An Analysis of BioHashing and Its Variants

[1,2]**Adams Kong,** [1]**King-Hong Cheung,** [1]**David Zhang,**
[2]**Mohamed Kamel** and [1]**Jane You**

[1]Biometrics Research Centre
Department of Computing
The Hong Kong Polytechnic University
Hung Hom, Kowloon, Hong Kong

[2]Pattern Analysis and Machine Intelligence Lab
University of Waterloo,
200 University Avenue West, Ontario, Canada

Corresponding author:

Dr Jane You

Biometrics Research Centre

Department of Computing

The Hong Kong Polytechnic University

Hung Hom, Kowloon, Hong Kong

Phone: (852) 2766-7293

Fax: (852) 2774-0842

E-mail: csyjia@comp.polyu.edu.hk

Abstract — As a result of the growing demand for accurate and reliable personal authentication, biometric recognition, a substitute for or complement to existing authentication technologies, has attracted considerable attention. It has recently been reported that, along with its variants, BioHashing, a new technique that combines biometric features and a tokenized (pseudo-) random number (TRN), has achieved perfect accuracy, having zero equal error rates (EER) for faces, fingerprints and palmprints. There are, however, anomalies in this approach. These are identified in this paper, in which we systematically analyze the details of the approach and conclude that the claim of having achieved a zero EER is based upon an impractical hidden assumption. We simulate the claimants' experiments and find that it is not possible to achieve their reported performance without the hidden assumption and that, indeed, the results are worse than when using the biometric alone.

Keywords: BioHashing, FaceHashing, PalmHashing, biometrics, verification, security, user identity, password.

1. Introduction

Accurate automatic personal authentication systems, which have been deployed in

many applications including access control, computer login and e-commerce for protecting our lives, physical properties and digital information, are essential for many security systems. There are two classical personal authentication approaches [1, 2]: token based approach, which relies on physical items such as smart cards, physical keys and passports and knowledge based approach which replies on private knowledge such as passwords. Both of these approaches have their limitations: it is possible for both “tokens” and “knowledge” to be forgotten, lost, stolen, or duplicated. Further, authorized users may share their “knowledge” and “tokens” with unauthorized users. These limitations do not apply to biometric means of authentication, which identify a person based on physiological characteristics, such as the iris, fingerprint, face or palmprint, and/or by behavioral characteristics, such as a person’s signature or gait [1].

Although biometric authentication has several inherent advantages over the classical approaches, all of biometric verification systems make two types of errors [2]: 1) misrecognizing measurements from two different persons to be from the same person, called false acceptance and 2) misrecognizing measurements from the same person to be from two different persons, called false rejection. The performance of a biometric system is commonly described by its false acceptance rate (FAR) and false rejection rate (FRR). These two measurements can be controlled by adjusting a threshold, but it is not

possible to exploit this threshold by simultaneously reducing FAR and FRR. FAR and FRR must be traded-off, as reducing FAR increases FRR and vice versa. Another important performance index of a biometric system is its equal error rate (EER) defined as at the point where FAR and FRR are equal. A perfect system in terms of accuracy would have EER of zero. Unfortunately, however, over thirty years' investigation, a perfect biometric verification system has not been developed. Numerous biometric researchers thus continue to work in this area, looking for new biometrics, developing new feature representations and matching methods and combining the existing techniques [3-9].

Recently, a group of researchers proposed a new personal authentication approach called BioHashing [10] (and its variants [11-17]) that combines a tokenized (pseudo-) random number (TRN) and biometric features. The authors reported zero EERs for faces, fingerprints and palmprints and demonstrated that BioHashing does not rely on specific biometrics, advanced feature representations or complex classifiers. Even with Fisher discrimination analysis for face recognition, BioHashing can still achieve perfect accuracy [13]. The authors say [10] that "The BioHashing has significant functional advantages over solely biometrics i.e. zero equal error rate point and clean separation of the genuine and impostor populations, thereby allowing elimination of false accept rates

without suffering from increased occurrence of false reject rates". In addition, they also mention [11] that "the proposed PalmHashing technique is able to produce zero equal error rate (EER) and yields clean separation of the genuine and impostor populations. Hence, the false acceptance rate (FAR) can be eliminated without suffering from the increased occurrence of the false rejection rate (FRR)". In general, a result of zero EER is the ultimate goal but it is extremely hard to achieve if not impossible. Naturally, reports of such impressive results and claims of perfection aroused our interest and motivated this further study.

This paper is organized as follows. Section 2 presents a general review of biometric verification systems. Section 3, highlights the details of the Biohashing approach. Section 4, provides a comprehensive analysis of this approach and Section 5 reports the results of our simulation tests. Section 6 offers our conclusions.

2. An Overview of Biometric Verification System

In this paper, we concentrate on biometric systems for verification tasks in which BioHashing and its variants are operated. Fig. 1 illustrates the operation flow of such biometric systems. To validate the user's claimed identity, verification systems conduct one-to-one comparison using two pieces of information: a claimed identity and

biometric data. The input biometric data is compared with biometric templates associated with the claimed identity in a given database. Generally speaking, user identities can be inputted via various devices such as keypads and smart card readers and should be unique to each person, like a primary key in a database. It should be noted that user identities in such forms can be shared, lost, forgotten and duplicated, just like the keys/cards of token-based and the PINs/passwords of knowledge-based authentication systems. Nonetheless, because biometric authentication is also required, to pass through the verification system requires more than the mere possession of a valid user identity i.e. an impostor cannot gain access unless the input biometric data matches the template of the claimed identity. We have to emphasize here that the performance of a biometric verification system should not depend solely on user identity or its equivalent and therefore, many biometric systems accept obvious user identities such as personal names.

A biometric verification system has five possible input combinations. For the sake of convenience, we use the notation $\{I, B\}$ to represent the pair-wise information, a claimed user identity I and its associated biometric data B. A registered user X stores his/her user identity and biometric template, $\{I_X, B_{XD}\}$, in a database after enrollment. Suppose user X provides his/her user identity and biometric data, $\{I_X, B_{XV}\}$ at the time of

verification. Even though B_{XD} and B_{XV} are from the same person, because of various noises, they are not identical. We also assume that an impostor *Y*, an unregistered person has an invalid user identity I_Y (which may have been obtained by, for example guessing) and biometric data B_{YV}.

Case 1 $\{I_X, B_{XV}\}$ vs. $\{I_X, B_{XD}\}$

User *X* inputs his/her user identity and biometric data $\{I_X, B_{XV}\}$ to the system to compare $\{I_X, B_{XD}\}$ in the database. The system would compare B_{XD} and B_{XV} and give a matching score. From this matching score, there are two possible responses: either "correct acceptance" or "false rejection".

Case 2 $\{I_X, B_{YV}\}$ vs. $\{I_X, B_{XD}\}$

Assume an impostor *Y* has the user identity of *X* and inputs *X*'s identity together with his/her biometric $\{I_X, B_{YV}\}$ to the system. The input will then be compared with $\{I_X, B_{XD}\}$ in the database. As Case 1, we have two possible responses, "false acceptance" and "correct rejection".

Case 3$\{I_Y, B_{YV}\}$

An impostor *Y* provides his/her user (invalid) identity and biometric data to the system. Since the user identity, I_Y, does not match any identity in the system, the system

simply rejects the user without error and will not attempt to match any biometric information.

Case 4 $\{I_{\sim X}, B_{XV}\}$

A registered user X inputs a wrong user identity $I_{\sim X}$, i.e. not his/her valid user identity, I_X. If $I_{\sim X}$. is a valid user identity, the system would output its decision based on matching the biometric information and the threshold, $\{I_{\sim X}, B_{XV}\}$ vs. $\{I_{\sim X}, B_{\sim XD}\}$, as in Case 2. If $I_{\sim X}$. is an invalid user identity, the system would simply reject the user, as in Case 3.

Case 5 $\{NULL, B_{XV}\}$ OR $\{NULL, B_{YV}\}$

No matter who operates the verification system, a registered user or an unregistered user, a user identity is required. A biometric verification system cannot operate without user identities, i.e. NULL. It would also be unreasonable to assign a temporary user identity to any user who did not provide a user identity at the time of verification.

From these analyses, we conclude the following: Case 5 is invalid; and testing a verification system on Case 3 produces trivial rejection; and Case 4 can be resolved to be either Case 2 or Case 3 depending on the user identity provided. As it happens, to evaluate the performance of a verification system, all biometric researchers assume a

situation in which impostors have obtained a valid user identity. Performance evaluation for genuine distributions are estimated using the matching scores from Case 1, for impostor distributions, those from Case 2.

If “knowledge” or “token” representing the user identity in verification would not be forgotten, lost or stolen, it made the introduction of biometric system less meaningful except for guarding against multiple users using the same identity through sharing or duplicating “knowledge” or “token”. If, further, “knowledge” or “token” would not be shared or duplicated, introducing biometrics became meaningless.

3. BioHashing

3.1 Summary of BioHashing

Fig. 2 illustrates two major processes in BioHashing and its variants [10-17]: biometric feature extraction and discretization. The process of extraction, shown on the right hand side of the figure includes signal acquisition, preprocessing and feature extraction, just as general biometric verification systems. Different biometric signals exploit different techniques in the first process but the focus of our analysis is discretization, the secret of BioHashing, consisting of four steps. Here, we review the most-reported discretization method used in [10-12, 14-17], while another method has

been reported which differs by thresholding and selection of basis forming TRN [13]. Discretization is conducted in four steps.

1) Employ the input token to generate a set of pseudo-random vectors, $\{r_i \in \Re^M \mid i = 1,.....,m\}$ based on a seed.

2) Apply the Gram-Schmidt process to $\{r_i \in \Re^M \mid i = 1,.....,m\}$ and thus obtain TRN, a set of orthonormal vectors $\{p_i \in \Re^M \mid i = 1,.....,m\}$.

3) Calculate the dot product of ***v,*** the feature vector obtained from Step 1 and each orthnonormal vector in TRN, $\boldsymbol{p_i}$, such that $\langle v,\ p_i \rangle$.

4) Use a threshold τ to obtain BioCode, ***b*** whose elements are defined as

$$b_i = \begin{cases} 0 & if \quad \langle v, p_i \rangle \le \tau \\ 1 & if \quad \langle v, p_i \rangle > \tau \end{cases},$$

where *i* is between 1 and *m*, the dimensionality of ***b***. Two BioCodes are compared by hamming distance.

3.2 Implementation of BioHashing

In order to have a better understanding of BioHashing and its variants, we decided to re-implement one of the variants, FaceHashing [12-15], as a demonstration. We have taken face images as our input biometrics since face recognition is a well known hard

problem, which has attracted considerable attention over ten years. A publicly available face database, the AR face database[18] from Purdue University, and a well known feature extraction technique, Principal Component Analysis (PCA), also called Eigenface for face recognition [19-20] are chosen for this demonstration so that all the results reported in this paper are reproducible. We do not employ other effective face recognition algorithms and other accurate biometrics such as fingerprint for this demonstration so that readers can clearly observe the performance differences due to the unrealistic assumption.

The AR face database contains over 4,000 color frontal still images obtained in 2 sessions (with 14 days apart between the 2 sessions) from 126 subjects (70 men and 56 women). In each session, 13 images were taken from each subject in an indoor environment; however, each of the 13 images is taken under various conditions: different facial expressions, illumination settings or occlusions (sunglasses and scarves). There were no limitations on the participant's clothes, make-up, ornaments or hair styles. [19]

The original AR database images are made up of raw, 768×576 colour images. We have converted these into 192×144 gray scale images. Since there is only one face per image and the face is roughly located at the center of the image, no face detection is

performed. The face subimages for feature extraction are 96×96 in size and were cropped from the central canvas of a gray scale face image. Since we are only doing a demonstration to facilitate our analysis and discussion, 50 subjects were randomly selected from the face database. Eight images of each subject were selected, four from each session. The facial expression in the four images from each session is neutral but the illuminations vary. Fig. 3 shows a set of sample images of a subject used in our demonstration; Figs. 3(a)-(d) are taken from the first session and Figs. 3(e)-(d) are taken from the second session.

The four images from the first session were used to determine the principal components and were stored in the database as gallery images. The four images from the second session were then used as query images to match against gallery images. This is known as matching “duplicates” [19].

Although we demonstrate here only FaceHashing, it does not lose any generality to analyze BioHashing and its variants. In this test, we first selected two hundred Principal Components in order to generate BioCode with different dimensions for our analysis. Table 1 lists the dimensions of the BioCode and the corresponding thresholds (τ) according to the deduction of made in [11, 14]. Each subject has a unique TRN and the same TRN is used for different dimensions of the BioCode under consideration.

3.3 Experimental Results

We simulated FaceHashing [12-15] with different dimensions of BioCode and their performances are reported in the form of Receiver Operating Characteristic (ROC) curves as a plot of the genuine acceptance rates (GAR) against the false acceptance rates (FAR) for all possible operating points in the first column of Fig. 4, i.e. (a), (c), (e), (g) and (i). It can be seen that as the BioCodes increase in dimensionality, the EERs gradually decrease to zero. Fig. 5 (a), (c), (e), (g) and (i) shows the corresponding genuine and imposter distributions. Here, as the BioCodes increase in dimensionality, the gap between the two distribution increases. The results of our demonstration are inline with the reported results. As in their reported results [10-17], it was possible to achieve zero EER when the dimensions of BioCode are large enough, for example, 100 or above.

4. Analysis of BioHashing

4.1 The Condition of zero EER

In Section 3, we demonstrated the “power” of FaceHashing, a variant of BioHashing, in achieving zero EER, as claimed in their published papers [10-17]. Obviously, the

high performance of BioHashing is resulted from the TRN, not from the biometric features. In our demonstration, we are able to obtain a zero EER by applying only a simple feature extraction approach, PCA, but in general, even with advanced classifiers, such as support vector machines, PCA is impossible to yield 100% accuracy along with zero EER.

The outstanding performance reported in [10-17] is based on the use of TRN's. In [10-14], the authors mentioned that a unique seed among different persons and applications is used to calculate the TRN such that 1) the seed and thus the TRN for each user used in enrollment and verification is the same; 2) different users (and applications) have different seeds and thus different TRNs. In other words, the seed and TRN are unique across users as well as applications. They also pointed out that the seed for calculating the TRN can be stored in a USB token or smart card. Comparing the properties of the seed in BioHashing (and its variants) and the user identity of a biometric verification system as described in Section 2, it is obvious that the seed, and thus the TRN can serve as a user identity. As the seed is stored in a physical media, TRN also suffers from the problems of "token", e.g. they can be lost, stolen, shared and duplicated.

The TRN has a central role in BioHashing and its variants and is requisite for

achieving zero EER. The authors assume that no impostor has the valid seed/TRN. That is, they assume that the "token" will not be lost, stolen, shared and duplicated. If their assumption is true, introducing any biometric becomes meaningless since the system can rely solely on the "tokens" without any risk. Undoubtedly, their assumption does not hold in general. In their experiments, they determine the genuine distribution using, in our notation, Case 1. However, they determine the impostor distribution using Case 3 in which no biometric should be involved because of the mismatch of with the "pseudo user identity", the seed/TRN.

4.2 The True Performance of BioHashing

To establish the true performance of BioHashing and its variants, we reran the demonstration again under the assumption that impostors have valid TRNs, just as the general practice of evaluating a biometric verification system. In our notation, Cases 1 and 2 are for genuine and imposter distributions, respectively. Fig. 4 (b), (d), (f), (h) and (j) show the performance in the form of ROC curves for each dimension of BioCode tested in Section 3 and their corresponding genuine and imposter distributions are shown in Fig. 5 (b), (d), (f), (h) and (j). In contrast with the reports in [10-17], it is clear that the performance is far from perfect. For ease of comparison, Fig. 6 provides an

integrated plot of the ROC curves shown in Fig. 4. The solid line without any marker is the ROC curve when using PCA and Euclidean distance. The dashed lines with markers are the ROC curves when assuming no loss of user identity/token/smart card. The dotted lines with markers are the ROC curves when using the general assumption for evaluating a biometric verification system. It can be seen that the true performance of BioCode is even worse than that of using PCA and Euclidean distance since BioHashing uses a random projection, which does not serve for any objective function.

5. Conclusion

After reviewing the key concepts and components of a biometric verification system, we have revealed that the outstanding achievements of BioHashing and its variants, zero EER are under a hidden and unpractical assumption — that the TRN would never be lost, stolen, shared or duplicated that does not hold generally. We also point out that if this assumption held, there would be no need for biometrics to combine the TRN since the TRN could serve as a perfect password. To further support our argument, we used a public face database and PCA to simulate their experiments. It is possible to achieve a zero EER by using the combination of a TRN and a biometric under their assumption. Adopting an assumption generally used in the biometric community, our experimental

results show that the true performance of BioHashing is far from perfect.

REFERENCES

[1] A. Jain, R. Bolle and S. Pankanti (eds.), *Biometrics: Personal Identification in Networked Society*, Boston, Mass: Kluwer Academic Publishers, 1999.

[2] 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.

[3] R. Chellappa, C.L. Wilson and A. Sirohey, "Human and machine recognition of faces: A survey", *Proceedings of the IEEE*, vol. 83, no. 5, pp. 705-740, 1995.

[4] B. Bhanu and X. Tan, "Fingerprint indexing based on novel features of minutiae triplets", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 5, pp. 616-622, 2003.

[5] A. Jain, L. Hong and R. Bolle, "On-line fingerprint verification", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 19, no. 4, pp. 302-314, 1997.

[6] D. Zhang, W.K. Kong, J. You and M. Wong, "On-line palmprint identification", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 9, pp. 1041-1050, 2003.

[7] J.O. Kim, W. Lee, J. Hwang, K.S. Baik and C.H. Chung, "Lip print recognition for security systems by multi-resolution architecture", *Future Generation Computer Systems*, vol. 20, pp. 295-301, 2004.

[8] A. Ross and A.K. Jain, "Information Fusion in Biometrics", *Pattern Recognition Letters*, vol. 24, no. 13, pp. 2115-2125, 2003.

[9] S.A. Israel, J.M. Irvine, A. Cheng, M.D. Wiederhold and B.K. Wiederhold, "ECG to identify individuals", *Pattern Recognition*, vol. 38, 133-142, 2005.

[10] A.B.J. Teoh, D.C.L Ngo and A. Goh, "BioHashing: two factor authentication featuring fingerprint data and tokenised random number", *Pattern Recognition*, vol. 37, pp. 2245-2255, 2004.

[11] T. Connie, A. Teoh, M. Goh and D. Ngo, “PalmHashing: A Novel Approach for Dual-Factor Authentication”, *Pattern Analysis and Application*, vol 7, no. 3, pp. 255-268.

[12] D.C.L. Ngo, A.B.J. Teoh and A. Goh, “Eigenspace-based face hashing”, *in Proc. of International Conference on Biometric Authentication (ICBA),* pp. 195-199, Hong Kong, July 2004.

[13] A.B.J. Teoh, D.C.L. Ngo and A. Goh, “An integrated dual factor authenticator based on the face data and tokenised random number”, *in Proc. of International Conference on Biometric Authentication (ICBA)*, pp. 117-123, Hong Kong, July 2004.

[14] A.B.J. Teoh, D.C.L. Ngo and A. Goh, “Personalised cryptographic key generation based on FaceHashing”, *Computers and Security Journal*, vol. 23, no. 7, pp. 606-614, 2004.

[15] A.B.J. Teoh and D.C.L. Ngo, “Cancellable biometrics featuring with tokenized random number”, To appear in *Pattern Recognition Letters*.*

[16] Y.H. Pang, A.B.J Teoh and D.C.L. Ngo, “Palmprint based cancelable biometric authentication system”, *International Journal of Signal Processing*, vol. 1, no. 2, pp. 98-104, 2004.*

[17] T. Connie, A. Teoh, M. Goh and D. Ngo, “PalmHashing: a novel approach to cancelable biometrics”, *Information Processing Letter*, vol. 93, no. 1, pp. 1-5, 2005.*

[18] A.M. Martinez, and R. Benavente, “The AR face database”, CVC Tech. Report #24, 1998. see also: http://rvl1.ecn.purdue.edu/~aleix/aleix_face_DB.html

[19] A.M. Martinez, and A.C. Kak, “PCA versus LDA”, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 23, no. 2, pp. 228-233, 2001.

[20] M. Turk, and A. Pentland, “Eigenfaces for recognition”, *Journal of Cognitive Neuroscience*, vol. 3, pp. 71-86, 1991.

[12-13] In: Zhang, D., Jain, A.K. (eds.): Biometric Authentication. Lecture Notes in Computer Science, Vol. 3072. Springer-Verlag, Berlin Heidelberg NewYork (2004)

* [15-17] are obtained from A.B.J Teoh

Figures:

Tables:

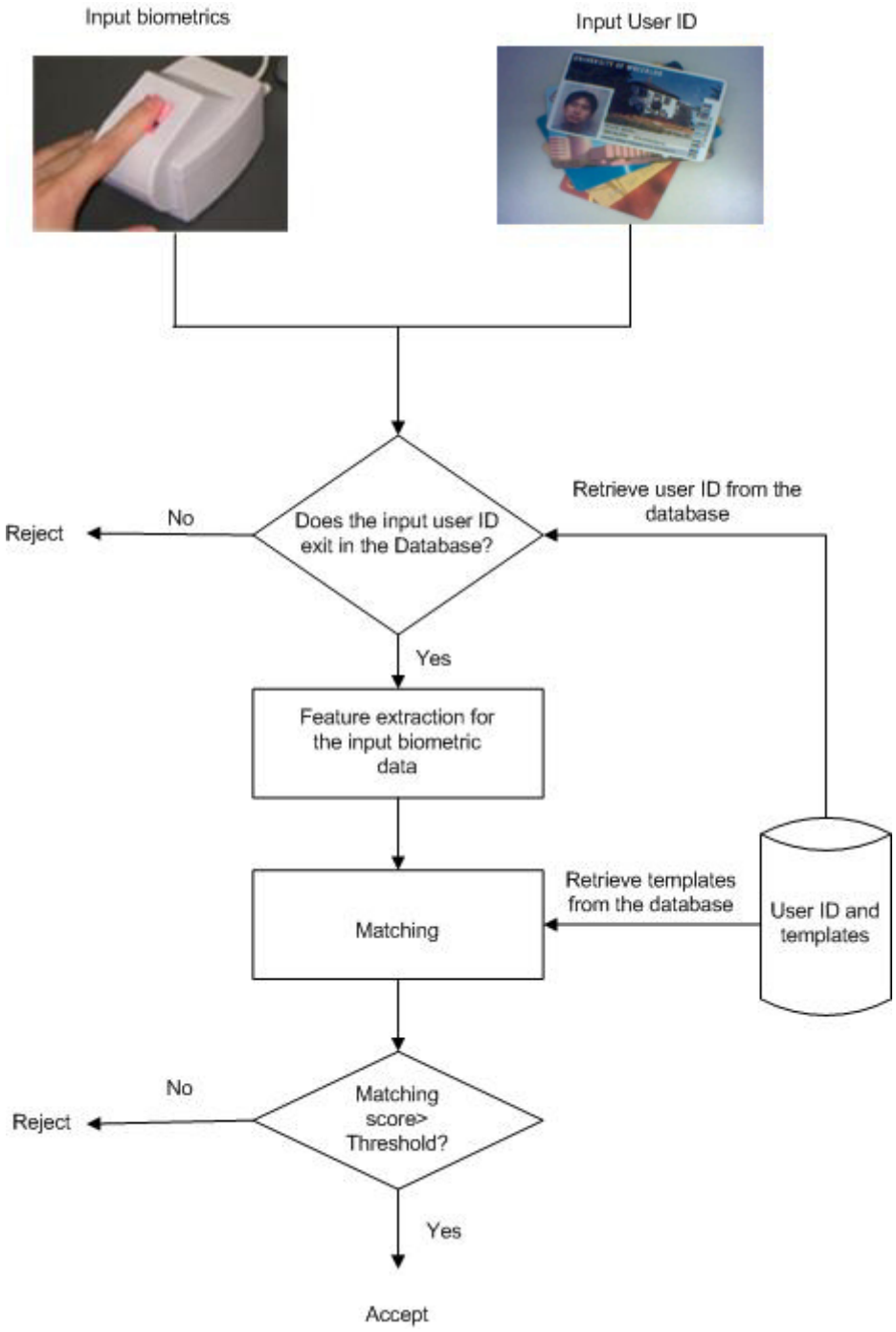

Input biometrics
Input User ID
Does the input user ID exit in the Database?
No
Reject
Retrieve user ID from the database
Yes
Feature extraction for the input biometric data
Matching
Retrieve templates from the database
User ID and templates
Matching score> Threshold?
No
Reject
Yes
Accept

Fig. 1

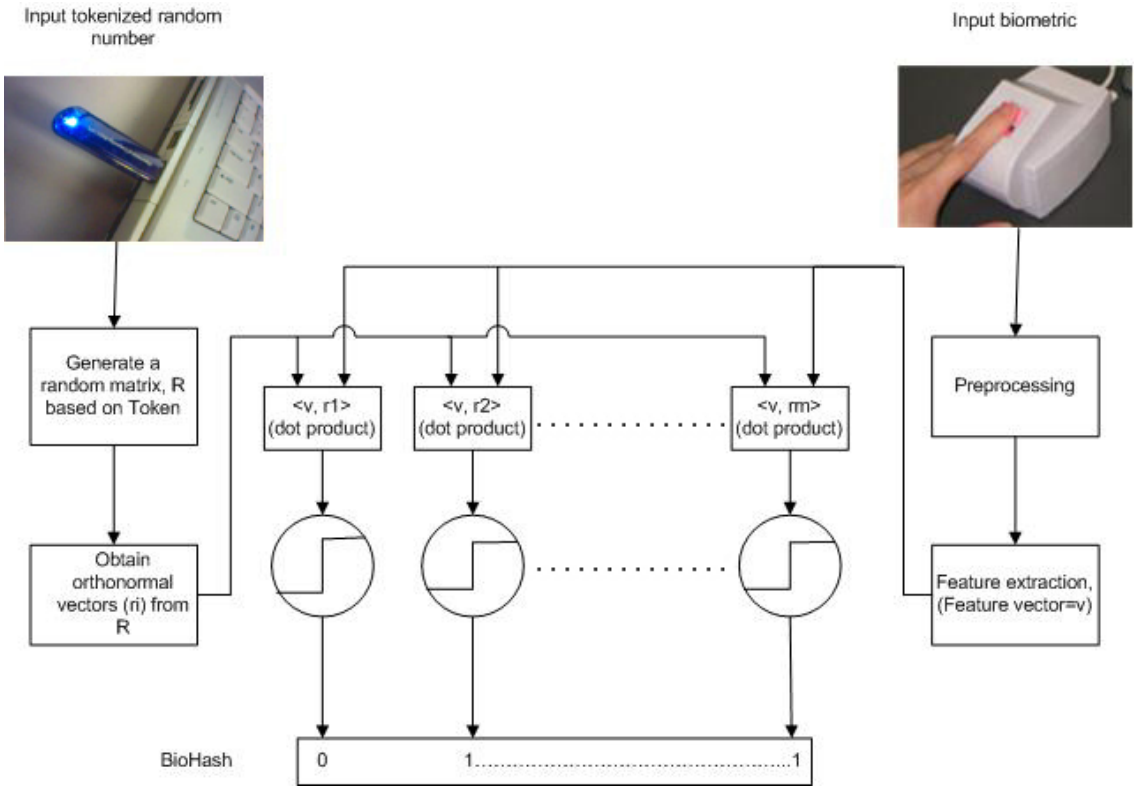
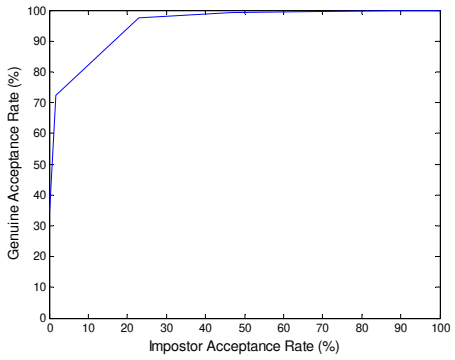

Input tokenized random number
Input biometric
Generate a random matrix, R based on Token
Obtain orthonormal vectors (ri) from R
<v, r1> (dot product)
<v, r2> (dot product)
<v, rm> (dot product)
Preprocessing
Feature extraction, (Feature vector=v)
BioHash
0
1
1

Fig. 2

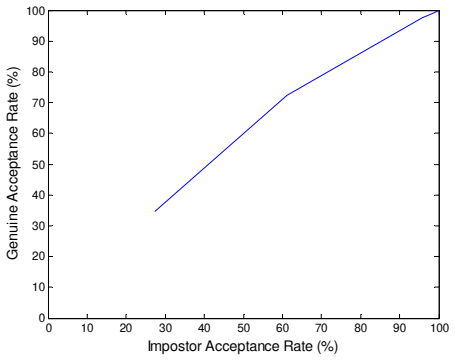
(a) (b) (c) (d)

(e) (f) (g) (h)

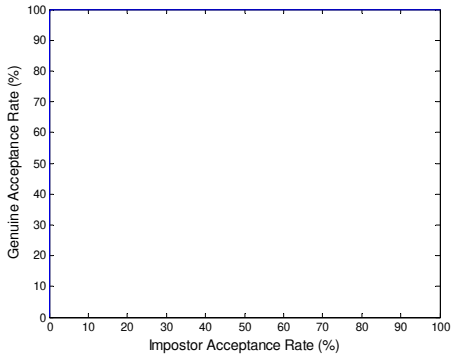
Fig. 3


Genuine Acceptance Rate (%)
Impostor Acceptance Rate (%)

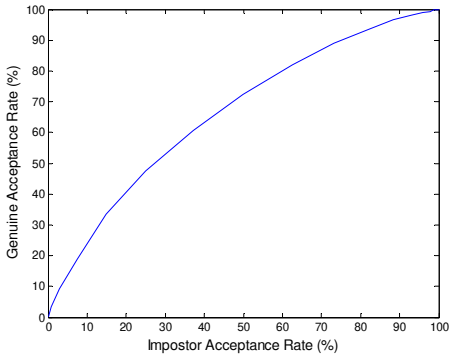
(a)


Genuine Acceptance Rate (%)
Impostor Acceptance Rate (%)

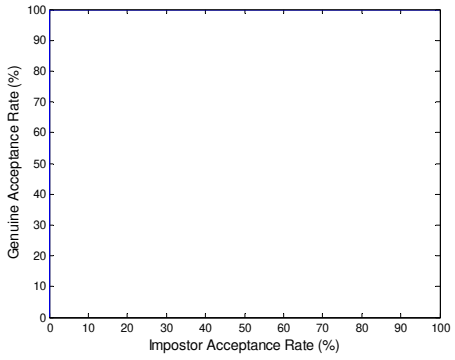
(b)


Genuine Acceptance Rate (%)
Impostor Acceptance Rate (%)

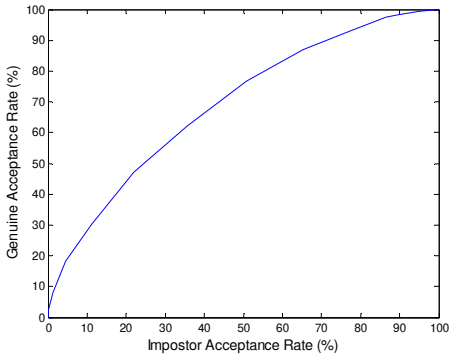
(c)


Genuine Acceptance Rate (%)
Impostor Acceptance Rate (%)

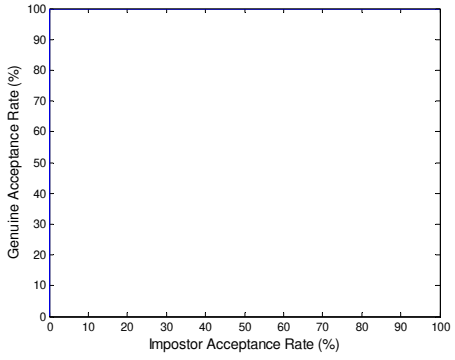
(d)


Genuine Acceptance Rate (%)
Impostor Acceptance Rate (%)

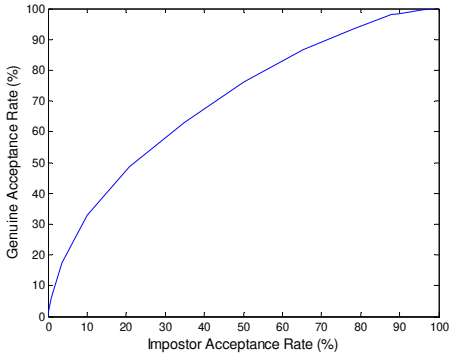
(e)


Genuine Acceptance Rate (%)
Impostor Acceptance Rate (%)

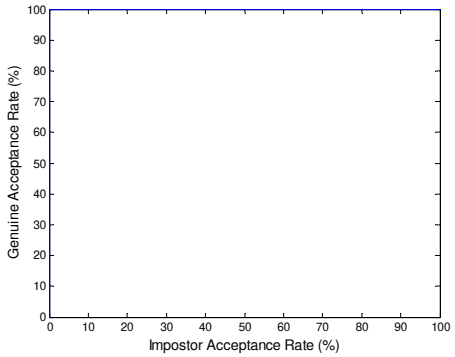
(f)


Genuine Acceptance Rate (%)
Impostor Acceptance Rate (%)

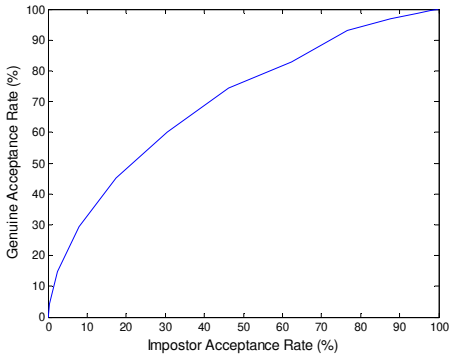
(g)


Genuine Acceptance Rate (%)
Impostor Acceptance Rate (%)

(h)

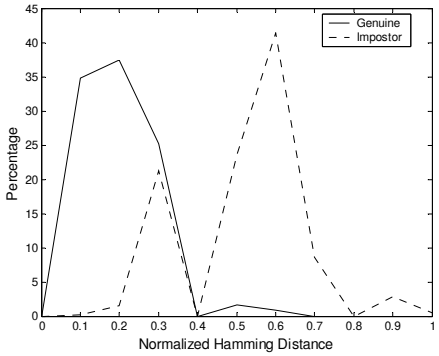

Genuine Acceptance Rate (%)
Impostor Acceptance Rate (%)
0
10
20
30
40
50
60
70
80
90
100

(i)

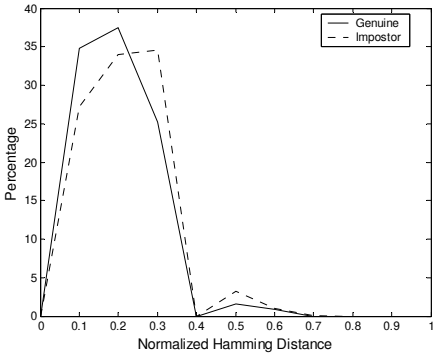

Genuine Acceptance Rate (%)
Impostor Acceptance Rate (%)
0
10
20
30
40
50
60
70
80
90
100

(j)

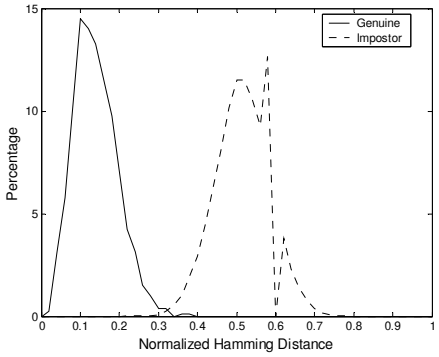
Fig. 4


Genuine
Impostor
Percentage
Normalized Hamming Distance

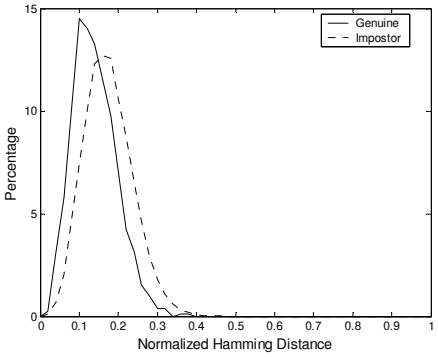
(a)


Genuine
Impostor
Percentage
Normalized Hamming Distance

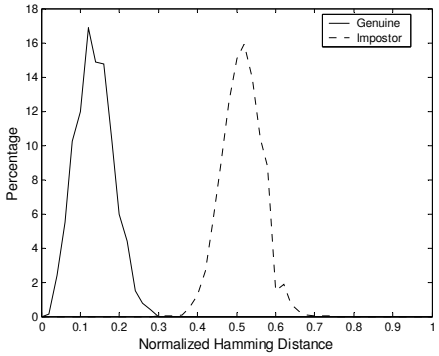
(b)


Genuine
Impostor
Percentage
Normalized Hamming Distance

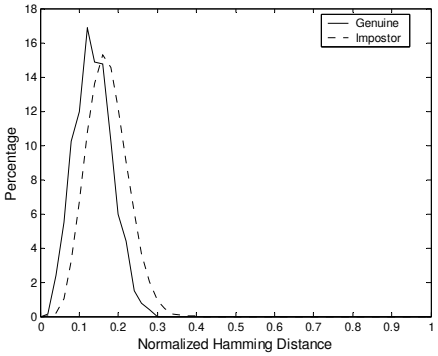
(c)


Genuine
Impostor
Percentage
Normalized Hamming Distance

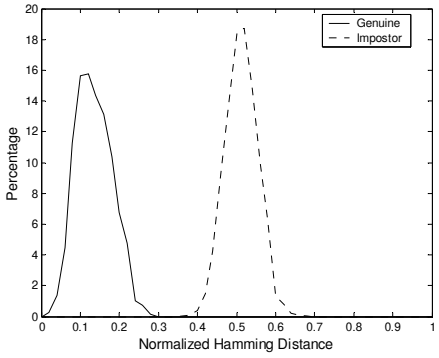
(d)


Genuine
Impostor
Percentage
Normalized Hamming Distance

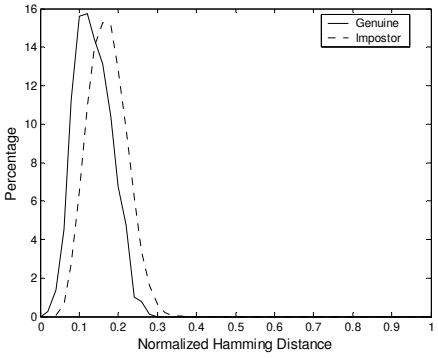
(e)


Genuine
Impostor
Percentage
Normalized Hamming Distance

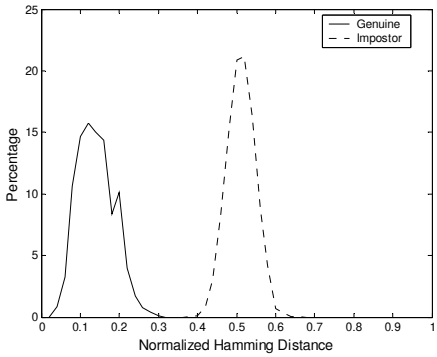
(f)


Genuine
Impostor
Percentage
Normalized Hamming Distance

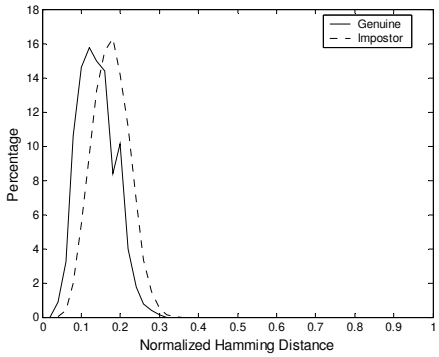
(g)


Genuine
Impostor
Percentage
Normalized Hamming Distance

(h)


Genuine
Impostor
Percentage
Normalized Hamming Distance

(i)


Genuine
Impostor
Percentage
Normalized Hamming Distance

(j)

Fig. 5

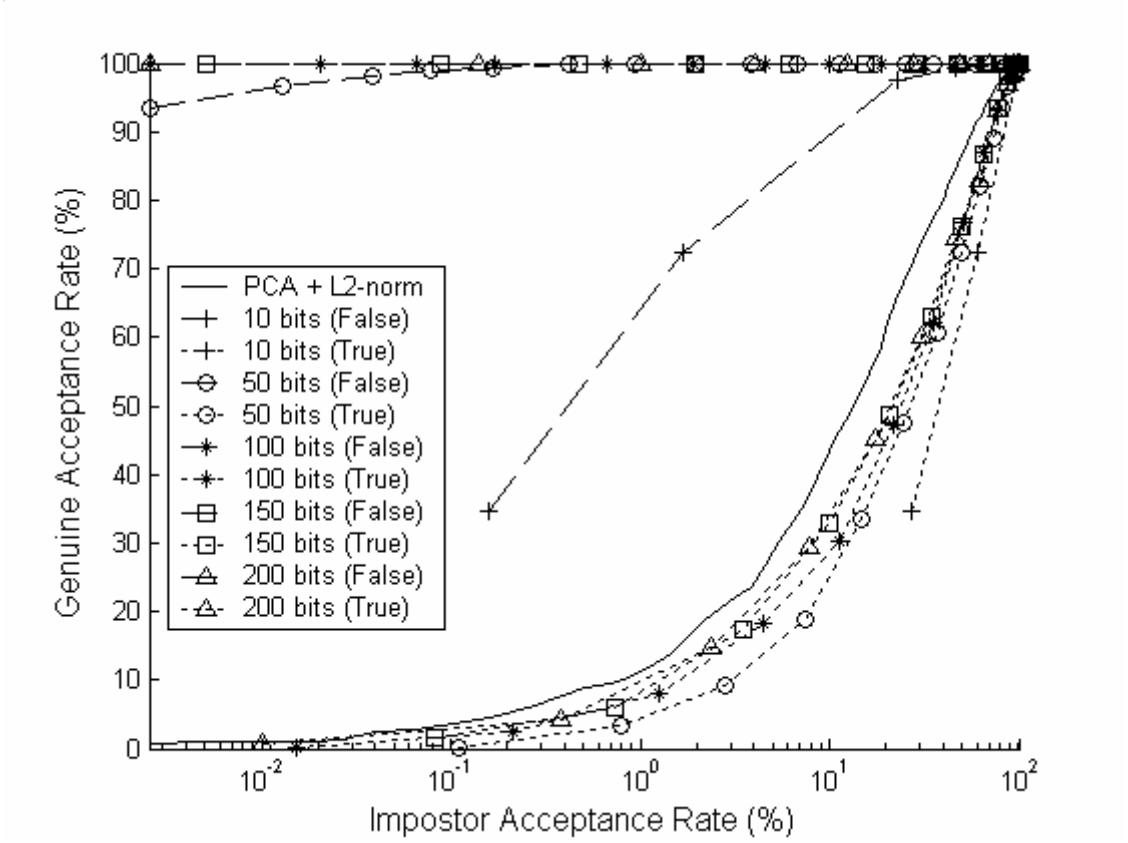

Genuine Acceptance Rate (%)
Impostor Acceptance Rate (%)
PCA + L2-norm
10 bits (False)
10 bits (True)
50 bits (False)
50 bits (True)
100 bits (False)
100 bits (True)
150 bits (False)
150 bits (True)
200 bits (False)
200 bits (True)

Fig. 6

Table 1

BioCode dimension	Threshold for BioCode (τ)
10	0
50	0
100	0
150	0
200	0