Biohashing and Fusion of Palmprint and Palm Vein Biometric Data

Rihards Fuksis, Arturs Kadikis, and Modris Greitans
Institute of Electronics and Computer Science
14 Dzerbenes Str., Riga, LV1006, Latvia
Email: {Rihards.Fuksis; Arturs.Kadikis; Modris.Greitans}@edi.lv
Telephone: (371) 67558238
Fax: (371) 67555337
http://www.edi.lv

***Abstract*—This paper combines the results of our previous experiments concerning acquisition of the images of the human palm in infrared and visible light, the extraction of features from images as well as our current results on biometric data hashing with the advanced biohashing algorithm. We first describe the properties of the complex 2D matched filtering for feature extraction from images, followed by biometric vector construction techniques and raw biometric data comparison. We address the problem of securing biometric data for multimodal biometric systems, by analyzing the biohashing algorithm and proposing our enhancements. Results of experiments that include raw biometric data comparison, biohashing and advanced biohashing biocode comparisons are presented at the end of the paper.**

I. Introduction

Multimodal biometric systems use two or more biometric parameters (e.g., fingerprint, face, iris, etc.) to increase the overall system's performance. However, along with accuracy it is also necessary to ensure a convenient enrollment procedure of the person. Therefore, it is necessary to select biometric parameters that are unique and easy to present. A number of different research activities on biometric parameter fusion have been presented in recent years, such as palm geometry and palmprint fusion [1], [2], palm print and face [3], finger vein and finger-dorsa texture fusion [4], multispectral hand biometrics [5] and palmprint and palm vein image fusion applied at the image level [6].

In this paper, we use two palm biometric features - palmprints and palm veins. The most significant problems associated with biometric systems are:

- Efficient acquisition of biometric parameters - the main biometric features should not be distorted; the acquisition system must recognize false features (image);
- Effective extraction of unique information from the acquired biometric data - the acquired images usually contain a lot of unwanted data or data that give no information for biometric matching;
- Biometric data security - how to generate a unique code from the biometric data so that real biometric data is not revealed;
- Biometric data comparison - how to compare two encrypted biometric vectors.

By using the palmprint and palm vein images, we have tried to address all of the four above-mentioned issues. Firstly, it is easy to present a palm to a biometric system. Also, it is hard to falsify a palmprint and palm vein pattern if the image of palm is taken in two different wavelengths within hundred of milliseconds. Secondly, we extract the predefined features from the images by using a complex 2D matched filter and construct the biometric data vector, thus reducing the amount of data. Thirdly, we use the extracted data to create a data vector and apply several enhancements of the biohashing algorithm to obtain a biocode. Fourthly, we introduce a biocode comparison method. All of these steps will be discussed further in this paper.

II. Image acquisition

It is important to acquire images of the palm so that the significant features that are used for person recognition are clearly visible. For palmprints, these are skin wrinkles, for palm veins - visible veins. The capturing of the palm images is performed by using only one image sensor, but dual spectrum illumination. Palm vein images are captured in the near infrared (NIR) spectrum, but images of the palmprint structure are captured in the visible light spectrum. Most of the popular methods of palm vein imaging are based on the infrared (IR) light absorption properties of the blood. Hemoglobin absorbs light of 760nm and 850nm depending on oxygen concentration; illuminating a palm with IR light, veins appear darker in the image than the rest of the palm because part of the IR light is absorbed in places where there are veins, and the rest is reflected from the surrounding tissue. Images taken in visible and IR light are shown in Fig. 1.

III. Biometric feature extraction from images

After the images of the palmprint and the palm veins are captured, they must be processed in order to extract the chosen features (wrinkles from palmprint image and veins from the palm vein image). Conventional image processing methods such as histogram equalization or global thresholding [7] are not acceptable due to the irregular intensity and noisy background of the images. A cross section of the captured palm vein and palm print images (Fig.2) reveals that the

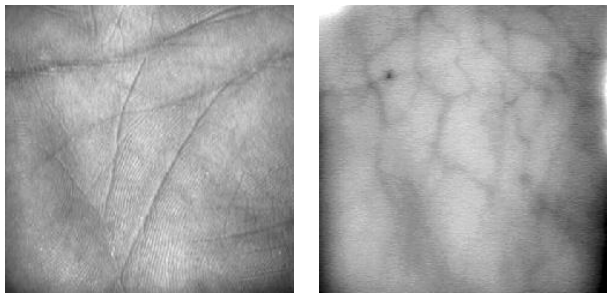

Fig. 1. One persons (left) palm print and (right) palm blood vessel images

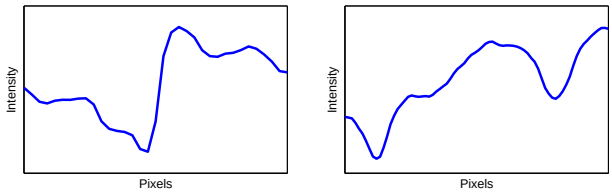

Fig. 2. Cross section of the palm print ridge (left) and two palm blood vessels (right)

corresponding features are different, as a result of which two different methods have to be used to extract the desired features.

A. Palmprint Feature Extraction

Various representations have been proposed for palmprint recognition. Those include, representation by lines [8], points [9], [10], Fourier spectrum [11], morphological representation [12], texture [13], wavelets [14] and complex wavelets [15], Gabor filters [16], fusion code [17], ordinal code [18] and representation with so called "Laplacianpalm" [6]. As shown in the Fig. 2 (left), the palm print ridge has a sharp intensity change. This sharp intensity change can be detected using the first derivatives which are implemented using the magnitude of the gradient. For a function $g[x, y]$, the gradient of g at coordinates $[x, y]$ is defined as the two-dimensional column vector [7]

$$\nabla g \equiv \text{grad}(g) = \begin{bmatrix} \frac{\partial g}{\partial x} \\ \frac{\partial g}{\partial y} \end{bmatrix} \tag{1}$$

Derivatives of discrete functions in a point [x_0,y_0] are calculated as the difference of nearest pixel values, for example:

$$\left.\frac{\partial g[x, y]}{\partial x}\right|_{[x_0, y_0]} = g[x_0 + d, y_0] - g[x_0 - d, y_0] \tag{2}$$

where d is the half of the distance between taken neighbourhood pixels.

Typically the image is corrupted with noise and the direct application of (2) can lead to an incorrect result. Therefore, before the derivatives are calculated, the image f[x,y] is smoothed using a Gaussian filter to reduce rapid intensity spikes that are initiated by noise.

$$g[x, y] = f[x, y] \otimes e^{-\frac{x^2+y^2}{\sigma^2}} \tag{3}$$

where σ specifies the smoothing rate, and $\otimes$ is the convolution operator.

Function's gradient vector grad(g) points at the greatest rate of intensity change of g, which corresponds to the cross section of the skin ridge. To facilitate the following stage of vector set construction and acquire the resulting matrix of vectors F_1, the gradient vector is rotated by 90°. Since the method used to extract the blood vessels is expressed in the complex form, for convenience, we rewrite (2) using the complex notation as:

$$\begin{aligned} \underline{F}_1[x_0, y_0] \quad &= (g[x_0, y_0 - d] - g[x_0, y_0 + d]) + \\ &\quad j\,(g[x_0 + d, y_0] - g[x_0 - d, y_0]) \end{aligned} \tag{4}$$

B. Palm Vein Feature Extraction

In our previous papers [19], [20], we have introduced a method for line-like object extraction that is based on the matched filtering (MF) approach [21] and is called Complex 2D Matched Filtering (CMF) [19]. CMF performs faster than MF because only two convolution operations with the CMF kernel are required. CMF also extracts the selected features from the images and provides additional information about the direction of the extracted features of the image. The nature of CMF can be explained by looking at the principles of Matched Filtering with the Gaussian 2D function $G(x, y)$ [21].

$$G(x, y) = \begin{cases} -exp\left(-\frac{y^2}{\sigma^2}\right), & |x| \le \frac{D}{2} \\ 0, & |x| > \frac{D}{2} \end{cases} \tag{5}$$

where D is the length of the filter kernel in direction x. In order to detect blood vessels, the filter mask must be scaled and rotated in different directions. Further in the paper the rotated and scaled Gaussian 2D kernel is referred to as:

$$G[x, y; \phi, c] \equiv G\left(\frac{x\cos\phi - y\sin\phi}{c}, \frac{x\sin\phi + y\cos\phi}{c}\right) \tag{6}$$

where c is the scaling factor and ϕ is the rotation angle.

The more rotation angles are used the more accurate is the extraction of blood vessels. However, this involves image convolution with the rotated Gaussian kernels and, therefore, is computationally inefficient for embedded systems. Eight differently rotated masks for MF are shown in Fig.3.

Fig. 3. Eight differently rotated MF masks for blood vessel extraction

To simplify the computational complexity of the MF approach, we use the CMF approach. This image processing method is slightly different from the MF approach. First of all, the filtering is done with one complex mask, instead of many rotated masks. This method obtains additional information about the analyzed feature orientation, in our case about the blood vessels and skin wrinkles. The output of the filtering procedure is a matrix of vectors that is of the same size as the input image. Vectors represent the correlation with the

previously defined mask representing the objects that have to be found. Instead of consecutive filtering with several differently oriented MF masks, CMF filters image only with one complex mask, which incorporates all the angles and scales. The kernel of the complex matched filter is defined by the following expression:

$$\underline{M}[x,y] = \sum_{n=1}^{N} \sum_{l=0}^{L-1} exp(j2\phi_l) G[x,y;\phi_l,c_n], \tag{7}$$

where N – total number of used scales,
L – total number of used angles,
$\phi_l = \frac{l}{L} \cdot \pi$.

The image is filtered with the CMF kernel:

$$\underline{C}[x,y] = f[x,y] \otimes \underline{M}[x,y]. \tag{8}$$

Additional operation of the angle decrement is performed to $\underline{C}$ to acquire the final CMF result:

$$\underline{F}_2[x_0,y_0] = |\underline{C}[x_0,y_0]|\, exp\left(j\frac{\mathrm{Arg}\underline{C}[x_0,y_0]}{2}\right). \tag{9}$$

The magnitude of the vectors represents the congruence between the filter mask and the object in the particular pixel of the image. The angle of the vector shows the orientation in which the maximum of $\underline{C}$ is found. This information is crucial in the segmentation and recognition stage.

C. Feature Vector Construction

Some of the information obtained in previous stages can be discarded, because most of it represents undesired regions of the palm where palmprint and vein features are not present. The goal is to extract most significant vectors that represent the blood vessels or ridges of the skin. The following procedure is repeated several times until R most significant vectors are found: the most significant vector from the processed image is extracted, and the region around each vector found is excluded from further processing to avoid multiple vector extraction from the same region.

D. Vector Set Comparison

After the vector set A of the most significant features is acquired, the recognition process can begin. First, vector set comparison without any encryption (using raw biometric data) is performed. Vector set A is compared with the database vector sets B_n to find the best match. To compare two sets of vectors, an approach similar to [20] can be used: each vector $v_p(\mathrm{A})$ from the first set A is compared with each vector $v_q(\mathrm{B})$ from the second set B. The similarity of two vectors is evaluated by positive $s_{p,q}$ and is a product of three terms:

$$s_{p,q} = \mathrm{magnitudes}_{p,q} \cdot \mathrm{angles}_{p,q} \cdot \mathrm{distance}_{p,q} \tag{10}$$

These three parts evaluate the positions of two vectors - distance:

$$\mathrm{distance} = exp\left(-\frac{d_\parallel^2}{\sigma_\parallel^2}\right) \cdot exp\left(-\frac{d_\perp^2}{\sigma_\perp^2}\right), \tag{11}$$

the angular difference - angles:

$$\mathrm{angles} = |\cos \angle(v_p(\mathrm{A}) \cdot v_q(\mathrm{B}))|, \tag{12}$$

and the significance of these vectors - magnitudes:

$$\mathrm{magnitudes} = |v_p(\mathrm{A})| \cdot |v_q(\mathrm{B})|. \tag{13}$$

All the similarities of a particular pair of vectors $s_{p,q}$ are summed together to evaluate the similarity of the vector sets in general:

$$s(\mathrm{A},\mathrm{B}) = \sum_p \sum_q s_{p,q} \tag{14}$$

The higher is the value of a particular $s_{p,q}$, the higher is their influence on the overall similarity value $s(\mathrm{A},\mathrm{B})$. The vector magnitude is proportional to the significance of the locally extracted feature that is represented by this vector. For this reason, magnitudes (13) are included in the similarity evaluation (10). Our experiments showed that, as a result of changes in the lightning conditions in the image acquisition stage, the same line-like objects appear differently on the filtered images: the positions of local maximums across the object vary. For this reason, we split the distance between vectors into parallel (to $v_p(\mathrm{A})$) and perpendicular parts, and evaluate them separately: the first mentioned is less critical for $s_{p,q}$ than the second one ($\sigma_\parallel > \sigma_\perp$). Both parts of the distance are found as the projections of the actual distance between $v_p(\mathrm{A})$ and $v_q(\mathrm{B})$ onto the vector $v_p(\mathrm{A})$. The similarity value $s(\mathrm{A},\mathrm{B})$ is influenced by the image contrast and the neighbourhood effect of many local maximums representing one and the same line-like object jointly compared with each other. In the evaluation stage it is normalized as described in [20].

$$S(\mathrm{A},\mathrm{B}) = \frac{s(\mathrm{A},\mathrm{B})}{\sqrt{s(\mathrm{A},\mathrm{A}) \cdot s(\mathrm{B},\mathrm{B})}} \tag{15}$$

The similarity index value $S(\mathrm{A},\mathrm{B})$ lies in the interval of $[0;1]$ and is used for evaluation of similarity of two images. The similarity index doesn't have commutative properties, $S(\mathrm{A},\mathrm{B}) \neq S(\mathrm{B},\mathrm{A})$.

However it is not safe to use raw biometric data. If the data is intercepted then the person's biometric information is stolen and cannot be changed. Therefore, in the next section, we look at the biometric data encryption method BioHash, and introduce enhancements of the encryption algorithm.

IV. The BioHash Algorithm

Many methods that integrate biometrics with cryptography have been proposed. As an example, the fuzzy vault approach that binds a key to the biometric template [22] and a fuzzy extractors, that can be used to extract keys from a biometric template [23].

In this paper, we chose to encrypt the biometric data with a one-way hash function called biohash [24]. It is a type of cancelable biometrics that has been introduced in [25], and it consists of an intentional, repeatable distortion of the original biometric template, satisfying the following properties:

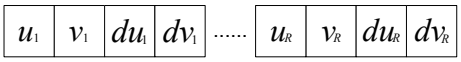

Fig. 4. Creation of data vector

- Renewability: it should be possible to revoke a compromised template and issue a new one based on the same biometric data (revocability);
- Security: the original biometric data cannot be recovered;
- Performance: the recognition performance of the protected system, in terms of Equal Error Rate (EER), should not degrade significantly with respect to a non-protected system.

Biohashing is a method that combines orthonormal random vectors with user specific biometric data. A token is a sequence of numbers or symbols that are used as a seed to generate random vectors. Each user can have its own private token or every person can use the public token.

The sequence of steps needed for biohash is the following:

1) acquisition of the biometric data and extraction of the most significant features to create a data vector;
2) usage of the token as a seed for the random number generator. Generating the random vectors and applying Gramm-Schmidt vector orthonormalization process;
3) calculation of the dot product from each orthonormal vector and the biometric feature vector;
4) thresholding of the result by some value T.

After these steps, the result is a series of bits, or biocode that can be used in further authentication.

The enrolment and recognition stages are similar. Both follow the previously described sequence of steps, but in the enrolment stage, multiple biometric samples could be used to extract more precise features. The similarity H_b of two biocode samples is calculated by using Hamming distance D_h of those samples and the length of the feature vector l (16).

$$H_b = \frac{l - D_h}{l} \tag{16}$$

A. Basic Biohash Algorithm

The biohashing algorithm performs computations on the biometric data vector and creates a biocode. As previously explained, biometric data vector is created using the features extracted from the palmprint or palm vein images.

The extracted features are the R most significant vectors from the processed image. Each vector is described by 4 components: vector's starting position coordinates (u, v) and coordinates (du, dv) that represent vector's orientation and magnitude.

The data vector is constructed by putting the components of each vector in order of succession. The sequence starts with the coordinates of the first vector u_1, v_1, du_1, dv_1, then the second vector and so on. The feature vector consists of $4R$ components (Fig. 4). Therefore, $4R$ orthonormal vectors will be created, and the resulting biocode will contain $4R$ bits.

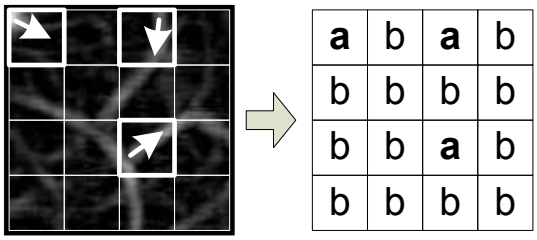

Fig. 5. Multiple most intensive vectors

B. Improved Biohash Algorithm

We have taken into account several observations and propose to use additional user specific information to improve the performance of the biohash algorithm. The improvements are achieved by using the statistical properties of the biometric data and the resulting biocodes.

In the captured palm images, some features (veins or ridges) are larger than others. As observed, environmental lighting and temperature will not affect the extraction of the main (larger) features. Therefore, one of the improvements of the algorithm presented in this paper is the use of additional information about the most intensive vectors that is added to the data vector. As previously described, most intensive vectors are found as follows: vector of maximal magnitude is found and the region with the size of o is excluded around it. The size of o defines how large is the region that represents the biometric feature. A limit on how many most intensive vectors need to be found can be set. Each cell of the matrix with the size of $k \times k$ describes the presence of at least one of the most intensive vectors w in the certain region of the image value a means that the region contains the vectors, value b means that no vectors were found in that region. This process is shown in Fig. 5, where $k = 4$ and $w = 3$. Information about the most intensive vector positions is added to the biometric data vector. If the following method is used to describe the most intensive vectors in the sample, then, even if the order of vectors changes, the added information will be the same.

By analyzing the biocodes obtained, it was observed that they are not identical for the same person. This can be explained by the variable nature of biometric data. But some bits between one person's biocodes vary more than the others (Fig. 6). This bit variation further will be called bit stability. Bits that vary less are more stable ("4" in Fig. 6) than bits that vary more ("2" in Fig. 6).

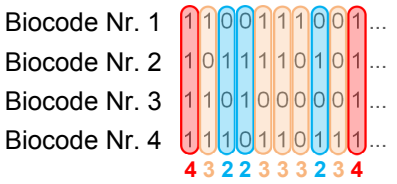

Fig. 6. Calculating the amount of equal bits

The stable bits of all biocodes are user specific. It is possible

to improve the method of biocode comparison by using information about the stable bits. For a more precise biocode comparison the errors of the more stable bits should be more emphasized than the errors of the unstable bits. Therefore, bits are arranged in descending order by bit stability. Training samples are used to obtain this information. Depending on the amount of samples used to sort the bits, more precise statistical information about the user can be obtained. After multiple biocode samples are collected, the bit stability is calculated (Fig. 6). First, the bits are sorted by the largest amount of equally valued bits between biocodes for a specific bit (Fig. 7 transform (a)). After that, the bits in each of the groups are sorted again, but this time by their total distance of equally valued bits from the threshold value T (Fig. 7 transform (b)). If the distance from the threshold T is larger, the bit is more stable than one which is closer to the threshold level.

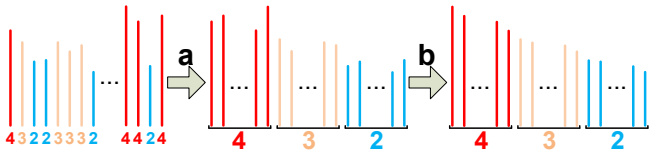

Fig. 7. Sorting of bits in their groups

After all these operations, a sequence of bit indexes b_i is obtained that allows comparison between two biocodes using specific weight coefficients that represent information about bit stability. i is the index of the bit in the original biocode (Fig. 7 before transform (a)), b_i is the position of the bit i in the sorted array (Fig. 7 after transform (b)), where the bits are sorted by their stability. This information does not reveal what values the specific bits should have, and it does not reveal the specific amount of bit stability. It only reveals which bits are more stable relatively to each other.

If Hamming distance is used to compare two biocodes, each difference between bits makes an equal contribution to the overall error. With the proposed comparison method the stable bits have a greater influence on the overall error if they differ. To calculate the error err_i for each bit an exponential function (17) is used. The value p describes how many of the bits are used in the comparison.

$$err_i = e^{-\frac{b_i^2}{p}} \tag{17}$$

V. Experimental Results

To evaluate the previously described methods, a database of palmprint and palm vein images was used. This database consists of 250 images of each image type, containing 5 images of 50 different persons - a total of 500 images. First, image processing techniques, like CMF and gradient filtering are applied to each of the database image to acquire the most significant vector set. Next, the database images are mutually compared without using biohash. The results for non-hashed comparison can be seen in Table I.

TABLE I
Raw biometric data comparison

	Prints	Veins	Fusion
EER	2.79 %	0.32 %	0.1 %

A crucial part of the biohashing algorithm is the tokens. As previously mentioned, a token is used as a seed for the random number generator to generate random vectors. Each set of generated random vectors is unique and with specific properties. Therefore, tests with different tokens must be employed. We performed 100 different tests, where each test employs its own, randomly generated token, and all persons in the database have the same token. As a result, from each test, the EER is calculated. The results including the mean value and the standard deviation of all EER can be seen in Table II.

TABLE II
Biohash algorithm test results (EER)

	Veins	Palm prints	Fused data
Mean	14,043	12,073	6,190
StDev	1,152	1,102	0,803

In the advanced algorithm, the information about the most intensive vectors is added. Empirically it was determined that the best results are achieved if the information of 32 or half of the available most intensive vectors is added to the feature vector (Fig. 8). In our case, the following values of coefficients were used: $a = 1, b = -0.5, k = 8, w = 32$.

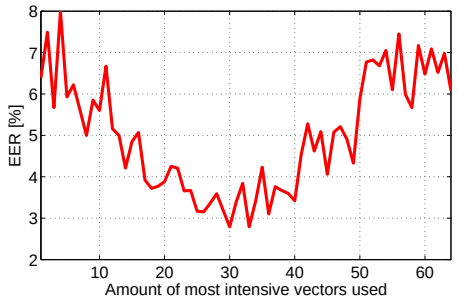

Fig. 8. Amount of intensive vectors used

The advanced algorithm uses a training set; therefore, all the possible combinations of training sets have to be checked. Each person has 5 data samples, 2 of those samples are used for the training process, but the other 3 samples are used for the testing process. That gives a total of 10 different training sets. The calculated biocodes from the training samples are used to find the most stable bits. This stability information is used by the other 3 samples. For each training set 100 tests with different tokens were performed, where each person has the same token. The results can be seen in the Table III, where the training set number denotes a different training set. Results show that the improved biohashing approach achieves a lower EER than comparing the results of the basic biohash algorithm and EER is close to raw data comparison.

TABLE III
IMPROVED BIOHASH ALGORITHM TEST RESULTS USING DIFFERENT TRAINING SETS (EER)

	Veins		Palm prints		Fused data	
Training set Nr.	Mean	StDev	Mean	StDev	Mean	StDev
1.	1,076	0,312	1,069	0,397	0,001	0,003
2.	1,122	0,289	1,369	0,439	0,003	0,006
3.	**1,073**	**0,304**	**0,471**	**0,231**	**0,000**	**0,000**
4.	1,440	0,609	0,712	0,382	0,000	0,000
5.	3,523	0,657	1,625	0,364	0,106	0,088
6.	4,051	0,568	1,326	0,023	0,035	0,029
7.	3,712	0,775	1,302	0,236	0,078	0,052
8.	3,876	0,843	5,195	0,658	0,217	0,118
9.	3,999	0,650	4,924	0,543	0,207	0,090
10.	4,721	0,834	5,475	0,915	0,297	0,174

VI. CONCLUSIONS

In this paper, we have discussed the four most important aspects of creating a biometric system: how to acquire biometric data, how to extract the valuable information from images, how to protect the biometric information and how to compare it. However, the main contribution is the biohashing algorithm enhancements. This research shows that by using the biohash algorithm, the statistical information obtained about the biocodes can improve the biocode comparison algorithm and obtain a lower EER. The proposed algorithm satisfies the requirements of the cancelable biometrics without sacrificing the recognition accuracy, compared to the raw biometric data comparison. The proposed biohashing approach could be useful for securing any type of biometric data.

Experimental results showed that results vary if different training samples are used. This can be explained by different lighting conditions that were employed to simulate real life conditions. For training, there should be more than two images to obtain more precise statistical information. This can improve the recognition results. It is once again shown that by using multimodality in biometric systems a lower EER can be achieved compared to using only one parameter. Our motivation is to build an easy to use, safe and reliable biometric system for everyday usage, and we believe that this article is a step towards to achieving our goals.

VII. ACKNOWLEDGEMENT

Reasearch of this paper is supported by European Regional Development Fund grant No. "2010/0285/2DP/2.1.1.1.0/10/APIA/VIAA/098."

REFERENCES

[1] A. Kumar and D. Zhang, "Personal recognition using hand shape and texture," in *IEEE Transactions on Image Processing, Vol. 15, Issue:8*. IEEE, 2006, pp. 2454–2461.

[2] M. G. K. Ong, T. Connie, A. T. B. Jin, and D. N. C. Ling, "A single-sensor hand geometry and palmprint verification system," in *WBMA '03: Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications*. New York, NY, USA: ACM, 2003, pp. 100–106.

[3] N. Nageshkumar, P. Mahesh, and M. Shanmukha Swamy, "An efficient secure multimodal biometric fusion using palmprint and face image," *International Journal of Computer Science Issues, IJCSI*, vol. 2, pp.49–53, 2009.

[4] W. Yang, X. Yu, and Q. Liao, "Personal authentication using finger vein pattern and finger-dorsa texture fusion," in *MM '09: Proceedings of the seventeen ACM international conference on Multimedia*. New York, NY, USA: ACM, 2009, pp. 905–908.

[5] R. K. Rowe, U. Uludag, M. Demirkus, S. Parthasaradhi, and A. K. Jain, "A multispectral whole-hand biometric authentication system," in *ICIS '09: Proceedings of the 2nd International Conference on Interaction Sciences*. New York, NY, USA: ACM, 2009, pp. 1207–1211.

[6] J.-G. Wang, W.-Y. Yau, A. Suwandy, and E. Sung, "Fusion of palmprint and palm vein images for person recognition based on "laplacianpalm" feature," in *Computer Vision and Pattern Recognition, 2007. CVPR '07. IEEE Conference on*, june 2007, pp. 1–8.

[7] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, 3rd ed. Prentice Hall, 2007.

[8] D. Zhang and W. Shu, "Two novel characteristics in palmprint verification: Datum point invariance and line feature matching," *Pattern Recognition*, vol. 32, pp. 691–702, 1999.

[9] N. Duta, A. Jain, and K. Mardia, "Matching of palmprint," *Pattern Recognition Letters*, vol. 23, pp. 477–485, 2002.

[10] J. Doi and M. Yamanaka, "Personal authentication using feature points on finger and palmar creases," in *Applied Imagery Pattern Recognition Workshop, 2003. Proceedings. 32nd*, oct. 2003, pp. 282–287.

[11] W. Li, D. Zhang, and Z. Xu, "Palmprint identification by fourier transform," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 16, pp. 417–432, 2002.

[12] C.-C. Han, H.-L. Cheng, C.-L. Lin, and K.-C. Fan, "Personal authentication using palm-print features," *Pattern Recognition*, vol. 36, no. 2, pp. 371–381, 2003.

[13] J. You, W.-K. Kong, D. Zhang, and K. H. Cheung, "On hierarchical palmprint coding with multiple features for personal identification in large databases," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol. 14, no. 2, pp. 234–243, feb. 2004.

[14] L. Zhang and D. Zhang, "Characterization of palmprints by wavelet signatures via directional context modeling," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 34, no. 3, pp. 1335–1347, june 2004.

[15] L. Zhang, Z. Guo, Z. Wang, and D. Zhang, "Palmprint verification using complex wavelet transform," in *Image Processing, 2007. ICIP 2007. IEEE International Conference on*, vol. 2, october 2007, pp. 417–420.

[16] W. K. Kong, D. Zhang, and W. Li, "Palmprint feature extraction using 2-d gabor filters," *Pattern Recognition*, vol. 36, no. 10, pp. 2339–2347, 2003.

[17] A. Kong and D. Zhang, "Feature-level fusion for effective palmprint authentication," in *Biometric Authentication*, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2004, vol. 3072, pp. 1–43.

[18] Z. Sun, T. Tan, Y. Wang, and S. Li, "Ordinal palmprint represention for personal identification [represention read representation]," in *Computer Vision and Pattern Recognition, 2005. CVPR 2005. IEEE Computer Society Conference on*, vol. 1, june 2005, pp. 279–284.

[19] M. Greitans, M. Pudzs, and R. Fuksis, "Object analysis in images using complex 2d matched filters," in *EUROCON 2009: Proceedings of IEEE Region 8 conference*. IEEE, 2009, pp. 1392–1397.

[20] M. Greitans, M. Pudzs, and R. Fuksis, "Palm vein biometrics based on infrared imaging and complex matched filtering," in *MM&Sec '10: Proceedings of the 12th ACM workshop on Multimedia and security*. New York, NY, USA: ACM, 2010, pp. 101–106.

[21] S. Chaudhuri, S. Chatterjee, N. Katz, M. Nelson, and M. Goldbaum, "Detection of blood vessels in retinal images using two-dimensional matched filters," in *IEEE transactions on medical imaging, Vol.8, Issue:3*. IEEE, 1989, pp. 263–269.

[22] K. Nandakumar, A. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," *Information Forensics and Security, IEEE Transactions on*, vol. 2, no. 4, pp. 744–757, dec. 2007.

[23] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput.*, vol. 38, pp. 97–139, March 2008.

[24] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognition*, vol. 37, pp. 2245–2255, 2004.

[25] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, pp. 614–634, March 2001.