Volume : 1 | Issue : 6 | Nov 2012 • ISSN No 2277 - 8179

Research Paper

Engineering

KEYWORDS : authentication, biometric system, iris recognition, FPGA, parallel processing, Hamming distance.

Hardware Implementation Of Iris Matching

Bethuna | Guru Nanak Institute of Technology, Student, M.Tech, VLSI-SD, E.C.E Dept., Hyderabad, India

ABSTRACT

Now a days, necessity of identifying users of secure facilities or other resources becomes very important to prevent fraudulent access. Biometrics is emerging as a technology that provides a higher level of security, efficiency and convenience than traditional ID or password methods for user authentication. A biometric system is essentially a pattern recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioural characteristic that a person posses. Human has many biometric features such as fingerprint, hand geometry, gait, face, voice and iris. Among these Iris recognition is especially attractive due to stability of the iris texture patterns with age and health conditions. However, the iris recognition algorithms are currently implemented on general purpose sequential processing systems, such as generic central processing units (CPUs). In this paper, we present a parallel processing alternative using field-programmable gate arrays (FPGAs), offering an opportunity to increase speed of the resulting system. Matching part of the iris recognition algorithm has been implemented using Verilog HDL targeting low-cost Spartan 3AN FPGA, achieving significant reduction in execution time when compared with a conventional software based applications. The Hamming distance is employed for classification of iris templates, and two templates were found to match if hamming distance between them is less than the threshold value. The goodness of the proposed approach has been tested using iris images from the CASIA database.

I.INTRODUCTION

From the Greek words "Bios" life and "metron" measure, Biometrics can be defined as the study of measuring those biological characteristics that make human beings unique. Authentication systems based on biometrics determine the user's identity on the principle that some physiological or behavioural characteristics are unique for each person, and are more tightly bound to a person than a token object or a secret which can be lost or transferred. . Human has many biometric features such as fingerprint, hand geometry, gait, face, voice and iris. Among these Iris recognition is more accurate and reliable due to the stability of the iris texture patterns with age and health conditions. Iris recognition is a process of identifying a person by analyzing the random pattern of the iris. It is a relatively new biometric technology, and has great advantages, such as variability, stability and security, thus is the most promising for high security environment. It has many potential applications such as access control, network security, etc.

Iris is a muscle with in the eye that regulates the amount of light entering into the eye. It is the colored part between pupil and sclera (white part of the eye) which lies behind carnia and immune to external environment. The patterns within the iris are very unique to each person, and even the left eye is unique in comparison to the right eye. Irides form in the first year of human life and remain unchanged over the lifetime. These properties of the iris make it superior to other biometric modalities for automatic authentication systems.

Generally the implementation of biometric algorithms is carried out using high-performance microprocessors working at clock frequencies in the GHz range. However, such software implementations could restrict the application of biometrics to specific markets because of the microprocessor cost. Devices available in the low-cost consumer market are generally too slow for applications requiring intensive computations. With advances in the VLSI (Very Large Scale Integrated) technology hardware implementation has become an attractive alternative. Implementing complex computation tasks on hardware and by exploiting parallelism and pipelining in algorithms yield significant reduction in execution times.

Implementing iris biometric algorithm on reconfigurable hardware minimizes the time-to market cost, enables rapid prototyping of complex algorithms and simplifies debugging and verification. Therefore, FPGAs are an ideal choice for implementation of real time iris recognition algorithms.

The purpose of this paper is to describe the implementation of iris matching using verilog HDL targeting low-cost Spartan-3AN FPGA.

II.IRIS RECOGNITION ALGORITHM

The implemented iris recognition system is based on the algorithm developed by Dr. Daugman. Iris recognition process is basically divided into five steps.

- Image acquisition
- Iris Localization
- Normalization
- Encoding
- Matching

A. Image acquisition

This work uses the images from the Chinese Academy of Sciences Institute of Automation (CASIA) iris database version 2 which includes grey scale eye images of resolution 640x480 pixels.

B. Iris Localization

The iris inner and outer boundaries are located by finding the edge image using the Canny edge detector [4]. Hough transform is used to localize the iris.

C. Normalization

Different circles with increasing radius and angle are drawn starting from the pupil centre till it reaches near the iris coordinates. In our case 8 concentric circles are drawn and each subdivided into 256 sectors. Then iris is unwrapped by converting into its polar equivalent. It is done using Daugman's Rubber sheet model[1].

$$x = c(x) - r * \sin(\theta)$$

$$y = c(y) + r * \cos(\theta) \quad \text{----- (1)}$$

where c(x, y) denotes centre coordinates, (x, y) denotes coordinates of the image, θ is the angle from horizontal axis with the range (0-360°) and r denotes the radius with the range (0-1).

For every pixel in the iris, an equivalent position is found out on polar axes.

D. Encoding

The final process is the generation of the iris code is encoding the unwrapped iris. The Gabor filters are used in this step. The iris code is formed by assigning 2 elements for each pixel of the image. Each element assigned a value 1 or 0 depending on the sign + or – of the real and imaginary parts of the complex plane. Noise bits are assigned to those elements whose magnitude is very small and combined with the noisy part obtained from normalization. In this way we got a code of 2048 bits.

Volume : 1 | Issue : 6 | Nov 2012 • ISSN No 2277 - 8179

$$h_{\{Re,Im\}} = \mathrm{sgn}_{\{Re,Im\}} \int_{\rho}\int_{\phi} I(\rho,\phi) e^{-i\omega(\theta_0-\phi)} \cdot e^{-(r_0-\rho)^2/\alpha^2} e^{-(\theta_0-\phi)^2/\beta^2} \rho d\rho d\phi$$

-----(2)

Where, h{Re, Im} has the real and imaginary part, each having the value 1 or 0, depending on which quadrant it lies.

E. Code Matching

Comparison of the bit patterns generated is done to check if the two irises belong to the same person. Calculation of Hamming Distance (HD) is done for this comparison. HD is a fractional measure of the number of bits disagreeing between two binary patterns.

$$HD = \frac{1}{n}\sum_{k=1}^{n} x_k \oplus y_k$$

-----(3)

III. ADOPTED ARCHITECTURE

Figure shows the architecture of the proposed system. Grey scale eye images are captured and processed to generate iris template database which will be stored on Rom. For lage databases, off-chip ROM will be interfaced to FPGA. Small databases can be stored on chip. Live template is compared with the templates in the database by calculating hamming distance between them.

For matched irides hamming distance should be less than predetermined threashold value. If match found search will be stopped after generating the result else search will continue for the entire database.Result can be displyed on monitor or through LED.

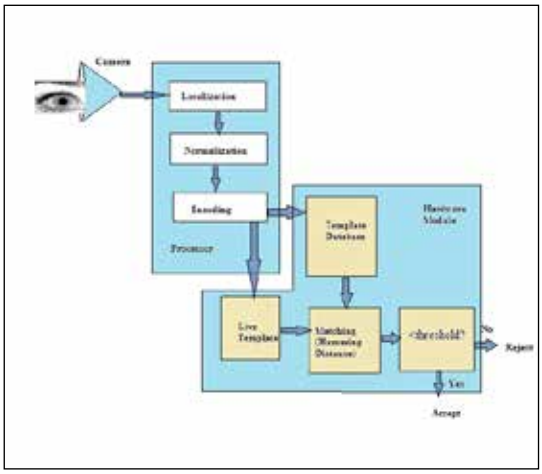

Figure 1 : System architecture

Figure 4 shows the block diagram of Matching module. It has the internal structure as follows:

- Memory Module
- HD modules
- Adder tree
- Comparator and display

Iris template database is created and stored in ROM. Live template received from the processor will be stored in RAM. Live template will be compared with each template in the datbase using hamming distance

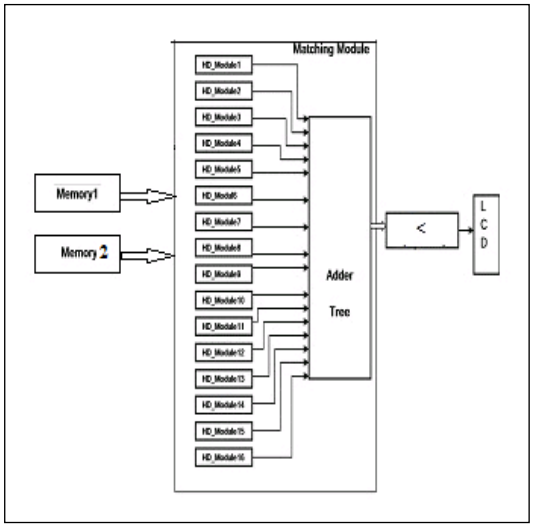

Figure 2: Architecture for matching Module

Each HD module will receive 128 bit inputs from the two templates to be compared and calculates hamming distance between them. Output from each HD module will be of 8 bits length. Outputs from all HD modules will be added together in adder tree to get final hamming distance between live and database templates. The final HD value will be of 12 bits length and is compared with the predetermined threashold value. Threashold is set to 30%. For matched irides HD should be less than threashold(HD<threashold).

IV. IMPLEMENTATION

Sample database is created by generating the templates for 4 sample eye images taken from CASIA database version 2. Localization , Normalization and Encoding is done using matlab.Thus generated templates will be stored in a text file which will be transferred to FPGA using UART.

Sample Verilog Code for 4 bit HD:

```
module ham(

a,b, HD

);

input [3:0] a;

input [3:0] b;

output [2:0] HD;

 wire [3:0] diff;

 wire [1:0] lev00,lev02;

 wire [2:0] lev10;

 assign diff = (a ^ b);

 assign lev00 = {1'b0 , diff[0]} + {1'b0 , diff[1]};

 assign lev02= {1'b0 , diff[2]} + {1'b0 , diff[3]};

 assign lev10 = {1'b0, lev00} + {1'b0 , lev02};

 assign HD=lev10;

 endmodule
```

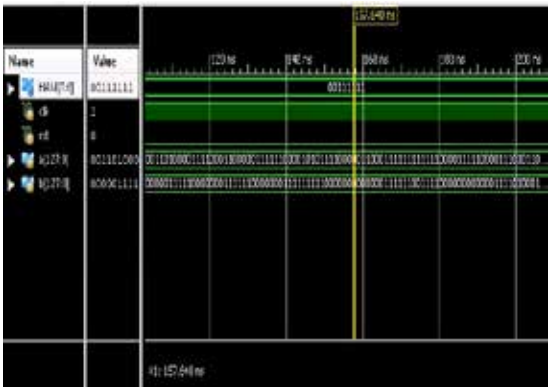

Figure 3:Simulation result of Hamming Distance

V. CONCLUSIONS

Low cost and fast execution are important parameters for real time authentication systems. The main purpose of the work described in this paper is to implement most time consuming part of iris recognition algorithm on a low-cost FPGA. The proposed design was implemented on a low-cost Spartan 3AN FPGA using verilog HDL. This design is suitable for small low cost applications.

FUTURE SCOPE

Future improvements in the system can be done by implementing the feaure extraction task on hardware which can further reduce the authentication time. Instead of using Matlab we can use Microblaze soft core processor and can implement the iris localization and iris normalization in C. By this we can implement entire system on single chip.

ACKNOWLEDGMENT

I would like to articulate my profound gratitude and indebtedness to Dr. T Srinivasulu, Principal, GNIT., and Prof. B. Kedarnadh, Head of the Department, GNIT, for guiding and encouraging me in all aspects. I wish to extend my sincere thanks to all the faculty members of Guru Nanak Institute of Technology.

REFERENCE

[1] Daugman, J. G.: "How iris recognition works," IEEE Trans. Circuits Syst. Video Technology, vol. 14, no. 1, pp. 21-30, Jan. 2004. | | [2] P. Wildes, S. C. Hsu R. J. Kolczynski . R. Matey J. C. Asmuth and S. E. McBride.: "Automated, noninvasive iris recognition system and method." U.S. Patent, No. 5,572,596. | | [3] Ryan N. Rakvic, Brandley J. Ulis, Randy P. Broussard, Robert W. Ives and Neil Steiner.: "Parellelizing Iris Recognition", IEEE Transactions on Information Forensics and Security, Vol. 4, No. 4, December 2009. | | [4] Daugman, J. G.: "The importance of being random: statistical principles of iris recognition," Pattern Recognition 36 p279-291, 2003. | | [5] ZHOU Hu-Lin, XIE Mei: "Iris Biometric Processor Enhanced Module FPGA based Design" 2010 Second International Conference on Computer Modeling and Simulation. | | [6] Liu-Jimenez, J.; Sanchez-Reillo R.; Miguel-Hurtado, O.: "Improving security in ID tokens through HW/SW co-design", Security Technology (ICCST), 2010 IEEE International Carnahan Conference on Spain ,December 2010. | | [7] Spartan 3AN datasheet and user guide available at: http://www.xilinx.com/support/ | | [8] Daugman, J. G.: "Probing the uniqueness and randomness of IrisCodes: Results from 200 billion iris pair comparisons," Proceedings of the IEEE, vol. 94, no. 11, Nov. 2006, pp 1927-1935.