Biometrics-based Key Generation Research: Accomplishments and Challenges

Lam Tran Ha*, Deokjai Choi**

Abstract

The security and privacy issues derived from unsecurely storing biometrics templates in biometric authentication/ recognition systems have opened a new research area about how to secure the stored biometric templates. Biometrics-based key generation is the newest approach that provides not only a mechanism to protect stored biometric templates in authentication/ recognition systems, but also a method to integrate biometric systems with cryptosystems. Therefore, this approach has attracted much attention from researchers worldwide. A review of current research state to summarize the achievements and remaining works is necessary for further works.

In this study, we first outlined the requirements and the primary challenges when implementing these systems. We then summarize the proposed techniques and achievements in representative studies on biometrics-based key generation. From that, we give a discussion about the accomplishments and remaining works with the corresponding challenges in order to provide a direction for further researches in this area.

■ keywords : Biometric Templates Protection | Biometric Cryptosystems | Key Generation, Fuzzy Extractor

I. Introduction

Biometrics refers to techniques that allow authenticating or recognizing individual based on their biological or behavioral characteristics. Comparing to password and token, biometrics is more convenient for users as they do not need to remember a secret string (password) or keep a portable device secretly (token) [34]. However, there are some issues in most of biometric systems that prevent them from applying worldwide in real life. One of the critical issues is the insecureness of stored biometric templates [5]. Securing biometric templates is a new research area that designs the methods to secure the stored biometric templates in the biometric systems. As summarized in [27], there are two main approaches for securing biometric templates techniques: feature transformation, biometric cryptosystem. Biometric cryptosystems are again classified into key binding approach and key generation approach.

The key generation is a newest and most potential one. This approach uses biometric data to generate a biometrics-dependent key which can be used to authenticate user in local system, or eCommerce system [41], or integrate with the existing cryptography systems.

Beside preserving user's privacy and enhancing system security as other securing biometric templates approaches [27], BKG (Biometric Key Genration) approach has a significant advantage as the extracted key can be used as secret key in existing security system (i.e. symmetric cryptography).

During last 5 years, there has been a significant number of studies which spreads from designing a key generation system for a specific biometric trait to a theoretical

* 학생회원, 전남대학교 대학원 전자컴퓨터공학과
** 정회원, 전남대학교 전자컴퓨터공학부 교수
Manuscript : 2017. 05. 17
Revised : 2017. 06. 22
Confirmation of Publication : 2017. 05. 27
Corresponding Author : Deokjai Choi, e-mail : dchoi@jnu.ac.kr

framework for extracting key from noisy data. However, to the best of our knowledge, there has been no study that reviews the current state of biometric-based key generation researches. So, in this paper, analysis of state-of-the-art BKGSs (Biometric Key Generation Systems) are given. Based on that, the accomplishments up to now, and the existing challenges are stated, and the outlook for future research are outlined.

We organize the remaining sections of this paper as following. Section II provides a background related to biometrics-based key generation system. In Section III, we summarize the state of researches in BKG. In Section IV, we discuss the acquirements and remaining challenges for future works. Finally, we give the conclusions in Section V.

II. Background

1. The biometric-based key generation approach

The main objective of BKGS is repeatedly extracting a unique and deterministic key for individual using characteristics of a specific (or multiple) biometric trait(s). As introduced above, BKGS operates in two main phases named key generation and key reproduction. The key generation phase uses training biometric templates to extract the key and generate some helper data. In the key reproduction (or reconstruction) phase, the system uses other biometric templates to construct the same key as the one extracted in generation phase with the assist of helper data. In the key generation approach, the system stores neither the biometric templates nor the extracted key. However, similar to other biometrics template protection, the BKGS has to store some helper data in order to assist reconstructing key. The helper data can include the system parameters or setting, some global informations for alignment, quantization, hash value of extracted key which do not directly reveal the enrolled user's information.

2. Challenges

Basically, implementing a BKGS has two main challenges which are primarily resulted from the variation (or instability) but permanence in nature of biometric characteristics. Specifically, the biometric data always contain much variations that can be caused by various factors such as environment conditions, limitations of data acquisition devices/ techniques, and the changing mood of users. However, the extracted key is required to be deterministic and unique. Thus, reducing the variation to get stable informations and extracting the key from raw biometrics is considered as main challenge in implementing BKGS. Additionally, the generated keys of different users should be different to each other.

On the other hand, there is another challenge comes from the permanence of biometric characteristics. Specifically, the biometric properties of individual are likely to remain unchanged in a long period. But, to be secure system, BKGS should allow changing key and helper data easily, which is against permanence nature of biometrics. So, the challenge is how to change key and helper data from the biometric trait of same user with different time.

3. Requirements and Evaluation Criteria

As the BKGS is a security scheme for a pattern recognition system, the criteria for evaluating a BKGS involve both the verification/recognition performance and security strength. In the BKGS, security and user's privacy are considered more important than other criteria. The security and privacy criteria for a BKGS mostly relate to the helper data which is usually placed publicly. There are three main requirements for the helper data including:

- Irreversibility: The attacker should not be able to revert to the original biometric template or reducing the effort to compromise the extracted key using the helper data in a specific system. At the same time, the user generate keys and helper data for his many devices such as smartphone, smart watch or other wearable devices. In this case, each device hold its own helper data which are different each other. The attacker should not be able to generate key by combining multiple instances in different devices.

– Revocability: It should be possible to revoke old instances of helper data and keys for the system when the current instance or the corresponding key is being compromised. This requirement also implies that it should be possible to extract different instances of helper data and keys from one biometric traits of the same user.

– Nonlinkability: It should be unable to perform cross-matching across multiple instances of the same biometric traits. This requirement also implies that it should be difficult to verify whether or not two or more instances were derived from a same biometric trait of a user.

Additionally, the security strength of the BKGS is also reflected by the length of extracted key which is required to have high entropy to resist against brute force attack.

Some other criteria are related to common verification/ recognition metrics as:

– False Acceptance Rate (FAR): FAR is the probability that the system reproduces the key as same as one generated in the generation phase when using biometric templates of impostor. In a security system, FAR is an important metric and is one of the factors used to measure the security level of a system, most of BKGS try to achieve FAR of 0 %.

– False Rejection Rate (FRR): FRR is the probability that the system uses biometric data of enrolled user to reproduce key but results to a different key with the one generated in key generation phase. The FRR represents for the friendliness of the system. In the BKGS, there is always a trade-off between FAR and FRR.

– Equal Error Rate (EER): EER is defined as the point at which FAR is equal to FRR. This criteria is useful when evaluating the overall accuracy of the system. The lower EER the system can achieve, the higher overall accuracy it is. Thus, some studies try to reduce the EER as low as possible when selecting system parameters.

Additionally, since BKGS may be deployed often in mobile or wearable devices, it requires resource efficiency such as memory, cpu, and power consumption etc.

III. Biometrics-based Key Generation Researches Summarization

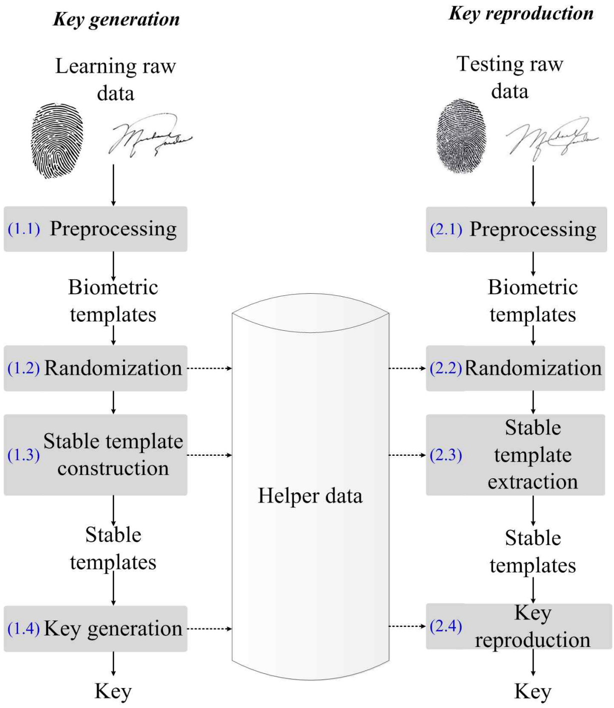

Fig. 1. The General Architecture Biometrics-based Key Generation System

As the concerns of security and privacy increase continuously, the biometrics-based key extraction researches have attracted much attention from researchers. The studies in this field can be classified into two branches. The first branch is to propose a theoretical framework for repeatedly generating deterministic key from noisy data. The representative research in this branch is the fuzzy extractor scheme [29, 30, 31]. The second branch is to propose and implement a bio-cryptosystem to repeatedly generate a key from data of one or multiple biometric trait(s) (i.e, iris, face, fingerprint, voice, signature).

As the reviewing of theoretical framework researches have been performed in some studies [32, 36], in this paper, we focus on summarizing the researches of proposing and implementing BKGS with specific biometric trait(s). Specifically, we summarize the general processes of state-of-the-art BKG researches, the addressed problems, the methods for evaluation and the achieved results. From the summarization, we find the drawbacks, remaining works and challenges for further researches.

1. Overall Systems Architecture

Various biometric traits have been used for key generation as Iris [8, 26], Face [3, 4, 6], Fingerprint [11, 12], Handwriting [10], Key-stroke [13], Signature [14]. Although these studies use different biometric traits, the system architectures in these researches are quite similar. The BKGS usually consists of following 4 primary steps which are sketched in Figure 1:

– *Preprocessing* (Step 1.1/2.1): it is used to eliminate noise in raw data and extract useful informations to make biometric templates which will be processed to extract key.

– *Randomization* (Step 1.2/2.2): as the biometrics characteristics does not change much in a process of time, it is difficult to generate different key for the same user in a different situation. It may weaken the security strength of the system. The randomization step is used to make the biometrics templates to be different in order to extract different keys in different occasion.

– *Stable template construction* (Step 1.3/2.3): this is an important step in BKGS. The objective of this step is to analyze the biometric templates, then extract stable and discriminative informations, which are used to form stable templates.

– *Key generation* (Step 1.4/2.4): usually, the stable templates still contain some variations and cannot be used as key. The key generation is the last step which is used to generate the deterministic key from the stable biometric templates. The auxiliary data extracted in this phase, which can be system parameters or informations for processing data, are stored publicly for using in key reproduction phase.

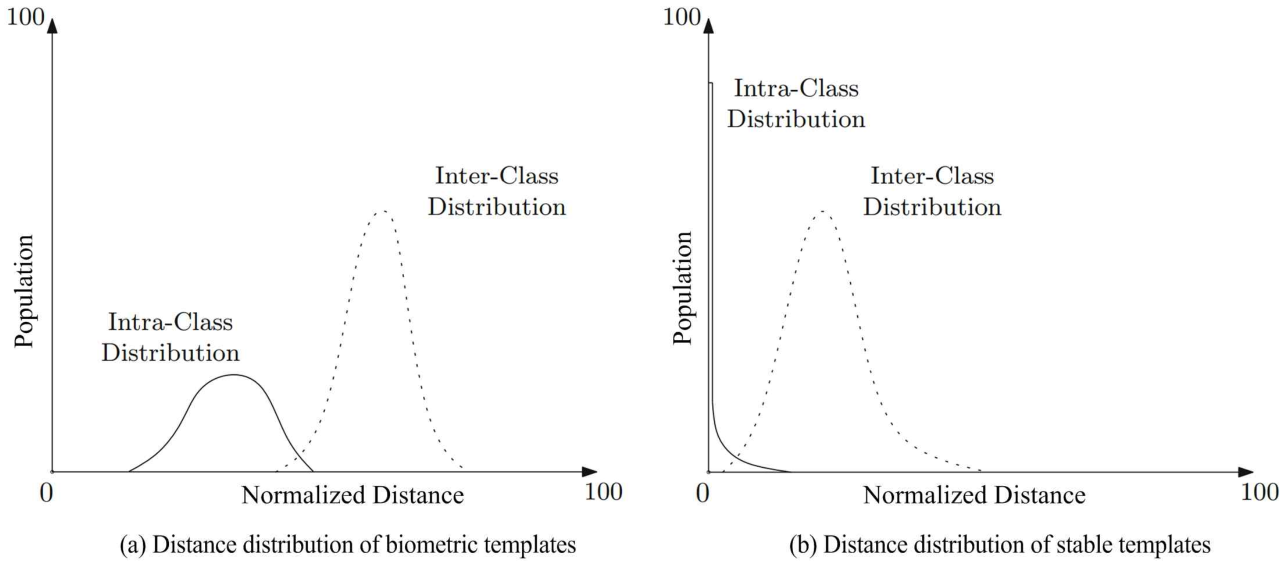

Fig. 2. The Difference in Distance Distribution between Biometric Templates and Stable Templates.

2. Challenges and Proposed Methods

There are 2 major challenges in biometric key generation system which are the instability of templates and relatively permanence of the biometric characteristics.

a) Instability of the biometric templates

The generated key of a specific user is required to be deterministic and the generated keys of different users are required to be different to each other. So, instead of only adopting methods for reducing the instability of intra-class biometric templates, most of the BKGSs also used methods for enhancing the separation of inter-class. Typically, a BKGS use two main stages to extract deterministic key:

– Stable templates extraction (*Fig 1, Step 1.3 / 2.3*): In order to get a stable and discriminative one representing in binary string or in real-valued, this step usually adopts techniques for reducing the variations in intra-class, or enhancing the separation of inter-class templates, or both:

(i) Classification techniques: these techniques provide methods to not only reduce intra-class variation but also enhance the inter-class separation [3, 4, 6, 13, 14].

(ii) Stable and discriminative components selection: some studies [3, 4, 6, 8, 10, 11, 12, 14] used statistical-based methods to analyze each component in biometric templates and select the discriminative and stable ones to form stable templates. The methods for analyzing components are different to each other and depend on the used biometric traits. These techniques also reduce the variation and enhance the separation simultaneously.

(iii) Quantization techniques [3, 4, 6, 11, 12, 13, 14]: these techniques mainly reduce the intra-class variation by quantizing the biometric templates from continuous values to discrete values or from real values to binary string.

The general impacts of this step are illustrated by distance distributions of biometric templates and stable ones displayed in Figure 2.

- Biometric-key extraction (*Figure 1, Step 1.4/2.4*): The stable template extraction step cannot eliminate all variations in biometric templates as illustrated in Figure 2b. The role of final step is to extract a deterministic key from the stable templates. An Error correcting code (ECC) [35][42] is the most popular technique to be used in this step [8, 13, 26]. Beside that, other studies used the quantization-based techniques [10, 11, 14].

b) Relative Permanence of the templates

For the challenge of permanence of biometric characteristics, many systems use the randomization techniques (*Figure 1, Step 1.2/2.2*). Specifically, the biometric templates is merged (i.e., projected, bind) with a random data (i.e., vectors, strings) which are generated randomly, to get a different instances before extracting key. The random data in this step is stored as helper data for using in key reproduction phase. For example, in

Table 1. The Summary of Representative Studies in Biometrics-based Key Generation Published after 2011.

Studies	Modality	Randomization	Key extraction process	Biometric-dependent key	Revocable
Physiological Biometrics					
Lim *et al.*, 2011 [3, 4, 6]	Face	-	LDA, ERE; LSSC Quantization;	-	-
Rathgeb *et al.*, 2011 [8]	Iris	-	Context-based reliable bits extraction; BCH code applying	YES	NO
Marino *et al.*, 2012 [26]	Iris	-	Features Extraction; FCS with Reed-solomon code	NO	NO
Sheng *et al.*, 2012 [11]	Fingerprint	User specified random sequence;	Orientation features extraction; Interval mapping	YES	YES
Chin *et al.*, 2014 [12]	Fingerprint & Palmprint	Random Tiling	Feature level fusion; Quantizing	YES	YES
Behavioral Biometrics					
Makrushin *et al.*, 2012 [10]	Hand-writing	-	Reliable features selection; Secure Sketch Adopting	YES	NO
Vsedvenka *et al.*, 2014 [13]	Key-stroke	-	LDA; scaled parity code quantizing; FCS Adopting	NO	NO
Sheng *et al.*, 2015 [14]	Signatures	-	Semisupervised clustering scheme; Consistent and discriminative features selection	YES	NO

studies [12], the author used Random Tiling [40] to randomly generate another instance of Iris templates; the random string was used in the studies [13, 14, 26].

3. Representative Researches Summarization

In this section, we present the a summary of representative BKG researches in details. The selected BKG studies are summarized in Table 1, which describes the used biometric trait, the randomization technique, key extraction process. It also tells whether the key is dependent to biometrics characteristics, and whether the proposed system can revoke compromised key or not. We arrange surveyed studies by type of biometric traits (physiological or behavioral) and year of publishing.

For the physiological biometric traits, there are some representative researches as following. Lim *et al.* [3, 4, 6] proposed an approach to generate discriminative and privacy-protective binary string from Face images. Their system mostly focused on the methods for extracting stable templates. First, they adopted the features extraction techniques as Fisher's Linear Discriminate Analysis (LDA) [38], Eigenfeature Regularization and Extraction (ERE) [39] to reduce the template dimensional, and also enhance separation and reduce variation of biometric templates. Then, they selected a specific amount of components for quantization and encoding with Linear Separable Subcode (LSSC) [2] to extract the binary string. Rathgeb *et al.* [8] proposed a context-based analysis method for determining the reliable bits extracted from Iris template. The reliable bits were then used to form the key. BCH code encoding [35] was applied to the key to get the check bits (the redundancy part in codeword of BCH code) which were stored as helper data for using in key reproduction phase. Marino *et al.* [26] presented a crypto-biometric scheme to allow a user to secure and retrieve a secret key, which was generated

Table 2. The Summarization of Data Set for Evaluating in Surveyed Studies.

Studies	Modality	Data set	Descriptions
Physiological Biometrics			
Lim *et al.*, 2011 [3, 4, 6]	Face	CMU PIE [15]	68 volunteers, each one has 32 images
		FRGC [16]	177 volunteers, each one has 12 images
Rathgeb *et al.*, 2011 [8]	Iris	CASIAv3-Interval [18]	2639 images of 249 volunteers
		IITDv1 [17]	2240 images of 224 volunteers
Marino *et al.*, 2012 [26]	Iris	CASIA [19]	756 iris images of 106 volunteers
Sheng *et al.*, 2012 [11]	Fingerprint	FVC2002 [20]	3520 fingerprint images from 440 fingers
Chin *et al.*, 2014 [12]	Fingerprint	FVC2004 DB1 [21]	800 greyscale fingerprint images of 100 subjects
		[22]	1030 color images of 103 subjects
		FVC2002 [20]	800 greyscale fingerprint images of 100 subjects
	Palmprint	PolyU [23]	7750 greyscale palmprint images of 386 subjects
		[24]	5160 color palmprint images of 208 subjects
Behavioral Biometrics			
Makrushin *et al.*, 2012 [10]	Handwriting	[10]	1590 handwriting instances of 53 volunteers
Vsedvenka *et al.*, 2014 [13]	Key-stroke	[13]	486 volunteers, at least 300 characters for each
Sheng *et al.*, 2015 [14]	Signatures	[25]	7430 signatures of 359 volunteers

Table 3. The Performance of Some Representative Studies in Biometrics-based Key Generation.

Studies	Modality	Key length (bits)	Metrics	Results
Physiological Biometrics				
Lim *et al.*, 2011 [3, 4, 6]	Face	-	EER	3
Rathgeb *et al.*, 2011 [8]	Iris	280	EER	< 0,5
Marino *et al.*, 2012 [26]	Iris	192	FAR FRR	4.42 9.67
Sheng *et al.*, 2012 [11]	Fingerprint	80	FAR FRR	0 6.9
Chin *et al.*, 2014 [12]	Fingerprint & Palmprint	200	EER	0
Behavioral Biometrics				
Makrushin *et al.*, 2012 [10]	Handwriting	-	FAR FRR	3.44 6.41
Vsedvenka *et al.*, 2014 [13]	Key-stroke	-	EER	3.6
Sheng *et al.*, 2015 [14]	Signatures	30	FAR FRR	0 21.4

randomly, by using the Iris templates. The Reed-solomon code [35] was adopted in this system to handle the variation of biometric templates. In this system, the key was generated randomly, so it is independent to biometric data. This study likely followed the key binding scheme [1] instead of key generation. Sheng *et al.* [11] proposed an approach to extract biometric-dependent key from Fingerprint images. They combined a user specified random sequence with the orientation fields and reference points information of Fingerprint images to extract the orientation features. The interval mapping process was applied to orientation features which the instruction of user dependent coding matrix to get the biometric-dependent key. Chin *et al.* [12] proposed a system to generate key by combining Fingerprint and Palmprint characteristics. First, they fused data of Fingerprint and Palmprint at the feature level. Then, they applied the Random Tiling technique [40] to the fused templates using the user-specified key to get the random features which were then discretized to the bit-string template.

A few researches proposed their BKGSs using behavioral biometric traits as [10, 13, 14]. Specifically, Marushin *et al.* [10] presented an approach to select relevant features of handwriting. The selected features were used as the input for secure sketch to extract biometric-dependent key. Vsedvenka *et al.* [13] proposed a system to generate key from key stroke signal. They used LDA to obtain a better representation of discriminable biometric signals. Then, they applied scaled parity code for key generation and construction. After this, Fuzzy Commitment Scheme (FCS) [33] was adopted to secure the key. Sheng *et al.* [14] presented a system to generate biometric-dependent key from Handwriting images. They used a semi-supervised clustering scheme to get an optimal clustering solution to model intra- and inter-user variations. Using the modeling results, they selected a set of consistent and discriminative features to generate the key for each user.

4. Evaluation Methods and Results

Until now, no study in this research field evaluated the proposed system in realistic conditions. Most of proposed systems were evaluated in laboratory conditions with some data set as summarized in Table 2. The studies in physiological biometrics were evaluated with common public data sets. However, the studies in behavioral biometric traits used self-collected data sets which are hard to verify the quality and reliability of the used data set.

The popular metrics for measuring system performance were FAR/FRR and EER combining with key length measured by bits number [8, 11, 12, 14, 26]. However, some studies used key as real-valued features which are hard for measuring the key strength [10, 13]. On the other hand, some studies just provided approaches to extracted stable string which could be used in biometric cryptosystems, no key was specified [3, 4, 6].

Beside analyzing the performance in terms of FAR/FRR, only study [13] provided an analyzing for the security strength and the computational overhead of the of the proposed methods. Oher studies did not provide the security and computational analyzing of their systems in details.

Table 3 summarizes the results of BKGS. As the behavioral biometrics are more noisy than physiological ones, the performances of behavioral biometrics-based systems in terms of FAR/ FRR/ ERR and key length are much lower comparing to physiological biometrics-based systems.

IV. Discussion

1. Acquirements

Although the BKG is the youngest approach for securing the biometric templates, there are significant achievements in this research field.

Firstly, beside the general framework as fuzzy extractor, for implementing BKGS, and variety of techniques have been proposed to address the primary challenge of the unstability of biometric templates.

Secondly, some techniques have been proposed to allow revoking compromised key from the same biometric trait.

Additionally, BKGS have been implemented with many biometric traits and achieved promising results in terms of system accuracy (FAR/FRR) and key strength.

2. Open Issues and Challenges

Although the achieved results in BKG research are promising, they are still far from practical using. There are several open issues which need more effort to provide a proper biometric-based security solution for BKGS to be applied widely in real applications. Improving the system performance in terms of FAR/FRR is the main task in this research.

The primary remaining challenge is still the unstability of biometrics data. Although there have been many solutions addressing this challenge, these approaches were evaluated in laboratory conditions. In realistic conditions, the biometrics data is more noisy which can degrade the system performance seriously. So, the main challenge still is how to handle the variation of biometric data in real-life conditions, and needs more effort from researchers worldwide.

Deeply analyzing the security strength of proposed BKGS under potential attacks should be performed in both theory and practice to ensure the system can meet the security requirements.

Additionally, more effort is needed in the task of experimenting the BKGS in real-time conditions. Beside the verification/recognition performance and security strength, the assessment for user friendliness, the resources requiring and power consumption, especially system for mobile devices, should be analyzed in more details.

V. Conclusions

In this paper, we presented a summary of the representative studies in implementing BKGS published since last 5 years. We provided the fundamental requirements and the primary challenges when implementing BKGS in practice. We gave the summary of techniques in proposed BKG systems. From the summary, we can see that although the BKG researches have attracted much attention from researchers and achieved significant results, there are serious limitations remaining in proposed systems which need more effort from researchers worldwide in order to apply BKGS to realistic applications.

References

[1] Rathgeb, Christian, and Andreas Uhl. "A survey on biometric cryptosystems and cancelable biometrics", EURASIP Journal on Information Security, 2011.

[2] Lim, Meng-Hui, and Andrew Beng Jin Teoh, "Linearly separable subcode: A novel output label with high separability for biometric discretization", In the 5th IEEE Conference on Industrial Electronics and Applications (ICIEA), pp. 290-294, IEEE, 2010.

[3] Lim, Meng-Hui, and Andrew Beng Jin Teoh, "Discriminative and Non-User Specific Binary Biometric Representation via Linearly-Separable SubCode Encoding-based Discretization", KSII Transactions on Internet & Information Systems 5, no. 2, 2011.

[4] Lim, Meng-Hui, and Andrew Beng Jin Teoh, "An effective biometric discretization approach to extract highly discriminative, informative, and privacy-protective binary representation", EURASIP Journal on Advances in Signal Processing 2011, no. 1, 2011.

[5] Jain, Anil K., Karthik Nandakumar, and Arun Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities", Pattern Recognition Letters 79: 80-105, 2016.

[6] Lim, Meng-Hui, Andrew Beng Jin Teoh, and Kar-Ann Toh, "An efficient dynamic reliability-dependent bit allocation for biometric discretization", Pattern Recognition 45, no. 5: 1960-1971, 2012.

[7] Sadkhan, Eng Sattar B., Baheeja K. Al-Shukur, and Ali K. Mattar, "Survey of biometrie based key generation to enhance security of cryptosystems", In Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA), pp. 1-6, IEEE, 2016.

[8] Rathgeb, Christian, and Andreas Uhl, "Context-based biometric key generation for Iris", IET computer vision 5, no. 6: 389-397, 2011.

[9] Scheuermann, Dirk, Bastian Wolfgruber, and Olaf Henniger, "On biometric key generation from handwritten signatures ", BIOSIG 11: 103-114, 2011.

[10] Makrushin, Andrey, Tobias Scheidat, and Claus Vielhauer, "Improving reliability of biometric hash generation through the selection of dynamic handwriting features", In Transactions on Data Hiding and Multimedia Security VIII, pp. 19-41, Springer Berlin Heidelberg, 2012.

[11] Sheng, Weiguo, Gareth Howells, Michael Fairhurst, Farzin Deravi, and Shengyong Chen, "Reliable and secure encryption key generation from fingerprints", Information Management & Computer Security 20, no. 3: 207-221, 2012.

[12] Chin, Yong Jian, Thian Song Ong, Andrew Beng Jin Teoh, and K. O. M. Goh, "Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion", Information Fusion 18 (2014): 161-174, 2014.

[13] Šeděnka, Jaroslav, Kiran S. Balagani, Vir Phoha, and Paolo Gasti, "Privacy-preserving population-enhanced biometric key generation from free-text keystroke dynamics", In Biometrics (IJCB), 2014 IEEE International Joint Conference on, pp. 1-8. IEEE, 2014.

[14] Sheng, Weiguo, Shengyong Chen, Gang Xiao, Jiafa Mao, and Yujun Zheng, "A biometric key generation method based on semisupervised data clustering", IEEE Transactions on Systems, Man, and Cybernetics: Systems 45, no. 9 (2015): 1205-1217, 2015.

[15] Sim, Terence, Simon Baker, and Maan Bsat, "The CMU pose, illumination, and expression (PIE) database", In Automatic Face and Gesture Recognition, 2002. Proceedings. Fifth IEEE International Conference on, pp. 53-58. IEEE, 2002.

[16] Phillips, P. Jonathon, Patrick J. Flynn, Todd Scruggs, Kevin W. Bowyer, Jin Chang, Kevin Hoffman, Joe Marques, Jaesik Min, and William Worek, "Overview of the face recognition grand challenge", In IEEE computer society

conference on Computer vision and pattern recognition. CVPR 2005, vol. 1, pp. 947-954. IEEE, 2005.

[17] "ITDv1 Database", (Online) Available from:(http://www4.comp.polyu.edu.hk/~csajaykr/IITD/Database_Iris.htm), 2007.

[18] "CASIA-IrisV3 Database", (Online) Available from:(http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp), 2010.

[19] "CASIA Database", (Online) Available from:(http://www.sinobiometrics.com), 2004.

[20] Maio, Dario, Davide Maltoni, Raffaele Cappelli, James L. Wayman, and Anil K. Jain, "FVC2002: Second fingerprint verification competition", In . Proceedings 16th international conference on Pattern recognition, 2002, vol. 3, pp. 811-814. IEEE, 2002.

[21] Maio, Dario, Davide Maltoni, Raffaele Cappelli, Jim L. Wayman, and Anil K. Jain, "FVC2004: Third fingerprint verification competition", In Biometric Authentication, pp. 1-7. Springer Berlin Heidelberg, 2004.

[22] Hiew, Bee Yan, Andrew BJ Teoh, and Ying-Han Pang, "Touch-less fingerprint recognition system", In 2007 IEEE Workshop on Automatic Identification Advanced Technologies, pp. 24-29. IEEE, 2007.

[23] Zhang, D, "PolyU palmprint database", Biometric Research Centre, Hong Kong Polytechnic University,(Online) Available from:(http://www. comp. polyu. edu. hk/~biometrics/), 2009.

[24] Goh, Michael KO, Tee Connie, Andrew BJ Teoh, and David CL Ngo, "A fast palm print verification system", In 2006 International Conference on Computer Graphics, Imaging and Visualisation, pp. 168-172. IEEE, 2006.

[25] Fairhurst, Michael, Sanaul Hoque, Gareth Howells, and Farzin Deravi, "Evaluating biometric encryption key generation", In Proc. 3rd Cost 275 Workshop Biometrics Internet, pp. 93-96. 2005.

[26] Mari□o, R. □lvarez, F. Hern□ndez □lvarez, and L. Hern□ndez Encinas, "A crypto-biometric scheme based on iris-templates with fuzzy extractors", Journal of Information Sciences 195 (2012): 91-102.

[27] Jain, Anil K., Karthik Nandakumar, and Abhishek Nagar, "Biometric template security", EURASIP Journal on advances in signal processing, 2008.

[28] Cavoukian, Ann, Alex Stoianov, and Fred Carter, "Keynote paper: biometric encryption: technology for strong authentication, security and privacy", In Policies and research in identity management, pp. 57-77. Springer US, 2008.

[29] Boyen, Xavier, "Reusable cryptographic fuzzy extractors", In Proceedings of the 11th ACM conference on Computer and communications security, pp. 82-91, ACM, 2004.

[30] Dodis, Yevgeniy, Leonid Reyzin, and Adam Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data", In International conference on the theory and applications of cryptographic techniques, pp. 523-540. Springer Berlin Heidelberg, 2004.

[31] Dodis, Yevgeniy, Leonid Reyzin, and Adam Smith, "Fuzzy Extractors-A Brief Survey of Results from 2004 to 2006", 2008.

[32] Natgunanathan, Iynkaran, Abid Mehmood, Yong Xiang, Gleb Beliakov, and John Yearwood, "Protection of privacy in biometric data", IEEE access 4 (2016): 880-892, 2016.

[33] Juels, Ari, and Martin Wattenberg, "A fuzzy commitment scheme", In Proceedings of the 6th ACM conference on Computer and communications security, pp. 28-36. ACM, 1999.

[34] O'Gorman, Lawrence, "Comparing passwords, tokens, and biometrics for user authentication", Proceedings of the IEEE 91, no. 12 (2003): 2021-2040, 2013.

[35] Morelos-Zaragoza, Robert H, "The art of error correcting coding", John Wiley & Sons, 2006.

[36] Breebaart, Jeroen, Bian Yang, Ileana Buhan-Dulman, and Christoph Busch, "Biometric template protection", Datenschutz und Datensicherheit-DuD 33, no. 5 (2009): 299-304, 2009.

[37] E. Bingham, and H. Mannila, "Random projection in dimensionality reduction: applications to image and text data", In Proceedings of the seventh ACM SIGKDD international conference on Knowledge discovery and data mining, pp. 245-250. ACM, 2001.

[38] Belhumeur, Peter N., Jo□o P. Hespanha, and David J. Kriegman, "Eigenfaces vs. fisherfaces: Recognition using

class specific linear projection", IEEE Transactions on pattern analysis and machine intelligence 19, no. 7 (1997): pp. 711-720, 1997

[39] Jiang, Xudong, Bappaditya Mandal, and Alex Kot, "Eigenfeature regularization and extraction in face recognition", IEEE Transactions on Pattern Analysis and Machine Intelligence 30, no. 3 (2008): pp. 383-394, 2008

[40] Chin, Yong Jian, Thian Song Ong, Andrew Beng Jin Teoh, and Michael KO Goh, "Multimodal biometrics based bit extraction method for template security", In 2011 6th IEEE Conference on Industrial Electronics and Applications (ICIEA), pp. 1971-1976. IEEE, 2011.

[41] Choi Se Ill, "A Study on the Future of eCommerce Systems", Smart Media Journal, vol.4, no.3, pp.68-73, 2015.

[42] Lee Jongsu, Hwang Eunhan, Song Sangseob, "LDPC Generation and Decoding concatenated to Viterbi Decoder based on Sytematic Convolutional Encoder", Smart Media Journal, v.2, no.2, pp.39-43, 2013.

Authors

Tran Ha Lam

Received the B.S. degrees in Information Technology from Ho Chi Minh University of Science in 2012.
During 2012-2015, he works as Teacher Assistant in Information Technology Faculty of Ho Chi Minh University of Science. He is currently studying for his MS Degree in School of Electronics and Computer Engineering, Chonnam National University, South Korea.

Deokjai Choi

Received BS degree in Department of Computer Engineering, Seoul National University, in 1982. He got MS degree in Department of Computer Science, KAIST, South Korea in 1984. He got PhD degree in Department of Computer Science and Telecommunications, University of MissouriKansas City, USA in 1995. He is currently Full Professor in the School of Electronics and Computer Engineering at the Chonnam National University, South Korea.