Revealing the secret of FaceHashing

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

[1] Biometrics Research Centre, Department of Computing,
The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong
{cskhc, cswkkong, csdzhang, csyjia}@comp.polyu.edu.hk
[2] Pattern Analysis and Machine Intelligence Lab, University of Waterloo,
200 University Avenue West, Ontario, Canada
mkamel@uwaterloo.ca

Abstract. Biometric authentication has attracted substantial attention over the past few years. It has been reported recently that a new technique called FaceHashing, which is proposed for personal authentication using face images, has achieved perfect accuracy and zero equal error rates (EER). In this paper, we are going to reveal that the secret of FaceHashing in achieving zero EER is based on a false assumption. This is done through simulating the claimants' experiments. Thus, we would like to alert the use of "safe" token.

1 Introduction

Biometric systems for personal authentication have been proposed for various applications based on single or a combination of biometrics, such as face [1], fingerprint [2], [3], iris [4] and palmprint [5] over the past few decades. Although biometric authentication poses several advantages over the classical authentication technologies, all biometric verification systems make two types of errors [6]: 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. [6]-[7]

The performance of a biometric system is usually assessed by two indexes: false acceptance rate (FAR) and false rejection rate (FRR). These two performance indexes are controlled by adjusting a threshold but it is impossible to reduce FAR and FRR simultaneously. Another important performance index of a biometric system is equal error rate (EER), which is at the point where FAR and FRR are equal. The EER of a system with perfect accuracy is zero.

Recently, a group of researchers proposed a new personal authentication approach called FaceHashing [8]-[11]. It is based on BioHashing [12], which has been widely applied in other biometrics [12]-[15], that combines facial features and tokenized (pseudo-) random number (TRN). The authors reported zero EERs for faces that does not rely on advanced feature representations or complex classifiers. Even with Fisher Discrimination Analysis (FDA), face recognition can still achieve perfect accuracy [8]. Those impressive results and claims of perfection aroused our interest and motivated our study on FaceHashing described below.

This paper is organized as follows. Section 2 presents the foundation for our study by giving a general review of biometric verification systems and FaceHashing. Section 3 gives the details of the simulation of FaceHashing. Section 4 reveals the secret and the true performance of FaceHashing and Section 5 offers our conclusions.

2 Review of Biometric Verification System and FaceHashing

In this paper, we concerned with biometric verification systems to which FaceHashing belongs. In this section, we will set the foundation for our study by reviewing some major characteristics of biometric verification systems of our interests and summarizing the processes in FaceHashing.

2.1 Biometric Verification System

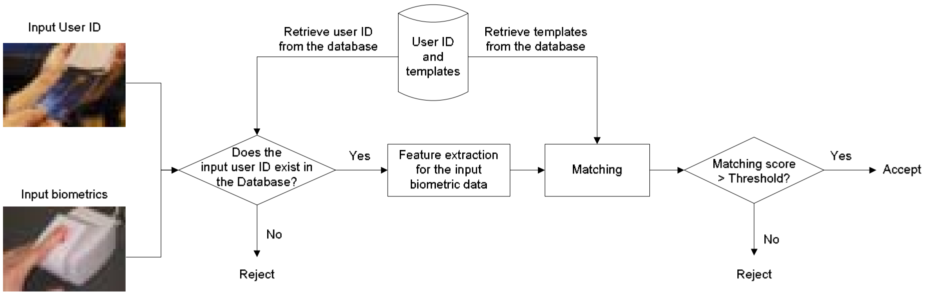
Input User ID
Input biometrics
Retrieve user ID from the database
User ID and templates
Retrieve templates from the database
Does the input user ID exist in the Database?
Yes
No
Reject
Feature extraction for the input biometric data
Matching
Matching score > Threshold?
Yes
Accept
No
Reject

Fig. 1 Operation flow of a biometric verification system

Biometric verification systems conduct one-to-one matching in personal authentication using two pieces of information: a claimed identity and biometric data. [7] The input biometric data is compared with biometric templates associated with the claimed identity in a given database. Fig. 1 illustrates the operation flow of a typical biometric verification system.

User identities should be unique to each person, as to a primary key in a database. They can be stored in smart card or in the form of keyboard/pad input. It is worth to pointed out that user identities may, therefore, be shared, lost, forgotten and duplicated like token/knowledge in traditional authentication technologies. Nonetheless, for biometric authentication, in order to pass through the verification system, user must possess a valid user identity and valid biometric features, which is verified by the biometric verification system. We would like to point out that a biometric verification system will not perform any comparison of biometrics template/data if the user identity is not valid. We have to make clear, moreover, that a biometric verification system should not depend solely on user identity or its equivalent. Therefore, it can accept user identities that are not secrets, such as personal names.

If “token” or “knowledge” 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 “token” or “knowledge”. If, further, “token” or “knowledge” would not be shared or duplicated, introducing biometrics became meaningless.

2.2 Summary of FaceHashing

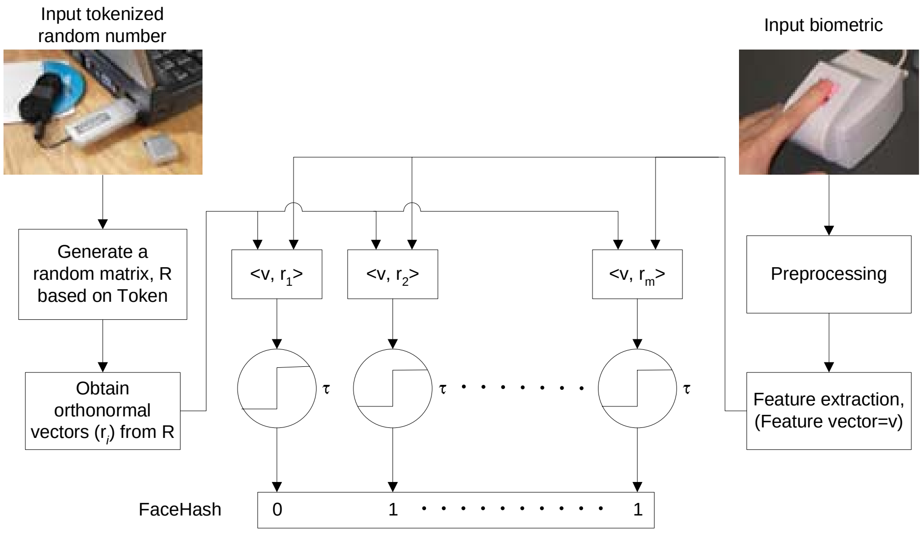
Input tokenized random number
Input biometric
Generate a random matrix, R based on Token
Obtain orthonormal vectors (r_i) from R
<v, r_1>
<v, r_2>
<v, r_m>
τ
τ
τ
Preprocessing
Feature extraction, (Feature vector=v)
FaceHash
0
1
1

Fig. 2 A schematic diagram of BioHashing

We recapitulate the mostly used method [9]-[11] (also in [12]-[15]), while another method has been reported [8] which differs by thresholding and selection of basis forming TRN [8]. Two major processes in FaceHashing [8]-[11]: facial feature extraction and discretization are illustrated in Fig. 2. Different techniques may be employed to extract features and our analysis is of more interests in discretization, the secret of FaceHashing, which 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 first step and each orthnonormal vector in TRN, $\boldsymbol{p_i}$, such that $\langle v,\ p_i \rangle$.
4) Use a threshold τ to obtain FaceHash, ***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 0 and m, the dimensionality of ***b***. Two FaceHashs are compared by hamming distance.

3 FaceHashing Simulated: Experiments and Results

In this section, we will lay down the details of simulating the FaceHashing experiments for our study. A publicly available face database, the ORL face database[16], which is also used in [9]-[11], and a well known feature extraction technique, Principal Component Analysis (PCA), also termed Eigenface for face recognition [17]-[18] are chosen for this simulation so that all the results reported in this paper are reproducible.

3.1 Experimental Setup

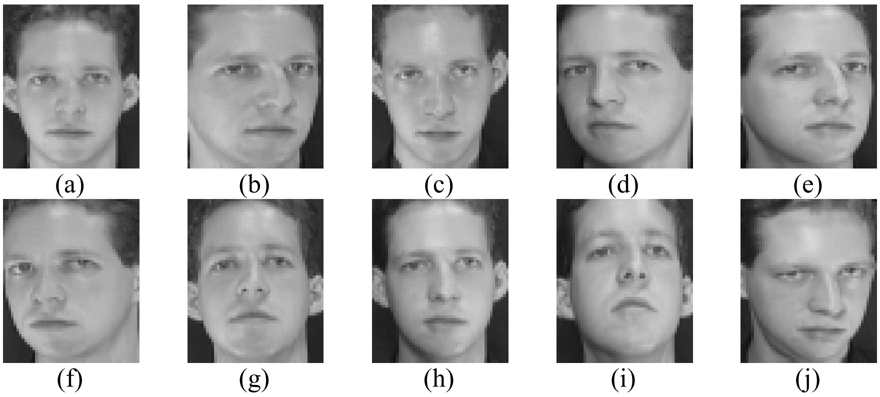

Fig. 3 Sample face images used in the ORL database.

The ORL face database contains 10 different images for each of 40 distinct subjects. For some of the subjects, the images were taken at different times, varying lighting slightly, facial expressions (open/closed eyes, smiling/non-smiling) and facial details (glasses/no-glasses). All the images are taken against a dark homogeneous background and the subjects are in up-right, frontal position (with tolerance for some side movement). The size of each image is 92×112 of 8-bit grey levels. Samples of a subject in ORL database is shown in Fig. 3

Principal components are obtained from all images of the ORL database. Each subject is assigned a unique token and the same token is used for different dimensions of the FaceHash under consideration. Table 1 lists the dimensions of the FaceHash and the corresponding thresholds (τ).

Table 1 Thresholds used for various dimensions of FaceHash

FaceHash dimension	Threshold for FaceHash (τ)
10	0
25	0
50	0
75	0
100	0

3.2 Experimental Results

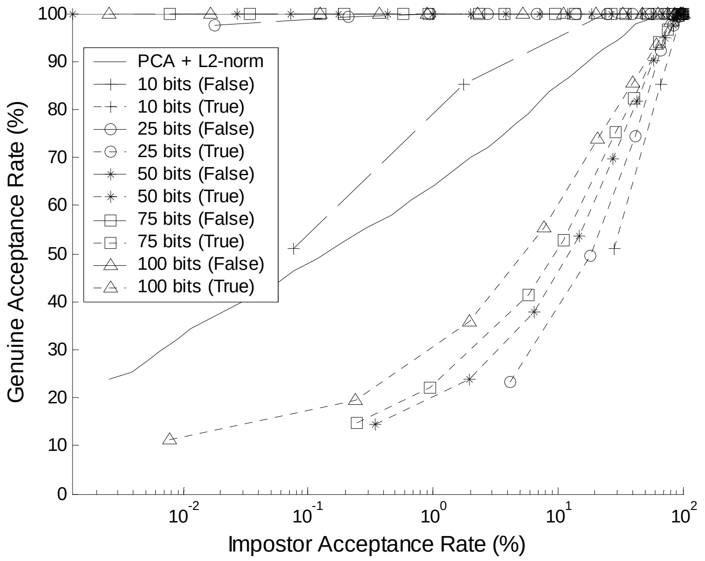

Fig. 4 ROC curves of various dimensions of FaceHash under different assumptions

We simulated FaceHashing [8]-[11] with different dimensions of FaceHash 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 Fig. 4 using dotted lines with markers. It can be seen that as the FaceHashs increase in dimensionality, the EERs gradually decrease to zero. The results of our simulation are inline with the reported results [8]-[11]. Providing FaceHash is large enough, it was possible to achieve zero EER.

4 The Secret of FaceHashing

In Section 3, we simulated FaceHashing in achieving zero EER, as in [8]-[11]. Obviously, the high performance of BioHashing is not resulted from the biometric features. In our simulation above, we are able to obtain zero EER by applying only a simple feature extraction method, PCA, but in general, even with advanced classifiers, such as support vector machines, PCA is impossible to yield 100% accuracy along with zero EER. We are going to reveal the secret of FaceHashing in this section.

4.1 The secret of FaceHashing in achieving zero EER

The TRN is generated from a token (seed) which is unique among different persons and applications [8]-[11]. The token and thus the TRN for each user used in enrollment and verification is the same; different users (and applications), moreover, have different tokens and thus different TRNs. It is trivial that the token and TRN are unique across users as well as applications. Contrasting a token in FaceHashing with a user identity of a biometric verification system, as described in Section 2, it is obvious that the token, and thus the TRN serve as a user identity.

The outstanding performance reported in FaceHashing [8]-[11] is based on the use of TRN. They assume that no impostor has a valid token/TRN. That is, they assume that the token, an user identity equivalent, 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 a flaw. Undoubtedly, their assumption does not hold in general. In their experiments, as simulated above in Section 3, they determine the genuine distribution correctly using the same token/user identity and different biometrics template/data of the same person. They determine the impostor distribution incorrectly, nevertheless, using different token/user identity and biometrics template/data of different person. As explained in Section 2, matching of biometrics template/data should not be performed because of the mismatch of the user identity equivalent, the token/TRN. Although FaceHashing does not explicitly verify the token as what is done on user identity, their determination of impostor distribution should not assume the token will not be lost, stolen, shared and duplicated. This also helps explaining why the performance of FaceHashing is better when the number of bits in FashHashs increases. It is because the effect of TRN becomes more significant as FashHashs' dimension (bits) increases.

4.2 The True Performance of FaceHashing

As discussed in Section 4.1, the impostor distribution should be determined under the assumption that impostors have valid TRNs, just as the general practice of evaluating a biometric verification system. The true performance of FaceHashing, in the form of ROC curves, for each dimension of FaceHash tested in Section 3 is shown in Fig. 4. The solid line without marker is the ROC curve when using PCA and Euclidean distance. The dashed lines with markers are the ROC curves assuming token, stolen, shared and duplicated. The dotted lines with markers are the ROC curves when using the general assumption for evaluating a biometric verification system, i.e. the true performance. It is easily observed that the true performance of FaceHash is even worse than that of using PCA and Euclidean distance. In opposite to results reported in [9]-[11], the performance of FaceHashing is far from perfect.

5 Conclusion

We, first, have reviewed the key concepts and components of a biometric verification system and FaceHashing. We, then, have revealed that the outstanding achievements of FaceHashing, zero EER, is achieved based on a false assumption that the token/TRN would never be lost, stolen, shared or duplicated. We also point out that it would be meaningless to combine the TRN with biometric features for verification if the assumption held. We used a public face database and PCA to simulate FaceHashing in achieving zero EER based on the false assumption. Afterwards, we uncover the true performance of FaceHashing, which is not as good as using PCA with Euclidean distance, with a valid assumption that is generally accepted by the research community. We would like to raise this issue to alert the use of "safe" token.

REFERENCES

1. Chellappa, R., Wilson, C.L., Sirohey, A.: Human and machine recognition of faces: A survey. Proceedings of the IEEE **83** (1995) 705-740
2. Jain, A., Hong, L., Bolle, R.: On-line fingerprint verification. IEEE Transactions on Pattern Analysis and Machine Intelligence **19** (1997) 302-314
3. Bhanu, B., Tan, X.: Fingerprint indexing based on novel features of minutiae triplets. IEEE Transactions on Pattern Analysis and Machine Intelligence **25** (2003) 616-622
4. Daugman, J.: High confidence visual recognition of persons by a test of statistical independence. IEEE Transactions on Pattern Analysis and Machine Intelligence **15** (1993) 1148-1161
5. Zhang, D., Kong, W.K., You J., Wong, M.: On-line palmprint identification. IEEE Transactions on Pattern Analysis and Machine Intelligence **25** (2003) 1041-1050
6. Jain, A.K., Ross, A., Prabhakar, S.: An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology **14** (2004) 4-20
7. Jain, A., Bolle, R., Pankanti, S. (eds.): Biometrics: Personal Identification in Networked Society. Kluwer Academic Publishers, Boston Mass (1999)
8. Teoh, A.B.J., Ngo, D.C.L, Goh, A.: An integrated dual factor authenticator based on the face data and tokenised random number. In: Zhang, D., Jain, A.K. (eds.): Biometric Authentication. Lecture Notes in Computer Science, Vol. 3072. Springer-Verlag, Berlin Heidelberg NewYork (ICBA 2004) 117-123
9. Ngo, D.C.L, Teoh, A.B.J., Goh, A.: Eigenspace-based face hashing. In: Zhang, D., Jain, A.K. (eds.): Biometric Authentication. Lecture Notes in Computer Science, Vol. 3072. Springer-Verlag, Berlin Heidelberg NewYork (ICBA 2004) 195-199
10. Teoh, A.B.J., Ngo, D.C.L, Goh, A.: Personalised cryptographic key generation based on FaceHashing. Computers and Security Journal **7** (2004) 606-614
11. Teoh, A.B.J., Ngo, D.C.L.: Cancellable biometerics featuring with tokenised random number. Pattern Recognition Letters **26** (2005) 1454-1460
12. Teoh, A.B.J., Ngo, D.C.L, Goh, A.: BioHashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recognition **37** (2004) 2245-2255
13. Connie, T., Teoh, A., Goh, M., Ngo, D: PalmHashing: A Novel Approach for Dual-Factor Authentication. Pattern Analysis and Application **7** 255-268
14. Pang, Y.H., Teoh, A.B.J., Ngo, D.C.L.: Palmprint based cancelable biometric authentication system. International Journal of Signal Processing **1** (2004) 98-104
15. Connie, T., Teoh, A., Goh, M., Ngo, D: PalmHashing: a novel approach to cancelable biometrics. Information Processing Letter **93** (2005) 1-5
16. Samaria, F., Harter, A.: Parameterisation of a stochastic model for human face identification. Proceedings of the 2nd IEEE Workshop on Applications of Computer Vision, Sarasota (Florida), (1994) 138-142 (paper and ORL face database both available online at http://www.uk.research.att.com/facedatabase.html)
17. Martinez, A.M., Kak, A.C.: PCA versus LDA. IEEE Transactions on Pattern Analysis and Machine Intelligence **23** (2001) 228-233
18. Turk, M., Pentland, A.: Eigenfaces for recognition. Journal of Cognitive Neuroscience **3** (1991) 71-86