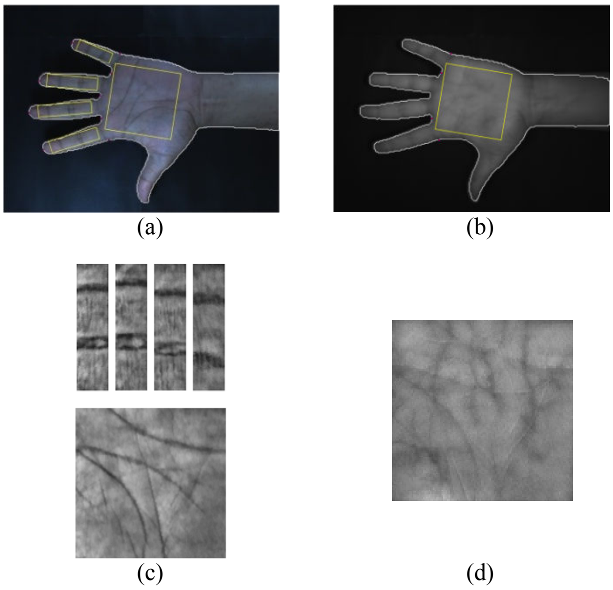
Figure 3 - (a) **-** Conceptual diagram for 2 CCD prism optics (image taken from **[13]**); (b) **-** image acquisition system.

The camera was mounted on a stand and adjusted to a height of approximately 45 cm above the base board, which is covered in matte black material to avoid light reflections (see Figure 3 (b)). To capture palm vein images, a dedicated NIR lighting system was built using two arrays of Light Emitting Diodes (LED), one on each side of the camera, to obtain a uniform lighting environment. The LEDs have a peak wavelength of 830 nm. This arrangement is made because deoxidized haemoglobin in the veins absorbs light at a wavelength of about 760 nm and appears as dark patterns to NIR sensitive sensors [14]. Similarly, to obtain well lit images in the visible, two Compact Fluorescent Lamps (CFL) are mounted on the base board, one on each side. This type of lamps was chosen because the light emitted by them has almost no contribution on the NIR band.

With this acquisition system, a multispectral hand database was built, containing a total of 1840 images. There are 20 images (10 visible + 10 NIR) from each hand of 46 individuals. Since the texture of left and right palms from the same user is assumed to be different, all right hands are flipped to be in a similar orientation as the left hands. Therefore, a total of 92 identities is considered. The database was built so that the first 5 images of each hand contain as much variability as possible to be used in the enrolment phase, i.e., when capturing the first 5 images, the user is asked to move his hand freely within the camera's field of view.

2.2. Pre-processing

The main objective of the pre-processing stage is to determine the hand contour and extract the palm and finger regions from the input images, also called the regions of interest (ROI). The ROIs are automatically extracted with the help of several reference points, which are computed from the hand contour using a combination of two techniques: radial distance to a reference point and contour curvegram [15]. Each ROI is then rotated to a vertical position and resized to 128x128 and 128x32, for palm and fingers respectively.



(a) (b)

(c) (d)

Figure 4 - ROI detection and extraction. (a) - Palmprint and fingers ROI detection; (b) - Palm veins ROI detection; (c) - Extracted palmprint and fingers ROI; (d) - Extracted palm veins ROI.

2.3. Feature Extraction

In this paper, three state-of-the-art palmprint feature extraction algorithms have been implemented. The implementation has been extended to finger surface and palm veins feature extraction. Hand geometry features are measured, in pixels, computed from the hand contour and include finger widths, lengths and perimeters as well as five palm distances between reference points.

2.3.1 Orthogonal Line Ordinal Features (OLOF)

This technique has been previously used to extract features from palmprint texture [16,17]. In this paper, OLOF feature extraction for palm veins and finger surface is proposed. The filters used in this technique are given by

$$OF(\theta) = f(x,y,\theta) - f\left(x,y,\theta+\pi/2\right), \quad (1)$$

$$f(x,y,\theta) = \exp\left[-\left(\tfrac{(x-x_0)\cos\theta+(y-y_0)\sin\theta}{\delta_x}\right)^2 - \left(\tfrac{-(x-x_0)\sin\theta+(y-y_0)\cos\theta}{\delta_y}\right)^2\right], \quad (2)$$

where θ denotes the 2D Gaussian filter orientation, δ_x and δ_y are the filter's horizontal and vertical scales, respectively. The filter parameters are shown in Table 1. For each pixel in the palmprint and palm veins ROIs, filtering with three orientations, $OF(0)$, $OF(\pi/6)$, $OF(\pi/3)$, is performed to obtain three bit ordinal codes based on the sign of the filtering results.

Table 1 - OLOF filter parameters.

	Palm & Veins	Finger Surface
Filter Size (Pixels)	35x35	11x11
Centre (x_0, y_0)	(17,17)	(5,5)
Horizontal Scale (δ_x)	9	2.50
Vertical Scale (δ_y)	3	0.83

In the pre-processed finger images, only one orientation, $\theta = 0$, is used because the texture found in the fingers usually has one main orientation.

2.3.2 Competitive Coding (CompCode)

The CompCode scheme has been used for extracting the orientation information from the palmprint [18] and palm veins [8]. CompCode uses six real parts of neurophysiology-based Gabor filters ψ_θ with the parameters defined in Table 2.

Table 2 - CompCode filter parameters.

	Palm & Veins	Finger Surface
Filter Size (Pixels)	35x35	17x17
Offset (x,y)	(17,17)	(9,9)
σ	5.6179	2.8090
ω	0.5137	1.0273

CompCode is based on a winner-take-all rule, which is defined as

$$I_{compcode} = \arg\min_j (I(x,y) * \psi_R(x,y,\omega,\theta_j)), \quad (3)$$

where I is a pre-processed image, ψ_R represents the real part of ψ, $\theta_j = j\pi/6$ and $j = \{0,1,2,3,4,5\}$ are the six orientations of the filters that are used here. CompCode uses three bits to represent each of these orientations.

2.3.3 PalmCode

PalmCode [19] uses a circular Gabor filter with optimized parameters (see Table 3) for feature extraction from the palmprint.

Table 3 - PalmCode filter parameters.

	Palm & Veins	Finger Surface
Filter Size (Pixels)	35x35	17x17
Offset (x,y)	(17,17)	(9,9)
θ	$\pi/4$	$\pi/4$
σ	5.6179	2.8090
u	0.0916	0.1833

For each pre-processed image, two matrices are obtained from the convolution with the Gabor filter: one for the real and another one for the imaginary part. These two matrices are converted into binary form by the following rules:

$$bit_{real} = \begin{cases} 1, \text{if Real}[G_{DC} * \text{Image}] \geq 0, \\ 0, \text{if Real}[G_{DC} * \text{Image}] < 0, \end{cases} \quad (4)$$

$$bit_{imaginary} = \begin{cases} 1, \text{if Imaginary}[G_{DC} * \text{Image}] \geq 0, \\ 0, \text{if Imaginary}[G_{DC} * \text{Image}] < 0, \end{cases} \quad (5)$$

The resulting binary matrices are the features to be used for the matching process.

3. SECURE TEMPLATE STORAGE& MATCHING

The proposed secure template storage and matching modules are illustrated in Figure 5 and Figure 6, respectively. When a user is enrolled, a set of parity bits, $[p_1 ... p_5]$, is computed by the LDPC encoder from the user's templates $[b_1 ... b_5]$. Parallel to this process, the bitwise exclusive disjunction (XOR) between $[b_1 ... b_5]$ and a randomly generated word, *w*, is computed. This is done to guarantee that templates from the same person are different in distinct biometric systems and to ensure that if a template is compromised, a new one can be issued just by changing *w*.
The result, $[x_1 ... x_5]$, is processed by a CHF to guarantee its privacy and the output, $[h_1 ... h_5]$, is stored in the database. A user noise model, η, is also computed. It consists of comparing the five templates with each other (i.e., a total of 10 comparisons) and updating η_i with the probability of the *i*-th bit changing its value due to intra-user variations. This will give the decoder a good measure of bit confidence and does not reveal any information about the bit value itself. Finally, the user's template is securely stored as (p, w, h, η) and is associated with an ID. The same ID is associated with the HG template.

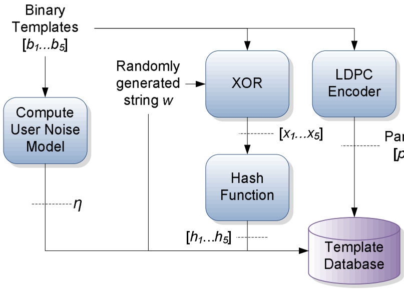


Figure 5 - Secure template storage block diagram.

In the secure template matching module, each probe template in $[b'_1 ... b'_5]$ is separately processed and compared against all stored templates, sorted according to the HG matching score. The first step is to compute the Log-Likelihood Ratio (LLR), given by

$$LLR(b_i \mid b'_i) = \log\left(\frac{P(b_i = 0 \mid b'_i)}{P(b_i = 1 \mid b'_i)}\right), \quad (6)$$

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 the value in η_i corresponds to the estimated probability of b_i changing value, the LLR is computed with the following values

$$P(b_i = 0 \mid b'_i) = \begin{cases} 1-\eta_i, & \text{if } b'_i = 0 \\ \eta_i, & \text{if } b'_i = 1 \end{cases}, \quad (7)$$

$$P(b_i = 1 \mid b'_i) = \begin{cases} \eta_i, & \text{if } b'_i = 0 \\ 1-\eta_i, & \text{if } b'_i = 1 \end{cases}. \quad (8)$$

If the decoding is successful, the hash value h' will match the stored hash value, h, and the user is identified. Otherwise, the identification algorithm takes the next ID in the list of candidates sorted according to the hand geometry matching score and repeats the process. If no more IDs are available, the algorithm takes the next probe template and restarts the identification process.

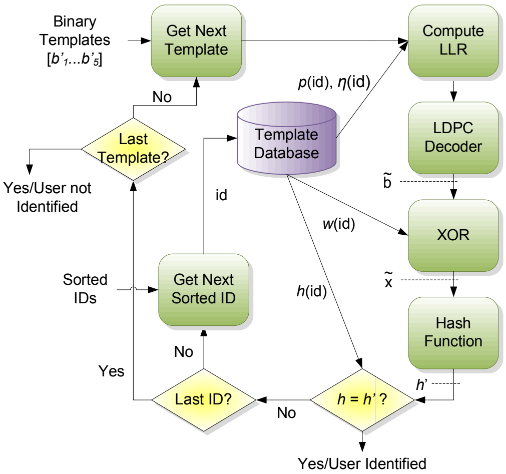


Figure 6 - Secure template matching block diagram.

Since the enrolled template is no longer available (only a hashed version of it), it is impossible to compute a matching score, which discards the possibility of using score-level fusion. In fact, a secure template matching module outputs a yes/no decision.

4. EXPERIMENTAL RESULTS

Three types of experiments were conducted on the database that was built with the proposed image acquisition system. In the first two experiments, templates are stored in the clear and the matching module consists of a Hamming distance classifier; the third experiment includes the secure template storage and matching modules.

The identification test is a one-to-N comparison procedure. In these experiments the total number of different hands in the database is used, i.e., $N = 92$. The database is divided into registration and test sets containing 920 images each, ten images per hand (5 visible + 5 NIR). Each PP, PV and FS image generates 5 correct and 455 incorrect Hamming distances. The minimum Hamming distances of correct and incorrect matching are used as the identification Hamming distances of genuine and impostor, respectively.

The recognition performance for PP, PV and FS (see Table 5) is computed in the first experiment. The objective is to choose the best feature extraction technique for each biometric trait. Since most Equal Error Rates (EER) are 0, another measure (d') is computed. This measure, called decidability index, was proposed by Daugman [20] and reflects how well separated are the genuine and impostor distributions. If the means and standard deviations of the genuine and impostor distributions are μ_1, μ_2, σ_1 and σ_2, respectively, then d' is given by

$$d' = \frac{|\mu_1 - \mu_2|}{\sqrt{\frac{(\sigma_1^2 + \sigma_2^2)}{2}}}. \tag{9}$$

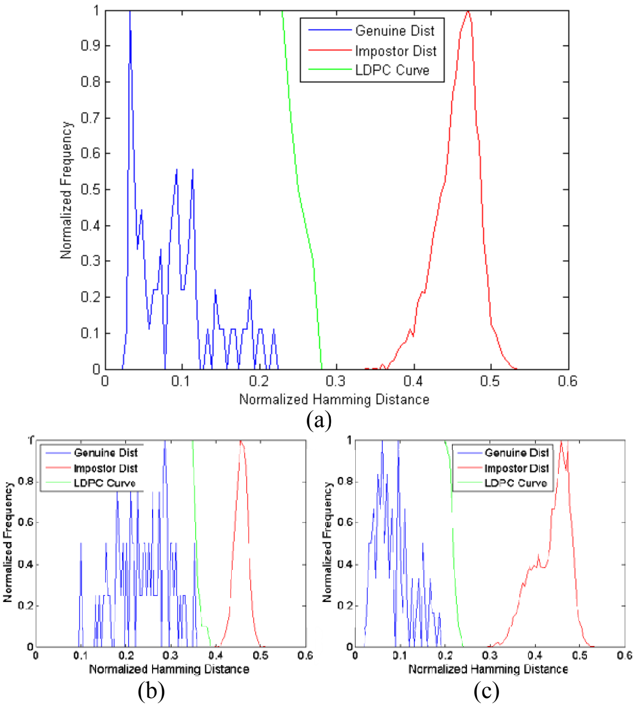
It is clear, from the results presented in Table 5, that the feature extraction technique presenting better performance is the OLOF.

In the second experiment, data fusion is performed at feature- and score-level (see Table 4), using the feature extraction technique selected in the previous experiment. When performing score-level fusion, all scores are normalized according to the min-max rule and the fusion follows the sum, weighted sum, product or min rules [6].

Table 4 - Recognition performance of PP, PV and FS at feature- and score-level fusion.

	EER (%)	d'
Feature-Level Fusion	0	7.54
Sum Rule	0	7.77
Weighted Sum Rule	0	8.14
Product Rule	0	9.49
Min Rule	0	9.66

The final experiment consists in setting a threshold using the LDPC code (see Figure 7) and computing the corresponding false acceptance rate (FAR) and false rejection rate (FRR).



(a)

(b)

(c)

Figure 7 - Genuine and impostor distributions with respective thresholds for: (a) palmprint; (b) finger surface; (c) palm veins.

Three LDPC codes with (n,k) of (3072,2810), (3072,2720) and (4096,4050) have been designed to correct genuine palmprint, palm veins and finger surface templates, respectively. Despite having the same size, palm and veins templates require different correcting capacities, as illustrated in Figure 7; finger surface templates are bigger and thus, a third LDPC code is required. The parity-check matrices, H, have a fixed number of 3 ones per column and a variable number of ones per row: $\rho_3 = 0.3034$ and $\rho_4 = 0.6966$ represent the ratio of rows that contain 3 and 4 ones, respectively. The LDPC decoding process is iterative and done by Belief Propagation. In this paper, the number of iterations is limited to 20, since experiments revealed that using more iterations degraded the recognition speed and did not improve the correcting capacity in a significant way.

The LDPC encoder generates a set of parity bits, which are the solution of the linear modulo-2 equation: $H \cdot b = p$, where H is the parity-check matrix and b the binary template. If b has length n and

Table 5 - Recognition results of PP, PV and FS using three feature extraction techniques.

	OLOF		CompCode		PalmCode ($\theta = 45^\circ$)	
	Palm / Veins	Finger Surface	Palm / Veins	Finger Surface	Palm / Veins	Finger Surface
Template Size (bits)	3072	4096	49152	49152	32768	32768
EER (%)	0 / 0	0	0 / 0	0	0 / 1.1	0.06
d'	8.42 / 8.43	4.60	6.24 / 6.64	3.69	6.24 / 5.80	3.34

p length k, there are k equations and n unknowns. When operating on a binary field, there are 2^{n-k} possible solutions [21]. According to Vetro et al. [12], the security metric in an ECC-based secure biometric system is the number of security bits, given by $n-k$. They report 90 and 31.25 security bits for iris and fingerprint recognition, respectively, with false rejection rates of 1.58% and 15%. The proposed system achieves 262, 352 and 46 security bits with FRR of 0%, 0% and 2.78% for palmprint, palm veins and finger surface, respectively. Since this is a multimodal system and the decision is taken by majority voting, an attacker would need to guess at least two biometric traits.

Using the hand geometry as a database indexing trait, it takes, in average, 119, 127 and 252 milliseconds to identify a palmprint, palm vein and finger surface image, respectively. These identification times include pre-processing and feature extraction delays. Without the hand geometry, a more exhaustive linear search on the database would be required, resulting in the following identification times (average): 16.39, 15.91 and 22.47 seconds for palmprint, palm veins and finger surface, respectively. These values are expected because (i) the LDPC decoding process is iterative and rather costly; (ii) without the hand geometry, there is no sorting in the matching procedure, so the number of decoding attempts is proportional to the user ID.

5. CONCLUSION AND FUTURE WORK

This paper proposes a fast multimodal identification system capable of achieving 0% FAR and FRR and an identification time of 252 ms if palmprint, palm veins and finger surface identification are performed in parallel. Storing hand geometry templates in the clear allows fast matching score computation but exposes some of the user's information. This is not problem in the proposed system because the final decision does not rely on hand geometry. Still, this may compromise the user's privacy if he/she is also registered in a biometric system that relies on hand geometry. In the future, this problem will be addressed. Results with more statistical significance are also expected, as the multi-spectral hand database is continuously growing. Future work will also focus on exploring new directions concerning secure template storage.

6. ACKNOWLEDGMENTS

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

7. REFERENCES

[1] J J Clark and A L Yuille, *Data Fusion for Sensory Information Processing Systems.*: Kluwer Academic Publishers, 1990.

[2] L Xu, A Krzyzak, and C Y Suen, "Methods of Combining Multiple Classifiers and Their Applications to Handwriting Recognition," *IEEE Transactions on Systems, Man and Cybernetics*, vol. 22, no. 3, p. 418, May/June 1992.

[3] R Brunelli and D Falavigna, "Person Identification Using Multiple Cues," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 17, no. 10, pp. 955-966, October 1995.

[4] L Hong and A Jain, "Integrating Faces and Fingerprints for Personal Identification," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no. 12, p. 1295, December 1998.

[5] L Hong, A Jain, and S Pankanti, "Can Multibiometrics Improve Performance?," Michigan State University, Technical Report MSU-CSE-99-39, 1999.

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

[7] J-G Wang, W-Y Yau, A Suwandy, and E Sung, "Person Recognition by Fusing Palmprint and Palm Vein Images Based on "Laplacianpalm" Representation," *Pattern Recognition*, vol. 41, no. 5, pp. 1514-1527, May 2008.

[8] D Zhang, Z Guo, G Lu, L Zhang, and W Zuo, "An Online System of Multispectral Palmprint Verification," *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 2, p. 480, February 2010.

[9] D Zhang et al., "Online Joint Palmprint and Palmvein Verification," *Expert Systems with Applications*, vol. 38, no. 3, pp. 2621-2631, March 2011.

[10] A Kumar and D Zhang, "Personal Authentication Using Multiple Palmprint Representation," *Pattern Recognition*, vol. 38, no. 10, pp. 1695-1704, October 2005.

[11] Y Zhou and A Kumar, "Contactless Palm Vein Identification using Multiple Representations," in *Fourth IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS),* Washington, DC, USA, 2010, p. 1.

[12] A Vetro, S C Draper, S Rane, and J Yedidia, "Securing Biometric Data," in *Distributed Source Coding - Theory and Applications.*: Elsevier Academic Press, 2009.

[13] (2011, February) Jai Camera Solutions, AD080-GE Camera Manual (htt p://w ww.jai.com/ProtectedDocuments/Manuals/ Manual_AD-080GE_Oct-09.pdf).

[14] J M Cross and C L Smith, "Thermographic Imaging of Subcutaneous Vascular Network of the Back of the Hand for Biometric Identification," in *IEEE International Carnahan Conference on Security Technology*, Surrey, UK, 1995, pp. 20-35.

[15] T Sanches, J Antunes, and P L Correia, "A Single Sensor Hand Biometric Multimodal System," in *15th European Signal Processing Conference (EUSIPCO)*, Poznan, Poland, 2007, pp. 30-34.

[16] 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*, 2005, p. 279.

[17] Z Guo, W Zuo, L Zhang, and D Zhang, "Palmprint Verification Using Consistent Orientation Coding," in *16th IEEE International Conference on Image Processing (ICIP)*, Cairo, Egypt, 2009, pp. 1985-1988.

[18] A W-K Kong and D Zhang, "Competitive Coding Scheme for Palmprint Verification," in *17th International Conference on Pattern Recognition*, 2004, p. 520.

[19] 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.

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

[21] 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.