International Journal of Engineering Research in Electrical and Electronic Engineering (IJEREEE) Vol 2, Issue 1, January 2016

State of Art : Embedded Security Trends in Personal Recognition Systems

[1]Anil Jadhav [2]Bhagyashree Mendake
[1][2]UG Students Department of Electrical & Electronics Engineering
VTU- Belagavi
[1]aj123627@gmail.com, [2]bhagyashreemendake@gmail.com,

***Abstract*— Nowadays biometrics and embedded systems technologies bring the required means to face those security challenges in the current technological age. The electronic age points to the embedded security as one efficient solution for those applications where confidential treatment of the information is needed. Moreover, the genuine biometric characteristics of each individual become the most reliable features to be used as personal identifiers in front of the world, replacing those low-security tokens such as ID cards, PINs and passwords. Following this direction, the HW-SW co-design of a fingerprint-based personal recognition system embedded on a dynamically reconfigurable platform is suggested in this work. The selected system architecture provides the power to design these high performance applications at low cost.**

I. INTRODUCTION

Human fingerprints are one of the oldest signs of identity. Their effectiveness has been proven along the time, in either civil or forensic personal identification applications. Two are the main reasons to build a reliable personal recognition system based on fingerprint biometrics. Uniqueness it is believed that there do not exist in the world two people with identical fingerprints. Every individual has his own fingerprints, different to the rest of the humanity, so fingerprint characteristics can be used as the genetic code inherent to the individual's identity. Permanence those distinctive traits (fingerprint patterns) are invariant with time. Their formation depends on the initial conditions of the embryonic development, and once the embryo is fully developed, the fingerprint ridge-valley flow pattern keeps invariant with time.

Although the discrimination power of human fingerprints is a reality, the design of an electronic system able to automate the matching process of two fingerprints in an accurate way is still an open research problem. The automatic fingerprint recognition system is responsible for matching two fingerprint impressions and generating a similarity score in the range 0% - 100%. The closer the score is to 100%, the more certain is the system that both fingerprints come from the same finger (so both fingerprints belong to the same individual). Similarly, the closer the score is to 0%, the more confident is the system that both fingerprints come from different fingers. The comparison of the similarity score with a certain threshold will state the final authentication result (match/non match). The accuracy of the recognition system is calculated by means of the false acceptance (FAR) and false rejection (FRR) rates.) Both rates are also in the range [0,1], and the closer the FAR and FRR rates are to 0, the more reliable is the recognition system. However, there exists a trade-off between FAR and FRR:decreasing/improving FAR implies increasing/worsening FRR, and vice versa. The selection of the matching threshold for the application normally involves a compromise and it strongly depends on the security level (FAR/FRR levels) required for the recognition system. Critical applications (e.g. access control systems to restricted areas) will require high thresholds (low FAR) whereas less critical daily-use applications can accept medium-low thresholds (low FRR). The remainder of the paper is organized as follows. In section 2 the different stages involved in an AFAS (automatic fingerprint authentication system) are detailed. The system architecture suggested for the application is covered in section 3. Finally, in section 4, the article ends with some concluding remarks.

II. FINGERPRINT AUTHENTICATION

Several processing tasks are involved in an automatic fingerprint-based recognition system:

A. Image Acquisition

The first step deals with the acquisition of a digital bitmap of the user's fingerprint. There are different types of electronic fingerprint sensors in the market according to the technology selected to build the sensor device (e.g. optical sensors, capacitive sensors, thermal sensors...). Moreover, a new classification can be done according to the size of the sensing surface: complete fingerprint sensors, where the sensing surface is big enough to acquire the complete image of the fingerprint in only one step, and sweeping sensors, where it is needed to sweep the finger over a rectangular sensing surface of several pixels tall to acquire the complete image. In this case, an additional processing stage consisting in the reconstruction of the consecutive slices is

required in order to obtain the complete bitmap. Thinking about low-cost embedded systems, authors have selected a thermal sweeping sensor as a good choice to develop a personal recognition system. Apart from the fact that less silicon area means less cost for the sensing device, the reduced size of the sensor is ideal to be embedded in a small platform such as a smart card. The sweeping technique can also improve the security of the system by removing the chance of latent whole fingerprint images on the sensing surface after the acquisition process. Fig. 1.a shows the consecutive slices acquired, and the complete fingerprint image reconstructed from them.

B. Image Processing

Many methods for matching fingerprints have been presented in literature [1]. A classification can be done according to the fingerprint features used in the matching process as image correlation-based, ridge-based and minutiae-based techniques. However, in order to increase as much as possible the reliability of the matching system, the general trends in fingerprint biometrics points to the development of hybrid systems that fusion all those techniques in order to take profit of their advantages while overcoming their weak points.

Several image-processing stages are needed before extracting those distinctive characteristics available in a fingerprint impression. After the fingerprint acquisition stage, a digital bitmap of the finger texture is obtained. This bitmap is normally composed of two parts: the real fingerprint area and the background. A first pre-processing stage called segmentation [2] is needed in order to discriminate between the image foreground and the background. After the segmentation process, only the foreground area will be taken into account, and further analyzed in the next processing stages.

Fingerprints are oriented texture patterns. The field orientation map denotes the average orientation of the fingerprint ridges in every local region of the image. Therefore, the original image is split in blocks and the ridge orientation is estimated for each block as suggested in [3].The ridge orientation of an image block can be obtained by computing the gradient for every pixel of the block. The gradient denotes the direction of those pixels on the image that present the maximum intensity change. Once computed the gradient for all the pixels of the block, the average magnitude determines the gradient of the block. Since the image is inherently rich in edges due to the ridge-valley alternation, the gradient response is high in those blocks corresponding to the finger, whereas those blocks related to the background of the image present a small gradient response. Therefore, once determined the gradient of each image block, it is possible to use it in order to perform the segmentation of the original image. The comparison of the gradient of each block with a certain threshold will determine if the block belongs to the foreground or to the background. As result of the image segmentation, the image background is separated from the fingerprint area. Fig. 1.b shows the segmentation result obtained from the original fingerprint image, and Fig. 1.c shows the field orientation map for the segmented image.

C. Feature extraction

Two are the main features extracted from a fingerprint to be used in the matching process, the field orientation map, obtained by computing the ridge orientation of each image block, and those characteristics points, called minutiae, and mainly based on the ridge discontinuities (ridge endings and ridge bifurcations).

D. Feature Matching

Fingerprint matching is a real challenging task. Many research lines have been developed coping with the nonlinear distortions originated during the fingerprint acquisition stage, when mapping a 3-dimensional and elastic fingertip onto a 2-dimensional sensor plane. These distortions are practically inevitable, and are caused by several factors such as the unevenly distributed pressure exerted by the finger over the scanning sensor, as well as the inherent elasticity of the skin.

The fingerprint matching technique used in this work does not deal with the complete images. As described in the above sections, the algorithm extracts those relevant features present in the fingerprint impressions. Once obtained the distinctive features for both fingerprints to be compared, the alignment of both images is done. After the spatial alignment of both fingerprint impressions, it is possible to identify the overlapped area between both prints.

This overlapped area becomes the region of interest to be further analyzed: the comparison of the field orientation maps and the minutiae points present in the region of interest results in a similarity score which is used to decide the final matching response. Either both fingerprints are genuine (generated from the same finger), when the similarity score is equal or bigger than the application threshold, or they are assumed to belong to different fingers when the similarity score is below the threshold.

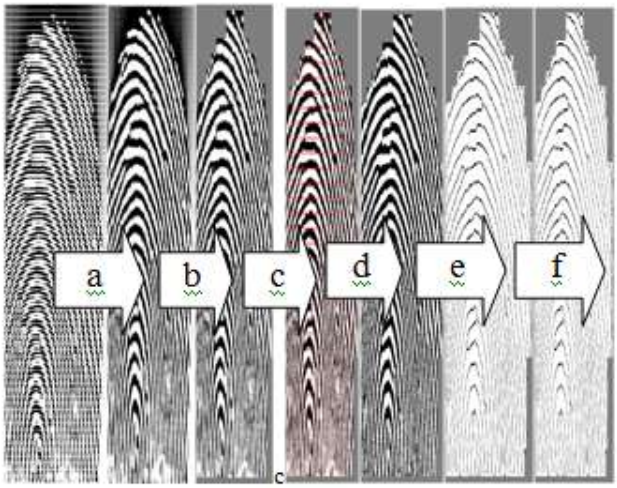

Figure 1. Fingerprint image processing stages: a) acquisition and reconstruction, b) segmentation,c) field orientation map extraction, d) binarization, e) thinning, f) minutiae extraction and filtering.

This overlapped area becomes the region of interest to be further analyzed: the comparison of the field orientation maps and the minutiae points present in the region of interest results in a similarity score which is used to decide the final matching response. Either both fingerprints are genuine (generated from the same finger), when the similarity score is equal or bigger than the application threshold, or they are assumed to belong to different fingers when the similarity score is below the threshold.

III. SYSTEM ARCHITECTURE

Most of the personal recognition systems available in the market today dealing with biometric features are based on purely software solutions. The typical implementation of these systems relies on personal computers equipped with powerful microprocessors and DSP (digital signal processors) platforms responsible for performing complex image processing and data computation tasks at high-speed rates [6]. However, this architecture is not suitable when transferring these applications to small and portable embedded systems such as smart cards. Current smart cards present limited computational resources such as one general purpose microprocessor and limited volatile and non-volatile memory blocks. A new system architecture concept needs to be introduced in order to implement those high performance applications featuring complex and real-time computing requirements on a small platform such as a smart card.

The advances made in VLSI technology offer the hardware-software co-design methodology as well as the hardware reconfigurability performance as a challenging alternative solution. An embedded system featuring a software block (MCU, DSP) and a dynamically reconfigurable hardware block (FPGA) presents much more advantages than traditional solutions.

The introduction of the field programmable hardware devices allows the partitioning of any application into hardware and software tasks: those complex and time consuming computational tasks can be accelerated by synthesizing them into the hardware core blocks (FPGA), while the rest of less computationally-expensive tasks can be kept under the control of the software block (MCU). There is a natural trade-off between application execution time and system cost when partitioning any industrial application in hardware and software tasks: software tasks mean more latency whereas hardware tasks mean more cost.

The reconfigurability performance allows the reuse of the hardware resources in those systems where the application flow can be based on the execution of sequential tasks. By using reconfigurable hardware, the total area needed for the FPGA is drastically reduced so the cost of the system is clearly improved, but additional execution time is introduced into the system for reconfigurability purposes. The balance of such constraints in any application will set the final hardware-software partitioning.

In the suggested architecture, two main processor units are present: one general-purpose microprocessor (MCU), and one general-purpose field programmable gate array device with dynamic reconfigurability performance (R-FPGA) [7]. Both processors work in parallel. The MCU becomes the master scheduler of the personal recognition system, responsible for controlling and monitoring the application flow, while the FPGA works as a slave block where specific coprocessors multiplexed in time can be synthesized in order to accelerate those critical tasks. Application-specific functions are downloaded into the FPGA as they are needed along the execution time, thus reducing the area needs for the device in comparison with the static implementation of all functional modules in a non-reconfigurable FPGA.

Moreover, the MCU is responsible for the reconfigurability of the FPGA. Thus, two new concepts such as hardware design and dynamic reconfigurability performance of the hardware resources are added to the software functionality in order to build a new concept of embedded system platform.

A first prototype board has been developed to evaluate the effectiveness of the system topology suggested in this work. By using the prototype depicted on Fig. 2, authors have successfully developed several mathematical coprocessors with reconfigurability performance [8]. Moreover, some of the stages that take place in the biometric process have been implemented by means of hardware software co-design techniques: the first one, consisting of the fingerprint acquisition [9], and the latest one, the fingerprint matching [10]. Authors are currently working on the physical implementation of the rest of intermediate stages (image enhancement and feature extraction) in order to complete the recognition system.

IV. CONCLUSIONS

Absolute security does not exist. However, there are many ways to improve the security of current personal recognition systems. The development of an AFAS embedded in a low cost platform is suggested in this work. A new architecture concept is proposed to be applied to the automatic personal authenticator systems: secure biometricsbased platforms dealing with automatic user recognition by means of electronic fingerprint sensors and flexible hardware embedded in the own portable embedded system or smart card. The fingerprint image acquisition, data processing and user authentication stages take place inside the embedded system, where all the information is well protected against external attacks. This new solution replaces the usage of secret PIN numbers or passwords as security tokens, and the user's fingerprint pattern becomes the genetic code to be used as personal identifier in front of the world. The development of such applications at low cost in the way of portable and secure embedded systems is still a real technological challenge but some work-in-progress is being done [11]. This solution could spread the security over a big range of daily-use applications such as access control systems, cash terminals, public transport, internet where reliable authenticator systems with on-line and high-security requirements are needed.

ACKNOWLEDGMENT

We would like to take this opportunity to express my deep sense of gratitude to Dr.K.G.Vishwanath, Principal & Director, Jain college of engineering, Belagavi, for his valuable inspiration and guidance without which the proposed work would not have progressed to its present state. We cannot forget the constant Encouragement And Help Provided By Our Parents, Friends For Their Extended Support.

REFERENCES

[1] D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, Handbook of Fingerprint Recognition, Springer, 2003, ISBN 0-387-95431-7.

[2] N. K. Ratha, S. Chen, A. K. Jain, "Adaptive flow orientation based feature extraction in fingerprint images", Pattern Recognition, vol. 28, 1995, pp. 1657-1672.

[3] L. Hong, Y. Wan, A. Jain, "Fingerprint image enhancement: algorithm and performance evaluation", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 8, 1998, pp. 777-789.

[4] L. O'Gorman, J. V. Nickerson, "An aproach to fingerprint filter design", Pattern Recognition, vol. 22, no. 1, 1989, pp. 29-38.

[5] L. Lam, S.-W. Lee, C. Y. Suen, "Thinning methodologies. A comprehensive survey", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 14, no. 9, 1992, pp. 869-885.

[6] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, A. K. Jain,"FVC2004: third fingerprint verification competition", Proceedings of ICBA 2004, LNCS 3072, 2004, pp. 1-7.

[7] S. Donthi, R.L. Haggard, "A survey of dynamically reconfigurable FPGA devices", IEEE Proceedings of the 35th Southeastern Symposium on System Theory, 2003, pp. 422-426.

[8] F. Fons, M. Fons, E. Cantó, M. López, "Trigonometric computing embedded in a dinamically reconfigurable CORDIC system-on-chip", International Workshop on Applied Reconfigurable Computing, ARC 2006, Springer-Verlag, LNCS 3985 (ISSN: 0302-9743), pp. 122-127.

[9] M. Fons, F. Fons, N. Canyellas, E. Cantó, M. López, "Hardwaresoftware co-design of an automatic fingerprint

acquisition system", IEEE International Symposium on Industrial Electronics, vol. 3, 2005, pp. 1123-1128.

[10] M. Fons, F. Fons, E. Cantó, M. López, "Hardware-software co-design of a fingerprint matcher on card", IEEE International Conference on Electro/Information Technology, 2006, Michigan, USA.

[11] Q. Su, J. Tian, X. Chen, X. Yang, "A fingerprint authentication system based on mobile phone", AVBPA 2005, LNCS 3546, 2005, pp. 151-159.