Turkish Journal of Computer and Mathematics Education
DOI: https://doi.org/10.17762/turcomat.v9i3.13913 *Vol.09 No.03 (2018), 1212-1219*

Research Article

Fingerprint Identification Using FPGA with a Newly Designed Architecture

Avnish Panwar

Asst. Professor, Department of CSE (Computer sc)

GEHU-Dehradun Campus

Abstract : The Aadhaar project was recently introduced by the Unique Identification Authority of India (UIDAI) to provide a Unique Identification (UID) number to every resident of India. Biometric and demographic information are used to create a unique identification number (Aadhaar). You may use your Aadhaar number to get a subsidy on LPG cylinders, a driving licence, a PAN card and a bank account. The software industry is crucial to the success of the Aadhaar system. The suggested work, including the pre-processing stage, fingerprint recognition process, and fingerprint recognition system, is carried out across three platforms, including MATLAB, field programmable gate array (FPGA), and application specific integrated circuit (ASIC). In order to improve the processing speed, resource utilisation, power consumption, and recognition rate of the proposed job, the FPGA is programmed with two specialised hardware methods: the CORDIC algorithm and IP cores. The suggested work largely focuses on fixing the processing time and accuracy issues. The concept is converted into an ASIC using FPGA technology with the goal of reducing power consumption and resource utilisation without sacrificing performance. In contrast to FPGA implementation, which makes use of look-up tables (LUTs) and customizable logic blocks (CLBs), ASIC implementation makes use of the basic cells directly. When compared to FPGA design, ASIC development speeds up recognition by 20%.

Keywords Unique Identification Authority of India, look-up tables (LUTs), application specific integrated circuit(ASIC), configurable logic blocks (CLBs)

Introduction

Typically, biometric systems have been developed using either software, hardware (based on a microprocessor or microcontroller), or a combination of the two. Embedded systems are constantly being put to the test by cutting-edge devices like smart cards and PDAs. A real-world effect of an embedded system. To optimise for adaptability, reusability, performance, and affordability, the functionality has been meticulously separated into software and hardware. Building a biometric verification system for an embedded setting when resources like power and space are limited is challenging. In [1], the authors present a safe and effective embedded fingerprint verification system based on the Thumb Pod embedded device equipped with a Leon-2 CPU. The suggested architecture is implemented in 10 stages, each of which is optimised for performance and memory use. The optimisation methods result in a 65% decrease in runtime and a 67% decrease in data size. Online fingerprint verification utilising feature extraction and feature matching is given in [4], along with its design and implementation. The suggested procedure uses a SPARC 20 workstation and is carried out in two phases. The experimental findings of an online fingerprint verification system demonstrate a verification accuracy of 99%, but a somewhat slow response time (in seconds). Using a 32-bit microcontroller, [7] describes an intelligent authentication system. Intelligent authentication systems are characterised by their small size, low power requirements, cheap cost, safety, and dependability. Significant performance gains over conventional systems are highlighted by hardware-based field-programmable gate arrays. Powerful system on a chip (SoC) platforms, such as field programmable gate arrays (FPGA) with extensive process resources and embedded processors 2, are progressively capturing the market's attention. Software, hardware (Microprocessor based or Microcontroller based), and hardware-software co-design for uni-modal biometric systems (Fingerprint, Iris, Face, palm, etc.) are suggested and tested for diverse applications. To get the desired results in terms of accuracy, performance,

cost, usability, dependability, and scalability, the complexity of such a system grows tremendously. Uni-modal biometric applications using field programmable gate arrays (FPGA) remain difficult to physically implement. In [8], the authors demonstrate a Spartan-3 FPGA implementation of a low-cost minutiae extraction technique.

A microprocessor and a specialised co-processor form the backbone of the system's internal design, allowing for finer-grained control. One open problem in modern biometrics is the creation of a fingerprint verification system for a cheap embedded platform. In [56], we see a technique for extracting and matching fingerprint fine details at a reasonable cost. The system runs on an integrated Leon2 open core CPU inside a Spartan-3 FPGA. To speed up the process of extracting finer details, the design includes a floating point unit and a discrete Fourier transform (DFT) co-processor. In [7], we demonstrate the parallel architecture of a fingerprint identification system running on a Xilinx Virtex -4 FPGA evaluation board. In spite of the informational burden, the design guarantees lightning-fast reaction times. Spatial binary filtering is used to collect data for feature extraction, and the matching process relies on Euclidean distance to pair together feature vectors. A 97% or higher recognition rate and a performance boost of three orders of magnitude are also hallmarks of the new system. In order to create a UID number, the current Aadhaar programme uses a combination of biometric information (from 10 fingers and the Iris) and demographic information. The processing time for Aadhaar is measured in seconds, making it unsuitable for use in real-time applications. Reconfigurable hardware has allowed for a decrease in processing time as technology has advanced.

FPGA is a programmable hardware that decreases processing time, allowing for a greater throughput (108 - 1012) in fingerprints processed per second. Physical and behavioural biometric traits are utilised in authentication systems, respectively. Fingerprints, hands, faces, irises, ears, and DNA are examples of physical traits, whereas signatures, voices, keystrokes, and other behavioural characteristics are examples of behavioural features. Fingerprints or retina scans could be the most reliable methods of identification. Some individuals may not agree with having their eyes scanned for different reasons, and those with ophthalmic issues may have difficulty with retina scanning. The practise of thumb imprint dates back hundreds of years. Fingerprints are used as a form of identification because (a) no two people, not even identical twins, have the same characteristics, (b) the intricacies of ridges on the hands and feet remain consistent as they develop, and (c) fingerprints do not change over the course of a person's lifetime and may even regenerate if they are damaged. Fingerprint identification has several benefits, including low cost, speed, ease of use, and security. In addition, fingerprints are used by two-thirds of the biometric global market and are widely accepted for government purposes. Many benefits, including cheap cost, minimal maintenance, and simple deployment, are associated with embedded biometric systems. It may be used to verify the legitimacy of an electronic passport or identification card. However, the nature of the application dictates both the kind and amount of biometric features used. Platforms for the implementation of biometric technologies are one possible solution, as shown in Figure 1.

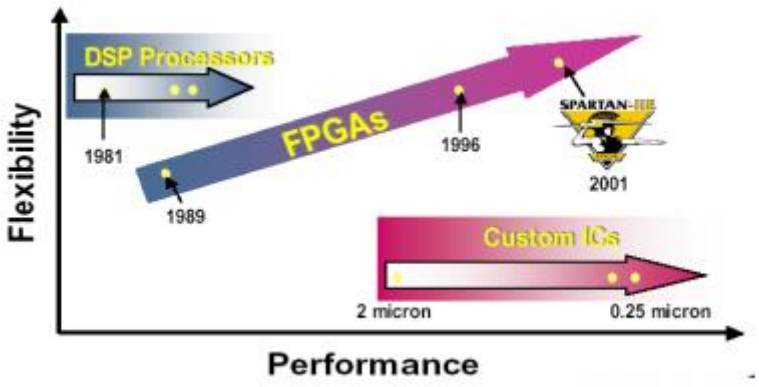

Figure 1: Implementation platforms

Problem statement

The increasing significance of digital resources highlights the need for secure methods of individual identification. The difficulties and restrictions of producing UID numbers for a large database (like the Aadhaar programme) inspired the development of a new fingerprint recognition procedure based on an innovative architectural design. Low-quality fingerprints cause significant FAR, while fingerprints that are illegible (because to scars, cuts, etc.) cause accuracy drops. Unlike the Aadhaar programme, which utilises 10 fingerprints to verify an individual's identity, the suggested concept employs either one fingerprint, or two fingers using a fusion approach. The thumb imprint is more reliable than the other four fingers since it contains the most important information. Research priorities include reducing processing times for biometric data in Aadhaar, as well as improving accuracy and fingerprint quality. The suggested architecture is built using field programmable gate arrays, a kind of reconfigurable hardware, and then converted into an ASIC using FPGA technology. The suggested design is also verified in MatLab, an FPGA, and an ASIC to ensure its viability.

Objectives

The proposed study seeks to improve identification rates by designing and implementing a new architecture for the fingerprint recognition process using field programmable gate arrays. This architecture will strive to minimise mistakes throughout the fingerprint recognition process, from sensing through template generation. The strategy employs a locally produced database made possible by an optical scanner. The suggested study delves into the seven-step procedure that culminates in the creation of a template using fingerprint data. The suggested study has as its criteria the reduction of issues related to fingerprint image quality, with the end result being an increase in FAR. The inability to read a fingerprint is mitigated by a fusion approach that increases accuracy in other ways. Additionally, the design prioritises minimising processing time.

Proposed novel architecture

Historically, identifying systems have prioritised safety above everything else. Security at various delivery / access points, such as financial accounts, credit accounts, utility records, etc., is provided by a wide variety of ID cards and ID numbers. This is supported by the fact that the United States began issuing social security numbers to citizens in 1936. Smartcard / RFID sophisticated security technologies evolved throughout time. Recently, biometric technology with fingerprints has sparked interest in this area and evolved into the pinnacle of individual identification methods. SSN was in high demand in the US because to its widespread adoption until 2006. However, reports of identity theft using Social Security numbers first began to surface in 2006. A person's SSN may also be estimated using just their date of birth and place of birth. The use of UID numbers backed by biometrics has helped alleviate these problems. The UID is a completely random number, making it very difficult to estimate. The use of biometrics in UID will guarantee individuality with a high degree of precision across a large population. Physical or behavioural biometric data may be collected. The collection and storage of physical data is far more practical than that of behavioural data. Fingerprints and irises are two of the most popular physical biometrics because of their reliability and accuracy. Compared to iris scanning, fingerprints have a number of advantages that make them more popular. So far, no evidence of biometric similarity between sets of identical twins has been uncovered, making biometrics the gold standard for personal identification and verification. Therefore, a fingerprint serves as a one-of-a-kind identifier. Enrollment for UIDs in India will occur on a massive scale and in a wide variety of settings. The most resource-heavy task performed by the UID server system is the 1:N biometric comparison, where N is the size of the UID database. The process of registering a UID request is followed by a thorough comparison of all available information (demographics and biometrics). UIDs are produced when the unique entry has been verified. It takes 5MB of space to keep all of a person's information safe and sound.

In comparison to the Aadhaar system, the fingerprint recognition process (FPRP) / fingerprint recognition system (FPRS) based on FPGAs is not only faster, but also more accurate, cheaper, and easier to maintain.

Using the suggested unique technique from acquisition through template creation may greatly reduce the number of incorrect matches. The apps may also be built for real-time operation.

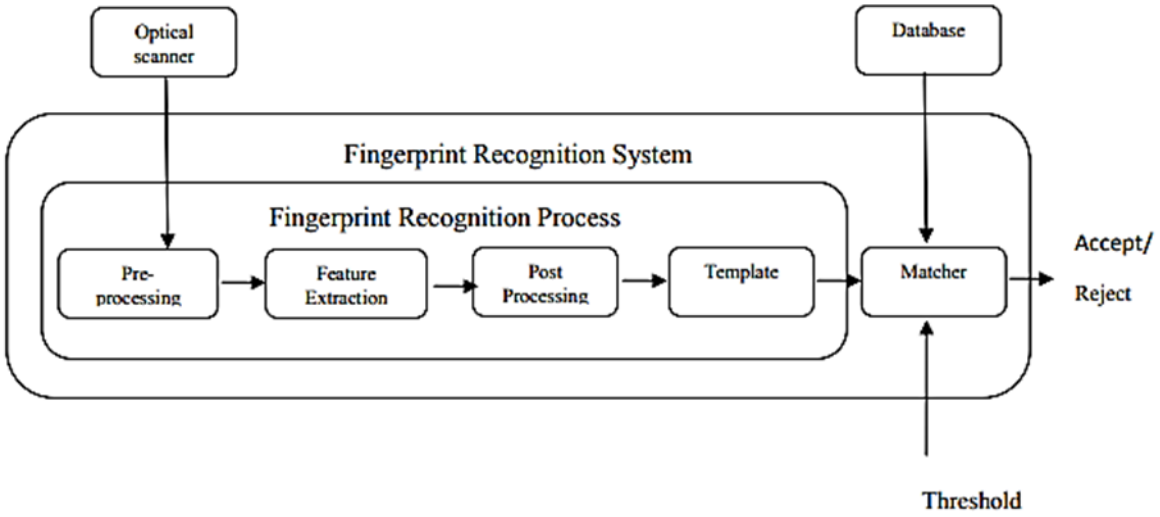

Figure2: Proposed block diagram of fingerprint recognition process / system

Experimental Results

The effectiveness of the planned work is measured in terms of its efficiency in terms of time, resources, and energy. Logic blocks for realising the fingerprint recognition process in hardware may be estimated via resource use. ASIC implementation using FPGA technology reduces the proposed architecture's overhead in terms of size and processing time. Reduced software footprint increases overall system security while also speeding up computations. Hardware can do DSP operations with minimal to no loss of precision. As a consequence, both processing time and power consumption are lowered. The suggested work's efficacy is measured both with and without the fingerprint identification system's pre- and post-processing stages. The filter block's serial and parallel architectures are implemented at the preprocessing step. Time spent processing data should be cut in half with a parallel architecture, compared to a serial one. Due to the parallel architecture's 4 symmetrical processing parts, the recognition process / system may run faster at the expense of more hardware. Existing fingerprint identification systems are compared to the proposed work's processing time, FAR, FRR, and power consumption. Taking into account hardware resources, processing time, and power consumption, the results of simulation and implementation using MatLab, FPGA, and ASIC platforms are described in three distinct parts. Since the ASIC design employs the fundamental cells instead of LUTs like in FGPA, the latency is shorter, guaranteeing higher performance. In addition, it uses less energy (as a result of fewer components) and takes up less room (which improves mobility).

Results of MATLAB implementation

The optical scanner collects a 248-by-292-pixel fingerprint picture in 8-bit greyscale. Input to the fingerprint identification system looks like the fingerprint picture in Figure 3,(A). In the normalisation block, the fingerprint image's differences along the ridges are reduced. After the picture has been normalised, the orientation angle may be calculated and used to set the filter's parameters. The noise in the oriented picture may be reduced via filtering. Design and analysis of parallel and serial architectures are performed. The process of binarization reduces a picture to a binary value. During the process of thinning, the width of the binarized picture is decreased to a single pixel. Figure 3(B) depicts the preprocessing stage's MatLab output, which is just a reduced version of the original fingerprint picture.

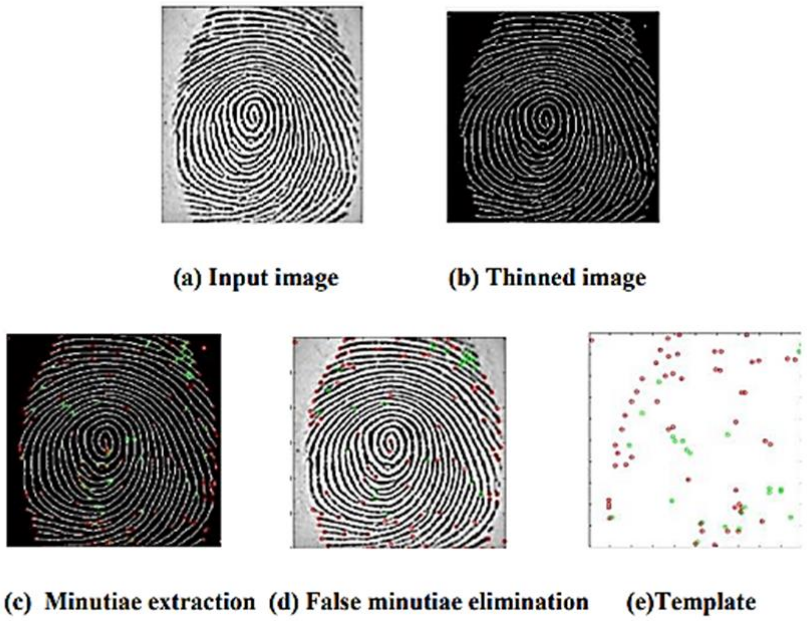

Figure 3: Images of fingerprint recognition process

Figure 3(c) illustrates how the thinned picture is used as input by the feature extraction step, which then extracts the finer details represented by the image's termination and bifurcation. Figure 3(d) shows how eliminating the erroneous minutiae caused by noise and artefacts yields trustworthy minutiae. As can be seen in Figure 3(e), the input fingerprint picture is broken down into its component parts and then saved as a template in the database for later matching.

Damaged fingerprint pictures of the same finger from the same individual are shown in Figure 4 (a) and (b). The combined fingerprint picture shown in Figure 4 (c) is the end outcome of this process. The resulting picture is educational and easier on the eyes.

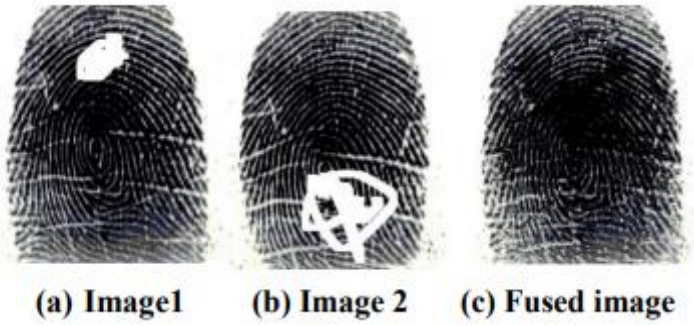

Figure 4. Retrieval of original fingerprint

Results of FPGA implementation

You may find information on the Virtex-5 FPGA development board and its XC5VLX110T target device, including its voltage rails, clocking schemes, functional and architectural aspects, in [Appendix B]. The FPGA implementation results are broken down into three distinct parts, each of which considers a unique angle: in order of importance: hardware resources, processing time, and power usage.

Resource utilization (estimated)

Table 1 details the slice registers, LUTs, IOBs, and DSPs that were made accessible and used during the preprocessing step (image enhancement approach). These numbers are approximations based on the RTL schematics of the appropriate design blocks..

Device Utilization Summary (estimated values)			[-]
Logic Utilization	**Used**	**Available**	**Utilization (%)**
Number of Slice Registers	3343	69120	4
Number of Slice LUTs	5455	69120	7
Number of fully used LUT-FF pairs	1666	7132	23
Number of bonded IOBs	9	640	1
Number of BUFG/BUFGCTRLs	1	32	3
Number of DSP48Es	3	64	4

Table 1: Device utilization of pre-processing stage

Device utilisation estimates for the various phases of the fingerprint recognition process are provided in Table 2. The figures in the table represent the hardware's utilisation, while the percentages in brackets represent that utilization's frequency..

Table 2: Device utilization of fingerprint recognition process

Device Utilization Summary (estimated values)								
Logic Utilization	**Norm**	Orient	Filter	Binar	Thinn	Min	False	FPRP
Numbe of Slice Registers	14 (0%)	1046 (3%)	950 (2%)	11 (0%)	14 (0%)	48 (0%)	48 (0%)	2076 (3%)
Number of Slice LUTs	16 (0%)	787 (2%)	1057 (3%)	13 (0%)	16 (0%)	51 (0%)	51 (0%)	864 (1%)
Number of fully used LUT-FF pairs	14 (11%)	26 (21%)	83 (68%)	11 (9%)	16 (13%)	32 (26%)	28 (22%)	685 (30%)
Number of bonded IOBs	3 (0%)	27 (5%)	8 (1%)	4 (0%)	3 (0%)	22 (4%)	22 (4%)	132 (20%)
Number of BUFG/BUFGCTRLs	1 (3%)	1 (3%)	6 (18%)	1 (3%)	1 (3%)	1 (3%)	1 (3%)	1 (3%)
Number of DSP48Es		5 (10%)	34 (70%)					30 (46%)

Conclusion

In order to carry out the suggested work, a Virtex-5 FPGA development board is used as the focal point. There will be extra time and space requirements since CLBs and LUTs form the foundation of the FPGA development board design. The wasted space from the LUTs, CLBs, IOB, and BRAMs is unavoidable. However, this problem is solved by using FPGA technology to build the suggested design on an ASIC platform. Existing system against FPGA and ASIC comparisons are also performed. FPGA's reprogrammability allows it to adapt to changing needs. In order to save processing time and power consumption, DSP activities may be performed in hardware with a small footprint without sacrificing precision.

References

1. Shenglin Yang and Ingrid Verbauwhede, "A Real time, memory efficient Fingerprint verification system", IEEE, Proceedings of International conference on acoustics, speech and signal processing, vol.5, pp 189-192, 2004.
2. Javed Ahmed Mahar and Syed Faisal Ahmed Bukhari, "Gabor based fingerprints verification of property documents", IEEE, Proceedings of International conference on Digital Image Processing, pp 247-251, 2009.
3. G Danese, M Giachero, F Leporati, N Nazzicari, "A Multicore Embedded Processor for Fingerprint Recognition", IEEE, Proceedings of 13th Euromicro conference on Digital system design : Architectures, Methods and Tools, pp 779- 784, 2010.
4. Anil Jain & Lin Hong, "On-Line Fingerprint Verification", IEEE, Proceedings of the 13th International conference on pattern recognition, vol.3, pp 596-600, 1996.
5. Mariano Fons, Francisco Fons, Enrique canto, Mariano Lopez, "Hardwaresoftware Co-design of a fingerprint matcher on card", IEEE, International conference on electro/information technology, pp 113-118, 2006.
6. Sung Bum pan, Daesung Moon, Kichul Kim, Yongwha Chung, "A VLSI Implementation of Minutiae Extraction for Secure Fingerprint Authentication", IEEE, International conference on computational intelligence and security, vol.2, pp 1217-1220, 2006.
7. Fengling wang and yuanyi Zhang, "Study and Design of Intelligent Authentication System based on Fingerprint Identification", IEEE, Second international Symposium on Knowledge acquisition and modeling, vol.3, pp 170- 173, 2009.
8. Francisco Fons, Mariano Fons, Enrique canto, Mariano Lopez, "Flexible Hardware for Fingerprint Image Processing", IEEE, 3 rd conference on Ph. D research in microelectronics and electronics, pp 169-172, 2-5 July, 2007.
9. Francisco Fons, Mariano Fons, Enrique Canto, "Approaching Fingerprint image Enhancement through Reconfigurable Hardware Accelerators", IEEE, International symposium on intelligent signal processing, pp 1-6, 2007.
10. M Fons, F Fons and E canto, "Fingerprint Image Processing Acceleration through run-time Reconfigurable Hardware", IEEE Transactions on circuits and systems –II Express Briefs, vol.57, N0.12, pp 991-995, December 2010.
11. Peng Jian, Wu Min and Liu Yadong, "Design and implementation of an embedded fingerprint identification system for the bank staff identity authentication", International conference on embedded software and systems symposia, pp 69-72, 2008.
12. Hui Xu, Yifan Qu, Yan Zhang, Feng Zhao, "FPGA Based Parallel Thinning for Binary Fingerprint Image", IEEE, Chinese conference on pattern recognition, pp 1- 4, 2009.
13. Amira M Saleh, Ayman M Bahaa Eldin, Abdel-moneim A Wahdam, "A modified thinning algorithm for fingerprint identification systems", IEEE, International conference on computer engineering and systems, pp 371-376, 2009.

14. N. Pavesic, S. Ribaric and B. Grad, "Finger-based personal authentication: A comparison of feature-extraction methods based on principal component analysis, most discriminant features and regularized direct-linear discriminant analysis", IET signal process, vol.3, Issue. 4, pp 269-281, 2009.
15. Lin Zhang, Lei Zhang and David Zhang, "Finger-Knuckle-Print: A new biometric identifier", IEEE, 16th International conference on Image processing, pp 1981-1984, 2009.
16. M. Usman. Akram, Anam. Tariq and Shoab. A. Khan, "Fingerprint image: pre- and post-processing", International journal on biometrics, vol. 1, No. 1, pp. 63-80, 2008.
17. Byung-Gyu Kim, Han-Ju Kim and Dong-Jo Park, "New Enhancement Algorithm for Fingerprint Images", IEEE, pp 1-4, 2002.
18. Lin Hong, Yifei.Wan, and Anil Jain, "Fingerprint image enhancement: Algorithm and performance evaluation", IEEE Transactions on pattern recognition and machine intelligence, vol.20, No.8, pp 777-789, 1998.
19. Sajid, Sotirios G. Ziavras and M.M. Ahmed, "FPGA-Based Normalization for modified Gramschmidt Orthogonalization", International Conference on Computer Vision Theory and Applications, France, pp 1-6, May 2010.
20. Chapa Martell Mario Alberto and Prof.ABE koki, "Fingerprint image enhancement algorithm implemented on an FPGA", pp 1-6, August 1, 2009.
21. Shahram Mohammadi and Ali Farajzadeh, "Fingerprint Reference Point Detection using Orientation Field and Curvature Measurements", IEEE, International conference on Intelligent Computing and Intelligent Systems, vol. 4 , pp 25 – 29, 20-22 November 2009.
22. Mariano Lopez Garcia, Enrique, F Canto Navarro, "FPGA Implementation of a Ridge Extraction Fingerprint Algorithm Based on Microblaze and Hardware Coprocessor", IEEE, International Conference on Field programmable logic and applications, pp 1 – 5, 28-30 August 2006.
23. Ting Tang, Xiaopei Wu, Ming Xiang, "An Improved Fingerprint Singular Point Detection Algorithm Based on Continuous Orientation Field", IEEE, International Symposium on Computer Science and Computational Technology, pp 454-457, 2008.
24. Soma Biswas, Nalini K. Ratha, Gaurav Aggarwal and Jonathan Connell, "Exploring Ridge Curvature for Fingerprint Indexing", IEEE, 2 nd International conference on Biometric: Theory, applications and systems, pp 1-6, 2008.
25. C. Militello, V. Conti, F. Sorbello, S. Vitabile, "A Novel Embedded Fingerprints Authentication System Based on Singularity Points", International Conference on Complex, Intelligent and Software Intensive Systems, pp 72 – 78, 2008