FPGA based palmprint and palm vein biometric system

Mihails Pudzs, Rihards Fuksis, Rinalds Ruskuls,
Teodors Eglitis, Arturs Kadikis, Modris Greitans
Institute of Electronics and Computer Science
14 Dzerbenes Street, Riga, LV1006, Latvia
Mihails.Pudzs@edi.lv; Rihards.Fuksis@edi.lv; Rinalds.Ruskuls@edi.lv
Teodors.Eglitis@edi.lv; Arturs.Kadikis@edi.lv; Modris.Greitans@edi.lv

Abstract: This paper presents an FPGA based multimodal palm biometric system. System is prototyped on an Altera DE2-115 board from Terasic, using an additional hardware for palm image acquisition in two light spectrums, communication with smart card, and debugging. System captures person's palmprint and palm vein images, extracts biometric data, encrypts it, and prepares for comparison. The comparison of the biometric data is performed on smart card for additional security. The proposed multimodal palm biometric system achieves a matching accuracy of EER of 16.65 % and a verification processing time of 0.8 seconds.

1 Introduction

Increasing identity fraud in recent years stimulates a development of new biometric systems. To obtain higher precision, developers more often employ more than one biometric parameter by developing multimodal biometric systems. Some recent papers discuss how to develop an FPGA based biometric system, for example, FPGA-based finger vein biometric system [KHE10]. However, this system is implemented in soft processor using Nios2-Linux Real Time Operating System (RTOS). In this paper, authors propose the implementation of an FPGA-based multimodal palm biometric system that does not use soft processor, instead all of the functionality is exclusively developed for the current task using FPGA logic.

Authors propose to use palm vein and palmprint images for human authentication. It is easy to use palm as a biometric feature because it is convenient to present the palm to a reading device. By acquiring images in infrared and visible light spectrum, the real palm can be distinguished from photography. To extract valuable information from the captured images Non-Halo Complex Matched Filter (NH-CMF) [PGF11a] is used. We also reduce the amount of the extracted data by eliminating the non-biometric information. This step further simplifies the encryption and comparison, because less data is used for processing. For biometric data encryption, we use BioHash to obtain unique biometric code. Biometric data comparison is performed on the smart card by employing the Match on Card concept.

Paper is organized as follows. First, the architecture of the biometric system is presented. Second, the processing techniques performed on the biometric data are explained, and

implementation of the techniques in the FPGA are discussed. Third, experimental setup is described and experimental results in terms of processing time and recognition accuracy are presented. Paper finishes with conclusions and future work.

2 System architecture

The block diagram of the proposed FPGA based biometric system is shown in Fig. 1. The biometric system can be divided into three main parts: image acquisition module, FPGA, and smart card module.

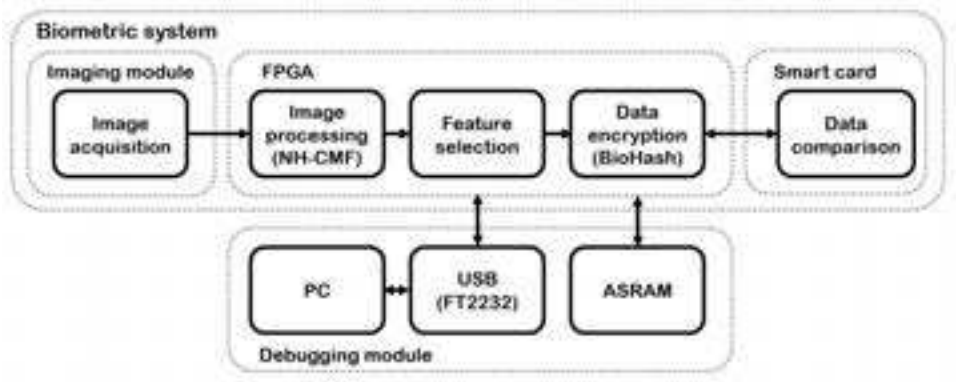

Figure 1: The architecture of the proposed biometric system

Because of the hemoglobin absorption properties described in [FGP10], palm print and palm vein images must be acquired in a different light spectrum - visible light and near infrared light, respectively. To be able to acquire both images using one image sensor an imaging acquisition module has been developed. This module consists of Aptina MT9V024 image sensor, which has quantum efficiency of more than 20% in the region of 400 - 900 nm. Two types of LEDs are used to illuminate palm during image acquisition - white LEDs and infrared LEDs of 850nm wavelength. To minimize the influence of ambient light on acquired image, two optical filters are used - one that transmits only the near infrared light (700-1400nm), and one that transmits only the visible light (400-700nm). An electromechanical switching device is used to toggle between the mentioned filters.

User authentication starts by connecting a smart card and presenting a palm to the image acquisition device. After the image is acquired, it is filtered using Non-Halo Complex Matched Filter (NH-CMF), which extracts information about visible line-like objects that include palmprint and palm veins. To acquire palmprint/palm vein biometric information, feature selection follows. Then biometric data is encrypted using the advanced BioHashing algorithm. The encrypted biometric data is sent to smart card to be compared with data stored in it. Smart card responds with similarity between compared data vectors and FPGA decides whether the person that tries to authenticate is the owner of presented smart card.

More details about data processing are presented in the next section.

Additional module is developed for debugging. This module uses USB interface to control the system from a PC. ASRAM is used only to display the acquired image.

3 Data processing

Data processing is divided into three parts: feature extraction and selection, data encryption using BioHash, and data comparison on smart card.

3.1 Feature extraction and selection

Feature extraction is accomplished using Non-Halo Complex Matched Filtering (NH-CMF) approach, which was firstly introduced in [PGF11b]. It is angle invariant line extraction filter that obtains angle of the extracted lines.

We use four rotated line extraction kernels for NH-CMF. Each kernel is convolved with the input image $f(x, y)$ using equation (1):

$$s(x_0, y_0; \varphi_n = n\pi/4) = \iint_D f(x, y) \cdot M(x - x_0, y - y_0; n\pi/4)\, dxdy, \tag{1}$$

where D is the area of image $f(x, y)$ overlapped with the mask M, and n is the index of mask rotation angle φ_n. To prevent filter from generating Halo artifacts, negative values of mask correlation with overlaid areas of the image are set to zero by using ramp function $R[x]$.

The corrected values of mask correlation are transformed to complex form, using:

$$\vec{c}_n(x, y; \varphi_n) = R[s_n(x_n, y_n; \varphi_n)] \cdot e^{j2\varphi_n} \tag{2}$$

Four mask rotation angles ($n = 0, 1, 2, 3$) are used for the following reasons:

- it is the minimum amount of rotated kernels, therefore, also convolution operations, without filter losing it extraction abilities,
- the multiplier $e^{j2n\pi/4}$ in equation (2) can be conveniently simplified to $e^{jn\pi/2} = \{+1, -1, +j, -j\}$, which doesn't require any embedded multipliers to perform.

After values are transformed into complex form, they are summed together to acquire a cumulative vector $\vec{c}(x, y)$:

$$\vec{c}(x, y) = \sum_{n=0}^{3} \vec{c}_n(x, y, \varphi_n). \tag{3}$$

The region of interest is divided into 64 subregions, and the most intense cumulative vector is selected from each subregion. Each selected cumulative vector $\vec{c}(x_i, y_i)$ is described by 4 parameters: its origin coordinates (x_i, y_i) and its projections $Re(\vec{c}(x_i, y_i))$, $Im(\vec{c}(x_i, y_i))$. The concatenation of $m = 64 \cdot 4$ parameters is used as a biometric feature vector in our system.

3.2 Data encryption

Data encryption is performed by using a one-way hash function – biohash [BRAA10] – a member of cancelable biometrics introduced in [RCB01].

Biohash performs a random orthonormal transform H to biometric data X, obtaining vector

$$Y = H \cdot X. \tag{4}$$

Elements of Y are then thresholded to acquire binary data sequence called BioCode. A token is a number that is used as a seed to generate random orthonormal vectors for transform matrix H. In the presented biometric system each user has his own private token that is stored on smart card and sent to biometric system at the beginning of the authentication process.

State of the art implementation of Biohash involves following steps: an $m \times m$ matrix consisting of pseudo-random values is generated using provided token; Gram-Schmidt process is applied to orthonormalize generated matrix vectors; matrix multiplication according to (4) is performed.

However, described approach can not be efficiently implemented on FPGA for the following reasons: it is necessary to store a minimum of $m \cdot m$ values in the memory (1Mb for 16bit coefficients if $m = 256$); a large amount of arithmetic operations must be performed, which can take more than a second and extend the authentication time.

The transformation (4) can be performed more efficiently if transformation matrix H is replaced by a product of simpler orthonormal random transformation matrices $(B_m)_i$. Stairs-like Orthonormal Generalized Rotation Matrices (SOGRM) introduced in [MT05] were chosen for this purpose:

$$H = \prod_{i=0}^{(log_2 m)-1} (B_m)_i, \tag{5}$$

where B_m is SOGRM with size m, which is defined using (6).

$$(B_m)_i = \begin{bmatrix} a\left(\Theta_{\frac{i\cdot m}{2}}\right) & b\left(\Theta_{\frac{i\cdot m}{2}}\right) & 0 & 0 & \cdots \\ 0 & 0 & a\left(\Theta_{\frac{i\cdot m}{2}+1}\right) & b\left(\Theta_{\frac{i\cdot m}{2}+1}\right) & \cdots \\ \vdots & \vdots & \vdots & \vdots & \cdots \\ b\left(\Theta_{\frac{i\cdot m}{2}}\right) & -a\left(\Theta_{\frac{i\cdot m}{2}}\right) & 0 & 0 & \cdots \\ 0 & 0 & b\left(\Theta_{\frac{i\cdot m}{2}+1}\right) & -a\left(\Theta_{\frac{i\cdot m}{2}+1}\right) & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix} \quad (6)$$

$\Theta_i, i \in \left[0...\frac{m\cdot log_2 m}{2} - 1\right]$ are pseudo-random numbers that are generated using provided token. To preserve orthonormality, $a()$ and $b()$ must satisfy the following requirement $(a(\Theta))^2 + (b(\Theta))^2 - 1 \to 0$.

It is convenient to use trigonometric functions, such as sin/cos, as $a()$ and $b()$, because they satisfy all necessary requirements and can be calculated using CORDIC algorithm. In this case, each subsequent pair of $(B_m)_i$ columns form an elementary rotation matrix. Because of the associative property of matrix product, elementary rotations might be applied to input vector X in an iterative way:

$$Y = (B_{256})_7 \cdot ((B_{256})_6 \cdot ... \cdot ((B_{256})_1 \cdot ((B_{256})_0 \cdot X))), \quad (7)$$

Each multiplication of data vector with transform matrix B_m is equivalent to $m/2$ elementary rotation operations, which can be performed in FPGA using the transposed FIR filter structure shown in Fig. 2. This unit is connected to 4 memory blocks: a pair for input data, and a pair for output data. Each pair contains samples 0 to $m/2 - 1$ and m to $m - 1$, respectively. This unit performs $log_2 m$ data processing cycles during which $m/2$ elementary rotation operations are performed. Starting data encryption process, biometric data vector X is stored in memory blocks A and B. During first processing cycle data is read from A and B and written to memory blocks C and D. After each processing cycle, reading/writing directions are toggled.

Every two input samples x_n and x_{n+1} ($n = 0, 2, 4...254$) and angle Θ are used to calculate two output samples $y_{n/2}$ and $y_{n/2+m/2}$, therefore, a new $sin\Theta$ and $cos\Theta$ values must be loaded after every two input samples.

Blum Blum Shub (BBS) pseudo-random number generator is used to calculate rotation angles Θ.

3.3 Data comparison

To compare acquired biocode with the one stored in the smart card, Hamming distance is used. To improve recognition accuracy, both resulting similarities (for palmprint and palm vein patterns) need to be fused. Weighted sum method [RJ03] is used for this purpose. For

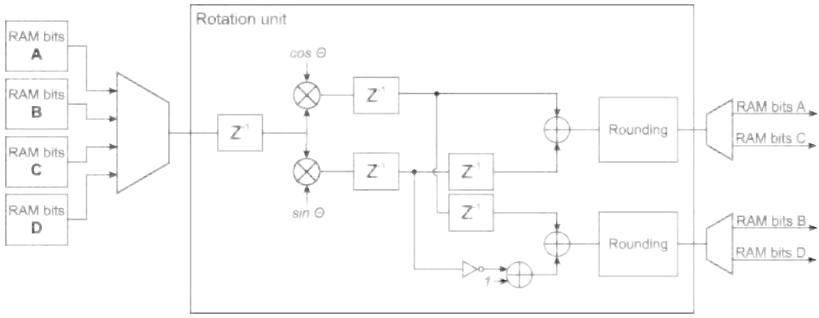

Figure 2: Implementation of vector rotation unit

two similarity values - s_1 and s_2, fused similarity can be estimated as $s_\Sigma = k \cdot s_1 + (1 - k) \cdot s_2$, where parameter $k \in [0, 1]$. After both similarities are fused together, the result is thresholded to decide whether to authenticate person, or not.

4 Experimental part

4.1 Test setup and procedure

To test proposed FPGA based biometric authentication system we have changed functionality of several system modules: image acquisition module was modified to receive images from PC; encryption module was modified to send biocodes to PC for further analysis. Images from CASIA Multi-Spectral Palmprint Database were used to test the performance of system's data processing.

Images from database (100 persons, 6 images per person; two light spectrums - white and infrared 850nm) are sent to FPGA and corresponding biocodes are received. Further analysis, such as similarity calculation and fusion, is performed on PC. False accept and false reject ratios are calculated by mutually comparing all similarity values.

4.2 Experimental results

Figure 3 shows False Accept Rate (FAR) and False Reject Rate (FRR) curves for three tests that were performed. Equal Error Rate (EER) for each test is provided in the table below. Recognition time is 0.8 seconds.

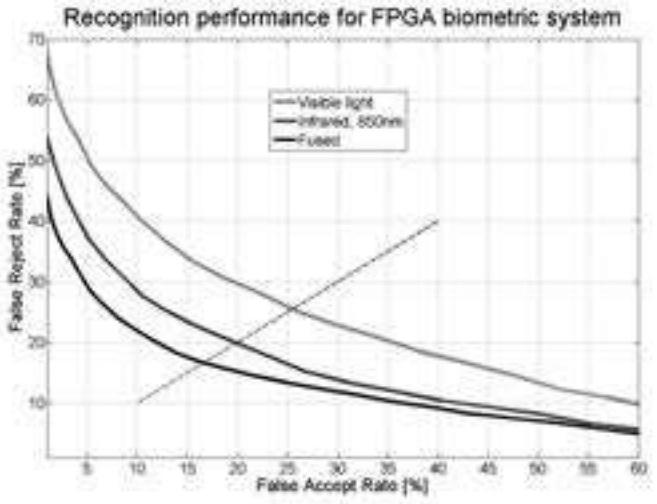

Figure 3: Experimental results

Test	EER [%]
palmprints	25.5
palm veins	19.9
fused data	16.65

5 Conclusions

In this paper we have discussed three main challenges, faced in the field of biometrics, such as acquisition, encryption, and comparison of biometric data. Each of the mentioned tasks are implemented in an FPGA-based system to achieve fast person authentication - it takes approximately 0.8 seconds from the moment when the smart card is inserted into the system until access is granted.

As expected, the least reliable parameter is palmprint, which is harder to distinguish from person to person, than palm vein pattern. Experimental results showed that by using more than one biometric parameter for person authentication, lower EER can be achieved, compared to cases when each of the parameters is used in isolation. The results showed that proposed system is not yet ready to be used in real life applications. However our motivation is to build an easy to use, safe and reliable biometric system for everyday usage, and we believe that this work is a step towards to achieving our goals. Future work involves improvement of a feature extraction algorithm.

Acknowledgments

This research is partially supported by European Regional Structural Funds project under the agreement No.2010/0285/2DP/2.1.1.1.0/10/APIA/VIAA/098.

References

[BRAA10] R. Belguechi, C. Rosenberger, and S. Ait-Aoudia. Biohashing for Securing Minutiae Template. In *Pattern Recognition (ICPR), 2010 20th International Conference on*, pages 1168–1171, 2010.

[FGP10] Rihards Fuksis, Modris Greitans, and Mihails Pudzs. Infrared Imaging System for Analysis of Blood Vessel Structure. In *Electronics and Electrical Engineering, No.1(97)*, pages 45–48. Kaunas Technologia, 2010.

[KHE10] M. Khalil-Hani and P. C. Eng. FPGA-based embedded system implementation of finger vein biometrics. In *Industrial Electronics Applications (ISIEA), 2010 IEEE Symposium on*, pages 700–705, 2010.

[MT05] P. Misans and M. Terauds. Introduction into the fast orthogonal transforms based on rotation angles: A new methodical approach only or a gateway to novel DSP algorithms? In *5th Electronic Circuits and Systems Conference ECS'05*, pages 85–94, Bratislava, Slovakia, September 2005.

[PGF11a] M. Pudzs, M. Greitans, and R. Fuksis. Complex 2D matched filtering without Halo artifacts. In *Systems, Signals and Image Processing (IWSSIP), 2011 18th International Conference on*, pages 1–4, 2011.

[PGF11b] M. Pudzs, M. Greitans, and R. Fuksis. Generalized Complex 2D Matched Filtering for Local Regular Line-like Feature Detection. In *19th European Signal Processing Conference (EUSIPCO 2011)*, pages 41–45. EURASIP, 2011.

[RCB01] N.K. Ratha, J.H. Connell, and R.M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3):614–634, 2001.

[RJ03] Arun Ross and Anil Jain. Information fusion in biometrics. *Pattern Recognition Letters*, 24:2115–2125, 2003.