# An Analysis on Accuracy of Cancelable Biometrics based on BioHashing

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

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

**Abstract.** Cancelable biometrics has been proposed for canceling and re-issuing biometric templates and for protecting privacy in biometrics systems. Recently, new cancelable biometric approaches are proposed based on BioHashing, which are random transformed feature-based cancelable biometrics. In this paper, we consider the accuracy of one of the cancelable biometrics based on BioHashing and face. Through this analysis, as an illustration, we would like to raise an issue to be considered in cancelable biometrics: accuracy may be traded for biometrics being cancelable.

## 1 Introduction

Biometric authentications are increasingly performed under unattended and/or over networked environments. Attackers can attack via the exposed communication channels. [2], [3]

Ratha et al. [6] introduce the concept of cancelable biometrics to protect privacy in biometric authentication systems. It is achieved through intentional and repeatable distortions (or transformations) on biometrics in either the signal domain or the feature domain. The distortions for cancelable biometrics are ideally noninvertible. Nevertheless, the distortions can be invertible in practical use.

Ratha et al. [6] have given some example transforms for cancelable biometrics. As invertible examples, grid morphing and block permutation are offered and as a noninvertible example, high order polynomial is offered.

Cancelable biometric templates are essential for biometric authentication systems, especially for those operated under unattended and/or over networked environments. [6], [8]

Recently, variants [1], [5], [10] of BioHashing [11] which consists of feature domain random transformation and discretization, were extended as a means to cancelable biometrics.

In this paper, we bring out the issue that accuracy is traded for biometrics being cancelable through a case study on BioHashing and face. This issue is important to cancelable biometrics and thus biometric authentications. The rest of this paper is organized as follows. Section 2 presents the issue that should be considered. Section 3 presents an empirical test to demonstrate the issue. Section 4 offers our conclusions.

## 2 Cancelable Biometrics

We have briefly reviewed the major reasons and concepts of cancelable biometrics in the above section. In this section, we would like discuss the issue in cancelable biometrics including accuracy in section 2.1. Accuracy is the short term for recognition accuracy of a biometric system.

### 2.1 Accuracy

To make biometric system practical, satisfactorily high recognition accuracy is required. Therefore, we have to make sure the recognition is accurate enough for an application. Noninvertible transforms in cancelable biometrics for both signal and feature domain can lead to information loss that affects the discriminating ability and results in deterioration of accuracy. Invertible transforms can replace noninvertible transforms to avoid information loss.

Since cancelable biometrics is matched in the transformed domain, we have to define a suitable feature extraction as well as similarity measure in the transformed domain. Otherwise, the accuracy may not be guaranteed. For example, if a monotonically decreasing function is the transform and $L_2$-norm is the similarity measure, it will be inaccurate to measure the similarity in the transformed domain using $L_2$-norm. We, therefore, have to look for transforms that keep meaningful relationships for feature extraction (for signal domain transforms) and similarity measure (for both domain) afterwards. Certain transforms may still be used for providing cancelable biometrics even though we cannot find a suitable strategy to maintain the original recognition accuracy.

Connie et al. [1], Pang et al. [5] and, Teoh and Ngo [10] presented prototypes of cancelable biometrics for palmprint and face based on BioHashing [11]. BioHashing consists of two major steps, feature domain random transformation, and discretization (a two level quantization). Their transform is a kind of noninvertible feature domain transform. As the transform is noninvertible, the raw template can be better protected. Random transform is one of the viable approaches to provide cancelable biometrics. Nonetheless, we believe that noninvertible random transformations will destroy the optimality of most feature representations and thus the recognition accuracy deteriorates. There is a tradeoff in the feature domain between optimality in representation and similarity matching and biometrics being cancelable, i.e. the error rate of authentication increases [12].

## 3 Analysis on accuracy of a BioHashing based cancelable biometric

In order to ensure cancelable biometrics is practical, we have to look at the system performance. We understand there is tradeoff between cancelability and recognition accuracy. So, we now look at the amount of recognition accuracy that can be traded for biometrics being cancelable by a test of a cancelable biometric for face based on BioHashing proposed by Teoh and Ngo in [10].

Wavelet Fourier Mellin Transform (WFMT) [4], [9] is the feature extraction technique used in [10]. The ORL face database [7] is a well-known public face database and is adopted in [10] and Lai et al. [4]. There are 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.

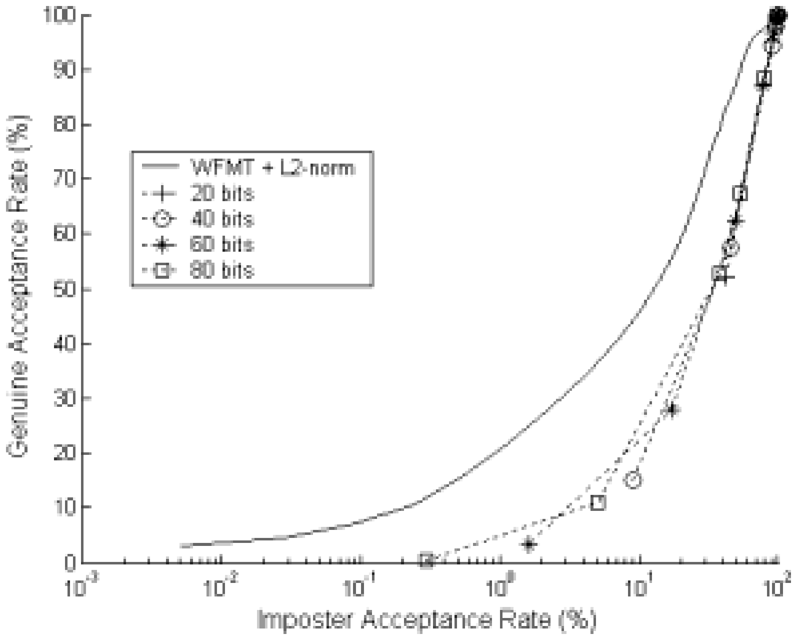

Figure 1. Test on accuracy of various BioCodes of BioHashing compared to Euclidean distance

The implementation details of WFMT are listed in Table 1 and thresholds (for quantization) used for various bits of BioHashing are listed in Table 2 for reference. The thresholds chosen are the same as indicated in [10], [11]. Moreover, the number of matching for estimating the genuine and impostor distributions based on the Teoh and

Ngo's matching scheme, which matches only the $n^{th}$ image of one person to the $n^{th}$ image of other persons to determine the impostor distribution where $n$ = 1…10, are 1800 (i.e. [(1+9)×(9/2)]×40) and 7800 (i.e. [(1+39)×(39/2)]×10) respectively. (for details please refer to [10])

The Receiver Operating Characteristic (ROC) curves [2], [3] of WFMT with BioHashing of 20, 40, 60 and 80 bits are plotted (dashed lines) along with WFMT with Euclidean distance, $L_2$-norm (solid line) in Figure 1. Nearest-Neighbour-Classifier is used to determine the matched identity for WFMT with BioHashing and Euclidean distance. From Figure 1, the optimality of feature representation is shown to be destroyed by the noninvertible random transform and quantization and thus the recognition accuracy deteriorates. The performance of WFMT with BioHashing is even worse than that of WFMT with Euclidean distance, i.e. dashed lines are beneath the solid line.

**Table 1** The details of WFMT implementation

| Processes/Variables/Parameters | Values/Descriptions |
|---|---|
| Raw image sizes | 92×112, no preprocessing |
| Wavelet | db7 |
| Level of Wavelet Decomposition | 1 |
| Wavelet transformed image sizes (LL band) | 52×62 |
| Log-polar transformation | Largest inscribed circle,<br>bicubic interpolation,<br>62 logarithmic levels |
| Highpass Filter | same as in [10], $H(x,y)$ =<br>$(1-\cos(\pi x)\cos(\pi y))\times(2-\cos(\pi x)\cos(\pi y))$ |

**Table 2** Thresholds used for various bits of BioHashing

| Bits | Thresholds |
|---|---|
| 20 | 0 |
| 40 | 0 |
| 60 | 0 |
| 80 | 0 |

## 4 Conclusions

We have presented a brief review of cancelable biometrics. We have raised an issue in cancelable biometrics worth for consideration. Through an analysis of accuracy of an existing approach to cancelable biometric, it is shown that biometrics being cancelable is not free lunch. The accuracy can be traded because we are not able to find a strategy to integrate the transform, feature extraction and similarity measure as a whole.

## Acknowledgement

The authors would like to thank for the partial support of the research grants from Hong Kong Government (UGC) and the research grants for iJADE projects PG50 and A-PF74 of The Hong Kong Polytechnic University.

## References

1. Connie, T., Teoh, A., Goh, M., Ngo, D: PalmHashing: a novel approach to cancelable biometrics. Information Processing Letter **93** (2005) 1-5
2. Jain, A., Bolle, R., Pankanti, S. (eds.): Biometrics: Personal Identification in Networked Society. Kluwer Academic Publishers, Boston Mass (1999)
3. 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
4. Lai, J.H., Yuen, P.C., Feng, D.C.: Face recognition using holistic Fourier invariant features. Pattern Recognition **34** (2001) 95-109
5. Pang, Y.H., Teoh, A.B.J., Ngo, D.C.L.: Palmprint based cancelable biometric authentication system. International Journal of Signal Processing **1** (2005) 98-104
6. Ratha, N.K., Connell, J.H., Bolle, R.M.: Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal **40** (2001) 614-634
7. 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]
8. Schneier, B.: The Uses and Abuses of Biometrics. Communications of the ACM **42** (1999) 136
9. Srinivasa Reddy, B., Chatterji, B.N.: An FFT-Based Technique for Translation, Rotation, and Scale-Invariant Image Registration. IEEE Transactions on Image Processing **5** (1996) 1266-1271
10. Teoh, A.B.J., Ngo, D.C.L.: Cancellable biometerics featuring with tokenised random number. To appear in Pattern Recognition Letters (2004) [available online but obtained from A.B.J. Teoh]
11. 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
12. Uludag, U., Pankanti, S., Prabhakar, S., Jain, A.K.: Biometirc Cryptosystems: Issues and Challenges. Proceedings of the IEEE **92** (2004) 948-960