

















Table 1  
Performance evaluation in terms of EER and FRR when FAR = 0%

	FAR (%)	FRR (%)	EER (%)	FRR (%) (FAR = 0%)	Threshold range when EER = 0% ([ $t_{max}$ – $t_{min}$ ])
<i>wfm</i>	5.93	5.38	5.66	47.16	—
<i>wfmm</i>	1.00	1.02	1.01	23.08	—
<i>wfmd-20</i>	3.91	4.12	4.02	15.86	—
<i>wfmd-40</i>	1.55	2.56	2.06	2.56	—
<i>wfmd-60</i>	0.14	0.00	0.07	0.04	—
<i>wfmd-80</i>	0.00	0.00	0.00	0.00	[0.18 – 0.05] 0.13
<i>wfmmd-20</i>	0.88	0.34	0.61	0.94	—
<i>wfmmd-40</i>	0.00	0.00	0.00	0.00	[0.32 – 0.08] 0.24
<i>wfmmd-60</i>	0.00	0.00	0.00	0.00	[0.38 – 0.05] 0.33
<i>wfmmd-80</i>	0.00	0.00	0.00	0.00	[0.41 – 0.03] 0.39

methodology is efficient to overcome the FAR–FRR interdependency problem whereas using *wfm* or *wfmm* alone yield intolerable high FRR—47.16% and 23.08%, respectively. On the other hand, it can be observed that *wfmmd-m* is outperformed *wfmd-m* as *wfmmd-m* obtained EER = 0% at  $m = 40$  whereas  $m = 80$  for *wfmd-m* for similar performance.

Since the verification rates are very high for *wfmd-80* and *wfmmd-m*,  $m = 40, 60$  and  $80$ , another performance indicator is through the observation of range of normalised threshold values,  $t \in [0, 1]$  when EER = 0%: the bigger range of threshold value yield the better performance, as a large range of operating points,  $t$  with zero errors can be obtained. Table 1 shows the range of  $t$  that result in a zero error, for *wfmd-m* and *wfmmd-m*. It can be observed that the range is getting wider when  $m$  grows, which implies system performance is boost for *wfmd-80* and *wfmmd-m* where  $m = 40, 60$  and  $80$ . In general, we can postulate that BioHash, **b** performance can be improved with the better biometric feature extractor, i.e. multiple WFMT or with the larger  $m$  where  $m < M$ .

In the practicability viewpoint, the fingerprint recognition system have been used under a huge database, and thus the size of fingerprint feature should be compact enough for enrollment and recognition, hence *wfmd-80* or *wfmmd-60* seem like the good compromise between the requirement of accuracy and computation speed. In addition, probability of **b** recovery for *wfmd-80* and *wfmmd-60* in security concern are not less than  $\frac{1}{2}^{60}$  and  $\frac{1}{2}^{80}$ , respectively of random guessing.

### 3.3. BioHashing one-way transformation validation

As mentioned in Section 2, the crucial concern of preventing biometric fabrication in the verification task is to ensure that BioHashing is a one-way and non-invertible transformation, in other words, there is no deterministic way to get the user specific code without having both token with random data and user fingerprint. In order to validate

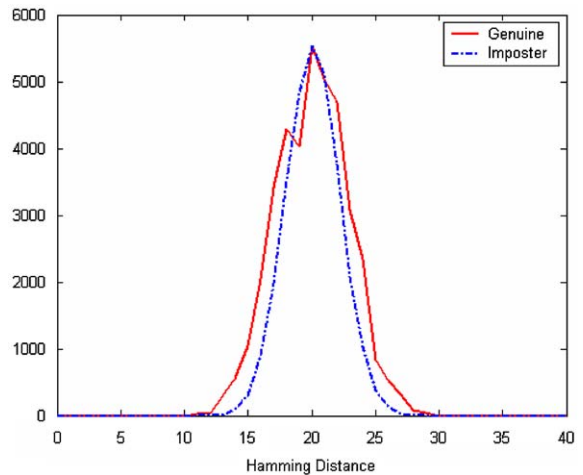


Fig. 7. Genuine and imposter population distribution histogram for case 2.

this, an experiment is conducted to simulate the situations below:

Let  $r_A$  the random pattern that generated by the genuine user with his/her token and inner-producted with  $\Gamma_{EA}$  (enrolled invariant fingerprint representation  $A$ ) and  $\Gamma_{TA}$  (test invariant fingerprint representation  $A$ ), with length of bit-string,  $m = 60$ .

Then, the following three cases can be derived:

Case 1:  $(r_A, \Gamma_{EA}) \Leftrightarrow (r_A, \Gamma_{TA})$ .

This is the case when  $A$  holds his/her  $r_A$  and combine with his/her own  $\Gamma_{EA}$  and  $\Gamma_{TA}$  during the enrollment and verification session, respectively. This has been vindicated and discussed in Sections 3.1 and 3.2.

Case 2:  $(r_A, \Gamma_{EA}) \Leftrightarrow (r_o, \Gamma_{TA})$ .

This case presumes  $A$  lost his/her token credential, i.e.  $r_A$  and replace with  $r_o$  without update his/her unique code in the enrollment session. The simulation result shows in Fig. 7. It can be observed that the strong overlapping in

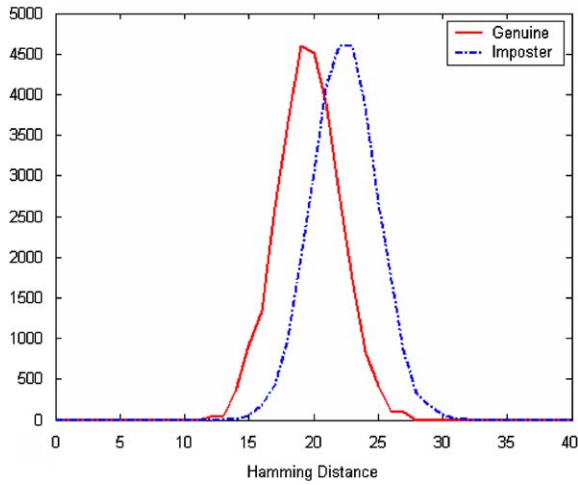


Fig. 8. Genuine and imposter population distribution histogram for case 3.

between genuine and imposter population (both peak at  $1/2m$ ) reveals that the uniqueness of bit string (BioHash code) for the genuine user is vanished when different random pattern, i.e.  $r_o$  is used to mix with  $\Gamma_{TA}$ .

Case 3:  $\langle r_A, \Gamma_{EA} \rangle \Leftarrow \langle r_A, \Gamma_{To} \rangle$ .

When  $\Gamma_{TA}$  is replaced with a non-legitimate fingerprint feature,  $\Gamma_{To}$ , the result is depicted in Fig. 8. Again, a similar outcome as in Fig. 7 is obtained, both populations also peak at  $1/2m$  and blunt drop-offs in the genuine population addressed the loss of unique bit string pattern of the genuine user if compare to Fig. 5, therefore the non-invertible property of  $b$  is vindicated.

**4. Concluding remarks**

This paper described a novel error-tolerant discretisation methodology from user-specific fingerprint images and uniquely serialised tokens. The two factor BioHashing has significant functional advantages over solely biometrics or token usage, such as extremely clear separation of the genuine and the imposter populations and zero EER level, thereby mitigate the suffering from increased occurrence of FRR when eliminate the FAR. The process of generating a token of pseudo-random vectors taking place only once for an individual, it can be considered secure in the sense that there is no way to recover the fingerprint data by getting hold on the token (one-way transformation). As a result, a unique compact code per person should be obtained, which is highly desirable in a secure environment and outperforms the classic verification scheme, considered a weak-security system for it needs to access an external database of user data. In addition, BioHashing technique also addressed the invasion of privacy issue, such as biometric fabrication.

It could be alleviated through the user specific credential revocation via token replacement.

The methodology presented here is able to extend in various directions via straightforward extensions, for instance incorporation image preprocessing or via adoption of alternative feature extraction method. Exploration of the later is particularly promising in that it would enable adaptation of the featured inner-product discretization mechanism to other biometric form i.e. face, irises and speech.

**5. Summary**

Human authentication is the security task whose job is to limit access to physical locations or computer network only to those with authorisation. This is done by equipped authorised users with passwords, tokens or using their biometrics. Unfortunately, the first two suffer a lack of security as they are easy being forgotten and stolen; even biometrics also suffers from some inherent limitation and specific security threats, for instance, if an attacker can intercept a person’s biometric data, then the attacker might use it to masquerade as the person. These concerns are aggravated by the fact that a biometrics cannot be changed. When a biometrics is compromised, however, a new one cannot be issued. Besides that, the nature of biometrics system offers binary (yes/no) decisions scheme, which provided four possible outcomes are normally called as FAR, CAR, FRR and CRR. By manipulating the decision criteria, the relative probabilities of these four outcomes can be adjusted in a way that reflected their associated cost and benefits. In practice, that is almost impossible to get both zero FAR and FRR errors due to the fact that the classes are difficult to completely separate in the measurement space. In this paper, a novel two factor authentication approach which combined tokenised random data with fingerprint feature to generate a unique compact code per person is highlighted. The discretization is carried out by iterated inner product between the pseudo-random number and the wavelet FMT fingerprint feature, and finally deciding each bit on the sign based on the predefined threshold. Direct mixing of random and biometric data is, in fact, an extremely convenient mechanism with which to incorporate serialised physical tokens, thereby resulting in two factors (token+biometrics) credentials via tokenised randomisation. The two factor BioHashing has significant functional advantages over solely biometrics or token usage, such as extremely clear separation of the genuine and the imposter populations and zero EER level, thereby mitigate the suffering from increased occurrence of FRR when eliminate the FAR. The process of generating a token of pseudo-random vectors taking place only once for an individual, it can be considered secure in the sense that there is no way to recover the fingerprint data by getting hold on the token (one-way transformation). As a result, a unique compact code per person should be obtained, which is highly desirable in a secure environment and outperforms the classic verification

scheme. In addition, BioHashing technique also addressed the invasion of privacy issue, such as biometric fabrication. It could be alleviated through the user specific credential revocation via token replacement.

## References

- [1] R.M. Bolle, J.H. Connel, N.K. Ratha, Biometric perils and patches, *Pattern Recognition* 35 (2002) 2727–2738.
- [2] J. Daugman, Biometric decision landscapes. Technical Report, No. 482, Cambridge University Computer Laboratory, 2002.
- [3] R.M. Bolle, S. Pankanti, N.K. Ratha, Evaluating techniques for biometrics based authentication systems (FRR), In: *Proceedings 15th IAPR International Conference on Pattern Recognition, Vol. II, Barcelona, Spain, 2000*, pp. 835–841.
- [4] L. Rila, Denial of access in biometrics-based authentication systems, In: *Proceedings of International Conference of Infrastructure Security (InfraSec 2002)*, Bristol, UK, 1–3 October, 2000.
- [5] A. Ross, A.K. Jain, J.Z. Qian, Information fusion in biometrics, In: *Proceedings of the Third International Conference on Audio- and Video-Based Person Authentication*, Sweden, June, 2001, pp. 354–359.
- [6] G.L. Marcialis, F. Roli, Experimental results on fusion of multiple fingerprint matchers, In: *Proceedings of the Fourth International Conference on Audio-Video Based Personal Authentication (AVBPA' 03)*, Guiford, UK, June, 2003, pp. 814–820.
- [7] Y. Wang, T. Tan, A.K. Jain, Combining face and iris biometrics for identity verification, In: *Proceedings of the Fourth International Conference on Audio-Video Based Personal Authentication (AVBPA' 03)*, Guiford, UK, June, 2003, pp. 805–813.
- [8] Y. Isobe, Y. Seto, M. Kataoka, Development of personal authentication system using fingerprint with digital signature technologies, In: *Proceedings of the 34th Hawaii International Conference on System Sciences, 2001*.
- [9] J. Armington, P. Ho, P. Koznek, R. Martinez, Biometric authentication in infrastructure security, In: *Proceedings of International Conference of Infrastructure Security (InfraSec 2002)*, Bristol, UK, 2002.
- [10] G. Lisimaque, Biometrics and smart cards, In: *Proceedings of Conference of the Biometric Consortium, 1999*.
- [11] R. Sanchez-Reillo, Including biometric authentication in a smart card operating system, In: *Proceedings of the International Conference on Audio-Video Based Personal Authentication (AVBPA'01)*, Switzerland, 2001.
- [12] P. Ho, J. Armington, A dual-factor authentication system featuring speaker verification and token technology, In: *Proceedings of the Fourth International Conference on Audio-Video Based Personal Authentication (AVBPA' 03)*, Guiford, UK, June, 2003, pp. 128–136.
- [13] A. Teoh, D. Ngo, Ong Thian Song, An efficient fingerprint verification system using integrated wavelet and Fourier-Mellin invariant transform, *Image Vision Comput.* 22 (6) (2004) 503–513.
- [14] S. Mallat, *A Wavelet Tour of Signal Processing*, Academic Press, San Diego, 1998.
- [15] J. Wood, Invariant pattern recognition: a review, *Pattern Recognition* 29 (1) (1996) 1–17.
- [16] A. Grace, M. Spann, A comparison between Fourier-Mellin descriptors and moment based features for invariant object recognition using neural networks, *Pattern Recogn. Lett.* 12 (1991) 635–643.
- [17] B.S. Reddy, B.N. Chatterji, An FFT-based technique for translation, rotation and scale-invariant image registration, *IEEE Trans. Image Process.* 5 (8) (1996) 1266–1271.
- [18] A. Menezes, P.V. Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, 1996.
- [19] D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, New York, 2003.
- [20] A. Teoh, T.S. Ong, N.C.L. David, In: T.D. Gedeon, Lance Chun Che Fung (Eds.), *Automatic Fingerprint Center Point Determination, Lecture Notes of Artificial Intelligent*, Vol. 2903, Springer, Berlin, 2003, pp. 633–640.

**About the Author**—ANDREW TEOH BENG JIN obtained his B.Eng. (Electronics) in 1999 and Ph.D. degree in 2003 from National University of Malaysia. He is currently a lecturer of Faculty of Information Science and Technology, Multimedia University. He held the post of co-chair (Biometrics Division) in Center of Excellent in Biometrics and Bioinformatics in the same university. His research interest is in multimodal biometrics, pattern recognition, multimedia signal processing and Internet security.

**About the Author**—DAVID CHEK LING NGO is an Associate Professor and the Dean of the Faculty of Information Science & Technology at Multimedia University, Malaysia. He has worked there since 1999. Ngo was awarded a BAI in Microelectronics & Electrical Engineering and Ph.D. in Computer Science in 1990 and 1995, respectively, both from Trinity College Dublin. Ngo's research interests lie in the area of Automatic Screen Design, Aesthetic Systems, Biometric Encryption, and Knowledge Management. He is author and co-author of over 20 invited and refereed papers. He is a member of Review Committee of Displays and Multimedia Cyberscape.

**About the Author**—ALWYN GOH is an experienced and well-published researcher in biometrics, cryptography and information security. His work is recognised by citations from the Malaysian National Science Foundation and the European Federation of Medical Informatics. He previously lectured Computer Sciences at Universiti Sains Malaysia where he specialised in data-defined problems, client server computing and cryptographic protocols. Goh has a Masters in Theoretical Physics from the University of Texas, and a Bachelors in Electrical Engineering and Physics from the University of Miami.