HARDWARE-BASED BIOMETRIC ENCRYPTION IMPLEMENTATION WITH GAUSS-JORDAN ALGORITHM ACCELERATOR CORE IN FIELD PROGRAMMABLE GATE ARRAYS

LIEW TEK YEE

UNIVERSITI TEKNOLOGI MALAYSIA

HARDWARE-BASED BIOMETRIC ENCRYPTION IMPLEMENTATION WITH GAUSS-JORDAN ALGORITHM ACCELERATOR CORE IN FIELD PROGRAMMABLE GATE ARRAYS

LIEW TEK YEE

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Master of Engineering (Electrical)

Faculty of Electrical Engineering
Universiti Teknologi Malaysia

NOVEMBER 2011

Specially dedicated to
my beloved family and friends

ACKNOWLEDGEMENT

First of all, I would like to express my deepest gratitude to my supervisor, Prof. Dr. Mohamed Khalil Mohd. Hani whom has given me a chance to work for him. Working with him is undoubtedly very stressful and torturing but when I look back my Master journey, I don't feel regretful at all. In fact, I feel a sense of satisfaction that I've gained lots of knowledge and skills within these two years journey. To me, he is an educator instead of just a supervisor or teacher. Because of this, I've learnt a lots not only from academics but also in term of life philosophy which shapes my prospect of life. Sincere thanks to his patience, supports and guidance that make this research very fruitful.

I would like to convey my gratefulness and appreciation to all my friends and co-workers who has helped me either directly or indirectly. Special thanks to my mentor, Rabia Bakhteri for tireless guidance who spend most of her time explaining and summarizing to me the ideas regarding my research. Thanks for Annuar, Sathi, Mogenesh, Vishnu, Dr. Hau Yuan Wen, Syafeeza and Pei Chee who always share research experience, giving opinions, and spend time playing games with me. I cherish the moment we celebrated birthdays and hang out to lighten stress. without them, my research experience would not be cheerful and enjoyable.

Last but not least, warmest regards to my mother and siblings for their endless caring and encouragement along my Master journey. They are always there whenever I need help either physically or metaphysically. Thanks for my eldest brother for providing me a car so that I could travel to work with ease. Thanks to me 4th brother who give me accommodation for free. I would like to thank my friend, Meow, who always lend me his ears for countless nights listening to my problems and give advices in my life. I wish to share all of my honours and achievements with them.

ABSTRACT

Modern security systems mostly utilize cryptographic scheme or biometric technology, each with its own vulnerabilities that degrade the security level. Biometric encryption (BE) provides higher security because it reaps the benefits from both mechanisms. Since BE is a complex system, a powerful personal computer (PC) is demanded to implement the system, although its mobility and portability are greatly reduced. This thesis proposes a hardware-based BE system implemented in Field Programmable Gate Array (FPGA). The design of the proposed BE system is based on the fuzzy vault scheme. One of the most critical function in the fuzzy vault scheme is the polynomial reconstruction which is based on the compute-intensive Gauss-Jordan Elimination algorithm. In this thesis, a hardware accelerator is proposed for this algorithm to enhance the timing performance of the BE system. The proposed BE system is implemented, together with finger-vein minutiae extraction subsystem and an Advanced Encryption Standard (AES) cryptographic subsystem, in an System-on-Chip (SoC) prototype for deployment in strong authentication data security application. The finger-vein minutiae extraction subsystem takes raw finger-vein image, processes, extracts and produces minutiae template for BE system while the cryptographic engine encrypts and decrypts the secret message. The BE system in turn takes cryptographic key and finger-vein minutiae template to combine them irrecoverably. The output of BE system is a secure vault template which leaks neither cryptographic key nor finger-vein minutiae. The system is prototyped on an Altera development board running at 100MHz clock rate. Experimental results show that the hardware-based BE system achieved relatively high matching accuracy with 0.8% False Acceptance Rate and 18% False Rejection Rate and the timing performance gain is 10 times over the software prototype on embedded system. The SoC prototype is successfully deployed in an emulation of a biometric Automated Teller Machine.

ABSTRAK

Sistem sekuriti moden kebanyakannya menggunakan skim kriptografi atau teknologi biometrik, masing-masing mempunyai beberapa kerantanan yang menyebabkan penurunan tahap sekuriti. Penyulitan biometrik menyediakan lebih sekuriti yang memanfaatkan kedua-dua mekanisme. Oleh kerana BE merupakan suatu sistem yang kompleks, komputer yang berkuasa diperlukan untuk melaksana sistem tersebut, walaupun mobiliti dan kemudahalihan sistem menurun. Tesis ini mencadangkan satu sistem perkakasan BE dilaksanakan dalam "*Field Programmable Gate Array*" (FPGA). Rekaan sistem BE yang dicadangkan adalah berdasarkan skim "*fuzzy vault*". Salah satu fungsi kritikal dalam skim *fuzzy vault* adalah berdasarkan algoritma "*Gauss-Jordan Elimination*" yang intensif. Dalam tesis ini, perkakasan algorithma tersebut dicadangkan untuk meningkatkan prestasi masa sistem BE. Seterusnya, sistem BE, subsistem penyarian sifat vena dan subsistem kriptografi AES dilaksanakan dalam prototaip SoC untuk melaksanakan aplikasi sekuriti data pengesahan yang ketat. Subsistem penyarian sifat vena menerima imej vena, memproses dan menghasilkan templat *minutiae* untuk sistem BE manakala enjin kriptografi menyulit dan mendekripsikan mesej rahsia. Sistem BE seterusnya mengabungkan templat *minutiae* dan kunci kriptografi. Keluaran sistem BE adalah sustu templat "*vault*" dimana ia tidak mengandungi maklumat sama ada kunci kriptografi atau vena. Sistem ini direka dalam papan peranti keras Altera yang beroperasi pada kadar jam 100MHz. Keputusan eksperimen menunjukkan bahawa sistem perkakasan BE mencapai ketepatan pemadanan amat tinggi dengan 0.8% "*False Acceptance Rate*", 18% "*False Rejection Rate*" dan pretasi masa menaik 10 kali ganda berbanding dengan perlaksanaan perisian. Prototaip SoC tersebut telah berjaya dilaksanakan dalam pelagakan ATM biometrik.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	–	Advanced Encryption Standard
ASIC	–	Application-Specified Integrated Circuit
ASM	–	Algorithmic State Machine
ATM	–	Automated Teller Machine
BE	–	Biometric Encryption
CRC	–	Cyclic Redundancy Check
CPU	–	Central Processing Unit
CU	–	Control Unit
DMA	–	Direct Memory Access
DSP	–	Digital Signal Processing
DUT	–	Design Under Test
EER	–	Equal Error Rate
FAR	–	False Acceptance Rate
FBD	–	Functional Block Diagram
FPGA	–	Field Programmable Gate Array
FRR	–	False Rejection Rate
FV	–	Fuzzy Vault
GJ	–	Gauss-Jordan
GJA	–	Gauss-Jordan Algorithm
GJE	–	Gauss-Jordan Elimination
GPEP	–	General Purpose Embedded Processor
GPS	–	Global Positioning System
GUI	–	Graphical User Interface

HDL	–	Hardware Description Language
HW	–	Hardware
HW/SW	–	Hardware/Software
IDE	–	Integrated Development Environment
IEEE	–	Institute of Electrical and Electronics Engineers
I/O	–	Input/Output
IP	–	Intellectual Properties
IR	–	Infrared Red
IT	–	Information Technology
LSB	–	Least Significant Bit
MHz	–	Mega Hertz
OS	–	Operating System
PC	–	Personal Computer
PIN	–	Personal Identification Number
PLL	–	Phase Lock Loop
RAM	–	Random Access Memory
ROI	–	Region of Interest
RTL	–	Register Transfer Level
RTOS	–	Real Time Operating System
SBE	–	Software-based BE
SCE	–	SystemC Eclipse Environment
SoC	–	System-on-Chip
SOPC	–	System-On-Programmable-Chip
USB	–	Universal Serial Bus
VHDL	–	VHSIC Hardware Description Language
VHSIC	–	Very-High-Speed Integrated Circuits

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

This thesis describes a Biometric Encryption System for implementation in hardware based on Field Programmable Gate Array (FPGA) technology. This chapter gives the overview of biometric encryption and presents the problem statement, objectives, scope of work and research contribution.

1.1 Overview

In our increasingly digital environment, electronic gadgets are becoming more ubiquitous in society as can be seen with embedded devices such as smart phones, Global Positioning System (GPS) and tablet personal computer (such as iPad). With advancement and wide deployment of communication networks, millions of personal computers (PC) and electronic devices all over the world are connected. Inevitably, resources such as user private data would be available in an open environment as long as they are connected to the network. Therefore, to protect confidential data as well as to avoid misuse, it has now become critically important that these networked embedded devices be incorporated with security features, particularly identity-based information/data security.

Data security methods, such as access control and authentication basically involve three mechanisms: (a) knowledge-based, something you know, e.g. passwords; (b) token-based, something you have, e.g. bank card; (c) biometrics-based, something you are, that is a measurable biometric traits such as iris, fingerprint, key stroke [4] . The combination of these mechanisms forms a factor of authentication. The Automated Teller Machine (ATM) for example, applies token and knowledge-based mechanisms, that is, money withdrawal requires both ATM card and password. The deployment of biometric-based security can be found in access control,

immigration and customs. Clearly, modern security systems requires the application of cryptography and biometrics for strong authentication, data integrity and information confidentiality to be realized in embedded digital systems.

1.1.1 Cryptography

Cryptography is a process of transforming data (plaintext) into unreadable form (cipher text) so that it is safe to keep the secret in database or to send over computer network and recovers data (plain text) when it is needed. The data is encrypted using cryptographic algorithm such as Advance Encryption Standard (AES) with cryptographic keys which can be summarized in Figure 1.1. This crypto key is usually very long (128 bits for AES and 2048 bits for Rivest, Shamir and Adleman(RSA) [5]) in which it is very difficult to remember. Due to large size of crypto key, it is not feasible for user to remember and provide key whenever it is required. As a result, a passcode is used to encrypt the cryptographic key which is stored on system, smart cards or hardware tokens and it can be retrieved by providing the correct passcode. However, most passwords are so simple that they can easily be guessed or broken by simple dictionary attack [6]. In short, the storage of cryptographic key is the critical issue in cryptographic security. Many drawbacks of this system can be ameliorated by incorporation of better user authentication system, biometric authentication.

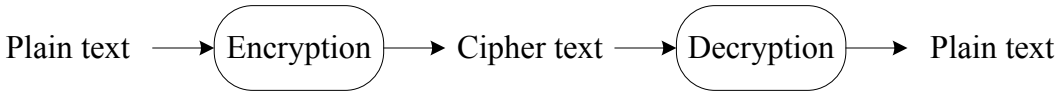

Figure 1.1: Encryption and Decryption Processes.

1.1.2 Biometric Authentication

Biometric authentication refers to verifying individuals based on their physiological and behavioural characteristics such as face, fingerprint, hand geometry, iris, keystroke, signature, voice, etc [7]. It is undoubtedly to say that biometric authentication system offers greater security than traditional password-based authentication system. Unlike cryptosystem, users need to be present at the time and

point of authentication which makes it more difficult to break compare to password-based authentication. Furthermore, one could get rid of memorizing passwords or long cryptographic keys because biometric data itself is unique and there is no such 'easy to guess' biometric. The biometric verification is based on comparison of features extracted from query image and a template which has been stored during enrolment [8]. Therefore, the storage of biometric template is playing a key role in the security of biometric authentication system. This is due to the fact that biometric data is unique for each individual and non-revocable, once compromised would only mean rendered useless. However, it is proven that biometrics could be stolen, recovered [9] [10] and in some cases, it has been proven vulnerable to attack at almost every stage of authentication process [11].

1.1.3 Biometric Encryption

Given the shortcoming of both biometrics and cryptographic system, a direct mean of enhancing security is to realize the strength of respective systems. In other words, combining biometric and cryptography has the potential to provide higher assurance of security system. A security scheme that utilizes both biometrics and crypto key is known as biometric encryption [12]. Biometric encryption combines both cryptographic keys and biometric data monolithically into a secure template, called fuzzy vault template which reveals neither biometric data nor cryptographic key. It indirectly adds one more security layer to conventional cryptographic scheme. One of the method of implementing biometric encryption is fuzzy vault scheme.

In order to access the resources, user biometric is collected during authentication to retrieve cryptographic keys. This key is then used to unlock the second layer of security system. Due to the noisiness of biometric data, fuzzy vault scheme is proposed by Juel and Sudan [13] to cater the fuzziness of biometric data. Fuzzy vault allows slight tolerance between query biometric data and the stored template since biometric data would change according to orientation of capturing, pressure, temperature and so on. In this scheme, no biometric data or cryptography key is stored. Instead, user biometric is transformed irreversibly and kept into fuzzy vault, neither key nor biometric data can be retrieved from fuzzy vault. Keys would be recreated only if correct user is authenticated. In short, biometric encryption enhances both security and privacy in positive-sum manner.

Apart from the challenges found in cryptography, biometric authentication and biometric encryption, another main problem is the technology and application related to biometric encryption. The number of application would be limited if the platform used is general purpose personal computer (PC). On the other hand, today's technology demands the computer application to be portable and as an embedded system implemented as SoC. This can be seen in the deployment of biometric authentication at door access or even fingerprint authentication system on car, like Mercedes-Benz S-Class [14]. However, prototyping a system on resource-constrain platform is challenging especially for a huge and sophisticated system like biometric encryption.

1.1.4 FPGA-based Embedded System

According to Moore's Law, the number of transistor can be put into single die doubles every 18 months which implies that more complex design could be implemented onto single chip. This is why there is an explosion development of putting a system onto a chip in electronics design such as mobile phone and GPS devices. An embedded system is defined as special-purpose computer system that performs certain task repeatedly, often responding to real-time computing constraint [1]. In recent years, there is huge improvement in speed, power consumption and complexity of integrated circuits that employ FPGA technology. The advancement of the FPGA technology has made possible the development of devices based on embedded digital system and System-on-Chip(SoC) designs.

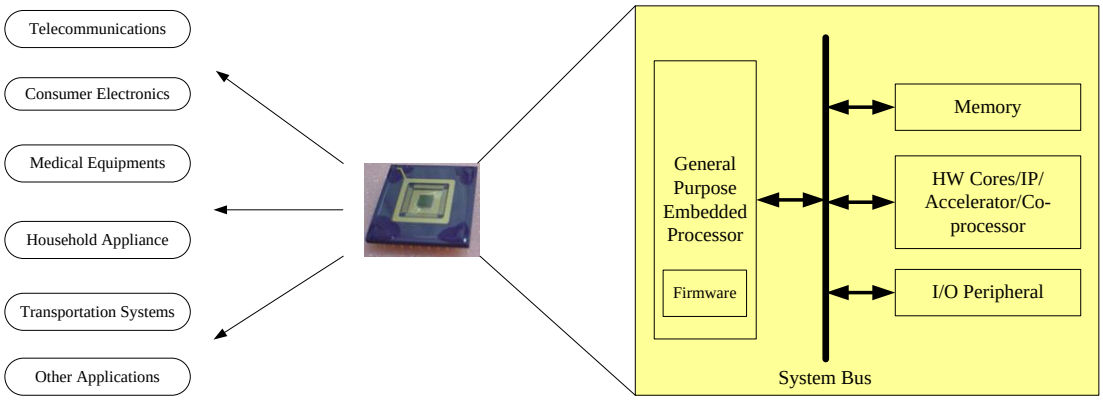

Figure 1.2: Architecture of Embedded Digital System and its Applications (adapted from [1])

An SoC is an advanced integrated circuit that includes at least a processor, memory, bus and other co-processor cores. Figure 1.2 shows the architecture of embedded digital system and its applications. The general purpose embedded processor (GPEP) executes the application software which, we will refer to as embedded software. Hardware driver or firmware is a piece of code that is executed on GPEP to communicate with Hardware (HW) cores. There are also dedicated HW accelerators to offload time consuming operations and Input/Output (I/O) peripherals which communicate with outside world. The application of SoC can range from non-volatile memory to mix signal circuit to logic circuits that can be found in medical equipments. The primary attraction of SoC devices are lower cost, smaller in size and lower power consumption. This can be verified in hand held products that SoC technology has replaced bulky mobile phones with small and compact devices. Due to higher functionality and lower power consumption, SoC design and devices are gaining popularity in recent years.

1.2 Problem Statement

Lately, much research have been carried out on the study and integration of biometric and cryptography, leading to combined system called biometric encryption. Biometric authentication measures unique human's traits such as finger print, voice, iris and so on. Due to nature that biometric data are noisy and inconsistent, biometric systems allow minor errors while maintaining high authentication accuracy. On the contrary, cryptographic schemes encrypt and decrypt secret information using cryptographic keys. Cryptography does not tolerate even a single bit of error. Therefore, integrating these two different fields of technology is a challenging task.

Most of the biometric encryption systems proposed in the past are implemented on PC, in other words, software. In such implementation, biometric templates are either stored in PC or in a central server so that it can be accessed from remote locations. However, there is a major drawback to software-based implementation; biometric templates are easily accessed by attackers, and this causes biometric information leakage issue [15]. Thus, software implementation of biometric encryption is insufficient in terms of security. In addition, biometric encryption system applies image processing and encryption algorithms, which means that the design blocks are highly compute-intensive. Hence to be viable, software-based design need to be implemented on powerful computers. This prevents biometric encryption to be deployed in portable devices embedded systems. Implementing the design on low-cost,

low-power embedded platform can lead to effective solutions to problems mentioned above. In addition, embedded digital hardware can provide secure communication, secure information storage, temper resistance which protects the system from both physical and software attacks.

Implementing any design on embedded system is a challenging task due to the fact that it has limited resources such as slow system clock and smaller storage. The embedded processor can easily be overwhelmed by the computational demands of algorithm [16] if biometric encryption system is implemented fully in software. Implementing all the computation blocks in hardware would be extremely time consuming. It does not guarantee improvement in performance an all-hardware design approach especially in a resource-constrained environment such as an embedded digital system. A suitable approach to this problem is to implement the biometric encryption system in a Hardware/Software (HW/SW) architecture that leads to FPGA-based SoC implementation. In this technique, a thorough analysis must first be carried out to determine the time-consuming modules and speed up their execution by implementing them in hardware. By offloading compute-intensive algorithms to dedicated hardware cores, the performance of system can therefore be enhanced.

1.3 Research Objectives

Considering the issues discussed in preceding sections, the objectives of the research are:

1. To design and implement the Gauss-Jordan Algorithm accelerator, so as to accelerate its compute-intensive operation in hardware. This algorithm is the core of polynomial reconstruction block in biometric encryption system.
2. To design a Biometric Encryption (BE) system based on fuzzy vault scheme that utilizes the hardware core proposed in objective number 1, and implement it in an FPGA-based embedded digital system.
3. To propose a real world SoC application prototype that integrates a finger-vein biometric subsystem, an AES cryptographic core and BE system proposed in objective number 2.

1.4 Scope of Work

The scope of this research are outlined as follows:

i) The biometric used in this project is finger-vein minutiae which is captured using modified Infra-red-Red (IR) webcam.

ii) PC serves as Graphical User Interface (GUI) that sends and receives data to/from embedded SoC via Universal Serial Bus (USB) communication cable.

iii) The focus of this thesis is mainly on the design of BE system. Biometric minutiae extraction subsystem is adopted from an in-house design by Eng [3] while AES encryption core is adopted from the work due to Vishnu [17].

iv) The fuzzy vault scheme proposed in [13] is applied in the design of the proposed BE system.

v) In this architecture, biometric feature extraction and BE are run on embedded processor as software. Biometric extraction subsystem, AES encryption, and a sub-module of BE, Gauss-Jordan Algorithm (GJA) are implemented in hardware.

vi) The SoC is implemented on Altera Stratix II EP2S180 FPGA development board running on Nios2-Linux embedded Operating System(OS) with a 100 Mega Hertz (MHz) clock frequency.

Figure 1.3 describes the proposed architecture of biometric encryption system on FPGA-based embedded system.

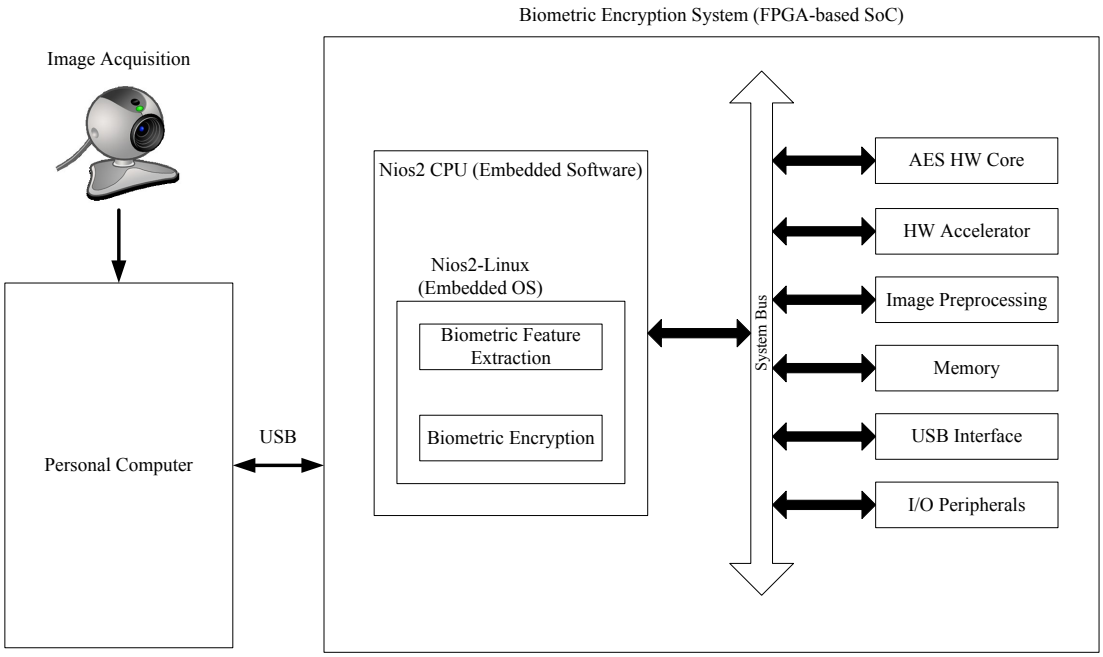

Figure 1.3: Architecture of FPGA-based SoC Biometric Encryption System

1.5 Research Contribution and Project Delivery

1. A hardware accelerator of GJA is designed.
2. An FPGA-based hardware embedded system of BE is delivered.
3. A SoC application prototype of financial security deployed in Automated Teller Machine (ATM) is developed that utilizes the biometric minutiae extraction system, the proposed BE system and AES encryption core.

1.6 Thesis Organization

Chapter 1 introduces the concept of biometric authentication system, conventional cryptographic scheme. It is followed by the shortcoming of both cryptography and biometric authentication systems which leads to problem statement. Research objectives and scope of work are defined. Finally, this chapter is summarized with research contribution and thesis organization.

Chapter 2 literature review of biometric encryption and hardware implementation of GJA. This includes literature review of different schemes of biometric encryption such as key release, key generation and key binding. Different chaff generation techniques are also discussed. This chapter also includes related work on biometric minutiae extraction.

Chapter 3 describes the theory, background, methodology and research procedure used throughout the research. Fuzzy vault scheme, GJA and biometric minutiae extraction subsystem is explained in detail. Meanwhile, several methods for verification and tools used also prepared in this chapter. Tools and techniques are also discussed in this chapter.

Chapter 4 demonstrates software implementation of BE and corresponding flowcharts are included. Then mapping of GJA into hardware are explained by using Algorithmic State Machine (ASM) flowchart and Functional Block Diagram (FBD). Designing interface unit and hardware driver is covered. Last but not least, the HW-based GJA co-processor is implemented into BE SoC.

Chapter 5 in the result and discussion. It first verify the functionality of biometric encryption system, then Gauss-Jordan elimination core with simulation results. The accuracy and timing performance analysis are also provided. Besides, an biometric ATM application that utilizes the BE is also developed.

Chapter 6 Summarizes this research and suggestions are made so as to enhance the system.

REFERENCES

1. Hau, Y. W. *Systemc-based Design Framework for an Embedded System Implemented as System-on-Chip*. Ph.D. Thesis. Universiti Teknologi Malaysia. 2009.
2. Jain, A. K., Ross, A. and Pankanti, S. Biometrics: A tool for information security. *IEEE Transactions On Information Forensics and Security*, 2006. 1(2): 125–143.
3. Eng, P. C. *Finger-Vein Biometric Authentication In A System-on-Chip Design Based On Field Programmable Gate Arrays*. Master's Thesis. Universiti Teknologi Malaysia. 2010.
4. Han, F., Hu, J., He, L. and Wang, Y. Generation of Reliable PINs from Fingerprints. *IEEE International Conference on Communications, 2007. ICC '07.* 2007. 1191 –1196.
5. Stallings, W. *Cryptography and Network Security: Principles and Practice*. 3rd ed. Pearson Education. 2002. ISBN 0130914290.
6. Klein, D. V. "Foiling the Cracker": A Survey of, and Improvements to, Password Security, 1990.
7. Uludag, U., Member, S., Pankanti, S., Jain, A. K., Member, S., Prabhakar, S., Anil and Jain, K. Biometric Cryptosystems: Issues and Challenges. *Proceedings of the IEEE.* 2004. 948–960.
8. Yang, S. and Verbauwhede, I. Automatic Secure Fingerprint Verification System Based on Fuzzy Vault Scheme. *International Conference on Acoustics, Speech, and Signal Processing*.
9. Adler, A. Sample images can be independently restored from face recognition templates. *Canadian Conference on Electrical and Computer Engineering, IEEE CCECE 2003.* 2003, vol. 2. 1163 – 1166.
10. Matsumoto, T., Matsumoto, H., Yamada, K. and Hoshino, S. Impact of Artificial "Gummy" Fingers on Fingerprint Systems. *Datenschutz Und Datensicherheit*, 2002. 26.

11. Ambalakat, P. Security of Biometric Authentication Systems, Computer Science Seminar. Rensselaer at Hartford, 2005.

12. Rabia, B. and Khalil, M. H. Securing cryptographic key with fuzzy vault based on a new chaff generation method. *International Conference on High Performance Computing and Simulation (HPCS), 2010.* 2010. 259–265.

13. Juels, A. and Sudan, M. A fuzzy vault scheme. *Information Theory, 2002. Proceedings. 2002 IEEE International Symposium on*. 2002. 408.

14. Kent, J. Malaysia car thieves steal finger. *http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm*, 31 March 2005.

15. Yang, S., Sakiyama, K. and Verbauwhede, I. A compact and efficient fingerprint verification system for secure embedded devices. *Conference Record of the Thirty-Seventh Asilomar Conference on Signals, Systems and Computers.* 2003, vol. 2. 2058 – 2062.

16. Kocher, P., Lee, R., Mcgraw, G. and Ravi, S. Security as a new dimension in embedded system design. *In Proceedings of the 41st Design Automation Conference (DAC) 04*. ACM Press. Moderator-Srivaths Ravi. 2004. 753–760.

17. Vishnu, P. *An Embedded System for Networking Security Applying Cryptographic Acceleration in Field Programmable Gate Arrays*. Master's Thesis. Universiti Teknologi Malaysia. 2009.

18. Nandakumar, K., Jain, A. K. and Pankanti, S. Fingerprint-Based Fuzzy Vault: Implementation and Performance. *IEEE Transactions on Information Forensics and Security*. 2007, vol. 2. 744–757.

19. Matyas, V., Riha, Z. and Rha, Z. . Biometric Authentication - Security And Usability. *In Proc. of IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security, Portoroz.* 2002.

20. Hao, F., Anderson, R. and Daugman, J. Combining Crypto with Biometrics Effectively. *IEEE Transactions on Computers*, 2006. 55(9): 1081 –1088. ISSN 0018-9340.

21. Group, E. B. The Relevance of Untraceable Biometrics and Biometric Encryption: A Discussion of Biometrics for Authentication Purposes. *Information and Privacy Commissioner Ontario, Canada*, August 2009.

22. Davida, G., Frankel, Y. and Matt, B. On enabling secure applications through off-line biometric identification. *Proceedings. 1998 IEEE Symposium on Security and Privacy, 1998.* 1998. 148 –157.

23. Dodis, Y., Ostrovsky, R., Reyzin, L. and Smith, A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *SIAM J. Comput.*, 2008. 38: 97–139. ISSN 0097-5397.

24. Soutar, C., Roberge, D., Stoianov, A., Gilroy, R. and Kumar, B. V. Biometric Encryption using Image Processing. *In Proc SPIE, Optical Security and Counterfeit Deterrence Techniques II. Vol. 3314*. 1998.

25. Monrose, F., Reiter, M. K., Li, Q. and Wetzel, S. Using Voice to Generate Cryptographic Keys. *In Proc. of Odyssey 2001, The Speaker Verification Workshop*. 2001. 237–242.

26. Juels, A. and Wattenberg, M. A Fuzzy Commitment Scheme. ACM Press. 1999. 28–36.

27. Clancy, T. C., Kiyavash, N. and Lin, D. J. Secure smartcardbased fingerprint authentication. *Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications*. New York, NY, USA: ACM. 2003, WBMA '03. ISBN 1-58113-779-6. 45–52.

28. Collins, C. R. and Stephenson, K. A Circle Packing Algorithm. *Computational Geometry: Theory and Applications*. 25: 233–256.

29. Zhang, H. and Hu, D. W. A Palm Vein Recognition System. *International Conference on Intelligent Computation Technology and Automation (ICICTA)*. 2010, vol. 1. 285–288.

30. Shrotri, A., Rethrekar, S. C., Patil, M. H. and Kore, S. N. IR-Webcam Imaging and Vascular Pattern Analysis Towards Hand Vein Authentication. *The 2nd International Conference on Computer and Automation Engineering*. Singapore. 2010, vol. 5. 876–880.

31. Wu, J. D. and Ye, S. H. Driver Identification Using Finger-Vein Patterns With Radon Transform and Neural Network. *Expert Systems with Applications*, 2009. 36(3, Part 2): 5793–5799.

32. Zhang, J. and Yang, J. F. Finger-Vein Image Enhancement Based on Combination of Gray-Level Grouping and Circular Gabor Filter. *International Conference on Information Engineering and Computer Science*. 2009. 1–4.

33. Zhang, Y., Han, X. and Ma, S. L. Feature Extraction of Hand-Vein Patterns Based on Ridgelet Transform and Local Interconnection Structure Neural Network. In: Huang, D.-S., Li, K. and Irwin, G., eds. *Intelligent Computing in Signal Processing and Pattern Recognition*. Springer Berlin / Heidelberg, *Lecture Notes in Control and Information Sciences*, vol. 345. 870–875. 2006.

34. Miura, N., Nagasaka, A. and Miyatake, T. Feature Extraction of Finger-Vein Patterns Based on Repeated Line Tracking and Its Application to Personal Identification. *Machine Vision and Applications*, 2004. 15(4): 194–203.

35. Li, X. Y., Guo, S. X., Gao, F. L. and Li, Y. Vein Pattern Recognitions by Moment Invariants. *International Conference on Bioinformatics and Biomedical Engineering*. Wuhan. 2007. 612.

36. Hoover, A., Kouznetsova, V. and Goldbaum, M. Locating Blood Vessels in Retinal Images by Piecewise Threshold Probing of a Matched Filter Response. *IEEE Transactions on Medical Imaging*, 2000. 19(3): 203 – 210.

37. Duarte, R., Neto, H. and Vestias, M. Double-precision Gauss-Jordan Algorithm with Partial Pivoting on FPGAs. *12th Euromicro Conference on Digital System Design, Architectures, Methods and Tools, 2009. DSD '09.* 2009. 273 –280.

38. De Matos, G. and Neto, H. On Reconfigurable Architectures for Efficient Matrix Inversion. *International Conference on Field Programmable Logic and Applications, 2006. FPL '06.* 2006. 1 –6.

39. Matos, D. *Reconfigurable systems for acceleration of matrix operation (in Portuguese)*. Master's Thesis. Technical University of Lisbon. March, 2006.

40. De Matos, G. and Neto, H. Memory Optimized Architecture for Efficient Gauss-Jordan Matrix Inversion. *3rd Southern Conference on Programmable Logic, 2007. SPL '07. 2007*. 2007. 33 –38.

41. Press, W., Flannery, B., Teukolsky, S. and Vetterling, W. *Numerical Recipes in C: The Art of Scientific Computing*. Cambridge University Press. 1992. ISBN 0521431085.

42. Wilkinson, J. *The Algebraic Eigenvalue Problem*. Oxford University Press. 1965.

43. Roslee Bin Mohd Sabri, M. K., Hani. *Register Transfer Level Design of Compression Processor Core Using Verilog Hardware Description Language*. Master's Thesis. Universiti Teknologi Malaysia. 2007.

44. Sagdeo, V. *The Complete Verilog Handbook*. Kluwer Academic Publisher. 1998.

45. Altera Corporation. *Introduction to Quartus II*, 2003a.

46. Altera Corporation. *SOPC Builder Data Sheet*, 2003b.

47. Online CRC Calculation, 2011. URL `http://zorc.breitbandkatze.de/crc.html`.