FPGA based palm print and palm vein biometric system

M.Pudzs, R.Fuksis, R.Ruskuls, T.Eglitis, A.Kadikis, M.Greitans

INSTITUTE OF ELECTRONICS AND COMPUTER SCIENCE

14 Dzerbenes Str., Riga, Latvia
e-mail: bite@edi.lv

Introduction

In this work we present FPGA-based embedded multimodal palm biometric system. Palm images are acquired in different light spectrums (visible and infrared) to help distinguish real palm from photography (in case of spoofing attack), and to increase recognition precision by fusion of biometric features. Biometric features are extracted using Non-Halo Complex Matched Filter (NH-CMF) [1] and encrypted using BioHash algorithm to obtain person-unique biometric code - *Biocode*. Biocode verification is performed on user's presented smart card.

Proposed approach

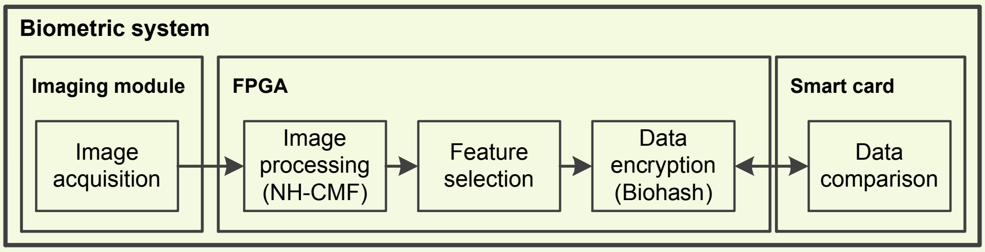


Image Acquisition

Images are acquired with only one image sensor using dual spectrum illumination and optical filtering:

- palm vein images are captured in the near infrared spectrum - 850nm,
- palm print images are captured in the visible light spectrum.

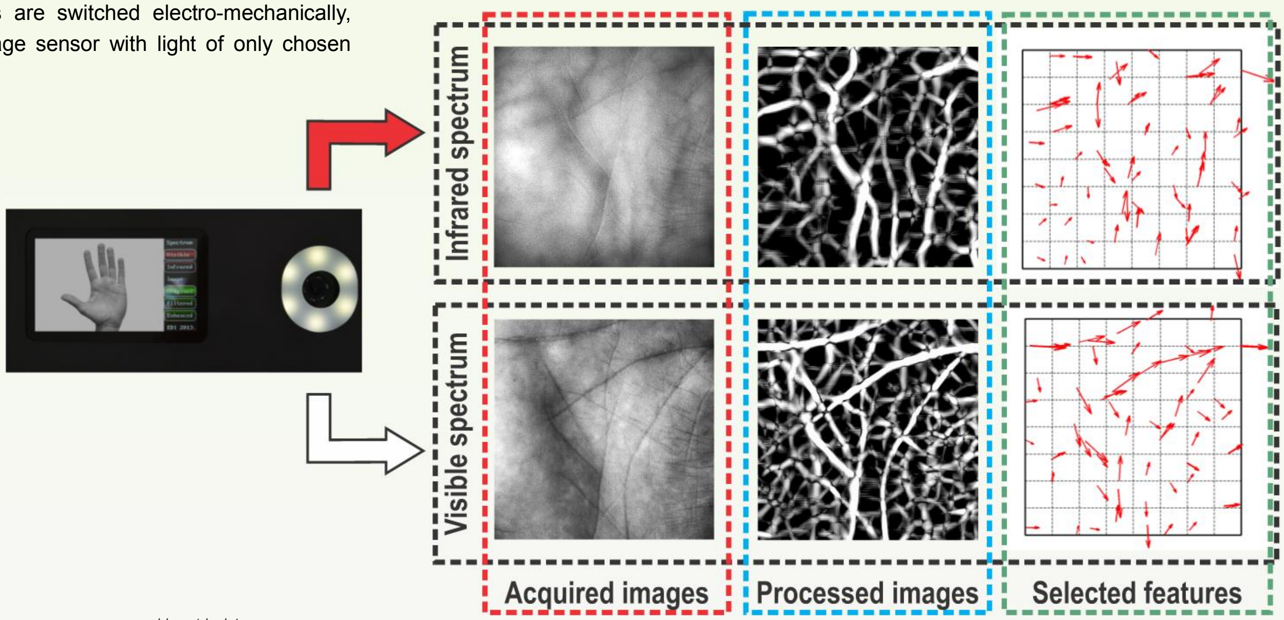
Optical filters are switched electro-mechanically, providing image sensor with light of only chosen wavelengths.

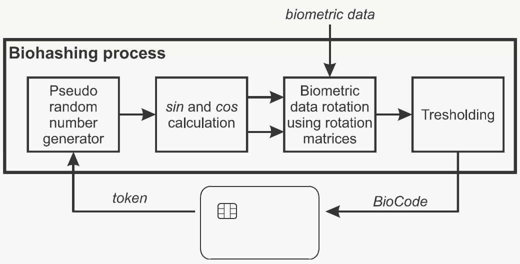
Image processing

Acquired images are processed using NH-CMF, which assigns matching intensity vector value for each pixel. Length of matching intensity vector shows pixel's neighborhood's similarity to a feature looked for (wrinkle or vein), whereas angle points feature's direction.

Feature selection

Visible palm area is divided into 64 sub-regions, and only one vector with the biggest magnitude is selected within each sub-region. Each selected vector is described by 4 parameters: its origin coordinates and its projections. The concatenation of 64x4 acquired parameters is used as a biometric data vector.





Data encryption

Data encryption is performed by using one-way hash function – biohash. Biohashing procedure consists of the following steps: token is received from smart card; depending on token value one of many random orthonormal transforms is applied to biometric data vector (implemented in FPGA using Stairs-like Orthonormal Generalized Rotation Matrices (SOGRM)); transformed data is thresholded to acquire binary data sequence called *biocode*. Biocodes are stored and compared on smart card. This approach ensures that the original biocode is never read from the smart card therefore eliminating the possibility of stealing the person's biometric data.

Conclusions

In this work we discuss acquisition, processing, encryption, and comparison of biometric data. Each of the mentioned tasks are implemented in an FPGA-based system to achieve fast person authentication. Main contribution is the use of SOGRM to achieve fast biocode computation.

References

[1] 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.

Acknowledgement

This research is partially supported by ERAF funding under the agreement No.2010/0285/2DP/2.1.1.1.0/10/APIA/VIA/098

ERAF EIROPAS REĢIONĀLĀS ATTĪSTĪBAS FONDS
IEGULDĪJUMS TAVĀ NĀKOTNĒ
EIROPAS SAVIENĪBA