A Novel Two-Stage Approach in Rectifying BioHash's Problem under Stolen Token Scenario

Meng-Hui Lim, MinYi Jeong and Andrew Beng Jin Teoh, *Member, KIMICS*

***Abstract*—Over recent years, much research attention has been devoted to a two-factor authentication mechanism which integrates both tokenized pseudorandom numbers with user specific biometric features for biometric verification, known as Biohash. The main advantage of Biohash over sole biometrics is that Biohash is able to achieve a zero equal error rate and provide a clean separation of the genuine and imposter populations, thereby allowing elimination of false accept rates without imperiling the false reject rates. Nonetheless, when the token of a user is compromised, the recognition performance of a biometric system drops drastically. As such, a few solutions have been proposed to improve the degraded performance but such improvements appear to be insignificant. In this paper, we investigate and pinpoint the basis of such deterioration. Subsequently, we propose a two-level approach by utilizing strong inner products and fuzzy logic weighting strategies accordingly to increase the original performance of Biohash under this scenario.**

***Index Terms*—BioHash, biometric, security.**

I. INTRODUCTION

CLASSICAL token/password-based authentication methods have been widely deployed over decades to provide users ability for selecting a password freely so that the password can be easily remembered and can be kept secret. In the case where a password is found to be compromised, it can be revoked and reissued conveniently. Such exact knowledge-based authentication method would grant a user access only when a query password perfectly matches an enrolled password. Nevertheless, for applications that desire a high level of security, classic authentication method may not be sufficiently secure. This is because most user-selected passwords probably come from a small subset of the full password space and such weak passwords with low entropy can be easily guessed by an adversary. Besides, if a token is stolen, a system may mistakenly authenticate an imposter who possesses it. In order to eliminate these devastated possibilities, biometric authentication method appears to be a more reliable and promising option. The main advantage of biometric authentication is that it bases recognition on an intrinsic aspect of a human being and the usage of biometric requires the person to be authenticated to be physically present at the point of authentication. Since biometric is inextricably linked to the users themselves, it is impossible for biometric to be lost (token) or forgotten (password).

Despite possessing aforementioned functional advantage, biometric authentication suffers a fatal drawback: it is possible for one's biometric to be compromised and once it is compromised, it will be irrevocable. One notable approach in overcoming such shortcoming is to distort or transform the biometric features intentionally in a repeatable but nonreversible manner to protect sensitive user-specific features [1]. Instead of using the original features for enrolment and verification, the converted features are used. If such a cancellable biometric template happens to be compromised, the distortion characteristics of the same original biometric can be changed and this would map the biometric features to a new template. As outlined by Teoh et al. [6][7], the four principal objectives of a cancellable biometric template include:

- Diversity: The same cancellable template cannot be used in two different applications.
- Reusability: Straightforward revocation and reissue in the event of compromise.
- One-way Transformation: Non-invertibility of template computation to prevent recovery of biometric data.
- Performance: The cancellable biometric template should not deteriorate the recognition performance.

In 2004, Teoh et al. [5] put forward a two-factor authenticator based on iterative inner products between tokenized pseudorandom numbers and user-specific biometric features. The resultant inner product bitstrings is termed as Biohash due to its non-invertibility property. Biohash is cancellable since if it is compromised, it can be revoked and reissued straightforwardly. By renewing the password or seed of the token, the newly converted biometric features will be utterly uncorrelated to the compromised ones since the set of token-generated pseudorandom numbers is random and independent of any other random bit strings. In terms of performance, Biohash is capable of improving recognition efficacy by providing a clean separation between genuine and

Manuscript received March 5, 2010; revised March 17, 2010; accepted April 5, 2010.

Meng-Hui Lim, MinYi Jeong and Andrew Beng Jin Teoh are with the School of Electrical and Electronic Engineering, College of Engineering, Yonsei University, Seoul, South Korea. (Email: menghui.lim@gmail.com, {myjeong, bjteoh}@yonsei.ac.kr)

imposter distributions, which results in zero false accept rate (FAR) and false reject rate (FRR) errors in the recognition performance. In fact, this is almost impossible to be achieved by using merely feature extraction scheme in practical case where FAR and FRR are naturally interdependent.

However, Kong et al. [2] have reported a year later that such claim on perfect accuracy of Biohash's recognition performance appears to be flawed when the token is compromised. By combining different sets of biometric features with the same set of tokenized pseudorandom numbers, their empirical results illustrate that the projected features become less discriminative, causing the recognition performance to drop drastically.

Subsequently, Teoh et al. presented a theoretical analysis of the Biohash technique in [6] using random multispace quantization as an analytic mechanism and justified the performance deterioration under stolen token scenario.

To rectify such a problem, Lumini and Nanni [3] introduced a few ideas by augmenting projection spaces and permute several feature coefficients to improve the degraded performance. However, the enhanced performance is still below the original performance of a recognition system without using Biohash technique.

In this paper, we propose a novel 2-stage approach to eradicate the degradation based on strong inner products utilization and fuzzy logic weighting strategies. The structure of this paper is organized as follows. In the next section, we will elaborate the original Biohash framework. In section III, we will cover a detailed explanation on our proposed countermeasures. In the sequel, we will describe our experiment settings in section IV and present our experimental findings and demonstrate its superiority over the original Biohash scheme in section V. Finally, we conclude this paper in section VI.

II. PRELIMINARIES

The general Biohash framework comprises of three stages, as described in Figure 1:

a) Feature Extraction: Projection of biometric features to a lower-dimensioned and more discriminative feature domain using linear transformation such as Principle Component Analysis (PCA) [8] so as to reduce computational complexity.
b) Inner Product: Projection of biometric features onto multiple random subspaces stems from dot product between biometric features and external input such as tokenized pseudorandom numbers. Note that before inner product operation is performed, orthogonalization of such pseudorandom numbers is required, for example, by applying Gram Schmidt algorithm on row vectors so that a set of orthogonal column vectors can be obtained for inner product operation. The reason of using orthogonal numbers is to render each resultant inner product element to be independent of all others, so that any legitimate variations on an element would not propagate through the preceding or subsequent elements.
c) Threshold Binarization: Quantization of each individual map based on a preset threshold, usually set to 0. Repetition of this procedure in obtaining multiple bits eliminates inter-bit correlations.

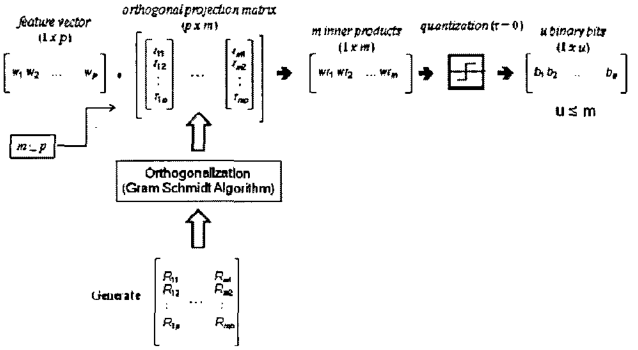


Fig. 1 An overview of Biohash framework.

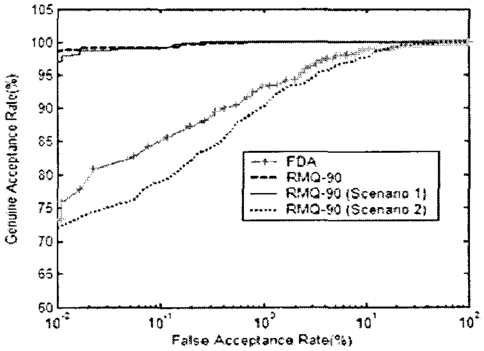


Fig. 2 Comparative Performance of FDA, RMQ-90 and its two compromised scenarios in ROC [6]

However, as token is compromised (refer to Scenario 2 in Figure 2), so does the orthogonal projection matrix, the recognition performance of Random Multispace Quantization (RMQ = Biohash) declines significantly and it becomes slightly poorer than the Fisher Discriminant Analysis (FDA) feature extraction technique, as shown in the comparison of Receiver Operating Curve (ROC) below.

III. RATIONALE OF OUR 2-STAGE APPROACH

A. Inner Product Approach

An inner product of two vectors ĕ and ň is defined as

$$ĕ \cdot ň = |ĕ|*|ň|*\cos\Theta \qquad (1)$$

where $|\breve{e}|$ denotes magnitude of vector $\breve{e}$ and Θ denotes the angle between the two vectors. The resultant value signifies scalar of the component of $\breve{e}$ in the direction of $\breve{n}$ and vice versa. Essentially, an inner product is considered strong when $\Theta \approx 0^\circ$ (both vectors are aligned) whereas an inner product is said to be weak when $\Theta \approx 90^\circ$ (both vectors are orthogonal).

In Biohash, a resultant inner product element may take any positive and negative values uniformly. Since every inner product element is quantized using threshold 0, we conjecture that any elements that take values near 0 are unreliable and should not be used for verification. An intuitive reasoning is that if an inner product element of the vector is weak, any slight legitimate variation in query biometric feature of the same element position may very likely caused a quantization error (since an opposite signed inner product element is likely to be resulted in this case). Therefore, it is clear that weak inner product is less error-tolerant. Intuitively, we can regard the strength of inner product as a reliability measure. The stronger the resulted inner product element is, the more reliable such an element would be. Since the entire elements in an inner product vector are quantized and used for verification regardless of their reliability, this explains the performance deterioration of original Biohash scheme in the less discriminative case where a compromised token is used to project different biometric features onto a common subspace.

Therefore, in this approach, we improve the discrimination of resultant quantized bit vectors by proposing several strategies which utilize strong inner products for verification comparison.

- **Discard strategy**: Based on a discarding threshold α, we discard weak inner product elements of each vector with values below α.
- **Discard and replace strategy**: We generate N inner product vectors by integrating N different orthogonal projection matrixes with the same feature vector. Based on a discarding threshold α, we discard weak inner product elements of the first inner product vector. By treating the first vector as our referenced vector, we iteratively replace as many as possible the discarded inner product elements in the first vector with strong elements (with values above α) from the other N - 1 vectors. Consequently, the resultant (first) inner product vector is used for verification comparison.
- **Weighting strategy**: In spite of discarding, we weight each inner product element according to their strength and the results are concatenated into a weight vector $\boldsymbol{w}$ of the same length as inner product vector during enrolment stage. During the experiment, we investigate several distinct weighting functions, g such as linear, quadratic, square root and a few others, and subsequently select an optimum g that produces the largest EER improvement.

$$\mathbf{IPW}=g(\boldsymbol{w}) \qquad (2)$$

Note that by carrying out this approach, we are also required to maintain an additional weight vector per user which is usually stored in the database. Correspondingly, for verification comparison, we modify the hamming distance computation between two bit sequences to be

$$HD(\boldsymbol{A},\boldsymbol{B})=\mathbf{IPW} * \mathrm{XOR}(\boldsymbol{A},\boldsymbol{B}) \qquad (3)$$

with $HD(\bullet)$ denoting the hamming distance computation, **IPW** denoting the inner product weight vector, $\boldsymbol{A}$ and $\boldsymbol{B}$ denoting two binary bit strings to be matched.

B. Fuzzy Logic Approach

Fuzzy logic is a form of multi-valued logic derived from fuzzy set theory to deal with approximate reasoning. Given imprecise, noisy or incomplete input information, fuzzy logic is able to offer a definite conclusion. Fuzzy logic variables usually range between 0 and 1.

As multiple sets of biometric features of the same class are quantized and converted into binary bit strings, intra-class variation usually exist and it is what we wish to minimize. Since some feature information is lost during each quantization process, the output information becomes incomplete. Each binary string can also be thought as a noisy version of one another. On the other hand, variations in biometric features of distinct classes should be maximized so that the output bit string that represents each user can be made more discriminative. Therefore, to increase the recognition performance, we adopt the concept of fuzzy logic to model intra-class variations as well as inter-class variations in order to provide a reliability measure to each and every binary output bit at the training stage.

B1. Tackling Intra-class Variation:

Suppose that there are n training feature vectors with m elements for each of k distinct classes. After being binarized, we obtain a group of n binary vectors within class j, denoted by $b^j = \{b^j_1, b^j_2, \dots, b^j_n\}$ where the n-th binary vector of class j can be denoted as $b^j_n = \{b^j_{n1}, b^j_{n2} \dots b^j_{nm}\}$ with b^j_{nm} representing the m-th bit of n-th binary vector in class j.

Initially, we average n binary vectors of each of the k classes with respect to their bit locations, $\overline{b^j} = \frac{1}{n}\sum_{i=1}^{n} b^j_i \mid j = 1,2,\dots,k$ and derive a unique weight vector for each of the k classes, $FLW^j = f(\overline{b^j}) \mid j = 1,2,\dots,k$ based on a pre-defined membership function f. Note that in fuzzy logic, a membership function represents the magnitude of each input and assigns an output weight for each of the inputs. To seek for an optimum intra-class membership function, we try out a linear (Intra-Linear) and two quadratic (Intra-Quad1 and Intra-Quad2) membership functions in our simulation, as shown in Figure 3.

Notice that the membership functions in Figure 3 are selected based on the reliability measure. For instance, the 3rd bit position of all n vectors has agreeing binary bits (all '0' or all '1'), yielding an average value of '0' or '1'. Therefore, an input of '0' or '1' to the membership function produces a membership value of '1', indicating that the 3rd bit position is highly reliable since intra-variation of such bit is minimal. In the case where reliability is low, it is easy to see that equal disagreeing bits at a particular bit location of n vectors which yield an average value of 0.5 would produce a membership value of 0.

During the verification comparison, we alter the hamming distance computation between two bit sequences to be

$$HD(A,B) = \mathbf{FLW}^{1} * XOR(A,B) \qquad (4)$$

with *HD* (•) denoting the hamming distance computation, **FLW** denoting the user-specific fuzzy logic weight vector, *A* and *B* denoting two binary bit strings to be matched.

B2. Tackling Inter-class Variation:

In handling inter-class variations, similar operations can be carried out as in deriving intra-class weight vector, except that we average n binary vectors of all j classes according to the following formulation:

$$\bar{b} = \frac{1}{nk}\sum_{i=1}^{n}\sum_{j=1}^{k} b_i^j \qquad (5)$$

Consequently, a global weight vector FLW $= f(\bar{b})$ can be derived. To determine a suitable inter-class membership function, we attempt a linear (Intra-Linear) and two quadratic (Inter-Quad1 and Inter-Quad2) membership functions in our simulation, as shown in Figure 4.

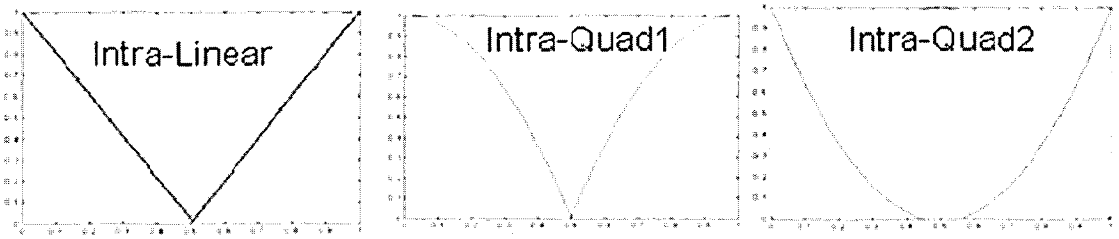
Since our objective is to maximize inter-class variation at each bit location, a suitable membership function would give a membership value of '1' when the average value at a bit position is 0.5.

During the matching process, the hamming distance computation is altered similarly as in Eq. (4).

IV. DATA SET AND EXPERIMENT SETTINGS

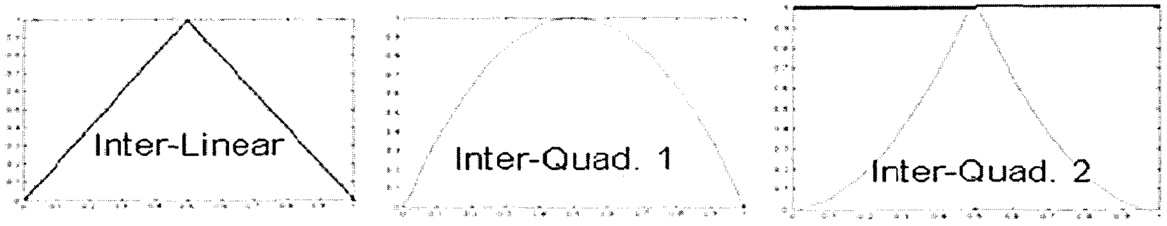
In the experiments, we examine the efficiency of our approach for face recognition on ORL data set [4] by adopting PCA [8] as our face feature extractor. ORL data set contains face images of 40 individuals with 10 images each, yielding a total of 400 images. Out of these 400 images, 200 images (5 samples x 40 individuals) are used for generating eigenvectors and deriving fuzzy logic weight vectors while another 200 images (5 samples x 40 individuals) are used for testing purpose. A total of 200 quantized inner product elements (binary bits) are used in representing each identity.

To generate the imposter distribution (for FAR test), we match the first image of an individual against the first image of all other individuals, resulting in a total of (40×39)/2=780 comparisons. By repeating the same procedure for all other images of an individual, we perform a total of 780 × 5 = 3900 evaluations. On the other hand, in generating the genuine distribution (for



$$f_{IL} = \begin{cases} 1-2x & 0 \le x < 0.5 \\ 2(x-0.5) & 0.5 \le x \le 1 \end{cases} \quad f_{IQ1} = \begin{cases} -4x^2+1 & 0 \le x < 0.5 \\ -4(x-1)^2+1 & 0.5 \le x \le 1 \end{cases} \quad f_{IQ2} = -4(x-0.5)^2 \quad 0 \le x < 1$$

Fig. 3 Intra-class Membership Functions



$$f_{IL} = \begin{cases} 2x & 0 \le x < 0.5 \\ 1-2(x-0.5) & 0.5 \le x \le 1 \end{cases} \quad f_{IQ1} = -4(x-0.5)^2+1 \quad 0 \le x < 1 \quad f_{IQ2} = \begin{cases} 4x^2 & 0 \le x < 0.5 \\ 4(x-1)^2 & 0.5 \le x \le 1 \end{cases}$$

Fig. 4 Inter-class Membership Functions

FRR test), we match the first image against all other images of an individual and repeat this procedure for all other individuals, yielding a total of (5 × 4 ×40)/2=400 computations. By generating both genuine and imposter distributions, we are thus able to compute the equal error rate (ERR) and adopt it as our measure in characterizing the security level of a biometric authentication system. EER refers to the average value of FAR and FRR. The same procedures are repeated 20 times for each of the following experiments. The results are then averaged in order to reduce statistical inconsistencies caused by the employment of different sets of generated pseudorandom numbers.

V. RESULTS AND DISCUSSIONS

The objective of our experiments is to evaluate the performance of our approaches in comparison to that of the original Biohash scheme under the compromised token situation. Experiments 1-3 examine different settings of our strong inner product approach; Experiment 4 examines our fuzzy logic weighting approach.

It is clear from the simulation results that under compromised token assumption, the performance of the original Biohash scheme achieves a slightly lower EER (≈ 0.2%) than the PCA feature extraction scheme alone, which is in contrast to a few results reported in [2][6]. This may be due to different experiment settings such as number of allocated training images and the number of binary bits used to represent an identity.

In experiments 1 and 2 (tables 1 and 2 respectively), we wish to find an optimum discarding threshold, α that would produce the lowest possible EER. Therefore, we conduct a systematic search by using a set of thresholds ranging from 0.025 to 0.5 with a step size of 0.025 for discard strategy and 0.1 to 0.7 with a step size of 0.03 for discard and replace strategy. Note that the choice of discarding threshold is strictly limited. If it is set exceeding a certain threshold, the binarized feature vector may become less discriminative since, insufficient bits will be resulted to represent each identity as a consequence of discarding weak inner product elements, causing recognition performance to drop drastically. This is where the discard & replace strategy is introduced to supplement this deficiency. Note that in experiment 2, N is set to 20, which means that 20 sets of random projection matrixes and thus 20 quantized inner product vectors are generated for implementation of the discard and replace strategy. However, despite our effort, both cases produce rather insignificant EER improvements: 0.2% for discard strategy while 0.1% for discard & replace strategy.

TABLE 1
(EXPERIMENT 1) EER COMPARISON USING DISCARD APPROACH WITH VARIOUS DIFFERENT DISCARDING THRESHOLDS

Method	Discarding Threshold, α	EER (%)		
PCA	-	11.1730		
Biohash	-	3.9069	Discarding Threshold, α	EER (%)
[Stolen Token] Biohash	0	10.9675		
[Stolen Token] Discard Approach	0.025	10.9935	0.275 (Best)	10.7575
	0.050	10.9719	0.300	10.7782
	0.075	10.9457	0.325	10.7802
	0.100	10.9631	0.350	10.7977
	0.125	10.9489	0.375	10.8459
	0.150	10.9033	0.400	10.7964
	0.175	10.9153	0.425	10.8140
	0.200	10.8675	0.450	10.8577
	0.225	10.8803	0.475	10.8895
	0.250	10.8932	0.500	10.8961

TABLE 2
(EXPERIMENT 2) EER COMPARISON USING DISCARD AND REPLACE APPROACH WITH DIFFERENT DISCARDING THRESHOLDS

Method	Discarding Threshold, α	EER (%)		
PCA	-	11.1730		
Biohash	-	3.7616	Discarding Threshold, α	EER (%)
[Stolen Token] Biohash	0	10.9369		
[Stolen Token] Discard and Replace Approach ($N = 20$)	0.13	10.9686	0.43	10.9517
	0.16	10.9786	0.46	10.9779
	0.19	10.9633	0.49	10.9439
	0.22	11.0236	0.52	10.9712
	0.25	11.0539	0.55	11.0210
	0.28	10.8935	0.58	10.9441
	0.31 (Best)	10.8531	0.61	11.0161
	0.34	10.8538	0.64	11.2095
	0.37	10.8689	0.67	11.3234
	0.40	10.8623	0.70	11.5692

In order to further vindicate our strong inner product utilization approach, inner product elements are weighted based on their strength using different weighting functions g before being quantized in experiment 3 (table 3). As a result, **IPW** = $\sqrt[4]{\mathbf{W}}$ gives the lowest EER value among several weighting functions as shown in Table 3, yielding an approximate improvement of 0.7% under stolen token scenario.

TABLE 3
(EXPERIMENT 3). EER COMPARISON USING INNER PRODUCT WEIGHTING WITH DISTINCT WEIGHTING FUNCTIONS

Method	Weighting Function, g	EER (%)
PCA	-	11.1730
Biohash	-	3.9437
[Stolen Token] Biohash	-	10.8993
[Stolen Token] Inner Product Weighting Approach	w^2	14.2181
	w	11.0698
	$\sqrt{w}$	10.2350
	$\sqrt[3]{w}$ (Best)	10.1907
	$\sqrt[4]{w}$	10.2421

In experiment 4 (table 4), it is observed that the first quadratic membership function (Intra-Quad1) modeled for intra-class variation achieves the best performance among all tested membership functions, resulting in an EER enhancement of 0.4. However, the performance of all membership functions modeled for inter-class variations is very close to that of the original Biohash scheme under stolen token scenario, resulting in trivial improvement.

TABLE 4
(EXPERIMENT 4). EER COMPARISON USING FUZZY LOGIC WEIGHTING WITH DISTINCT MEMBERSHIP FUNCTIONS

Method	Membership Function, f	EER
PCA	-	11.1730
Biohash	-	3.9245
[Stolen Token] Biohash	-	10.5507
[Stolen Token] Fuzzy Logic Weighting Approach	Intra-Linear	10.7941
	Intra-Quad1 (Best)	10.1445
	Intra-Quad2	10.2350
	Inter-Linear	10.5574
	Inter-Quad1	10.5525
	Inter-Quad2	10.5704

By integrating the best configuration of the inner product weighting and fuzzy logic weighting approaches, we are able to achieve a total EER improvement of 1.0 as shown in Table 5, which is very close to the sum of the best individual results from Experiment 3 and 4. Note that in our integrated approach, the modified hamming distance computation during the matching process is calculated as

$$HD(A,B) = (\mathbf{FLW}^{j} + \mathbf{IPW}) \times \mathrm{XOR}(A,B) \qquad (6)$$

where $\mathbf{FLW}^j$ denotes the j-th user's fuzzy logic weight vector, **IPW** denotes the inner product weight vector, A and B denoting two binary bit strings to be matched. This enables us to combine both weight vectors in our hamming distance calculation.

VI. CONCLUSIONS

In this paper, we have employed a 2-stage methodology to rectify the degradation problem of Biohash when the token is compromised. In our first approach, we utilize strong inner product elements for matching by

1) discarding weak elements
2) discarding and replacing weak elements
3) weighting inner product elements based on their individual strength

to minimize the quantization error effect caused by weak elements, especially in the case where all different feature vectors are projected onto a common subspace. Subsequently, in our second approach, we further minimize the within-class variations by adopting fuzzy logic weighting strategy to weight every bit of the binary strings in the training data set according to its reliability (probability of occurrence). Empirical results shown that by using appropriate weighting function and membership function respectively, both inner product weighting and fuzzy logic weighting methodologies are capable of achieving some improvement in the system performance. The combination of these two techniques in fact produces the best results with an EER improvement of about 1.0%.

TABLE 5
A GLANCE OF EER IMPROVEMENT USING THE BEST CONFIGURATION OF EACH APPROACH/COMBINATION OF APPROACHES

Strategy					
Discard	Discard & Replace	Inner Product Weighting	Fuzzy Logic Weighting	Best α / Weighting /Membership func.	EER Improvement
Yes	No	No	No	α = 0.275	0.2
No	Yes	No	No	α = 0.31	0.1
No	No	Yes	No	W.func: $FLW^F = \sqrt[3]{w}$	0.7
No	No	No	Yes	M.func: Intra-Quad1	0.4
No	No	Yes	Yes	$\sqrt[3]{w}$ + Intra-Quad	1.0

ACKNOWLEDGMENT

This work was supported by the Korea Science and Engineering Foundation (KOSEF) via the Biometrics Engineering Research Center (BERC) at Yonsei University.(Grant Number: R112002105080020 (2010)).

REFERENCES

[1] R.M. Bolle, J.H. Connel and N.K. Ratha, "Biometric Perils and Patches," Pattern Recognition 35 (2002) pp. 2727-2738.

[2] A. Kong, K.-H. Cheung, D. Zhang, M. Kamel and J. You, "An Analysis of Biohashing and its variants," Pattern Recognition, vol. 39, pp. 1359–1368, 2006.

[3] A. Lumini and L. Nanni, "An Improved Biohashing for Human Authentication," Pattern Recognition, vol. 40, pp. 1057-1065, 2007.

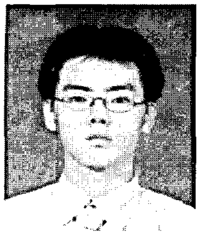
[4] F. Samaria and A. Harter, "Parametrisation of a Stochastic Model for Human Face Identification," 2nd IEEE Workshop on Applications of Computer Vision, pp.138-142, 1994.

[5] A.B.J. Teoh, D.C.L. Ngo and A. Goh, "Biohashing: Two Factor Authentication Featuring Fingerprint Data and Tokenized Random Number," Pattern Recognition, vol. 37, pp. 2245-2255, 2004.

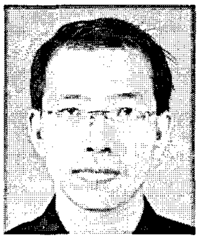
[6] A.B.J. Teoh, A. Goh and D.C.L. Ngo, "Random Multispace Quantization as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs," IEEE transactions on Pattern Analysis and Machine Intelligence, vol. 28, no. 12, 2006.

[7] A.B.J. Teoh and C.T. Yuang, "Cancelable Biometrics Realization with Multispace Random Projections," IEEE Transactions on Systems, Man, and Cybernetics – Part B: Cybernetics, vol. 37, no. 5, 2007.

[8] M. Turk and A. Pentland, "Eigenfaces for Recognition, Journal of Cognitive," Neuroscience, vol. 3, no. 1, pp. 71-86, 1991.



Meng-Hui Lim obtained his BEng in 2006 from Multimedia University in Malaysia and MEng degree in 2009 from Dongseo University in Korea. He is currently a Ph.D. student in EE Department, College Engineering of Yonsei University, South Korea. His research interests include cryptography, key establishment protocols, biometric security and biometric discretization.



Andrew Beng Jin Teoh obtained his BEng (Electronic) in 1999 and Ph.D degree in 2003 from National University of Malaysia. He is currently an assistant professor in EE Department, College Engineering of Yonsei University, South Korea. His research interest is in biometrics security and pattern recognition. He had published around 160 international journal and conference papers in his area.

MinYi Jeong received B.S. degree in Information and Communication Engineering from the Sejong University, in Seoul, Korea, in 2005, and her M.S. degree in Graduate Program in Biometrics from Yonsei University, in Seoul, Korea, in 2007. And she is a Ph.D. course student in Yonsei University from 2007. Her research interests are in computer vision, pattern recognition, image processing, and biometrics.