

Enhancing Accuracy Performance of Fuzzy Vault Non-Random Chaff Point Generator for Mobile Payment Authentication

Annisa Istiqomah Arrahmah^{1,2,a}, Yudi Satria Gondokaryono^{1,b}, Kyung-Hyune Rhee^{*}

Abstract

Biometric authentication for account-based mobile payment continues to gain attention because of improvements on sensors that can collect biometric information. We propose an enhanced method for mobile payment security based on biometric authentication. In this mobile payment system, the communication between the user and the relying party is based on public key infrastructure. This method secures both the key and the biometric template in the user side using fuzzy vault biometric cryptosystems, which is based on non-random chaff point generator. In this paper, we consider an important process for the common fuzzy vault system, that is, the feature extraction method. We evaluate various feature extraction methods to enhance the accurate performance of the system.

Key Words: Mobile payment, Biometric cryptosystem, Fuzzy vault, Feature extraction.

I. INTRODUCTION

Authentication process is one of the security concerns in mobile payment account-based scenarios. Nowadays, biometric authentication is becoming a popular technique for authentication in mobile phones because of its simplicity and ease of execution [1]. Moreover, sensor improvements in mobile phones make it possible to easily collect biometric data, e.g. fingerprint scanners have already been embedded in mobile phones. Biometric authentication has more advantages over other forms of authentication. One of the advantages is that a unique identity is used which is hard to imitate.

The main concern of biometric authentication system is to secure the biometric templates of the user. Because the biometric features are immutable and limited, a compromise of biometric templates causes permanent loss of a subject's biometrics [2]. As a consequence, a robust security scheme is needed to protect the biometric templates. There are several methods for securing biometric templates [2, 3], one of them is biometric cryptosystems (BCs). BCs require a storage of biometric information to

retrieve or generate cryptographic keys, referred as helper data. These helper data are stored as an encrypted form and do not reveal significant information about the biometric templates and the cryptographic keys. BCs are more practical than other methods because most of the mobile payment systems use a cryptographic key for securing mobile payment transaction over open networks [4-7].

In this paper, a method to enhance biometric authentication security in account-based mobile payment systems over open networks using biometric cryptosystems based on fuzzy vault non-random chaff point generator is introduced. One of the important steps in fuzzy vault non-random chaff point generator is feature extraction. This paper evaluates some feature extraction methods to enhance the accuracy of the system. In Section 2, recent developments of fuzzy vault method are reviewed. In Section 3, fingerprint feature extraction as a preprocessing step in fuzzy vault is explained. The proposed method is explained in Section 4. Section 5 shows the experiment and result. Section 6 contains discussion, while future works and the conclusion are presented in Section 7.

Manuscript received July 05, 2016; Revised July 16, 2016; Accepted July 28, 2016. (ID No. JMIS-2016-0004)

Corresponding Author (*): Kyung-Hyune Rhee, Department of IT Convergence and Application Engineering, Pukyong National University, South Korea, +82 51-629-6245, khrhee@pknu.ac.kr

¹Department of Electrical Engineering, Institut Teknologi Bandung, Bandung, Indonesia.

²Department of IT Convergence and Application Engineering, Pukyong National University, Busan, South Korea, E-mail: ^aistiqomahannisa11@gmail.com, ^bygondokaryono@stei.itb.ac.id

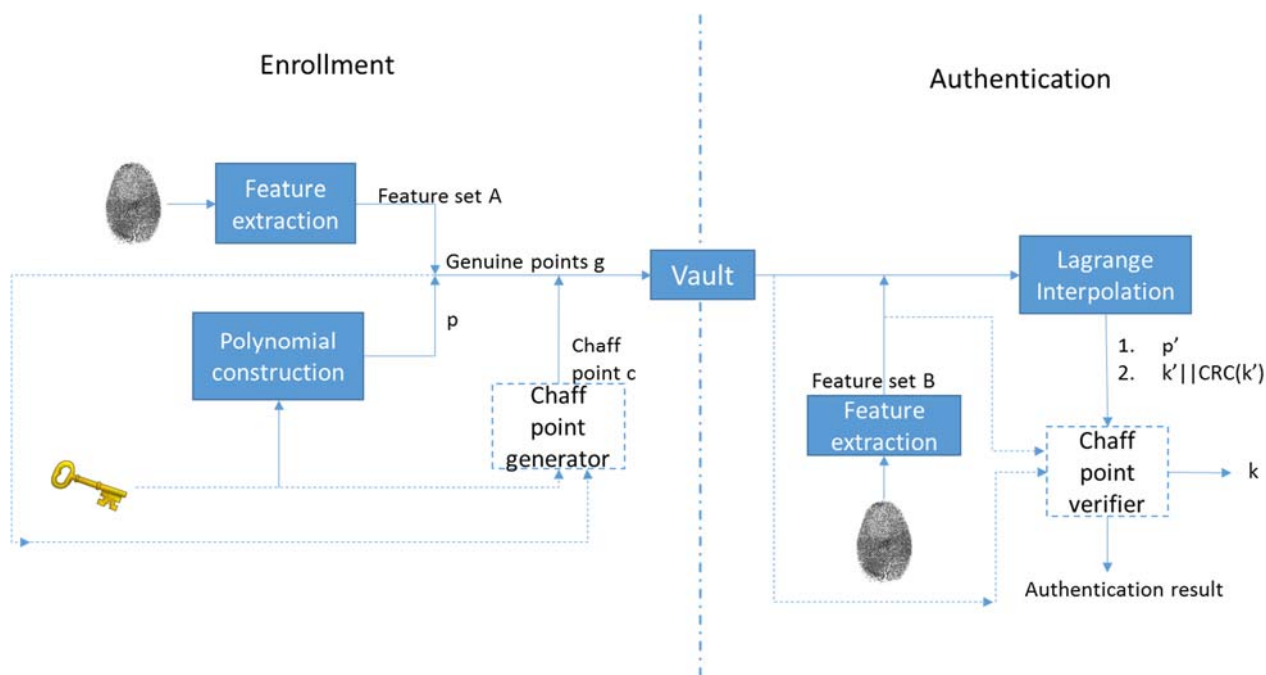


Fig. 1. CRC-based fuzzy vault using non-random chaff point generator [14].

II. LITERATURE REVIEW

Fuzzy vault is one of the biometric cryptosystems based on key binding schemes that were introduced by Juels and Sudan in 2002 [8]. Since then, various developments of fuzzy vault have been proposed. The original scheme uses the Reed-Solomon code for error-correcting code that can handle noisy data and is designed for an unordered set of data. In recent years, the implementation of Cyclic Redundancy Check code (CRC) and Lagrange interpolation are introduced to replace Reed-Solomon code. However, the CRC-based fuzzy vault scheme still needs some improvements. Recent research on CRC-based fuzzy vault methods focus on preventing attacks such as brute force attack, statistical analysis attack, collusion attack, and blend substitution attack [9].

Benhammedi et al. [10] proposed a new method using password hardened fuzzy vault based on an improvement of fingerprint feature representation. Khalil-Hani et al. [11] changes the whole scheme by considering non-random chaff point generator which is computationally fast. These two methods only prevent statistical analysis attack. Nguyen et al. [12] proposed a new fuzzy vault method using ridge features. This method resists against advanced brute force attack. Dang et al. [13] proposed a cancellable fuzzy vault. The proposed method performs a periodic transformation on the biometric template. This method is robust against brute force attack. However, this method is possible to be cracked by statistical analysis attack.

Another scheme was proposed by M.T. Nguyen et al. [14] in early 2016. This method focuses on preventing the

aforementioned attacks, especially blend substitution attack. This scheme introduces a modified chaff point generator and verifier. This non-random chaff point generator and verifier substitute CRC algorithm for error correcting check. The schematic of this method can be seen in Figure 1. Continuous hashing and linear projection are used to generate chaff from cryptographic key and biometric template in enrollment phase. As a consequence, the same chaff point will be regenerated as a verifier in the authentication phase. In this scheme, chaff point is not a random point but a point that is treated as the signature for the combination of biometric template and cryptographic key. If there are any modifications in the vault, then this system can detect the modification and the authentication will fail.

III. FINGERPRINT FEATURE EXTRACTION

In this section, a brief introduction to fingerprint feature extraction is explained. Minutiae extraction is one of the feature extraction methods for fingerprint. Minutiae extraction is widely used and is also one of the old methods in feature extraction field. In fuzzy vault, feature extraction is a preprocessing step for getting genuine points from the biometric sample. The input for this step is a biometric image from the sensor, and the output is a set of genuine points as the unique identity of the biometric sample. To get a high performance of the fuzzy vault system, we have to select an accurate feature extraction method. Accurate feature extraction will help in decreasing False Acceptance

Rate (FAR) and False Rejection Rate (FRR). An accurate extraction method must have the capability of extracting salient features from fingerprints in a robust way. The False Negative (FN) rate and False Positive (FP) rate of the extracted genuine points should be minimized.

There are many minutiae extraction methods that have been introduced by researchers to obtain a high performance fingerprint feature extraction [15]. Distortion is a major concern in developing feature extraction methods. Distortion in fingerprints comes from variations in skin and impression condition when the user inserts their fingerprint from the sensor.

Minutiae extraction can be done in binarized fingerprint image or gray scale fingerprint image. Binarized fingerprint image can be divided into two types, unthinned binarized images and thinned binarized images. One of the example methods that uses unthinned binarized images is ridge flow and local pixel analysis. In [16] a method based on ridge flow was used. This proposed method scans the binary images of a fingerprint, identifying localized pixel patterns that indicate the ending or splitting of a ridge. For example, a pattern may represent the end of a black ridge protruding into the pattern. Another example method that uses thinned binarized images is based on Crossing Number. In [17], Wu Zhili uses a modified crossing number method to extract minutiae points from fingerprint.

In Section 5, several minutiae extraction methods are evaluated. The purpose of the section is to select an accurate and suitable minutiae extraction method for the fuzzy vault system.

IV. PROPOSED METHOD

In this section, we propose a method to enhance the security in mobile payment authentication systems with account-based remote payment scenario. The interactions among concerned parties in an account-based remote payment scenario are illustrated in Figure 1. There are four components included in this scenario: the client, the merchant, the merchant's bank, and the Online Payment Provider. Communications among these concerned parties are done in a secure protocol.

First, the user registers their account to the Online Payment Provider together with their fingerprint information through the sensor. In this phase, the online payment provider will configure the client phone to generate private and public keys for the next communication. Authentication is done if the client makes a transfer request from their mobile phone. The authentication process between the client side and the server side of the online payment provider can be seen in Figure 2. Matching is done in the client side using fuzzy

vault non-random chaff point generator scheme. Vault points as helper data are stored in the mobile phone's local data. These vault points come from a non-random chaff point generator and polynomial reconstruction of the biometric template and the cryptographic key.

Public key infrastructure is involved in the authentication process between the Online Payment Provider's server and the client's mobile phone. The client's private key is used for signing an authentication response. Then the server validates the authentication response using the client's public key on the database. After that, the server checks the client account's balance. If there are sufficient funds, then the Online Payment Provider initiates a money transfer to the merchant's bank. Then the merchant gives a notification to the client that the transaction has been approved.

The overall process in mobile payment authentication system based on the fuzzy vault non-random chaff point generator is described in the explanation below.

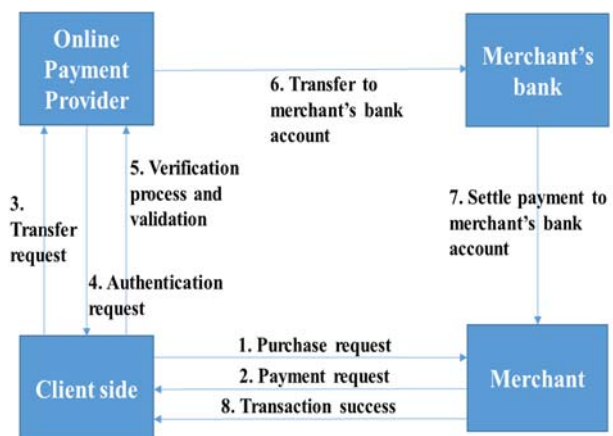


Fig. 2. Scenario in account-based remote mobile payment system.

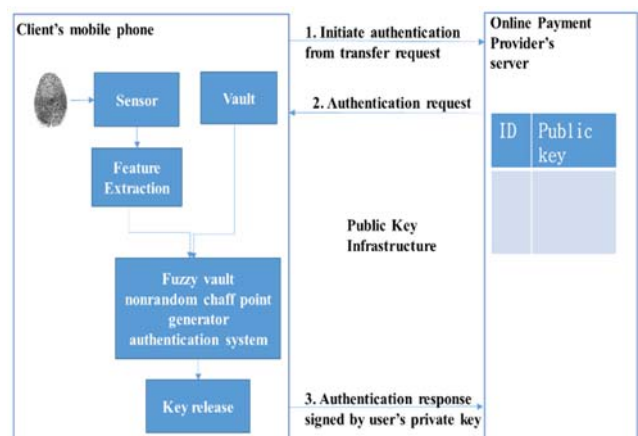


Fig. 3. Authentication process

4.1. Enrollment Phase

In enrollment phase, the user makes an account in Online Payment Provider including their unique ID. A random pair of public key and private key is generated in the user's

mobile phone. Then the user's mobile phone requests the certificate to Certificate Authority (CA). If the registration data of the user are valid, the Online Payment Provider (OPP) will enroll the user ID together with his corresponding public key to OPP's server database. After that, the user inserts his fingerprint template. This fingerprint template will become an input for the feature extraction module. Feature points are extracted from the fingerprint template in the feature extraction module using the minutiae extraction method. Genuine points are constructed by polynomial construction using the registered private key and feature points as inputs. Chaff points are generated using Chaff Points Generator in [14]. Genuine points and chaff points are combined together and become vault points. These vault points are stored in the user's mobile phone, for future usage in authentication phase.

4.2 Authentication Phase

In the authentication phase, if a user sends a transfer request to OPP, an authentication request and challenge message are sent back by OPP to the user's mobile phone. The system then requests the user to insert his fingerprint. This fingerprint image that is captured by the mobile phone's sensor is inserted to the feature extraction module. Once again, feature points are obtained from the biometric sample. A candidate genuine set is selected by selecting vault points based on the feature points. Using Lagrange interpolation, the polynomial equation is reconstructed and private key is generated. After the private key is acquired, the system executes Chaff Point Verifier in [14] and the authentication result and private key are issued. This private key is used to sign the challenge message request from the OPP, and the OPP will verify the identity of the user in the OPP server.

Performance of biometric authentication is considered in terms of FRR, FAR and Equal Error Rate (EER) [18], [19]. These metrics are used to measure the performance of fuzzy vault non-random chaff point generator which is implemented in mobile payment system. To reduce FAR and increase FRR, choosing an optimal value of variables in fuzzy vault system is an important task.

V. EXPERIMENT AND RESULT

The proposed method is still in a work in progress, therefore not all of the modules in the scheme have been implemented. In this section, feature extraction for fuzzy vault system on mobile payment authentication is selected and implemented.

5.1 Input Data

The input data that is used for testing the system is fingerprint NIST Special Database 04 (SD04). The original SD04 data is an ANSI/NIST format (AN2) file. This database contains 8-bit grayscale images of randomly selected fingerprints. This file contains 4000 (2000 pairs) fingerprints stored in PNG (image) files format and TXT (data) files with information extracted from the AN2 file. Each print is 512×512 pixels with 32 rows of white space at the bottom of the print. The fingerprints are classified into one of five categories (L = left loop, W = whirl, R = right loop, T = tented arch, and A = arch). For this implementation, the database from figs_0 is used. The record file holds the image for the subject and some information pertaining to the image in text file. The field that has the CLASS and HISTORY values e.g., "CLASS:R, History: f0023_04.pct R a2804.pct" is extracted and put onto the text file together with the Gender value.

5.2 Software

The feature extraction method is implemented in Xamarin IDE that is already embedded in Microsoft Visual Studio 2015. Xamarin is an IDE for mobile application development that uses C# and can be used for code compiling across all mobile development platforms such as iOS, Windows Mobile and Android.


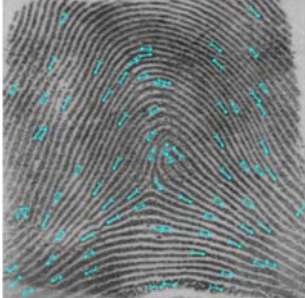
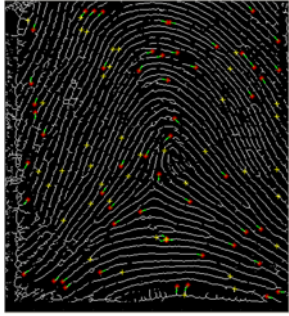

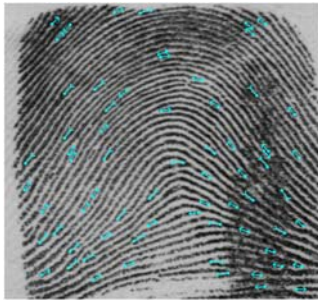
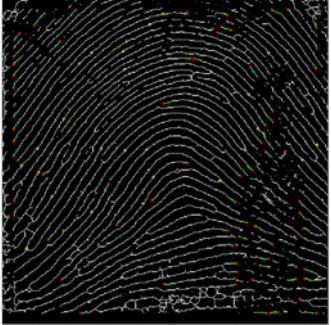
5.3 Feature Extraction

In this section, a comparison between two minutiae feature extractions is shown in Table 1 and performance is evaluated. The first algorithm is SourceAFIS SDK [20] for feature extraction based on ridge flow and local pixel analysis [16]. The second algorithm [21] is based on modified Crossing Number [17].



Fig. 4. Example png file f0023_04 from fingerprint database NIST SD04

Table 1. Feature extraction output example for each algorithm.

Input Image	Output [20]	Output [21]
		
		

VI. DISCUSSION

Securing biometric templates is a major concern in biometric authentication. If the matching process only uses the biometric template itself, then it is better to store the biometric data in the server side since attacking the server is more difficult than attacking the client (i.e. mobile phone). However, there are some disadvantages if the biometric templates are stored in the server side. First, if an attack occurs, then the possibility of data loss is high. Second, there is no privacy for client's biometric data in the server side. To protect the client's privacy, it is more convenient to store the biometric data in the client's mobile phone. To prevent data leakage, the biometric templates must be stored in a secure manner. Biometric cryptosystems are a suitable solution to secure biometric templates for authentication method in the client side.

To enhance the performance of the fuzzy vault system, we must consider every step, including the feature extraction step. The feature extraction step produces genuine points from fingerprint as an input for fuzzy vault system. These genuine points are used in the enrollment and authentication phases in the mobile payment system. Accurate genuine points are an important parameter to enhance the accurate performance of the system. Considering the best feature extraction algorithm for the

system is a must, especially given distortion in the input image while the enrollment process is performed. We have to select an algorithm that can handle distortion regions in the input images. A distortion region can be a low quality region, border area, or high curve region. In such a distortion region, the possibility of false minutiae as genuine points is high.

Based on the comparison result in section 5, the algorithm in [20] can handle the distortion region to reduce false minutiae detection, in contrast with the algorithm in [21]. Table 1 shows many false minutiae in border region are detected by the algorithm in [21].

VII. CONCLUSION AND FUTURE WORK

In this paper, a method is proposed to enhance the authentication security in account-based mobile payment systems while the matching process is done on the client side. Communication between the client and the Online Provider Payment's server is done using public key infrastructure. The proposed method uses fuzzy vault BCs key binding technique based on non-random chaff point generator in [14]. This method resolves the previous attacks reported in [9]. A fingerprint feature extraction method is evaluated as an important step in the fuzzy vault system to enhance the accuracy of the system.

For future work, we will implement the proposed method as a mobile application. To achieve a high performance of the proposed method, optimal values of other variables in fuzzy vault non-random chaff point generator should be considered.

Acknowledgement

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government(MSIP)(No.NRF-2014R1A2A1A11052981).

REFERENCES

- [1] W. Yang, J. Hu, J. Yang, S. Wang, and L. Shu, "Biometrics for Securing Mobile Payments: Benefits, Challenges and Solutions," *Image and Signal Processing* Vol. 2, 2013.
- [2] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security* 2011.1, pp. 1-25, 2011.
- [3] S. Rane, Y. Wang, S.C. Draper, and P. Ishwar, "Secure Biometrics: Concepts, Authentication Architectures & Challenges," *Signal Processing Magazine*, Vol. 30, No. 5, pp. 51-64, 2013.
- [4] M. Hassinen, K. Hyppönen, and E. Trichina, "Utilizing National Public-key Infrastructure in Mobile Payment Systems," *Electronic Commerce Research and Applications*, Vol. 7, No. 2, pp. 214–231, 2008.
- [5] J.T. Isaac, and S. Zeadally, "Secure Mobile Payment Systems," *IT Professional*, Vol. 16, No.3, pp. 36-43, 2014.
- [6] S. Elfakharany, A.F. Amin, and M. Zaki, "Secure Mobile Payment Protocol using Asymmetric Encryption for Authorization," *Journal of Network Communications and Emerging Technologies*, Vol. 2, 2015.
- [7] T. Dahlberg, J. Guo, and J. Ondrus, "A critical review of mobile payment research," *Electronic Commerce Research and Applications*, Vol. 14, No. 5, pp.265-284, 2015.
- [8] A. Juels and M. Sudan, "A fuzzy vault scheme," in Proc. IEEE Int. Symp. Information Theory, Lausanne, Switzerland, pp. 408, 2002.
- [9] W.J. Scheirer and T.E. Boulton, "Cracking Fuzzy vaults and Biometric Encryption," *Biometrics Symposium*, 2007.
- [10] F. Benhammadi and K.B. Bey, "Password hardened fuzzy vault for fingerprint authentication system," *Image and Vision Computing*, Vol. 32, No. 8, pp. 487-496, 2014.
- [11] M. Khalil-Hani, M. N. Marsono, and R. Bakhteri, "Biometric encryption based on a fuzzy vault scheme with a fast chaff generation algorithm," *Future Generation Computer Systems*, Vol. 29, No. 3, pp. 800-810, 2013.
- [12] T. H. Nguyen, Y. Wang, Y. Ha, and R. Li, "Performance and security-enhanced fuzzy vault scheme based on ridge features for distorted fingerprints," *IET Biometrics*, Vol. 4, No. 1, pp. 29-39, 2015.
- [13] T. K. Dang, Q. C. Truong, T. T. B. Le, and H. Truong, "Cancellable fuzzy vault with periodic transformation for biometric template protection," *Biometrics, IET*, pp. 1-7, 2016.
- [14] M.T. Nguyen, Q.H. Truong, and T.K. Dang. "Enhance fuzzy vault security using nonrandom chaff point generator," *Information Processing Letters*, Vol. 116, No.1, pp. 53-64, 2016.
- [15] R. Bansal, P. Sehgal and P. Bedi. "Minutiae Extraction from Fingerprint Images – a Review," *International Journal of Computer Science Issues*, Vol.8, Issue 5, No. 3, pp.74-85, 2011.
- [16] C.I. Watson, M.D. Garris, E. Tabassi, C.L. Wilson, R.M. McCabe, S. Janet and K.Ko, "User's Guide to NIST Biometric Image Software" National Institute of Standards and Technologies. 2007.
- [17] Wu Zhili, "Fingerprint Recognition," M.S. thesis, Department of Computer Science, Hong Kong Baptist University, Hongkong, 2002.
- [18] A. K. Jain, A. Ross, and S. Prabhakar. "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 14, No. 1, pp. 4-20, 2004.
- [19] A. Jain, P. Flynn, and A. A. Ross. *Handbook of Biometrics*. Springer Science & Business Media, 2007.
- [20] Robert Fazan, "SourceAFIS — Fingerprint recognition toolkit," Jun. 2016; <http://www.sourceafis.org/blog/sourceafis-1-7/>
- [21] Wu Zhili, "Fingerprint Recognition," Jun. 2016; <http://www.comp.hkbu.edu.hk/~vincent/resPaper.htm>

Authors



Annisa Istiqomah Arrahmah has received her bachelor degree in electrical engineering from Institut Teknologi Bandung, Indonesia, in 2015. She is currently pursuing master dual-degree both in electrical engineering from Institut Teknologi Bandung, Indonesia, and in IT convergence and application engineering from Pukyong National University, South Korea. Her main research interests include mobile payment system, biocryptosystems, image processing, biometric feature extraction and VLSI circuits.



Yudi Satria Gondokaryono is an assistant professor of computer engineering and the Director of Information System and Technology Office of Institut Teknologi Bandung (ITB). His research interests include high performance system and computer security. He received his bachelor degree from Institut Teknologi Bandung in 1989, and an MS in electrical engineering (1997) and a PhD in electrical engineering (2003) from New Mexico State University. He is a member of the Technical Committee on Parallel Processing (TCPP) IEEE and member of IEEE and ACM



Kyung-Hyune Rhee received his M.S. and Ph.D. degrees from Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea in 1985 and 1992, respectively. He worked as a senior researcher in Electronic and Telecommunications Research Institute (ETRI), Daejeon, Korea from 1985 to 1993. He also worked as a visiting scholar in the University of Adelaide in Australia, the University of Tokyo in Japan, the University of California at Irvine in USA, and Kyushu University in Japan. He has served as a Chairman of Division of Information and Communication Technology, Colombo Plan Staff College for Technician Education in Manila, the Philippines. He is currently a professor in the Department of IT Convergence and Application Engineering, Pukyong National University, Busan, Korea. His research interests center on multimedia security and analysis, key management protocols and mobile ad-hoc and VANET communication security.

