IEICE Electronics Express, Vol.7, No.13, 899–905

VLSI implementation of the fuzzy fingerprint vault system

Sung Jim Lim[1], **Seung-Hoon Chae**[1], **and Sung Bum Pan**[1,2a)]

[1] *Dept. of Information and Communication Engineering, Chosun Univ., 375, Seosuk-dong Dong-gu, Gwangju, 501–759, Korea*

[2] *Dept. of Control, Instrumentation, and Robot Engineering, Chosun Univ., 375, Seosuk-dong Dong-gu, Gwangju, 501–759, Korea*

a) *sbpan@chosun.ac.kr*

Abstract: Biometrics-based user authentication has several advantages over traditional password-based systems for standalone authentication applications. The fingerprint is evaluated as the most realistic alternative up to the present time in the perspectives of availability, accuracy and economy. However, serious problems may cause if fingerprint information stored for user authentication is used illegally by a different person since it cannot be changed freely as a password due to a limited number of fingers. Recently, research in fuzzy fingerprint vault system has been carried out actively to safely protect fingerprint information in a fingerprint authentication system. In this paper, we propose the FPGA-based fuzzy fingerprint vault system for real-time processing. Based on the experimental results, we confirmed that the proposed system takes 0.53 second with 36 real minutiae and 400 chaff minutiae.

Keywords: biometrics, fingerprint verification, fuzzy fingerprint vault

Classification: Integrated circuits

References

[1] K. Nandakumar, A. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 4, pp. 744–757, 2007.

[2] A. Juels and M. Sudan, "A fuzzy vault scheme," *Proc. IEEE Int. Symp. Inf. Theory*, p. 408, 2002.

[3] U. Uludag, S. Pankanti, and A. Jain, "Fuzzy vault for fingerprints," *LNCS 3546*, pp. 310–319, 2005.

[4] Y. Chung, D. Moon, S. Lee, S. Jung, T. Kim, and D. Ahn, "Automatic alignment of fingerprint features for fuzzy fingerprint vault," *LNCS 3822*, pp. 358–369, 2006.

[5] S. Lee, D. Moon, S. Jung, and Y. Chung, "Protecting secret keys with fuzzy fingerprint vault based on a 3D geometric hash table," *LNCS 4432*, pp. 432–439, 2007.

[6] D. Moon, S. Lee, and Y. Chung, "Configurable fuzzy fingerprint vault for match-on-card system," *IEICE Electron. Express*, vol. 6, no. 14, pp. 993–999, 2009.

DOI: 10.1587/elex.7.899
Received April 06, 2010
Accepted June 08, 2010
Published July 10, 2010

[7] H. Wolfson and I. Rigoutsos, "Geometric hashing: An overview," *IEEE Comput. Sci. Eng.*, vol. 4, pp. 10–21, 1997.
[8] S. Lim, S. Chae, D. Moon, Y. Chung, N. Lee, and S. Pan, "VLSI architecture for the fuzzy fingerprint vault with automatic alignment module," *Proc. Int. Conf. FGCN*, pp. 470–476, 2009.
[9] D. Ahn, et al., "Specification of ETRI fingerprint database (in Korean)," *Technical Report-ETRI*, 2002.

1 Introduction

Fingerprint authentication is evaluated as the most realistic alternative up to the present time in the perspectives of availability, accuracy and economy. There are several problems in the user authentication system of using fingerprint. First, it has a disadvantage that the fingerprint information obtained by the identical finger of the same person is not exactly matched though it is similar for every time. Also since the fingers of human are highly limited, it is difficult to change them at the time of exposure and has the problem that the exposed fingerprint information can be reused. Accordingly, the studies for protecting the biometric data safely from illegal acquisition and falsification/alteration are needed [1].

While Juels and Sudan were proposing the fuzzy vault scheme, they have conducted a study on the fuzzy fingerprint vault that can be applied on the fingerprint recognition. The fuzzy fingerprint vault is an cryptographic method that allows only the justified user to have the secret key by combining the fingerprint information with the secret key of user. The fuzzy fingerprint vault system generates a polynomial by using the secret key of user and protects the fingerprint minutiae of user by constructing a fingerprint template together with the real fingerprint minutiae of user after generating the chaff minutiae randomly.

Although a few studies have been reported to protect the secret key of user as well as the fingerprint information of user while using the fuzzy fingerprint vault, they have a problem that cannot be practically used since they have omitted the alignment process due to the absence of fingerprint reference point [2, 3]. In order to solve this fingerprint alignment problem, the method to apply a geometric hashing technique to the fuzzy fingerprint vault system has been proposed [4, 5, 6]. The geometric hashing technique is the algorithm that searches and saves the information of transformed object to a database by extracting the information of the object through an object recognition algorithm and by performing the geometric transformation [7].

This paper proposes hardware architecture of the fuzzy fingerprint vault system based on the geometric hashing. The proposed architecture performs the system by integrating the software and hardware modules. The software module consists of the modules such as for fingerprint minutiae extraction, fingerprint template generation, fingerprint hash table generation, and database saving. The hardware module consists of the matching module,

DOI: 10.1587/elex.7.899
Received April 06, 2010
Accepted June 08, 2010
Published July 10, 2010

verification module, each memory of enrollment hash table and verification hash table. The matching module compares the transformed minutiae of enrollment hash table with the transformed minutiae of verification hash table. The verification module takes the role of similarity calculation according to the result of matching module. Based on the experimental result, we confirmed that it takes 0.24 second in 200 chaff minutiae and 0.53 second in 400 chaff minutiae when real minutiae are 36.

The organization of the paper is as follows. The Section 2 explains the proposed hardware architecture. The Section 3 describes the experimental result and the Section 4 draws the conclusion of this paper.

2 Hardware architecture of the proposed fuzzy fingerprint vault

This section proposes the hardware architecture of fuzzy fingerprint vault system based on the geometric hashing, which protects the fingerprint template by using the fuzzy vault scheme and geometric hashing technique. The fuzzy fingerprint vault has the problem of fingerprint alignment. The fingerprint alignment is executed by using the structural information having each fingerprint minutiae. However, the fuzzy fingerprint vault system adds hundreds of chaff minutiae information to the fingerprint information. It is difficult to separate the fingerprint minutiae and added chaff minutiae from the fingerprint template. Accordingly, it has a difficulty in executing the alignment process because of inaccurate structural information can be used. Although the existing studies assume that they have executed the alignment process that is the middle stage of fingerprint authentication, it is not realistic since they have been aligned manually. Hence, it has the problem that cannot be implemented as an automated system. In order to solve this problem, Chung et al. have executed the alignment automatically by applying the geometric hashing technique [4, 5, 6]. The geometric hashing technique refers to the method that automatically aligns the fingerprint information by selecting the real minutiae and chaff minutiae of user as the reference point.

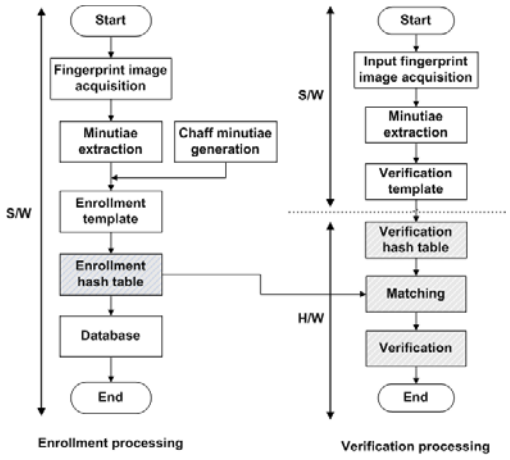
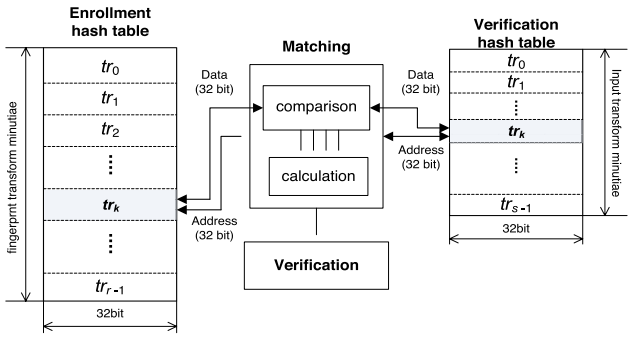


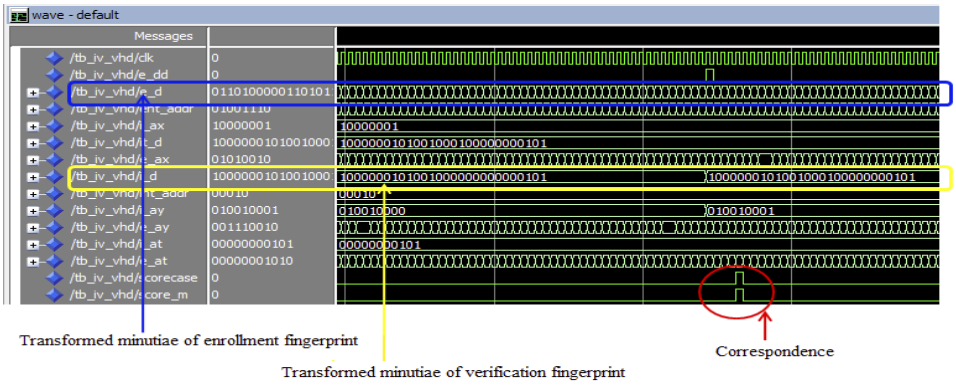
Fig. 1. Integrated implementation of fuzzy fingerprint vault system

DOI: 10.1587/elex.7.899
Received April 06, 2010
Accepted June 08, 2010
Published July 10, 2010

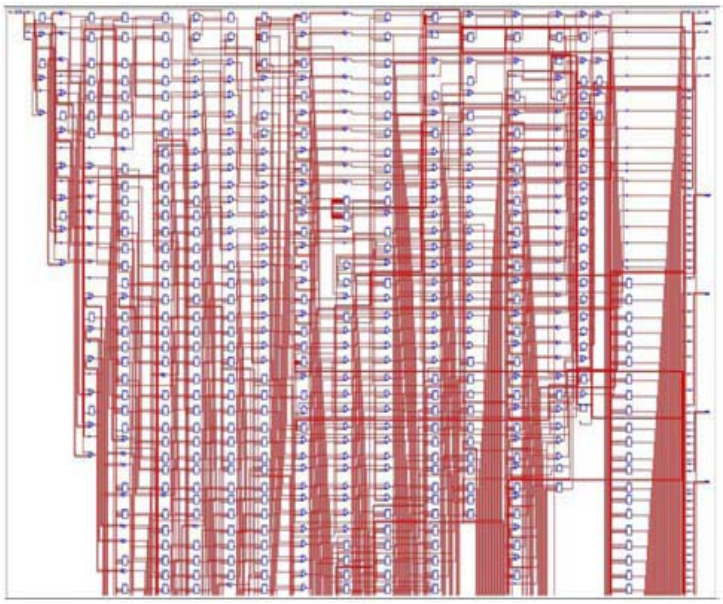
In order to implement the hardware system of fuzzy fingerprint vault, the proposed architecture was performed by integrating the software and hardware modules as shown in Fig. 1. The enrollment phase of fuzzy fingerprint vault system consists of the stages such as fingerprint minutiae extraction, chaff minutiae generation, fingerprint template generation, fingerprint hash table creation, and fingerprint database saving. The verification phase con-



(a) Proposed hardware architecture



(b) Simulation result of the proposed hardware module



(c) Synthesis result of the proposed hardware module

Fig. 2. Proposed hardware architecture and simulation result

DOI: 10.1587/elex.7.899
Received April 06, 2010
Accepted June 08, 2010
Published July 10, 2010

sists of the stages such as minutiae extraction from the input of fingerprint, fingerprint hash table creation, matching, and verification [8]. The matching and verification stage in the verification phase are implemented into the hardware. As for the matching stage and verification stage in the enrollment phase, it is desirable to implement them into the hardware since the amount of calculation in the matching stage of verification phase gets large as the number of chaff minutiae increases. On the other hand, the fingerprint input hash table creation stage of enrollment process and verification phase is implemented into the software.

As shown in Fig. 2 (a), the proposed hardware module consists of the respective memories for saving the enrollment hash table and verification hash table, matching module, and authentication module. Each hash table consists of the transformation minutiae. The enrollment transformation minutiae are the minutiae that the chaff minutiae inserted to protect the fingerprint minutiae of user in the enrollment phase are generated through the geometric transformation. The verification transformation minutiae are the minutiae that the fingerprint minutiae for verification are created through the geometric transformation. The transformation minutiae consist of a total of 32 bits from 11 bits each for the x-axis and y-axis, 9 bits for the angle, and 1 bit for the type. The enrollment transformation minutiae is expressed as $E = \{tr_i | 0 \leq i \leq r-1\}$ where r refers to the number of enrollment templates. tr_i, as the hash table created through the geometric hashing, is selected based on the of fingerprint templates and is consisted of $r-1$ transformation minutiae. The verification transformation minutiae is expressed as $V = \{tr_j | 0 \leq j \leq s-1\}$ where s refers to the number of verification templates.

Note that the memory size for saving the hash table is $p(r \times (r-1))$ for the number of each enrollment transformation minutiae and $q(s \times (s-1))$ for the number of verification transformation minutiae. The architectures of matching module and verification module are as shown in Fig. 2 (a). The matching module consists of the compare module and count module. The compare module compares the enrollment transformation minutiae and verification transformation minutiae and the count module calculates the number of matched transformation minutiae. The verification module refers to the module that aligns the calculated similarity in the order of higher similarity. The verification module performs the alignment of calculated similarity. By using the number of obtained and matched transformation minutiae, measure the similarity and generate the candidate list in the order of higher similarity.

3 Experimental results

The number of fingerprint minutiae, which was used in the hardware architecture experiment of the fuzzy fingerprint vault system based on the geometric hashing proposed in this paper, is a maximum of 90 minutiae and minimum of 16 minutiae. As for the number of chaff minutiae, this paper has performed the experiment by adding 100, 200, 300, and 400 respectively. For

DOI: 10.1587/elex.7.899
Received April 06, 2010
Accepted June 08, 2010
Published July 10, 2010

the purpose of evaluating the proposed approach, a data set of 100 fingerprint images composed of four fingerprint images per one finger was collected from 100 individuals by using the optical fingerprint sensor [9].

The hardware module was performed by using the development board of Spartan 3E Starter Board. The development board is built with Xilinx XC3S500E FPGA. The hardware module was designed by using the VHDL language from the environment of Xilinx ISE 9.2. The hardware simulation was tested from the Moledmsim XE 6.0. Fig. 2 (b) shows the matching module simulation result of the hardware architecture proposed in the fuzzy fingerprint vault system. The experiment was performed by adding 36 fingerprint minutiae and 200 chaff minutiae. The verification fingerprint minutiae were 34 units. The matching of proposed hardware architecture compares the verification hash transformation minutiae and enrollment hash transformation minutiae. This judges the matching status between two transformation minutiae, measures the number of units, and gets the similarity. The simulation result of the proposed architecture was the same as software developed by Lee et al [5]. Therefore, it was confirmed that the security of the proposed hardware architecture is the same as the algorithm developed by Lee. Et al [5]. Also, Fig. 2 (c) shows the circuit synthesis result of proposed hardware structure.

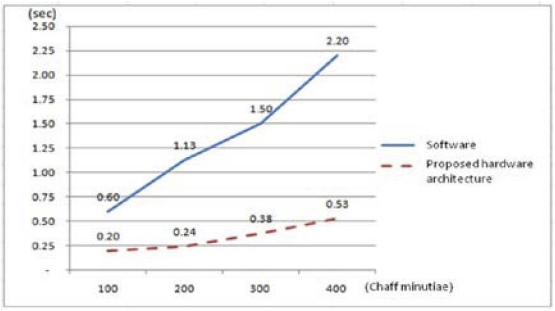


Fig. 3. Required execution time in the matching according to the number of chaff minutiae

The execution time in the hardware module of fuzzy fingerprint vault system was measured by varying the number of chaff minutiae as 100, 200, 300, and 400. The numbers of chaff minutiae, execution time, and security have a correlation. The execution time is extended with more chaff minutiae but the security is enhanced. Fig. 3 represents the required execution time of the proposed matching hardware module. As for the proposed hardware architecture, we confirmed that the real-time processing is possible even after increasing the number of chaff minutiae for the security improvement.

4 Conclusion

Recently for the protection of fingerprint templates, the studies on the fuzzy fingerprint vault using the fuzzy vault scheme have been conducted. This paper proposes hardware architecture of the fuzzy fingerprint vault system

DOI: 10.1587/elex.7.899
Received April 06, 2010
Accepted June 08, 2010
Published July 10, 2010

based on the geometric hashing. The proposed hardware architecture was implemented by matching all the transformation minutiae of enrollment hash table for every transformation minutiae of verification hash table. The execution time of proposed hardware architecture was 0.24 second when 36 fingerprint minutiae and 200 chaff minutiae and 0.53 second when 400 chaff minutiae. Based on the experimental result, we confirmed that the real-time fingerprint authentication is possible by using the hardware architecture of proposed fuzzy fingerprint vault system. In the future, we plan to study on how to reconstruct the polynomial of fuzzy fingerprint vault and how to implement this onto hardware.

Acknowledgments

This study was supported by research funds from Chosun University, 2007.

DOI: 10.1587/elex.7.899
Received April 06, 2010
Accepted June 08, 2010
Published July 10, 2010