PERGAMON

Available at
www.ElsevierComputerScience.com
POWERED BY SCIENCE DIRECT®

Pattern Recognition 37 (2004) 2245–2255

PATTERN RECOGNITION
THE JOURNAL OF THE PATTERN RECOGNITION SOCIETY

www.elsevier.com/locate/patcog

Biohashing: two factor authentication featuring fingerprint data and tokenised random number

Andrew Teoh Beng Jin[a,*], David Ngo Chek Ling[a], Alwyn Goh[b]

[a]*Faculty of Information Science and Technology (FIST), Multimedia University, Jalan Ayer Keroh Lama, Bukit Beruang, Melaka 75450, Malaysia*

[b]*Distinctive Biometrics Sdn. Bhd. B-S-06, Kelana Jaya 47301, Petaling Jaya, Selangar, Malaysia*

Received 1 August 2003; received in revised form 3 March 2004; accepted 27 April 2004

Abstract

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. A more practical approach is to combine two or more factor authenticator to reap benefits in security or convenient or both. This paper proposed a novel two factor authenticator based on iterated inner products between tokenised pseudo-random number and the user specific fingerprint feature, which generated from the integrated wavelet and Fourier–Mellin transform, and hence produce a set of user specific compact code that coined as BioHashing. BioHashing highly tolerant of data capture offsets, with same user fingerprint data resulting in highly correlated bitstrings. Moreover, there is no deterministic way to get the user specific code without having both token with random data and user fingerprint feature. This would protect us for instance against biometric fabrication by changing the user specific credential, is as simple as changing the token containing the random data. The BioHashing has significant functional advantages over solely biometrics i.e. zero equal error rate point and clean separation of the genuine and imposter populations, thereby allowing elimination of false accept rates without suffering from increased occurrence of false reject rates.

Keywords: BioHashing; Two factor authentication; Biometrics; Fingerprint; Token

1. Introduction

Today's human authentication factors have been placed in three categories, namely What you know, e.g password, secret, personal identification number (PIN); What you have, such as token, smart card etc. and What you are, biometrics for example. However, the first two factors can be easily fooled. For instance, password and PINs can be shared among users of a system or resource. Moreover, password and PINs can be illicitly acquired by direct observation. The main advantage of biometrics is that it bases recognition on an intrinsic aspect of a human being and the usage of biometrics requires the person to be authenticated to be physically present at the point of the authentication. These characteristics overcome the problems whereas password and token are unable to differentiate between the legitimate user and an attacker. In addition biometric authentication information cannot be transferred or shared; it is a powerful weapon against repudiation. However, it also suffers from some inherent biometrics-specific threats [1]. The main concern

* Corresponding author. Tel.: +60-6-252-3404; fax: +60-6-231-8840.

E-mail addresses: bjteoh@mmu.edu.my (A.T.B. Jin), david.ngo@mmu.edu.my (D.N.C. Ling), alwyn_goh@yahoo.co.uk (A. Goh).

0031-3203/$30.00
doi:10.1016/j.patcog.2004.04.011

of the public for the biometric usage is the privacy risks in biometric system. If an attacker can intercept a person's biometric data, then the attacker might use it to masquerade as the person, or perhaps simple to monitor that person's private activities. 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.

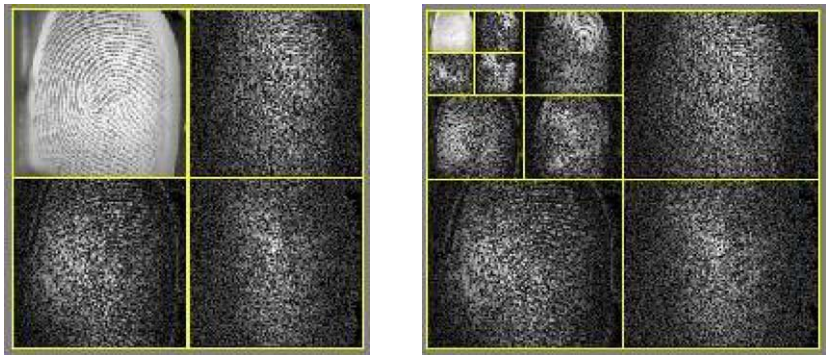
Besides that, the nature of biometrics system offers binary (yes/no) decisions scheme, which is well defined in the classical framework of statistical decision theory, thereby provided four possible outcomes are normally called as false accept rate (FAR), correct accept rate (CAR), false reject rate (FRR) and correct reject rate (CRR) [2]. 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. According to Bolle et al. [3], the biometrics industry emphasis heavily on security issues relating to FAR with relaxed the FRR requirement. However, the overall performance of a biometric system cannot be assessed based only on this metric. High FRR, i.e. rejection of valid users, which is resulted by low FAR, is often largely neglected in the evaluation of biometric systems. However, this will give an impact on all major aspects of a biometric system as pointed in Ref. [4]. Denial of access in biometric systems greatly impacts on the usability of the system by failing to identify genuine user, and hence on the public acceptance of biometrics in the emerging technology. Both aspects may represent significant obstacles to the wide deployment of biometric systems.

Multimodal biometrics fusion i.e. systems employing more than one biometric technology to establish the identity of an individual, is able to improve the overall performance of the biometric system by checking multiple evidences of the same identity [5]. Multimodal biometrics can reduce the probability of denial of access without sacrificing the FAR performance by increasing the discrimination between the genuine and imposter classes [6,7]. Despite of that, multimodal biometrics is not a solution for the privacy invasion problem, though the difficulty of attack activities may increase to certain degree. Moreover, use of multiple biometric measurement devices will certainly impose significant additional costs, more complex user-machine interfaces and additional management complexity [4].

The most practical way of addressing the privacy invasion problem is to combine two or more factor authenticators. A common multi-factor authenticator is an ATM card, which combines a token with a secret (PIN). Combination of password or secret with a biometrics is not so favorable, since one of the liabilities of biometrics is to get rid of the task of memorising the password. As a user has difficulty remembering the secret, a token may be combined with a biometrics. A token is a physical device that can be thought of as a portable storage for authenticator, such as ATM card, smart card, or an active device that yields time-changing or challenged-based passwords. The token can store human-chosen passwords, but an advantage is to use these devices to store longer codewords or pseudo-random sequence that a human cannot remember, and thus they are much less easily attacked. Presently, there are quite a number of literature reported the integration of biometrics into the smartcard [8–10]. However, the only effort being applied in this line is to store the user's template inside a smart card, protected with Administrators Keys, and extracted from the card by the terminal to perform verification. Some are allowed to verify themselves in the card, whenever the verification is positive, the card allows the access to the biometrically protected information and/or operations [11]. Obviously, these configurations are neither a remedy for the afore-mentioned invasion of privacy problem nor reduce the probability of denial of access with no expense of an increase in the FAR. Most recently, Ho and Armington [12] reported a dual-factor authentication system that designed to counteract imposter by pre-recorded speech and the text-to-speech voice cloning technology, as well as to regulate the inconsistency of audio characteristics among different handsets. The token device generates and prompts an one time password (OTP) to the user. The spoken OTP is then forwarded simultaneously to both a speaker verification module, which verifies the user's voice, and a speech recognition module, which converts the spoken OTP to text and validates it. Despite of that, no attempt for the FAR–FRR interdependent problem is reported.

In this paper, a novel two factor authentication approach which combined user specified tokenised random data with fingerprint feature to generate a unique compact code per person is highlighted. The discretisation is carried out by iterated inner product between the pseudo-random number and the wavelet Fourier–Mellin transform (FMT) fingerprint feature, and finally deciding each bit on the sign based on the predefined threshold. Direct mixing of pseudo-random number and biometric data—BioHashing is an extremely convenient mechanism with which to incorporate physical tokens, such as smart card, USB token etc. thereby resulting in two factors (token+biometrics) credentials via tokenised randomisation. Hence, it protects against biometric fabrication without adversarial knowledge of the randomisation or equivalently possession of the corresponding token. Tokenised discretisation also enables straightforward revocation via token replacement, and furthermore, biohashing has significant functional advantages over solely biometrics i.e. zero equal error rate (EER) point and eliminate the occurrence of FAR without overly imperil the FRR performance.

The outline of the paper is as follow: Section 2 presents the integrated framework of wavelet transform and the FMT for representing the invariant fingerprint feature as well as BioHashing procedure. Section 3 presents the experimental results and the discussion, and followed by concluding remarks in Section 4.



(a) (b)

Fig. 1. 2D wavelet decomposition of a fingerprint image: (a) 1-level wavelet decomposition and (b) 3-level wavelet decomposition.

2. BioHashing overview

BioHashing methodology can be decomposed into two components: (a) an invariant and discriminative integral transform feature of the fingerprint data, with a moderate degree of offset tolerance. This would involve the use of integrated wavelet and Fourier–Mellin transform framework (WFMT) that reported in Ref. [13]. In this framework, wavelet transform preserves the local edges and noise reduction in the low-frequency domain (high energy compacted) after the image decomposition, and hence makes the fingerprint images less sensitive to shape distortion. In addition to that, the reduced dimension of the images also helps to improve the computation efficiency. FMT produces a translation, rotation in plane and scale invariant feature. The linearity property of FMT enables multiple WFMT features to be used to form a reference invariant feature and hence reduce the variability of the input fingerprint images; (b) a discretisation of the data via an inner-product of tokenised random number and user data, i.e. $s = \int \mathrm{d}x \int \mathrm{d}x'.a(x')b^*(x - x')$ for integral transform functions $a,\ b \in L^2$ with enhance offset tolerance. The subsequent sections will detail these two components.

2.1. Invariant WFMT feature

Wavelet theory provides a multiresolution representation for interpreting the image information with the multilevel decomposition [14]. Fig. 1(a) shows the decomposition process by applying the 2D wavelet transform on a fingerprint image in level 1. Similarly, two levels of the wavelet decomposition as shown in Fig. 1(b) by applying wavelet transform on the low-frequency band sequentially. In Fig. 1, the subband L_1 corresponds to the low-frequency components in both vertical and horizontal directions of the original images, making it the low-frequency subband of the original image. The subband $D_{1horizontal}$ corresponds to the high-frequency component in the horizontal direction (horizontal edges). A similar interpretation is made on the subbands $D_{1vertical}$ (vertical edges) and $D_{1Diagonal}$ (both directions).

For fingerprint images, the ridge structure can be viewed as an oriented texture pattern, which often runs parallel in omni direction. According to wavelet theory, the wavelet transform conserves the energy of signals and redistributes this energy into more compact form. It is commonly found that most of the energy content will be concentrated in low-frequency subband, L_j if compare to high-frequency subbands, D_j. Obviously D_js are not suitable to represent the ridge structure because of their low energy content and its high pass feature that tends to enhance the edges detail, including noise and the shape distortion whereas the subband L_j is the smoothed version of original image and thus helps to reduce the influence of noise on one hand, and on the other hand, it also preserves the local edges well which helps to capture the features that insensitive to the small distortion.

However, how well is the L_j can preserve the energy is depend to the chosen wavelet bases. In general, the orthogonal/biorthogonal and high-order wavelet bases are able to preserve the energy efficiently in subband L_j which is only quarter size of the original image [13]. In turn, the computational complexity will be reduced dramatically by working on a lower resolution image.

In the fingerprint authentication, the varying position, scale and the orientation angle of the fingerprint image during the capturing time may severely reduce performance. These alignment problems can be solved by transforming a fingerprint image into an invariant feature. Various translation, rotation and scale invariant methods such as integral transforms, moment invariants and neural network approaches have been proposed [15]. These techniques provide good invariance theories but suffer from the presence of noise, computation complexity or accuracy problem [16]. Among the various invariant techniques, integral transform-based invariants—FMT is adopted as it is a relatively simple generalisation of transform domain and performs well under noise. In addition, mapping to and from the

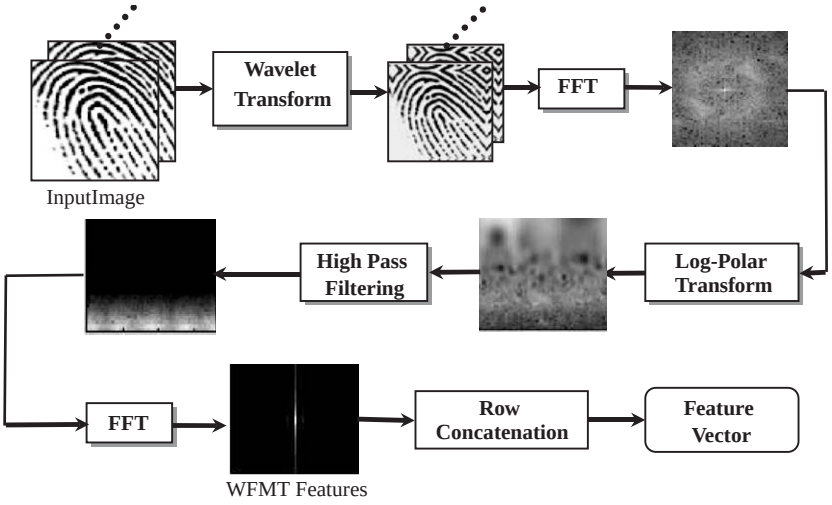


Fig. 2. Block diagram of generating the WFMT features, Γ.

invariant domain to the spatial domain is well defined and it is in general not computationally heavy. FMT is translation invariant and represents rotation and scaling as translations along the corresponding axes in parameter space.

Consider an image $f_2(x, y)$ that is a rotated, scaled and translated replica of $f_1(x, y)$,

$$f_2(x, y) = f_1(\sigma(x\cos\alpha + y\sin\alpha) - x_0, \sigma(-x\sin\alpha + y\cos\alpha) - y_0), \quad (1)$$

where α is the rotation angle, σ the uniform scale factor, and x_0 and y_0 are translational offsets. The Fourier transform of $f_1(x, y)$ and $f_2(x, y)$ are related by

$$F_2(u, v) = \mathrm{e}^{-j\phi_s(u,v)}\sigma^{-2}(F_1(\sigma^{-1}(u\cos\alpha + v\sin\alpha), \sigma^{-1}(-u\sin\alpha + v\cos\alpha))), \quad (2)$$

where $\phi_s(u, v)$ is the spectra phase of the image $f_2(x, y)$. This phase depends on the translation, scaling and rotation, but the spectral magnitude

$$|F_2(u, v)| = \sigma^{-2}|F_1(\sigma^{-1}(u\cos\alpha + v\sin\alpha), \sigma^{-1}(-u\sin\alpha + v\cos\alpha))| \quad (3)$$

is translation invariant.

Rotation and scaling can be decoupled by defining the spectral magnitudes of f_1 and f_2 in the polar coordinates (θ, r) as follows:

$$f_{2p}(\theta, r) = \sigma^{-2} f_{1p}(\theta - \alpha, r/\sigma). \quad (4)$$

Hence, an image rotation shifts the function $f_{1p}(\theta, r)$ along the angular axis. A scaling is reduced to a scaling of the radial coordinate and to a magnification of the intensity by a constant factor σ^2. Scaling can be further reduced to a translation by using a logarithmic scale for the radial coordinate, thus

$$f_{2pl}(\theta, \lambda) = \sigma^{-2} f_{1pl}(\theta - \alpha, r - \eta), \quad (5)$$

where λ=log(r) and η=log(σ). In this polar-logarithmic representation, both rotation and scaling are reduced to translation. By Fourier transforming the polar-logarithm representations (5),

$$F_{2pl}(\zeta, \xi) = \sigma^{-2}\mathrm{e}^{-j2\pi(\zeta\eta + \xi\lambda)} F_{1pl}(\zeta, \xi), \quad (6)$$

where

$$F_{1pl}(\zeta, \xi) = \int_{-\infty}^{\infty}\int_{0}^{2\pi} f_{1pl}(\theta, \lambda)\mathrm{e}^{j(\zeta\lambda + \xi\theta)}\,\mathrm{d}\theta\,\mathrm{d}\lambda, \quad (7)$$

the rotation and scaling now appear as phase shifts. This technique decouples images rotation, scaling and translation, and is therefore very efficient numerically. However, the result stated for the continuous case does not carry over exactly to the discrete case in the actual implementation. Some artifacts may be introduced due to the sampling and truncation if the implementation is not done with care; this is due to the difficulty of numerical instability of coordinates near to the origin. Here care has to be taken in selecting the starting point of the logarithm resampling, since $\lim_{r\to 0}\log r = -\infty$. Therefore, a high-pass filter is apply on the logarithm spectra [17],

$$H(x, y) = (1.0 - \cos(\pi x)\cos(\pi y)) \quad (8)$$

$$(2.0 - \cos(\pi x)\cos(\pi y)) \quad (9)$$

with $-0.5 \leqslant x, y \leqslant 0.5$.

And hence, the block diagram of WFMT feature representation, Γ is shown in Fig. 2.

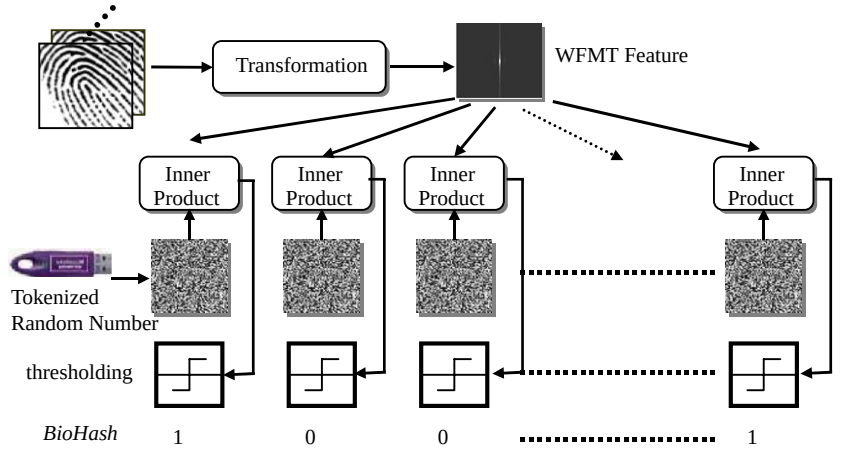


Fig. 3. BioHashing progression.

In this framework, FMT is based on Fourier transform theory, which has a linear property as below:

If $f_i \in \mathbb{R}^2$, a and $b \in C$ (i.e. complex domain), then

$$F_{pl}\left\{\sum_{i=1}^{l} a_i f_i\right\} = \sum_{i=1}^{l} F_{pl}\{a_i f_i\} \tag{10}$$

This implies that multiple $l\Gamma$ can be used to form a reference Γ and just only one representation per user needs to be stored. The representation for each user, Γ_{Ui} can be formulated as follows:

$$\Gamma_{Ui} = \frac{1}{l}\sum_{j=1}^{l} \Gamma^i_j, \tag{11}$$

where Γ^j_i is the invariance feature of the jth view image of the ith person. Producing a Γ_U from different training images, could relax various variability's that occur during the acquisition process, such as sharp distortion and noise.

2.2. Biometrics discretisation

At this stage, the invariant fingerprint feature, $\Gamma \in \mathbb{R}^M$ with M, the log-polar spatial frequency dimension, is reducing down to a set of single bit, $\boldsymbol{b} \in \{0,1\}^m$, with m the length of the bit string via a tokenised pseudo random pattern, $\boldsymbol{r} \in \mathbb{R}^m$, which distributed according to uniform distribution $U[-1\ 1]$. In practice, random number sequence, $\boldsymbol{r}$ could be generated from a physical device, i.e. USB token or smartcard. For a specific application, $\boldsymbol{r}$ is calculated based on a seed that stores in USB token or smart card microprocessor through a random number generator. The seed is the same as those users recorded during the enrollment, and is different among different user and different application. A lot of pseudo random bit/number algorithms are publicly available, to name a few, such as ad hoc scheme—ANSI X9.17 generator, FIPS 186 generator and highly secure scheme: cryptographically secure pseudorandom bit generator (CSPBG)—RSA pseudorandom bit generator, Micali–Schnorr pseudorandom bit generator or Blum–Blum–Shub pseudorandom bit generator [18].

BioHashing is describable in terms of successive simplifications on the following:

(a) Raw intensity image representation: $\boldsymbol{I} \in \mathbb{R}^N$, with N the image pixelisation dimension.
(b) Wavelet Fourier–Mellin representation in a vector format: $\Gamma \in \mathbb{R}^M$, with M, the log-polar spatial frequency dimension.
(c) Discretization, $\boldsymbol{b} \in \{0,1\}^m$

The transition between (a) and (b) is vital in so far as good feature location and extraction can reduce substantially the offset between two fingerprint images of the same person, and thus yield a set of highly offset-tolerant user specific code, $\boldsymbol{b}$ as will be vindicated through the experimental results in Section 3.

The BioHashing progression can be illustrated as in Fig. 3.

Achieving (c) requires an offset-tolerant transformation by projected Γ onto each random pattern, and the choice of a threshold, τ to assign a single bit for each projection, specifically let $\Gamma \in \mathbb{R}^M$

(1) Use token to generate a set of pseudo random number, $\{\boldsymbol{r}_i \in \mathbb{R}^M | i = 1, \ldots, m\}$.
(2) Apply the Gram–Schmidt process to transform the basis $\{\boldsymbol{r}_i \in \mathbb{R}^M | i = 1, \ldots, m\}$ into an orthonormal set of matrices $\{\boldsymbol{r}_{\perp i} \in \mathbb{R}^M | i = 1, \ldots, m\}$.
(3) Compute $\{< \Gamma | \boldsymbol{r}_{\perp i} > \in \mathbb{R} |\ i = 1, \ldots, m\}$ where $\langle \cdot | \cdot \rangle$ indicates inner product operation.

(4) Compute m bits BioHash, $\boldsymbol{b}_i \in 2^m$ from $\boldsymbol{b}_i = \begin{cases} 0 & \text{if } \langle \Gamma | \boldsymbol{r}_{\perp i} \rangle \leqslant \tau \\ 1 & \text{if } \langle \Gamma | \boldsymbol{r}_{\perp i} \rangle > \tau \end{cases}$ $m \leqslant M$, where τ is a preset threshold.

Repetition of this procedure to obtain multiple bits render the issue of inter-bit correlations, which is addressed via orthonormal set $\varsigma = \{\boldsymbol{r}_{\perp k},\ k = 1, 2, \ldots, m\}$. Each bit $\boldsymbol{b}_i$ is hence rendered independent of all others, so that legitimate (and unavoidable) variations in Γ that invert $\boldsymbol{b}_i$ would not necessarily have the same effect on $\boldsymbol{b}_i + 1$.

The primary concern from the security viewpoint centres on protection of information during the representational transformations, and in particular whether (or how) these transformations can be inverted to recover the input information, i.e. biometric fabrication. The above-listed parameters are said to be zero knowledge representations of their inputs if the transformations are non-invertible, as in the case of cryptographic hash $h(\boldsymbol{r}, k) : 2^m \times \underset{m'}{\forall} 2^{m'} \rightarrow 2^m$ for token serialisation $\boldsymbol{r}$ and secret knowledge (arbitrary-length password) k. Note the non-recovery of key-factors $\langle \boldsymbol{r}, k \rangle$ from $h(\boldsymbol{r}, k)$, which motivates an equivalent level of protection for biometric Γ. This is accomplished via token-specification of BioHash representation, i.e. $H(\boldsymbol{r}, \Gamma) : 2^m \times \mathbb{R}^M \rightarrow 2^m$. Note that $H(\boldsymbol{r}, \Gamma)$ cannot be computed with both $\boldsymbol{r}$ and Γ, so that adversarial deduction is no more than probable than random guessing of order 2^{-m}. Besides that, it is highly unlikely for $\boldsymbol{r}$ to have same or close number set if it was generated from two different seeds, especially in CSPBG which protected by the target collision resistance of Hash function.

3. Experiments and discussion

In this paper, the proposed methodology is evaluated on images taken from FVC 2002 (Set A), which is available in DVD included in Ref. [19]. FVC2002 (Set A) provided four different fingerprint databases: DB1, DB2, DB3 and DB4, three of these databases are acquired by various sensors, low cost and high quality, optical and capacitive whereas the fourth contains synthetically generated images. In this paper, we had selected DB1 as the experiment benchmark to vindicate the propose methodology. DB1 contain eight impressions of 100 different fingers, hence 800 images in total. However, the comparison only can be done if both fingerprint images contain their respective core points, but two out of eight impressions for each finger in FVC2002 have no core point due to the exaggerate displacement. In our experiments, these two impressions were excluded as WFMT approach requires to detect the core point in priori and hence, there are only six impressions per finger yielding 600 (6×100) fingerprint images in total for each database. Every finger image will be performed core point detection via the method proposed in Ref. [20] and a 128×128 square region centred in the reference point of the fingerprint images can be cropped. Even though some false core points were detected, they were not deviating too much from the actual core point location. It is commonly known that the slight translation is invariant under FMT and thus we still included those false detected core point images as our experimenting subjects.

Recall the focus of this paper on the effect of post-integral transformation discretisation; hence the experiments of invariant property of WFMT were omitted though the results could be obtained in Ref. [13]. In order to generate WFMT feature, two levels decomposition are performed on a fingerprint image due to the consideration that too coarse resolution is inappropriate, as down sampling process would eliminate the orientation characteristics of ridge structures. However, L_1 subband ($M = 64 \times 64$) with Spline Biorthogonal filter order 5.5 gives the best performance whereas the usage of L_2 seems to decrease the performance [13].

For the FAR test and imposter population distribution as well, the first impression of each finger is matched against the first impression of all other fingers and the same matching process was repeated for subsequent impressions, leading to 29,700 (4950×6) imposter attempts. For the FRR test and genuine population distribution creation, each impression of each finger is matched against all other impressions of the same finger, leading to 1500 (15 attempts of each finger $\times 10$).

The experimental settings are as follows:

- *wfm*: denoting wavelet Fourier–Mellin transformation configuration.
- *wfmm*: denoting multiple representation of wavelet Fourier–Mellin transformation configuration described in Eq. (10), where $l = 4$, an optimum configuration [13].
- *wfmd-m*: denoting 2^m discretisation on *wfm* with the threshold value, $\tau = 0$ where m is the bit length.
- *wfmmd-m*: denoting 2^m discretisation on *wfmm* with $\tau = 0$ where m is the bit length.

The experimental data is acquired for $m = 20$, 40, 60 and 80 in all cases while for the similarity matching, a simple Euclidean distance metric is adopted for *wfm* as well as *wfmm* whereas Hamming distance is used in *wfmd-m* and *wfmmd-m*.

3.1. Genuine and imposter population distribution histograms

Fig. 4 illustrated the genuine and imposter population distribution for *wfm* and *wfmm*, respectively. The genuine distribution shows the results when different images of the same fingerprint are compared; but when images from different fingerprints are compared, the imposter distribution is the outcome. The results show the smaller overlapping in between genuine and imposter populations for *wfmm* compared to *wfm*. It implies that *wfmm* minimise the distance between images from the same class, and hence make

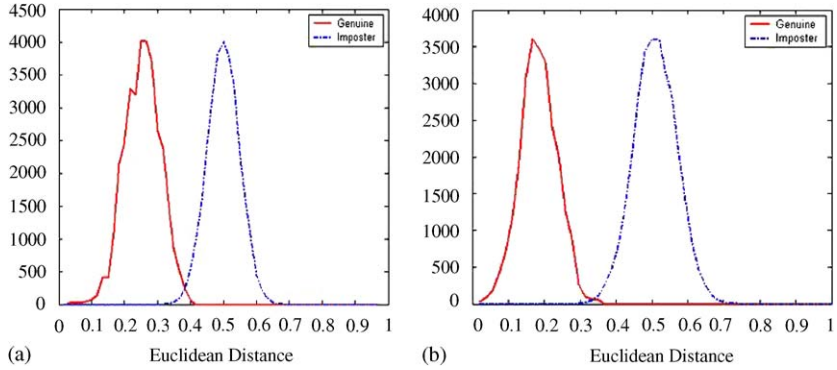


Fig. 4. Euclidean distance histograms for *wfm* and *wfmm*: (a) *wfm* and (b) *wfmm*.

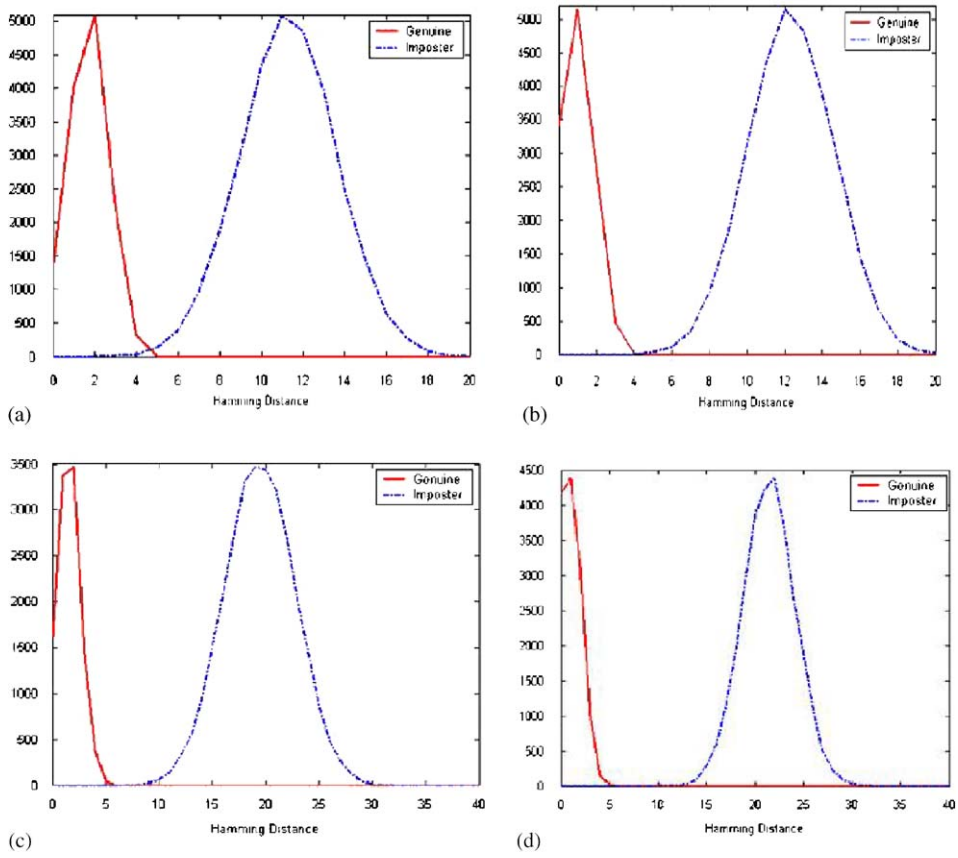


Fig. 5. Genuine and imposter population distribution for *wfmd-m* and *wfmmd-m*: (a) *wfmm*-20, (b) *wfmmd*-20, (c) *wfmd*-40, (d) *wfmmd*-40, (e) *wfmd*-60, (f) *wfmmd*-60 (g) *wfmd*-80 and (h) *wfmmd*-80.

it more favor in the classification task. However, a clean separation in between genuine and imposter populations is substantial for the FRR–FAR interdependent problem, i.e. denial of access issue in the conventional biometrics context. Clean separation and centralization of the genuine populations of *wfmd*-80 and *wfmmd-m* with $m = 40$, 60 and 80 in Fig. 5 at Hamming distances of near 0—indicate that disagreeing bits is very tightly packed around 1% whereas for

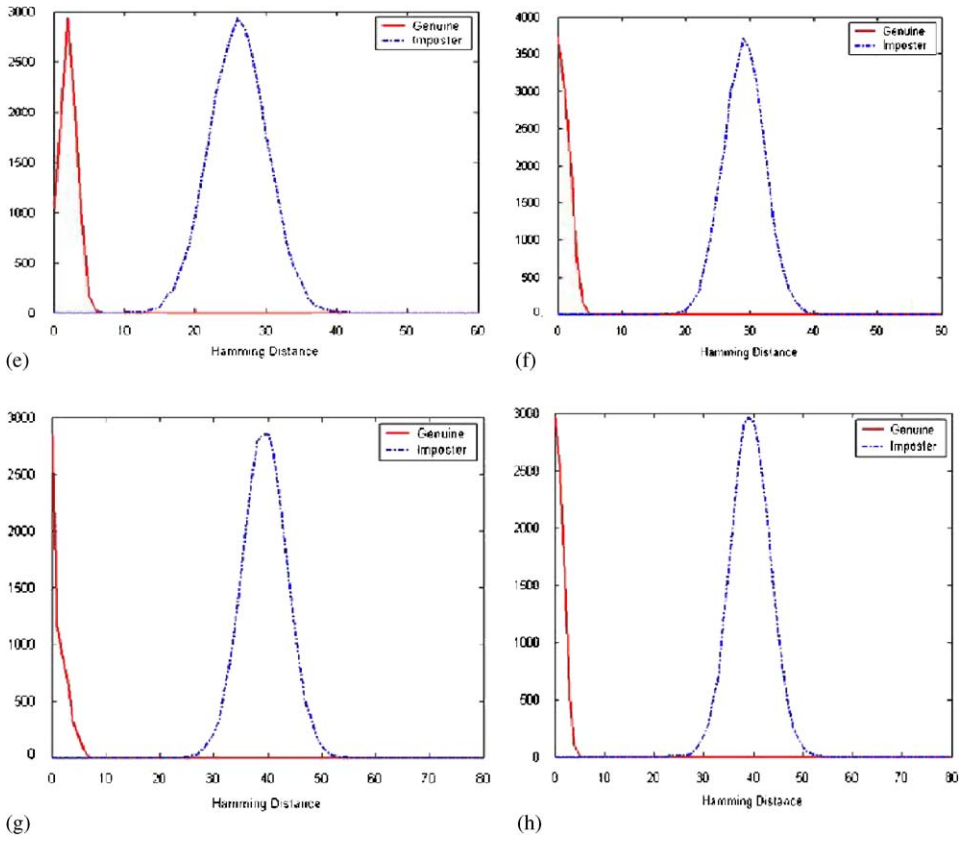


Fig. 5. (*continued*).

imposter populations: about $\frac{1}{2}m$—50% bits may differ; both of which vindications of the proposed approach. This indicates *wfmd-m* as well as *wfmmd-m* outweighs both *wfm* and *wfmm* by minimising the intra-class distance and maximising the inter-class distance, hence the attractiveness of the *wfmd-m* and *wfmmd-m* genuine population with its steeper peak-to-plateau drop-offs compared to the corresponding *wfm* and *wfmm* profiles is apparent. These sharp drop-offs are clearly seen in *wfmd*-80 and *wfmmd-m* with $m = 40$–80, and thus allow for specification of zero FAR without jeopardizing the FRR performance, which will further clarify in next section.

3.2. FAR, FRR and EER characteristics

Establishment of FRR (FAR = 0%) and the EER criteria, at which point (FAR+FRR)/2 for a particular configuration requires analysis of FAR–FRR receiver operating curve (ROC), which can be developed by varying a range of normalised threshold values in between 0 and 1, as illustrated in Fig. 6.

Note that EER near to zero of *wfmd-m* and EER = 0% of *wfmmd-m* compared to both *wfm* and *wfmm* in Table 1

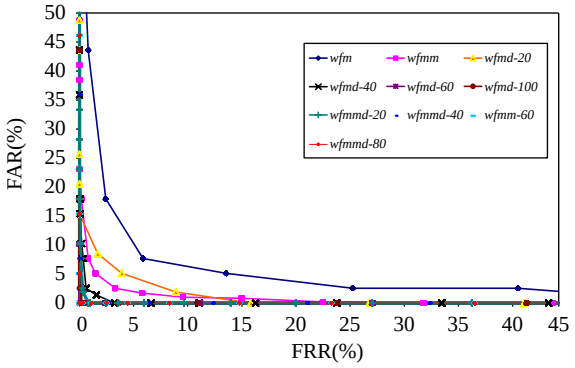


Fig. 6. Receiver operating curve for *wfm*, *wfmm*, *wfmd-m* and *wfmmd-m*.

reveals the robustness of *wfmd-m* and *wfmmd-m* in the verification task, this also can be seen from the consistent locations of *wfmd-m* and *wfmmd-m* inside the corresponding *wfm* and *wfmm* profile that shown in Fig. 6. This confirms the previous observation in Section 3.1 in term of the criteria for FRR when FAR = 0%, thereby the proposed

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

	FAR (%)	FRR (%)	EER (%)	FRR (%) (FAR = 0%)	Threshold range when EER = 0% ($[t_{max} - t_{min}]$
wfm	5.93	5.38	5.66	47.16	—
wfmm	1.00	1.02	1.01	23.08	—
wfmd-20	3.91	4.12	4.02	15.86	—
wfmd-40	1.55	2.56	2.06	2.56	—
wfmd-60	0.14	0.00	0.07	0.04	—
wfmd-80	0.00	0.00	0.00	0.00	[0.18 − 0.05] 0.13
wfmmd-20	0.88	0.34	0.61	0.94	—
wfmmd-40	0.00	0.00	0.00	0.00	[0.32 − 0.08] 0.24
wfmmd-60	0.00	0.00	0.00	0.00	[0.38 − 0.05] 0.33
wfmmd-80	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, $\boldsymbol{b}$ 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 $\boldsymbol{b}$ 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, thre is no deterministic way to get the user specific code without having both token with random data and user fingerprint. In order to validate this, an experiment is conducted to simulate the situations below:

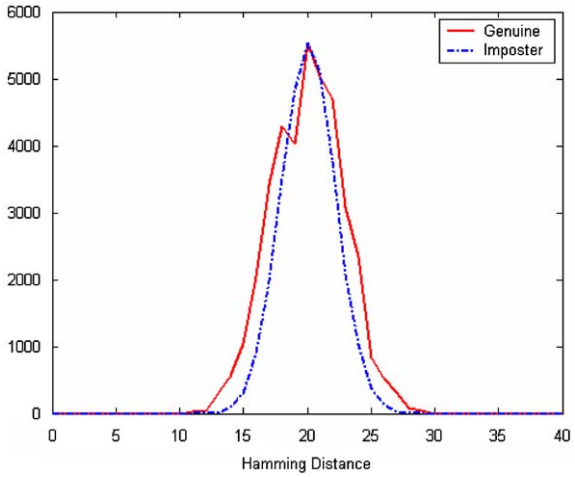


Fig. 7. Genuine and imposter population distribution histogram for case 2.

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

Then, the following three cases can be derived:

Case 1: $\langle \boldsymbol{r}_A, \Gamma_{EA} \rangle \leftrightarrows \langle \boldsymbol{r}_A, \Gamma_{TA} \rangle$.

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

Case 2: $\langle \boldsymbol{r}_A, \Gamma_{EA} \rangle \leftrightarrows \langle \boldsymbol{r}_o, \Gamma_{TA} \rangle$.

This case presumes A lost his/her token credential, i.e. $\boldsymbol{r}_A$ and replace with $\boldsymbol{r}_o$ 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

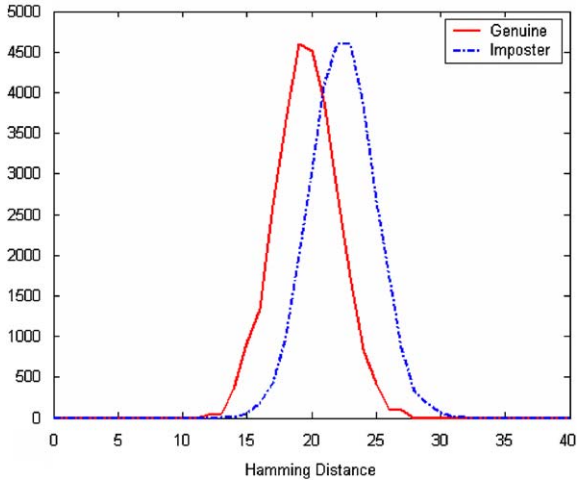


Fig. 8. Genuine and imposter population distribution histogram for case 3.

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. $\boldsymbol{r}_o$ is used to mix with Γ_{TA}.

Case 3: $\langle \boldsymbol{r}_A, \Gamma_{EA}\rangle \leftrightarrows \langle \boldsymbol{r}_A, \Gamma_{To}\rangle$.

When Γ_{TA} is replaced with a non-legitimate fingerprint feature, Γ_{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 $\boldsymbol{b}$ 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 allieviated 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.