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 © 2004 Pattern Recognition Society. Published by Elsevier Ltd. All rights reserved.
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.

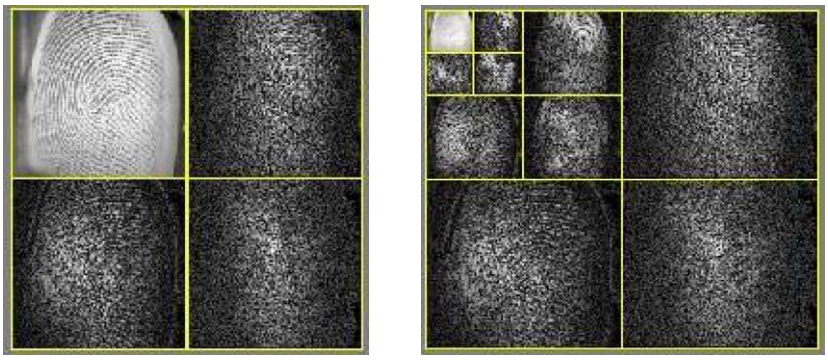
Besides that, the nature of biometrics system offers binary (yes/no) decisions scheme, which is well defined in the classical framework of statistical decision theory, thereby provided four possible outcomes are normally called as false accept rate (FAR), correct accept rate (CAR), false reject rate (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

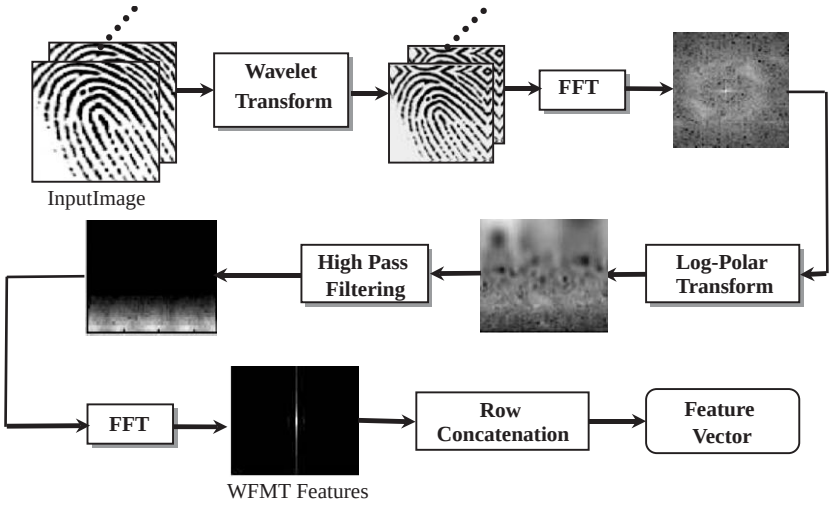


Fig. 2. Block diagram of generating the WFMT features, Γ.

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.

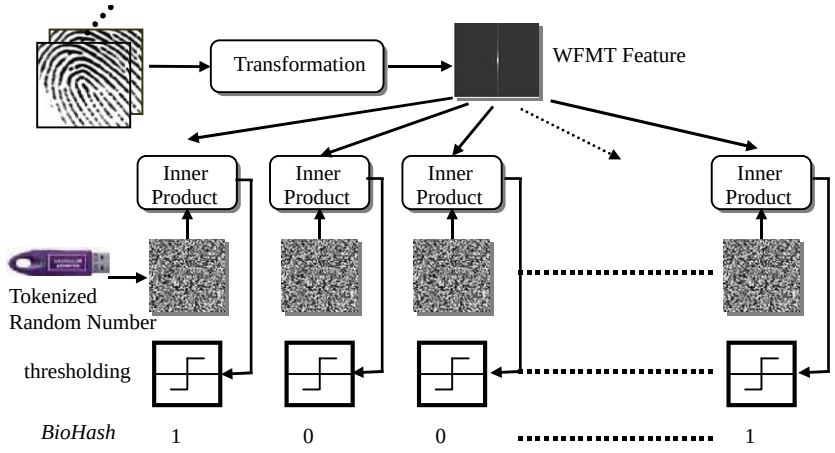


Fig. 3. BioHashing progression.

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:

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

where Γ_i^j 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.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.