International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 11
November 2017

FPGA Implementation of Iris Recognition with Error Detection and Reconstruction

Sushant Sadangi
ITC Infotech India Limited

Viswajeet Lenka
ITC Infotech India Limited

ABSTRACT:

Security of the database is of utmost importance in the Biometric Security System. In the biometric security most of the algorithm decrypts the whole dataset before the match will take place. So, the process takes a lot of time to authenticate. It is challenging-cum-impossible to work with a damaged encrypted dataset stored in a database. That is where the whole concept fails. To eradicate this issue a new method with the algorithm called fallacy clear-up algorithm is introduced which gives security to iris feature without upsetting the system performance. The method includes detecting errors and reconstructing the damaged dataset. In this paper, algorithm is used to show the method of detecting errors and reconstructing binary iris dataset. The automatic error detecting and reconstructing the dataset is developed and tested using an UBIRIS database. Before every iteration, the algorithm gives the rate of recognition to be 99% and 100% accuracy in detecting error. This brief also proposesa detailed hardware architecture using Xilinx FPGA to address the aforementioned algorithm and comparisons have been made between the memory required and the rate of recognition of the system of the fallacy clear-up algorithm and also the performance are compared on the basis of computations, time and memory efficiency.

Keywords: Biometric Security System, Fallacy clear-up algorithm, Xilinx FPGA

1.INTRODUCTION:

In the era of this digital world, security has been the major concern of the people as protecting the confidential information like corporate info and personal info has become a real issue for the world. The traditional methodology of password, keys doesn't provide the enough security against the world with Hackers. As a matter of fact, password found to be the weakest link to secure a confidential data as they are shareable and can be cracked by various methods. So, strong authentication method is needed in today's time. This is where biometric technology has proved to be the best way to protect one's data. As comparative to other mode of biometric authentication system iris scan is simple, reliable and has higher accuracy. This feature makes iris scan a promising security solution. The process starts by pre-processing iris images to cancel noisy parameter. After that, concerning features are extracted and matched with the ones stored in database. The matching total is given to the decision device to decide for a successful match.

Author A. K. Jain, K. Nandakumar, and A. Nagar in Biometric Template Security [1] have proposed the vulnerabilities and their countermeasures of biometric system in which they focused on biometric template security. In paper Cancelable Iris Biometrics and Using Error Correcting Codes to Reduce Variability in Biometric Data [2] the author S. Kanade, D. P. Delacretaz, and B. Dorizzi proposed a 2-factor structure to produce cancelable iris templates by iris-biometric and password. They also introduced a novel approach to use error correcting codes which reduces the variation in biometric data. Author C. J. Hill in Risk of Masquerade Arising from the Storage of Biometrics [3] has proposed analysis of template storage formats and their location. He also developed generic masquerade method that can applicable to any biometric system. In paper Iris Biometric Cryptography for Identity Document [4] the author S. H. Moi, N. B. A. Rahim, P. Saad, P. L. Sim and Z. Zakaria proposed a way to generate a unique and more securely encrypted key from iris

template. Author A. K. Jain, A. Ross and S. Pankanti in Biometrics: A Tool for Information Security [5] proposed about examination of applications where biometrics can solve issues related to information security. Further explained the challenged faced by biometric systems in real-world applications. They also discussed for a large-scale authentication system the problems about security and scalability. In paper Biometric Attack Vectors and Defenses [6], the author C. Roberts explained with a broader and practical concept of biometric system attack vectors by placing them in risk-based system method to security and outlining defence. The author T. E. Boult, W. J. Scheirer, R. Woodworth in Revocable Fingerprint Biotokens: Accuracy and Security Analysis [7] reviews the dilemma of biometric i.e., the threat which can limit the application of biometric in security applications. In paper High Confidence Visual Recognition of Persons by a Test of Statistical Independence [8] the author J. G. Daugman described a procedure which is based on the failure of arithmetical test of independence to rapidly recognize visual template of personal identity.

The advantages of Field Programmable Gate Array (FPGA) like the speed, accuracy, parallel processing etc. make it a perfect platform for the efficient implementation of various real time algorithms such as the one proposed in the paper. The algorithms has been such implemented to address the optimum utilization of memory, speed and the area constraints and various other constraints.

The orientation of the paper is as follows: Section1 gives an Introduction of the work proposed in the paper followed by Section 2 that describes the algorithm that has been implemented. Next Section 3 describes about the necessary preprocessing for the algorithms followed by section 4 that describes the carefully tailored architecture for the algorithms. Section 5 briefs about the results and the analysis. Finally Section 6 concludes the paper.

2. IRIS RECOGNITION SYSTEM:

The proposed architecture consists of three phases:

1. Enrollment Phase
2. Security Check Phase
3. Testing Phase

A.Enrollment Phase: In this phase basically deals with the recognition, authentication, normalization and feature extraction of the iris template which is then stored in the database (the BRAM) of the FPGA. This database is used for the creation of standard fallacy clear-up table (SFTC) as shown in Fig1.

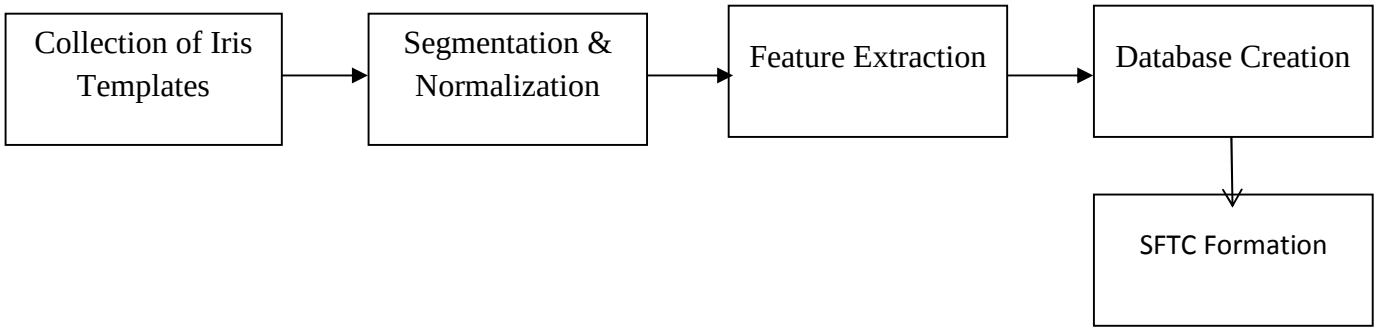

Fig 1: Block Diagram describing Enrollment Phase

B. Security Check Phase: A real-time fallacy clear-up table (RFCT) is created for the whole database, which consists of the real-time fallacy clear-up value (RFCV). Both the SFCT and RFCT are compared as shown in Fig2. If SFTC and RFTC turn out to be the same then the database is considered to be uncorrupted else the database is considered damaged.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 11
November 2017

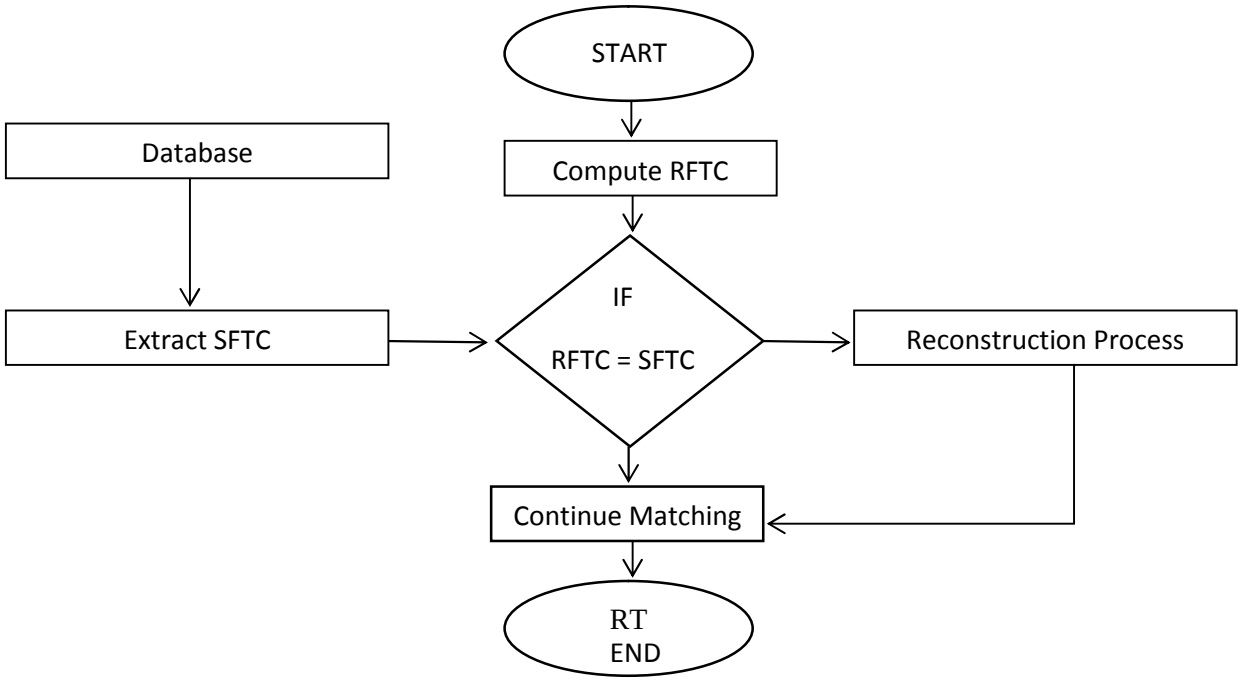

Fig 2: Block Diagram describing Security Check

C. Testing Phase: In this phase the sample template is mapped to a template stored in the database using a one-to-many matching strategy. The results are either recognized or not. Accordingly further actions are taken.

3. PRE-PROCESSING FOR IRIS FEATURESET:

The iris images are pre-processed to extract the texture. These textures are used to create a database on which the algorithm of detecting error and reconstructing is applied. For iris processing, there are three steps implemented. Those are,

A. Segmentation: It involves appropriate image processing technique for noise cancellation and separating iris portion. To cancel noise, an efficient method was to use filters i.e., median filter. A programmed segmentation structure is implemented which depends on change in circular Hough for segmenting iris region and operating morphologically to restrict the region around pupil and tested on the UBIRIS database.

B. Normalization: With this procedure, the steady areas can be considered as iris areas. Daugman's rubber sheet model is utilized for normalization. The standardization technique of Daugman's rubber sheet model changes a narrowed iris surface from Cartesian to polar directions. This procedure is perfect for managing the random variation because of the separated camera eye and its position concerning the camera.

C. Feature Extraction: In an iris region, the segregated data present is extracted to give a detailed knowledge. Iris's important feature is considered and extracted and comparison is made between datasets. The normalized image of 100 * 400 is divided into 3 parts. The size of 40 * 200 is selected and on that region 3-level of haar wavelet decomposition is applied. The detail coefficient of 3rd level that are horizontal, vertical and diagonal details are considered because they signify the best of iris texture. Using a 2-bit quantizer is used to quantize the extracted coefficient. Iris code of 375-bit is obtained and stored in database.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 11
November 2017

4. PROPOSED ARCHITECTURE:

In the process of decryption of the encrypted biometric datasets there often arises a case when the dataset becomes corrupted. These shortcomings paved the path for the development of a novel method known as the fallacy clear-up algorithms. The fallacy clear-up algorithms have proved to be a novel approach to detect errors and reconstruction of corrupted datasets. The architecture has been tailored so as to address the trade-off between speed, timing and area constraints. It architecture consists of the following components as shown in Fig3:

A. Generation of SFTC Block

B. Mapping and Error Detection Block

C. Reconstruction Block.

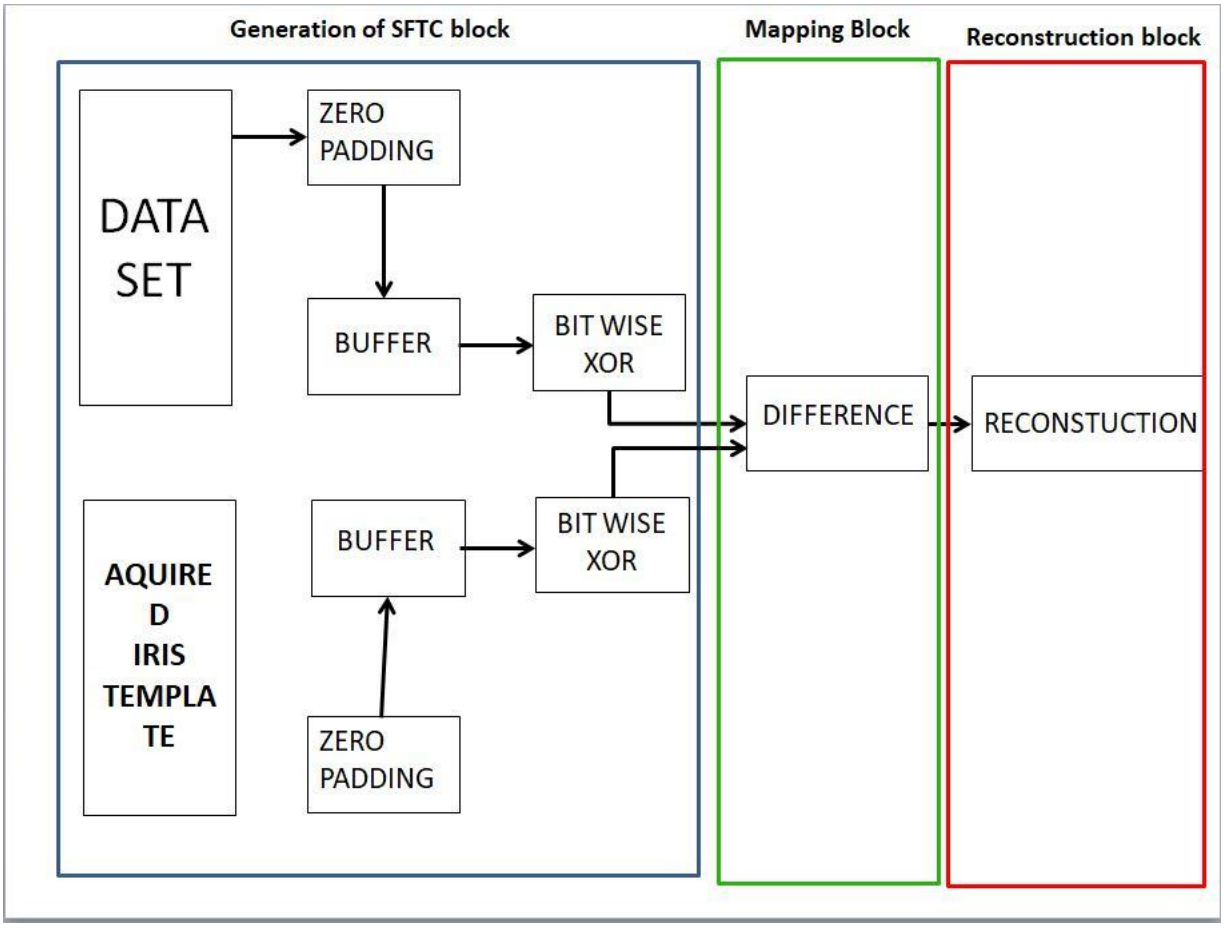

Fig 3: Hardware Realization of Iris Recognition Error Detection and Reconstruction

A.Generation of SFTC Block:

Basically this block deals with the storing of the data and creating the Standard Hash Value (SHV). The process initiates with enrollment of the iris dataset. First the data set is stored in the BRAM of the FPGA for the initial processing. From the BRAM the SFTC dataset is generated as follows: first the dataset is padded with a '0' in the beginning of the template. Next the bitwise EX-OR operation is carried out on the padded dataset. This procedure is repeated throughout the padded vector. Following explains the calculation of the SFTC for one data:

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 11
November 2017

DATA = 1 0 1 1 0 0

AFTER '0' padding = 0 1 0 1 1 0 0

SHV = 1 1 1 0 1 0

The size of each data remains the same in the database as well as in the Standard hash Value table.

B. Mapping and Error Detection Block:

Before the mapping process the query is first preprocessed and the RFCT has been calculated for the whole vector of size 375 bits and the deviation (error) was calculated for the alternate bits of the RFTC dataset as one bit change in the vector will result in a change of two consecutive bits. If the error turns out to be zero then the dataset is uncorrupted else the database is considered corrupted and is considered for reconstruction. The above can be described as follows:

ORIGINAL TEMPLATE = 0 1 0 1 1 0 0

SHV = 1 1 1 0 1 0

DAMAGED TEMPLATE = 0 1 11 1 0 0

REAL TIME HASH VALUE = 1 000 1 0

ALTERNATE VALUES FROM SHV = 1 1 1

ALTERNATE VALUES FROM RTHV = 1 0 1

DIFF = 0 1 0

This is an extremely efficient algorithm to find the error because it stores and calculates the difference between alternate values which reduces the memory consumption and greatly improves the speed of the system.

C. Reconstruction Block:

The error in the N^{th} bit results in the mismatch of $N^{th}$and $(N+1)^{th}$position in the hash value. Hence the two bits are inverted and the procedure of error correction is repeated until the error was found to be zero.

5.RESULT AND ANALYSIS:

The proposed architecture has been coded using the XILINX ISE platform and was implemented onXilinx FPGA device XC6SLX16 of Spartan 6 family having speed grade -3 and the result was verified using MATLAB. The degree of accuracy was calculated using Mean Square Error (MSE) that is given by formula (1) and the recognition rate (R.R)which is given by formula (2) and the results were tabulated.

$$MSE = \frac{1}{MN}\sum_{k=1}^{M}\sum_{l=1}^{N}[\hat{J}(k,l) - J(k,l)]^2$$

----------(1)

$$RR = \frac{Correctly\ recognized\ users}{Total\ number\ of\ users}$$

----------(2)

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 11
November 2017

Table 1 describes the hardware utilization for the proposed algorithm. It is observed that the hardware utilization has been quite less for the addressing the algorithm in the brief.

Table 1.Hardware consumption in the algorithm

Device Utilization Summary (estimated values)			[-]
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Registers	557	93120	0%
Number of Slice LUTs	980	46560	2%
Number of fully used LUT-FF pairs	487	1050	46%
Number of bonded IOBs	79	240	32%
Number of Block RAM/FIFO	5	156	3%
Number of BUFG/BUFGCTRLs	5	32	15%

Table 2 gives the comparison between two different and two same iris templates and their error detection and time taken by MATLAB and XILINX FPGA to implement the algorithms.

Table 2.Comparison between MATLAB and XILINX performance

Sr No	Image1	Image 2	Error in MATLAB	Error in XILINX	Time consumed by MATLAB (in sec)	Time consumed by FPGA (in milli - sec)
1			28.2%	28.4%	29	12
2			0%	0%	27	14

6. CONCLUSION:

The brief has addressed the hardware implementation of iris recognition with error detection and reconstruction. It can be concluded that the iris recognition using fallacy clear-up algorithm has yielded perfect results in both FPGA as well as in MATLAB. The study provides scope for the real time implementation of the algorithm. The result for the error detection was found to be 100% and that of recognition rate was 99% that stands quite upto the expectations. Efforts has been made to reduce the hardware consumption and to improve the performance at the same time special attention was given for reducing the error.

REFERENCES:

[1] Anil K. Jain, KarthikNandakumar, and Abhishek Nagar, “Biometric Template Security”, EURASIP Journal on Advances in Signal Processing, Volume 2008, Article ID 579416.
[2] S. Kanade, D. Petrovska-Delacretaz, B. Dorizzi, “Cancelable iris biometrics and using Error Correcting Codes to reduce variability in biometric data”. IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2009), June 2009, 120 -127
[3] J. Hill, “Risk of masquerade arising from the storage of biometrics,” B.S. Thesis, Australian National University, November 2001, http://chris.fornax.net/biometrics.html.
[4] S. H. Moi, N. Rahim, B. Abdul, et al., “Iris Biometric Cryptography for Identity Document”.International Conference of Soft Computing and Pattern Recognition (SOCPAR ¨09), Dec.2009, 736-741

[5] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security," IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125–143, 2006.
[6] C. Roberts, "Biometric attack vectors and defences," Computers and Security, vol. 26, no. 1, pp. 14–25, 2007.
[7] T. E. Boult, W. J. Scheirer, and R. Woodworth. Revocable fingerprint biotokens: Accuracy and security analysis. In IEEE Conference on Computer Vision and Pattern Recognition, pages 1–8, June 2007.
[8] Daugman J. G., "High confidence visual recogn test of statistical independence," IEEE Trans. Pa Intell., vol. 15, pp. 1148–1161, Nov. 1993.