Research Article

Security Enhancement for Smartphone Using Biometrics in Cyber-Physical Systems

Seung-Hoon Chae,1 Daesung Moon,2 Kyeong-Ri Ko,3 JuHyun Shin,4 and Sung Bum Pan4

1 The Research Institute of IT, Chosun University, 309 Pilmun-daero, Dong-gu, Gwangju 501-759, Republic of Korea
2 Electronics and Telecommunications Research Institute, 161 Gajeong-dong, Yuseong-gu, Daejeon 305-350, Republic of Korea
3 Department of Control and Instrumentation Engineering, Chosun University, 309 Pilmun-daero, Dong-gu, Gwangju 501-759, Republic of Korea
4 Department of Control, Instrumentation, and Robot Engineering, Chosun University, 309 Pilmun-daero, Dong-gu, Gwangju 501-759, Republic of Korea

Correspondence should be addressed to Sung Bum Pan; sbpan@chosun.ac.kr

Received 6 December 2013; Accepted 11 March 2014; Published 3 April 2014

Academic Editor: Hoon Ko

With the expansion of the Cyber-Physical System (CPS) concept, smartphones have come to constitute a competitive platform that connects humans and the surrounding physical world. Along with the communication functions and mobility of cellular phones, smartphones have various sensors in addition to greatly enhanced performances and storage space compared with existing cellular phones. However the “unlock” process of smartphones and the need for user passwords when accessing SNSs prove to be great weaknesses in smartphone security. Therefore, smartphone security should be enhanced through biometrics, which can make up for the shortcomings of passwords. The present study proposes minutiae-ridge based fingerprint verification for enhancing the security of fingerprint verification, a biometrics, to improve smartphone security. To evaluate the proposed minutiae-ridge based fingerprint verification performance in smartphones, its performance was compared with existing fingerprint verification methods in terms of Equal Error Rate (EER), False Non-Match Rate (FNMR), and required number of cycles. The results show that although the required number of cycles increased by 1.5% with the proposed method, EER and FNMR improved by 53% and 92%, respectively.

1. Introduction

Given the increased importance of the relationship of physical systems existing in real space with cyber space, or software running on computers, the existing concept of embedded systems has been expanded to Cyber-Physical Systems (CPS). Various embedded devices compute based on the observed status of the physical system. And then, A CPS forms a feedback system which influences the physical system itself. In other words, it is an integrated system that observes, adjusts, and controls a physical system’s actions. As shown in Figure 1, the CPS concept covers a broad range of artificial intelligence systems such as road traffic control, social system, and real-time information sharing [1–3].

Smartphones equipped with various sensors have recently witnessed widespread adoption. They can be considered a field where mobile CPS has been applied. The performance of mobile devices such as smartphones is improving rapidly. Along with information processing capabilities, various sensor modules such as mobile communication such as camera, accelerometer, and gravity sensor, as well as hardware capabilities such as storage space, 2nd, 3rd, and 4th generation mobile communication, WiFi, Global Positioning System (GPS), and Bluetooth enable mobile CPS through mobile devices. Unlike traditional embedded systems, which generally are immobile given the high cost of mobility, smartphone users can carry a mobile conveniently and acquire information about their surroundings using various sensors. In addition, smartphones users react to the physical world through the smartphone regardless of time or space. Hence, smartphones are used as a convenient, competitive platform between humans and the surrounding physical world.
Social Networking Services (SNS) users share their thoughts, meditations, status, and cultures. Given that users can share information through SNS using a smartphone and regardless of time and space, online SNS usage through smartphones is increasing rapidly. Moreover, many SNS companies have been announcing smartphone mobile applications that allow quick and easy access to various SNSs [4].

The greatest strength of a SNS is that it allows communication with numerous other SNS users through chatting, messaging, file sharing, wikis, e-mails, voice mails, and videos. When communicating through SNS, in most cases, users only recognize others through their SNS IDs and not by their physical forms. Hence, one can impersonate another by cracking that person’s account information and logging into a SNS using that information or by creating and operating an alternative SNS account in that person’s name. Recently, such incidents have actually been occurring in SNSs. Most SNSs perform personal verification with a user ID and a password, both of which are easy to steal. Furthermore, when using smartphones for accessing SNSs, the respective IDs and passwords are stored in the system for automatic login. The automatic login feature ensures that users are not required to type their ID and password at each log in, as well as to avoid any inconvenience due to forgotten passwords. Furthermore, given that smartphones contain sensitive personal information such as Internet banking information or pictures, losing a smartphone could lead to privacy problems. As communication channels can be protected using protocols such as HTTPS, SSL, and TLS, the weakest point in controlling user access to web services such as SNSs is the human authentication, such as typing a password [5–7]. In the light of these issues, the password-based user authentication currently used in smartphones, as well as the security of the password-typing process, requires improvements. Recognizing this need, of late, smartphone manufacturers have been implementing biometric features such as fingerprint or facial verification, such as the examples shown in Figure 2, in smartphones. Biometrics can replace not only smartphone security itself but also the ID- and password-based login methods used currently.

The present paper proposes a minutiae-ridge based fingerprint verification scheme that improves upon fingerprint verification, a biometrics, for enhancing smartphone protection. The proposed minutiae-ridge based fingerprint verification scheme uses fingerprint ridge information for improving the performance of existing fingerprint verification systems. For effectively combining the minutiae-based fingerprint verification with ridge-based fingerprint verification, similarity distribution of the former scheme was used. Minutiae-based fingerprint verification employs the threshold values of the similarity of minutiae for verification. However, more errors are detected in the region around the threshold values than in the other regions. Therefore, the use of ridge-based fingerprint verification in the region around the threshold values, where many errors occur, verification performance can be improved. In addition, for verifying the real-time feasibility of the proposed method on a smartphone, the size of the ridge data was measured in the minutiae standard format by executing a performance cycle. Consequently, the total data size increased to 1,961 bytes, but it was confirmed that this could be saved in the extended partition of the minutiae standard fingerprint format file. The number of processing cycles increased by 1.5% from $5.22 \times 10^{11}$ cycles with minutiae to $5.30 \times 10^{11}$ cycles with the minutiae-ridge-based method.

The thesis is composed of the following. First, the method of strengthening smartphone security using fingerprint verification is explained. Then, Section 3 introduces the proposed fingerprint verification method to be applied to smartphones, and Section 4 shows the experiment results. Finally, Section 5 concludes the thesis.

2. Smartphone Security Intensification Using Fingerprint Verification

More services are being provided to customers thanks to the development of computer and communication technologies, which do not impose any time or location-based limits on service delivery. Given that the importance of smartphone use is increasing in real life owing to services such as SNS and Internet banking, faceless verification services are gaining importance. Currently, verification systems such as password or Personal Identification Number (PIN) are mainly used. However, these methods have problems such as users forgetting key information and easy misuse by others of data exposed externally. Several studies have focused on various solutions solving such problems. Among those solutions, biometrics has drawn much attention as an appropriate means for solving such problems as well as enhancing security [8, 9].

For strengthening smartphone security through fingerprint verification, smartphones’ “unlock” process needs to be strengthened. Smartphones are generally unlocked using passwords and patterns. When typing passwords or drawing patterns, however, they can be easily spied on or deduced. In contrast, fingerprint-based verification is safer because
even if someone tries to spy on the fingerprint input process, fingerprint information cannot be leaked or deduced. Moreover, because the user simply has to touch the fingerprint sensor, the inconvenience resulted from the typing password when using SNSs is avoided. Even smartphone manufacturers are implementing fingerprint sensors in their products or developing fingerprint sensors for smartphones for improving smartphone security. Hence, the security of the password input process, which is the weakest link in controlling user access to smartphones or SNSs, can be improved by using fingerprint verification, as shown in Figure 3. Moreover, this method can be used not only for smartphone unlocking and access but also for user verification in various smartphone applications.

3. Proposed Fingerprint Verification System

The minutiae-based fingerprint verification method is the most commonly used fingerprint verification method. Given that this method is very effective for comparing fingerprints and the required data size is small, a verification system based on it can be miniaturized and would be good for real-time processing. This is also the reason for the method’s widespread use. However, the minutiae-based fingerprint verification method is plagued by low performance in regions where preregistered and current input fingerprints overlap or when the input fingerprint image is small and the minutiae extracted are insufficient for verification. These problems lead to the occurrence of faulty matching, thus rejecting authorized persons. To avoid faulty matching and improve verification performance, many researchers have investigated the preprocessing of fingerprint images for improving fingerprint verification performance, enhancement of the registered templates’ quality, adoption of fingerprint matching methods that can use the extracted templates effectively, and template protection for preventing leaks of registered templates. Many studies on methods for overcoming the problems associated with the fingerprint matching method using direction filters (instead of minutiae), phase information, and fingerprint images have been carried out [10–15].

In this study, experiments were conducted for improving fingerprint verification performance using fingerprint ridges. In addition, the integration of minutiae and ridge-based fingerprint verification using the partial band is proposed for efficient use of the proposed fingerprint verification scheme in smartphones.

3.1. Minutiae-Ridge Based Fingerprint Verification Algorithm.

Among the various fingerprint verification methods, the minutiae-based fingerprint verification method offers excellent security and convenience. Additionally, because the method required small-sized data and a small fingerprint sensor, a system based on it can be miniaturized easily. However, there is the problem of faulty matching due to fingerprint sensor miniaturization. The method’s performance of the method can be improved by creating high quality minutiae but only up to a certain extent. In this study, the performance was verifiably improved by using ridge information from fingerprints. Because fingerprint data is not aligned, a process for aligning the data of two fingerprints is required. Methods for aligning fingerprint images include ridge-based methods and minutiae-based methods that use the cores or deltas of two fingerprints [16, 17]. However, because image-based methods require a lot of calculation and there are cases when there are no minutiae such as core or deltas in the input images, their use is limited. Therefore, the image-based fingerprint data alignment process is less efficient than the minutiae-based method.

The ridge-based fingerprint verification method used in this paper takes more time than the minutiae-based system. If the ridge information is calibrated using the compensation process of minutiae-based fingerprint matching, the analysis time required for ridge-based fingerprint matching can be reduced. Furthermore, the performance of the minutiae-based fingerprint verification is superior when there is high similarity of minutiae, but verification errors occur around threshold values with low similarity. The area around the threshold values is called the partial band. This paper proposes a hybrid fingerprint verification system that does not use ridge-based verification in areas with high confidence but
uses it for fingerprints with minutiae similarity in the partial band area. Therefore, ridge-based fingerprint matching was conducted using minutiae-based similarity and compensation information. Figure 4 shows the proposed minutiae-ridge based fingerprint verification system proposed in this paper.

This system determines whether to perform ridge-based fingerprint matching after conducting minutiae-based fingerprint matching. For minimizing the computational burden due to the execution of ridge-based fingerprint matching, ridge-based fingerprint matching is used in a limited manner, as determined by the partial band. If there is minutiae similarity within the partial band, which requires ridge-based verification, then ridge-based verification is performed and the result is used for verification. However, if there is minutiae similarity in areas except the partial band, where the results of minutiae-based fingerprint verification are reliable, only minutiae-based verification is used for verification. When performing ridge-based fingerprint matching, the compensation stage uses compensation information from the minutiae-based fingerprint matching results. By combining minutiae-based matching, which lacks verification information and faces difficulties in the compensation stage, with ridge-based fingerprint matching, a fingerprint verification system that delivers improved performance in real-time is realized. In Sections 3.2 and 3.3, the ridge-based fingerprint matching scheme and the partial band are described.

3.2. Ridge-Based Fingerprint Matching Method. Ridges are basic elements of fingerprints, and their minutiae such as bifurcation points and ending points are decided according to the bifurcations of ridges and their ending forms. Thus, ridges are components containing fingerprint verification data. The ridge images used in this study were thinned through preprocessing for easier selection. The fingerprint ridge images obtained via thinning have a thickness of 1 pixel.

The thinned ridge images can effectively and simply express fingerprint images. Therefore, the capacity requirement of the template fingerprint images can be reduced. In addition, the minutiae are distributed randomly. However, because the ridges are distributed evenly and contain data of entire fingerprints, much of the data that can be obtained from the overlapped area of two fingerprint images is small. This paper uses data on the distance between two ridges for comparison. It can reduce errors in cases where two fingerprints cannot be fully matched or where fingerprints are distorted, as in Figure 5, as distance is used.

The ridge-based matching method used in this paper consists of three stages: stage of generating comparing points, compensation stage, and distance calculation stage between compared points. The ridge image used in the matching step is a thinned fingerprint image. The stage of generating comparing points is where comparing points are generated at regular intervals on a ridge by tracking the ridges in said image. The advantage of doing so is that it reduces the difference between the computed and measured distance by inputting all coordinates of the ridge into the comparing points. The experiment in this paper generated comparing points at intervals of 10 pixels.

In the compensation stage, the distance between the comparing points of registered fingerprints and input fingerprints is measured. The comparing points of two fingerprints are placed in the same topological space and the distance between the comparing points is measured. Similarity between two ridges is obtained by using the distances between pairs of comparison points on each ridge. The mean distance of a pair of comparison ridges, standard deviation, and the number of pairs of comparison points are obtained.
based on the distance value calculated. The data obtained by measuring the distance between ridges and the numbers of pairs of whole corresponding ridges existing in the two fingerprint images are used for verification:

$$S_R = \frac{\sum_{n=0}^{N-1} R(n)}{R_{MAX}} \times 100.$$  \hspace{1cm} (1)

$S_R$, or similarity between the two fingerprints, is calculated according to (1). $R(n)$ is the score of pairs of the nth corresponding ridges of $N$ ridges, and $R_{MAX}$ is the maximum number of comparison points. The ridge pairs’ score approaches 1 as the standard deviation of mean distance decreases and approaches 0 because the mean distance has a higher standard deviation. Additionally, because confidence is low when the number of comparison ridges is less than 10, a low weight is assigned.

Figure 6 presents the Receiver Operating Characteristics (ROC) of ridge- and minutiae-based fingerprint verification. As shown in Figure 3, we confirmed that ridges can be used for fingerprint verification. The Zero False-Match Rate (ZeroFMR) of the ridge-based verification method was lower than that of minutiae-based verification.

3.3. Partial Band Setting. Ridge-based fingerprint matching requires more computation than minutiae-based fingerprint matching. Thus, it is necessary to limit its use during fingerprint matching using the partial band. This partial band is determined through fingerprint minutiae similarity distribution. If there is minutiae similarity within the partial band, which requires ridge-based verification, then ridge-based verification is performed and the result is used for verification. However, if there are minutiae similarities in areas other than the partial band, where the results of minutiae-based fingerprint verification are reliable, only minutiae-based verification is used. Therefore, the partial band has a significant influence on fingerprint verification performance. Figure 4 presents the similarity distribution of the minutiae-based fingerprint verification system.
Errors of the minutiae-based fingerprint verification method are distributed centering on the threshold value, as shown in Figure 7. These errors occur when genuine users’ fingerprint similarities are below the threshold value and when impostors’ fingerprint similarities are above the threshold value. They are called false nonmatch and false-match, respectively. This study used the partial bands between similarity $\alpha$, where false nonmatch is 0, and similarity $\beta$, where false-match is 0, as the maximum bands, as shown in Figure 4. $S_i$ and $S_g$ have similar values in between $th$ and $\alpha$, and $th$ and $\beta$, and similar ranges of the partial band. Because impostors’ and genuine users’ similarity distributions are similar around the threshold value within the partial band, that is where most errors occur. If ridge-based fingerprint verification with excellent false-match resistance can be performed, verification performance can be improved.

Because ridge-based fingerprint verification uses a considerably large amount of comparison data, false-match errors can be reduced. However, its Equal Error Rate (EER) performance is lower than that of the minutiae-based verification method because rejection errors occur owing to the distortion of fingerprint images. When ridge-based verification is conducted within the partial band of the threshold value where minutiae similarity exists, the distribution is similar; that is, the gain from decreased false-match errors is bigger than the loss from rejection errors.

### 4. Experimental Results

This paper conducted a test using a DB of Set A fingerprints of FVC 2002 [18]. Tests of genuine users and impostors were conducted 2,800 and 4,950 times, respectively. For the partial band of the minutiae for in ridge-based fingerprint verification, similarity distribution was used. The minutiae similarity partial band with $P$ distribution was selected according to (2):

$$P = \frac{I(th, si) + G(th, si)}{I(th, \alpha) + G(th, \alpha)} \times 100$$

$$I(th, \beta) + G(th, \beta) \times 100,$$

$$0 \leq th \leq 100.0,$$

$$si = th, th - 1.0, th - 2.0, \ldots, \alpha,$$

$$sg = th, th + 1.0, th + 2.0, \ldots, \beta,$$

$I(i, j)$: Number of impostor fingerprints in similarities $i$ and $j$.

$G(i, j)$: Number of genuine fingerprints in similarities $i$ and $j$.

The compensation values used for ridge-based fingerprint verification in the experiment were from the top three candidates with the highest similarities among the compensation values of minutiae-based fingerprint matching. The number of ridges used for comparison in one fingerprint image and the average number of comparison points extracted per ridge were 37 and 13, respectively. That is, this study tested fingerprint verification performance after finding similarity values below and above the threshold with the number of fingerprints of proportion $P$ based on the threshold value.

Table 1 summarizes fingerprint verification performance based on $P$. The verification results were obtained in the partial bands between 0% and 100% of $P$, and performance was confirmed. Table 1 lists the results of the test using only the minutiae-based verification system when the $P$ of the partial band was 0. To confirm the improvement in and reduction of false-match errors, the FNMR was fixed and the changes in the FMR were tested. For evaluating verification performance, EER was measured. As a result, when the FNMR was fixed,
at 3.25%, its FMR performance was better than that with the minutiae-based verification method. In particular, it was confirmed that it improved from 2.77% to 0.22% when 50% of the partial band was used. Furthermore, the EER of the proposed method was improved from 3.01% to 1.4%. Through the test results, it was confirmed that the proposed verification system improved the FMR and verification performance.

Regarding the standard format of finger minutiae specified by ISO/IEC, the structures of minutiae data and extended data are shown in Figure 8 [19]. In this paper, data structuring, as shown in Figure 9, was used for applying the ridge data to the standard format.

Using the data structures shown in Figures 8 and 9, the average data sizes of FVC 2002DB used in this study for minutiae and ridges were calculated, and the cycles for performing fingerprint verification were measured. The results are listed in Table 2.

**Table 2: Hardware capacity by matching method.**

| Methods         | Average cycles | Average data size |
|-----------------|----------------|-------------------|
| Minutiae-based  | 66,074 cycles  | 192 bytes         |
| Ridge-based     | 873,113 cycles | 1,961 bytes       |

The average number of minutiae extracted from the fingerprints used in the experiment was 32. To determine the average data size of the minutiae based on Figure 8(a), a total of 192 bytes, which is 32 (number of minutiae) × 6 (data size per minutiae) is used. In this paper, 37 ridges were extracted for one fingerprint, and then 13 comparison points were extracted per ridge. If the ridge data is stored in the same way as in Figure 9, its size would be 1,961 bytes. Therefore, the data size of ridge information is approximately 10 times the data size of minutiae. The size of extended data, which is supported in the standard format, as shown in Figure 8(b), is 65,531 bytes. Therefore, the average 1,961 bytes of ridge data can be saved in a standard fingerprint format file. In addition, when performing fingerprint matching, several compensation values are used. Therefore, the number of average cycles of minutiae-based fingerprint matching used in this experiment to match one fingerprint is 67,423,757. Because the top compensation values used in minutiae similarity are used for ridge-based fingerprint matching, approximately 2,619,341 additional cycles are needed. In other words, if ridge-based fingerprint matching is used in the fingerprint verification system proposed in this paper, the required cycles will be 3.8% higher than the cycles needed in minutiae-based fingerprint matching. Therefore, the method proposed in this
paper can enhance fingerprint verification performance and perform verification in real-time.

Table 3 lists the number of cycles generated in the process of performance measurement in Table 1. For 2,800 genuine user attempts and 4,950 impostor attempts, the total number of cycles of minutiae-based fingerprint matching is $5.22 \times 10^{11}$. However, in the method proposed in this paper, if the partial band is set as 50%, the number of cycles increases to $5.30 \times 10^{11}$. This is a 1.5% increase compared with the case of minutiae-based fingerprint matching. Based on this result, if the method proposed in this paper is used, it is confirmed that although the computation burden increases by 1.5%, the verification performance is improved by 53%. Additionally, ridge information can be stored by using the extended partition of existing minutiae standard data format, and then verification can be performed.

5. Conclusions

Lately, the utilities of smartphones are greatly increased. The use of SNSs, which are used for sharing personal information and status through web services, is increasing in conjunction with the spread of high-performance smartphones. SNSs are fundamentally changing not only personal life patterns but also modern political, economic, and social environments. SNSs can replace conventional media that cannot perform its role properly by the control in countries. Elsewhere, they act as alternative media outlets. Hence, SNS security is very important. When accessing SNSs, especially, through smartphones, password information can be leaked during the user login process or SNSs can be hacked if one loses their smartphone. The present study proposed using fingerprint verification for improving security of smartphones as well as that of the SNS login process. In addition, it proposed the use of fingerprint ridges for improving the security of existing fingerprint verification systems. Furthermore, the study proposed the use of minutiae- and ridge-based fingerprint verification using the partial band for effectively improving fingerprint verification performance within the limited environment of a smartphone. Experiments using the proposed fingerprint verification method showed that the FMR was reduced from 2.77% to 0.22%, or by 92%, and EER was improved by 53% over minutiae-based verification. In addition, for evaluating the computation load of the verification method, the number of cycles required for a pair of fingerprints and the number of cycles required for the entire fingerprint verification experiment were measured. As a result, the number of cycles in the proposed method increased by 3.8% and 1.5%, respectively, compared with the minutiae-based fingerprint matching. However, it was confirmed that the verification performance increased by 53%. In future, we will study the efficient storage of ridge data and its optimal use in small systems.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This study was supported by research fund from Chosun University, 2013.

References

[1] M. Conti, S. K. Das, C. Bisnikian et al., “Looking ahead in pervasive computing: challenges and opportunities in the era of cyberphysical convergence,” Pervasive and Mobile Computing, vol. 8, no. 1, pp. 2–21, 2012.
[2] S. Karnouskos, “Cyber-physical systems in the SmartGrid,” in Proceedings of the 9th IEEE International Conference on Industrial Informatics (INDIN ’11), pp. 20–23, July 2011.
[3] Q. Gao, “Biometric authentication in smart grid,” in Proceedings of the IEEE International Energy and Sustainability Conference (IESC ’12), pp. 1–5, March 2012.
[4] M. Salehan and A. Negahban, “Social networking on smartphones: when mobile phones become addictive,” Computers in Human Behavior, vol. 29, no. 6, pp. 2632–2639, 2013.
[5] P. Kaur and A. Singh, “User authentication in social networking sites using face recognition,” in Proceedings of the 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, pp. 773–778, December 2012.
[6] A. Sanzgiri, A. Nandugudi, S. Upadhyaya, and C. Qiao, “SESAME: smartphone enabled secure access to multiple entities,” in Proceedings of the International Conference on Computing, Networking and Communications (ICNC ’13), Internet Services and Applications Symposium, January 2013.
[7] N. Bruce, T. Kim, and H. J. Lee, “Improved security patch on secure communication among cell phones and sensor networks,” International Journal of Distributed Sensor Networks, vol. 2013, Article ID 348783, 8 pages, 2013.
[8] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer, 2003.
[9] S. Prabhakar and A. K. Jain, Automatic Fingerprint Recognition System, Springer, 2007.
[10] S. B. Pan, Y. H. Gil, D. Moon, Y. Chung, and C. H. Park, “A memory-efficient fingerprint verification algorithm using a multi-resolution accumulator array,” ETRI Journal, vol. 25, no. 3, pp. 179–186, 2003.
[11] K. Lee, K. R. Park, J. Jang, S. Lee, and J. Kim, “A study on multi-unit fingerprint verification,” in Audio- and Video-Based Biometric Person Authentication, vol. 3546 of Lecture Notes in Computer Science, pp. 141–150, Springer, 2005.
[12] X. Xie, F. Su, and A. Cai, “Ridge-based fingerprint recognition,” in Advances in Biometrics, vol. 3832 of Lecture Notes in Computer Science, pp. 273–279, Springer, 2005.
[13] K. Ito, A. Morita, T. Aoki, H. Nakajima, K. Kobayashi, and T. Higuchi, “A fingerprint recognition algorithm combining phase-based image matching and feature-based matching,” in Advances in Biometrics, vol. 3832 of Lecture Notes in Computer Science, pp. 316–325, Springer, 2005.

Table 3: Number of cycles required for testing.

| Method                  | Number of cycles |
|-------------------------|------------------|
| Minutiae-based          | $5.22 \times 10^{11}$ cycles |
| The proposed method ($P = 50$) | $5.30 \times 10^{11}$ cycles |
[14] S. Chae, J. K. Kim, S. B. Pan, D. Moon, and K. Moon, “Fingerprint matching system for contents protection,” in Proceedings of the 2007 Asia Pacific International Conference on Information Science and Technology, pp. 103–111, December 2007.

[15] Y. Gil, D. Ahn, C. Ryu, S. Pan, and Y. Chung, “User enrollment using multiple snapshots of fingerprint,” in Neural Information Processing, vol. 3316 of Lecture Notes in Computer Science, pp. 344–349, Springer, 2004.

[16] A. N. Marana and A. K. Jain, “Ridge-based fingerprint matching using hough transform,” in Proceedings of the 18th Brazilian Symposium on Computer Graphics and Image Processing (SIBGRAPI ’05), pp. 112–119, October 2005.

[17] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, “Filterbank-based fingerprint matching,” IEEE Transactions on Image Processing, vol. 9, no. 5, pp. 846–859, 2000.

[18] FVC, 2002 Database, http://bias.csr.unibo.it/fvc2002/databases.asp.

[19] ISO/IEC JTC1/SC37 IS, “Biometric data interchange formats part 2: finger minutiae data,” Tech. Rep. 19794-2, 2005.