Computers & Security (2004) **23**, 606–614

ELSEVIER

Computers & Security

www.elsevier.com/locate/cose

Personalised cryptographic key generation based on FaceHashing

Andrew B.J. Teoh[a,*], David C.L. Ngo[a,1], Alwyn Goh[b,2]

[a]*Faculty of Information Science and Technology, Multimedia University, Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia*
[b]*Corentix Laboratories, 32 Jalan Tempua 5, 47100 Puchong, Malaysia*

Received 8 January 2004; accepted 2 June 2004

KEYWORDS
Biometric based key cryptography;
Face recognition;
Wavelet Fourier-Mellin transform;
Tokenised pseudo random number;
Shamir's secret-sharing scheme;

Abstract Among the various computer security techniques practice today, cryptography has been identified as one of the most important solutions in the integrated digital security system. Cryptographic techniques such as encryption can provide very long passwords that are not required to be remembered but are in turn protected by simple password, hence defecting their purpose. In this paper, we proposed a novel two-stage technique to generate personalized cryptographic keys from the face biometric, which offers the inextricably link to its owner. At the first stage, integral transform of biometric input is to discretise to produce a set of bit representation with a set of tokenised pseudo random number, coined as FaceHash. In the second stage, FaceHash is then securely reduced to a single cryptographic key via Shamir secret-sharing. Tokenised FaceHashing is rigorously protective of the face data, with security comparable to cryptographic hashing of token and knowledge key-factor. The key is constructed to resist cryptanalysis even against an adversary who captures the user device or the feature descriptor.

* Corresponding author. Tel.: +606 252 3457; fax: +606 231 8840.
E-mail addresses: bjteoh@mmu.edu.my (A.B.J. Teoh), david.ngo@mmu.edu.my (D.C.L. Ngo), alwyn_goh@yahoo.co.uk (A. Goh).
[1] Tel.: +606 252 3111/3485.
[2] Tel.: +603 58910155.

0167-4048/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2004.06.002

Introduction

Security is a major concern in today's digital era. Cryptography has been recognized as one of the most popular technology to solve the four principle security goals, i.e. privacy, authentication, integrity and authorization (Smith, 1997). In general, data will be secured using symmetric crypto system, while public-key system will be deployed for digital signatures and for secure key exchange between users. Cryptographic techniques such as encryption can provide very long passwords (strong cryptographic keys) which are not required to be remembered but are in turn protected by a simple password, but once the password is compromised, the entire solution may fall apart.

A biometric is a feature measured from the human body that is distinguishing enough to be used for user authentication. Examples include voice, handwriting, face, eye and face and signature. Biometric offers to inextricably link the authenticator to its owner, something passwords or token cannot do, since they can be lent or stolen. When used in cryptographic key generation context, this inextricable link can be adopted to replace password to rectify the aforementioned problem. In the simplest biometrics-cryptographic key application, an external specific crypto key may be stored as a portion of a user's particular, i.e. user name, biometric template, access privileges, etc. which may be released upon a successful match. This is fine in key management but secure only when the user's particular is placed and the matching is done in secure region. Apparently, it is useful to generate cryptographic key directly from the user-specific biometrics. This can be done by deriving some independent, non-recovery parameters that are solely tied to a particular person, and thus crypto techniques can utilize these parameters as crypto key for encryption or decryption purposes. Basically, the biometrics based key generation process could be made either in a front-end approach or in a back-end approach (Peyravian et al., 1999). In front-end approach, the designation of the initial seed value of PRNG (Pseudo Random Number Generator) is modified or extended to include a user-specific data, i.e. biometrics component whereas in the back-end approach, the random numbers which are produced by the PRNG are processed to make it dependent on biometrics data. However, the representation problem is simply that biometric data are continuous and statistically frustrated, while cryptographic parameters are discrete and have zero-uncertainty. Biometric consistency measured from the difference between reference and test data is similar but never equal and hence inadequate for cryptographic purposes which require exact reproduction.

The first notion of using biometric parameter directly as a crypto key was proposed by Bodo (1994). However, instability of biometrics during the course of time and non-appreciable equal error rate—the error rate occurring when the decision threshold of a system is set so that the proportion of false rejections will be approximately equal to the proportion of false acceptances—hinders its direct use as a crypto key. Also if the key is ever compromised, the use of that biometrics will be lost irrevocably which is inconsistent with a system that requires periodic updating. The Soutar et al. (1999) research outlines cryptographic key recovery from the integral correlation of fingerprint data and previously registered *Bioscrypts*. *Bioscrypts* result from the mixing of random and user-specific data, thereby preventing recovery of the original fingerprint data with data capture uncertainties addressed via multiply-redundant majority-result table lookups. The Soutar et al. formulation is nevertheless restrictive in that keys are externally specified and then recovered, rather than internally computed. The Davida et al. (1998) formulation outlines cryptographic signature verification of iris data without stored references. This is accomplished via open token-based storage of user-specific Hamming codes necessary to rectify offsets in the test data, thereby allowing verification of the corrected biometrics. Such self-correcting biometric representations are applicable towards key computation, with recovery of iris data via analysis of these codes prevented by complexity theory. Monrose et al. key computation from user-specific keystroke (Monrose et al., 1999) and voice (Monrose et al., 2001) data is both deterministic and probabilistic. The methodology (broadly similar in both cases) specifies the deterministic concatenation of single bit outputs based on logical characterizations of the biometric data, in particular whether user-specific features are below (0) or above (1) some population-generic threshold. This accumulation of 0 and 1 response with the additional possibility of an indeterminate ($\varnothing$) output for certain features is then used in conjunction with randomized lookup tables formulated via Shamir secret-sharing (Shamir, 1979).

This paper proposed a novel cryptographic key computation technique from face biometrics. The proposed technique can be characterized as having two stages: feature extraction and key computation (cryptographic key interpolation) Goh and

Ngo, 2003. In the feature extraction stage, certain features of raw input from a biometric-measuring device are examined and used to compute a set of bit string, coined as *FaceHash*. The key computation stage develops a cryptographic key from the *FaceHash* and stored cryptographic data in the device. If two *FaceHash* are sufficiently similar, then the same cryptographic key will be generated from them. We provide the experimental results to illustrate high stability of *FaceHash*, which is vital for key generation. *FaceHash* is rigorously protective of the face data, with security comparable to cryptographic hashing of token and knowledge key-factor. The key is constructed to resist cryptanalysis even against an adversary who captures the user device or the feature descriptor.

The following section provides an overview of our approach while the next three sections present its components in detail. Further the experimental results and a security analysis in terms of key-factor independent and non-recovery are discussed. Finally, the last section gives the concluding remarks of this paper.

Biometric based cryptographic key derivation overview

As aforementioned, biometrics and cryptography are the two opposed paradigms and this had motivated the formulation of highly offset-tolerant discretisation methodology—*FaceHashing*. The process is crucial to our biometric based crypto key derivation through our two-stage scheme as illustrated in Fig. 1.

The proposed scheme contains two stages while stage one could be subdivided into two parts:

Stage 1: Feature extraction

(a) The first step is to transform the raw face data, $I \in \Re^N$, where N is the image pixelisation dimension into another image representation in log-polar frequency domain, $\Gamma \in \Re^M$, where $M < N$ denotes log-polar spatial frequency dimension by using integrated Wavelet and Fourier-Mellin transform framework (WFMT) (Andrew and David, 2003). Wavelet transform, with its approximate decomposition is used to reduce the noise and produce a representation in the low frequency domain, and hence makes the facial images insensitive to facial expression and small occlusion. The Fourier-Mellin transform served to produce a translation, rotation and scale invariant feature.

(b) This step engaged discretisation process of the data via a repeated inner-product of a secret number (a number uniquely associated with a token) and user data, i.e. $s = \int_c dx f'(x) g(x)$ for integral transform functions f, $g \in L^2$ with enhance offset tolerance. The goal is to extract the main features of the face data, which are the most stable for images from same user, and vary a lot for different users. The extracted bit strings are coined as *FaceHash*.

Stage 2: Key computation (cryptographic key interpolation)

By using a secret-sharing scheme (called Shamir's threshold scheme), we develop a cryptographic key k_c (an element of the field Z_q, for some prime q) from *FaceHash* with length l_b, $\boldsymbol{b} \in \{0,1\}^{l_b}$, and stored cryptographic data in the device. It can be shown that this scheme satisfies both the availability (i.e., a quorum number of key shares suffice to reconstruct the secret key) and non-recovery (i.e., compromise of certain number of key shares does not expose the secret key) properties. The subsequent sections will detail these three components.

Stage 1(a): wavelet Fourier-Mellin transform feature construction

The wavelet decomposition of a signal $f(x)$ can be obtained by convolution of signal with a family of real orthonormal basis, $\psi_{a,b}(x)$

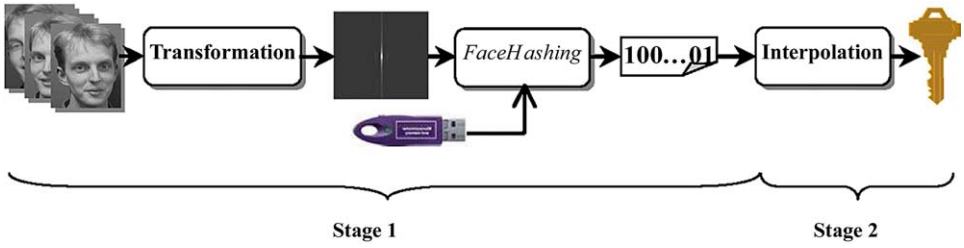


Figure 1 Biometric based cryptographic key derivation procedure.

$$(W_\psi f(x))(a,b) = |a|^{-1/2} \int_{\Re} f(x)\psi\left(\frac{x-b}{a}\right) dx \qquad (1)$$

where a, b and $a \neq 0$ are the dilation parameter and the translation parameter, respectively. Two-dimensional wavelet transform leads to a decomposition of approximation coefficients at level $j-1$ in four components: the approximations at level j, L_j and the details in three orientations (horizontal, vertical and diagonal), $D_{j\text{vertical}}$, $D_{j\text{horizontal}}$ and $D_{j\text{diagonal}}$ (Mallat, 1998).

In an early study, Harmon (1973) found that information in low spatial frequency bands have a dominant role in face recognition. Besides, Nastar et al. (1997) found that facial expressions and small occlusion affect the high-frequency spectrum whereas changes in pose or scale of a face affect their low frequency spectrum, while a change in face will affect all frequency components. As such, L_j, as the smoothed version that corresponded to low or middle band in the frequency spectrum, are insensitive to the facial expressions and small occlusion and optimal for the recognition purpose.

In the face authentication, the varying position, scale and the orientation angle of the face image during the capturing time may severely reduce performance. These alignment problems can be solved by transforming a face image into an invariant feature by using Fourier-Mellin transform (FMT) Reddy and Chatterji, 1996. FMT is translation invariant and represents rotation and scaling as translations along the corresponding axes in parameter space, and thus this technique decouples images rotation, scaling and translation, and is also therefore very efficient numerically by utilizing the Fast Fourier transform (FFT). However, the result stated for the continuous case does not carry over exactly to the discrete case. Some artifacts may be introduced due to the sampling and truncation if the implementation is not done with care. Therefore a high-pass filter is applied on the logarithm spectra, $H(x,y) = (1-\cos(\pi x)\cos(\pi y))(2-\cos(\pi x)\cos(\pi y))$ with $-0.5 \leq x, y \leq 0.5$. And hence, the block diagram of Wavelet Fourier-Mellin transform (WFMT) feature representation, Γ is shown in Fig. 2.

Stage 1(b): biometrics discretisation

At this stage, the invariant face feature, $\Gamma \in \Re^M$ with M, the log-polar spatial frequency dimension, is reducing down to a set of single bit, $\boldsymbol{b} \in \{0,1\}^{l_b}$, with l_b the length of the bit string via a uniform distributed secret pseudo random number, $\boldsymbol{r} \in \{-1,1\}$ that is uniquely associated with a token.

Specifically, let $\Gamma \in \Re^M$,

(1) Use token to generate a set of pseudo random number, $\{\boldsymbol{r}_i \in \Re^M | i = 1,\ldots,l_b\}$.
(2) Apply the Gram-Schmidt process to transform the basis $\{\boldsymbol{r}_i \in \Re^M | i = 1,\ldots,l_b\}$ into an orthonormal set of matrices $\{\boldsymbol{r}_{\perp i} \in \Re^M | i = 1,\ldots,l_b\}$.
(3) Compute $\{\langle \Gamma | \boldsymbol{r}_{\perp i} \rangle \in \Re | i = 1,\ldots,l_b\}$ where $\langle\ |\ \rangle$ indicates inner-product operation.
(4) Compute l_b bits *FaceHash*, $\boldsymbol{b}_i \in 2^{l_b}$ from

$$\boldsymbol{b}_i = \begin{cases} 0 & \text{if } \langle \Gamma | \boldsymbol{r}_{\perp i} \rangle \leq \tau \\ 1 & \text{if } \langle \Gamma | \boldsymbol{r}_{\perp i} \rangle > \tau \end{cases} \quad l_b \leq M,$$

where τ is a preset threshold. In this paper, the τ is set to 0.

Repetition of this procedure to obtain multiple bits renders the issue of inter-bit correlations, this issue is addressed via Gram-Schmidt process to obtain orthonormal set $\varsigma = \{\boldsymbol{r}_{\perp k} | k = 1,2,\ldots,l_b\}$. Each bit $\boldsymbol{b}_i(\boldsymbol{x})$ is hence rendered independent of

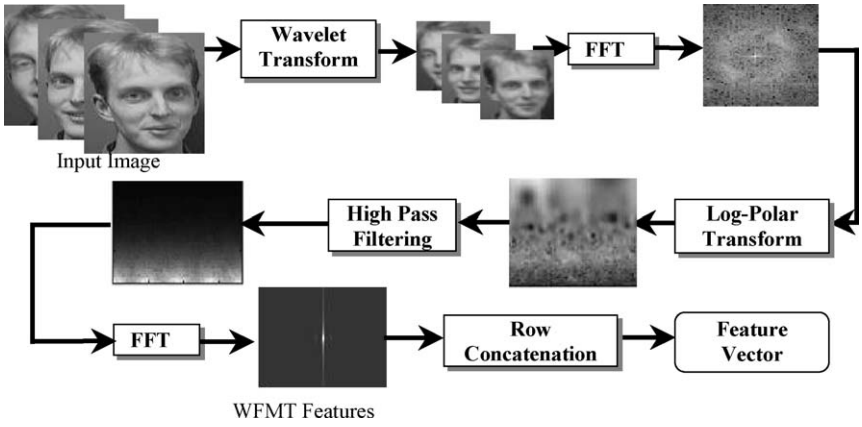


Figure 2 Block diagram of generating the WFMT features.

all others, so that legitimate (and unavoidable) variations in Γ that invert $\boldsymbol{b}_i(\boldsymbol{x})$ would not necessarily have the same effect on $\boldsymbol{b}_{l+1}(\boldsymbol{x})$. Besides, the progression is worth noting that there is no apriori restriction on the value of l_b, though $l_b < M$ and that by the virtue of using pseudo random pattern, $\boldsymbol{b} \in \{0,1\}^{l_b}$ can be interpolated.

The above-listed parameters are said to be zero knowledge (ZK) representations of their inputs if the transformations are non-invertible, as in the case of cryptographic hash

$$h(\boldsymbol{r},k) : 2^{l_b} \times \underset{l_b'}{\forall} 2^{l_b'} \rightarrow 2^{l_b}$$

for tokenised pseudo random number, $\boldsymbol{r}$ and secret knowledge (arbitrary-length password) k. The non-recovery of key-factors $\langle \boldsymbol{r}, k \rangle$ from $h(\boldsymbol{r}, k)$ motivates an equivalent level of protection for biometric Γ, which is accomplished via token-specification of representations in this stage 1(b) and stage 2 briefed in the section following 'Introduction', such that *FaceHash* $H(\boldsymbol{r}_\perp, \Gamma) : 2^{l_b} \times \Re^M \rightarrow 2^{l_b}$ does not jeopardize $\langle \boldsymbol{r}_\perp, \Gamma \rangle$. This is crucial from the security viewpoint whether (or how) these transformations can be inverted to recover the input information because once a biometric image or template is stolen; it is stolen forever and cannot be reissued, updated or destroyed as well as its corresponding crypto key. ZK representation $H(\boldsymbol{r}_\perp, \Gamma)$ is subsequently useful for standard cryptographic operations, such as signature generation and message decryption. Note H has an important (and challenging) additional requirement over h, namely offset tolerance so that $H(\boldsymbol{r}_\perp, \Gamma)$ is stable for $\Gamma \in \Re^M$. This requirement essentially addresses the fundamental gap between biometric similarity and cryptographic equality.

Cryptographic key interpolation (Shamir's (2, l_s)-thresholding scheme)

The limited uncertainty of *FaceHash*, $\boldsymbol{b} \in \{0,1\}^{l_b}$ is addressed via Shamir secret-sharing (Shamir, 1979); which uses modular polynomial $p(x) : Z_q \rightarrow Z_q$ where q is a prime for secret encoding $p(0) = k_c$ i.e. the $2^{l_b} \subset Z_q$ cryptographic key in our context. In the simplest case of linear polynomials, this allows secret recovery via

$$k_c = \frac{H(\boldsymbol{b})p(H(\boldsymbol{r}_\perp))}{H(\boldsymbol{b}) - H(\boldsymbol{r}_\perp)} + \frac{H(\boldsymbol{r}_\perp)p(H(\boldsymbol{b}))}{H(\boldsymbol{r}_\perp) - H(\boldsymbol{b})} (\text{mod } q) \qquad (2)$$

where $\boldsymbol{r}_\perp$ be the orthonormalized token number used to compute the *FaceHash*, $\boldsymbol{b}$ and $H(\ )$ is the hashing function. The details of the implementation of the biometrics based cryptographic key derivation, which occurs during the enrollment and the verification stage are provided below. This constitutes a rigorous 2 of l_s threshold system with l_s the number $\boldsymbol{b}$ of a particular user.

Enrollment

Let k_c be a secret key and $\{\boldsymbol{b}_i^0 | i = 1, \ldots, l_s\}$ denotes l_s possible *FaceHash* associated with a particular user. The superscript 0 refers to the images acquired during the enrollment.

1. Choose a random degree-1 polynomial $p \in Z_q$ such that $p(0) = k_c$.
2. Compute coordinate pair $\{X^0, Y^0\}$ to constitute a secret-share, such as
   $X^0 : \{x_{r_\perp}^0 = H(\boldsymbol{r}_\perp) \cup x_i^0 = H(\mathrm{b}_i^0) | i = 1, \ldots, l_s\}$,
   $H^0 : \{h_i^0 = H(x_i^0), | i = 1, \ldots, l_s\}$ and
   $Y^0 : \{y_{r_\perp}^0 = p(x_{r_\perp}^0) \cup y_i^0 = p(x_i^0) | i = 1, \ldots, l_s\}$.
3. Store $\chi = \{H^0, Y^0\}$ on token.

Verification (key retrieval)

Let $\{\boldsymbol{b}_i^1 | i = 1, \ldots l_s\}$. The superscript 1 represents an image used in verification.

1. Compute
   $X^1 : \{x_{r_\perp}^1 = H(\boldsymbol{r}_\perp) \cup x_i^1 = H(\mathrm{b}_i^1) | i = 1, \ldots, l_s\}$ and
   $H^1 : \{h_i^1 = H(x_i^1) | i = 1, \ldots, l_s\}$.
2. Retrieve $H^0 : \{h_i^0 | i = 1, \ldots, l_s\}$ and $Y^0 : \{y_{r_\perp}^0 \cup y_i^0 | i = 1, \ldots, l_s\}$ from χ in token.
3. Extract k_c iff $h_i^0 = h_j^1$ for any $i, j \in \{1, \ldots, l_s\}$,

$$k_c = \frac{y_{r_\perp}^0 x_j^1}{x_j^1 - x_{r_\perp}^1} + \frac{y_i^0 x_{r_\perp}^1}{x_{r_\perp}^1 - x_j^1} (\text{mod } q).$$

Note that k_c cannot be computed without one of the *FaceHash*, $\boldsymbol{b}$ or correct token $\boldsymbol{r}_\perp$ and that neither of these can be recovered from the ZK representations in χ. The latter can in fact be stored completely in the open, which is illustrative of the protocol-level security.

Key interpolation is interpreted as a final error-correcting step in this context, supplementing the basic robustness of *FaceHash* and the replacement of bits over-sensitive to legitimate variations in Γ. End result $H(\boldsymbol{r}_\perp, \Gamma)$ is hence:

- Sensitively dependant on $\boldsymbol{r}_\perp$: so that exact correctness is required for $\boldsymbol{r}_\perp$ and $H(\boldsymbol{r}_\perp)$, the former of which contributes sensitively towards $\boldsymbol{b} \in \{0,1\}^{l_b}$.

- Robustly dependant on $\boldsymbol{b}$ so that:
  1. Minor variations (corresponding to the same user) still result in $\boldsymbol{b}$.
  2. Major variations (corresponding to different users) result in $\boldsymbol{b}'$ ($\neq \boldsymbol{b}$) commensurate with the discrete $\boldsymbol{r}_{\perp}$ and continuous k_c key-factors.

Experiments and discussion

In this section, we provide the experimental results to illustrate highly error tolerant of *Face-Hash*, which is vital for key generation. The proposed method has been evaluated in terms of their same user (genuine)/different user (imposter) population distribution achieved in *Essex Faces 94* and *Olivetti Face Database* (*ORL database*). *Essex Faces 94* contains frontal face photos taken from a fixed camera distance and under the uniform background and the illumination, with the subjects asked to speak: throughout the process; resulting very minor variations in turn, tilt and slant as well as rotation in plane face images and in fix illumination and scale. The test set contains 153 subjects with 20 images for each subject. *Fnces 94* is considered to be somewhat less challenging in comparison to *ORL database* from the viewpoint of scale, aspect and illumination offsets; but it is well suited to simulate our anticipated operational scenario, such as individual users in desktop or kiosk environments. This database is assembled by the Computer Vision Group of Essex University, and made publicly available at URL http://cswww.essex.ac.uk/mv/allfaces/index.html. On the other hand, *ORL database* is made up of 10 different images of 40 distinct subjects. For some subjects, the images were taken at different times, varying lighting, facial expressions (open/closed eyes, smiling/not smiling), and facial details (glasses/no glasses). All the images were taken against a dark homogeneous background with the subjects in an upright, frontal position with variations in turn, tilt and slant. *ORL database* is publicly available at the URL http://www.uk.research.att.com/facedatabase.html. Fig. 3 shows a few samples that are taken from *ORL Face Database*.

For the imposter population generation, the first image of each subject is matched by using a certain dissimilarity measure against the first image of all other subjects and the same matching process was repeated for subsequent impressions, leading to 232,560 ($23{,}256 \times 20$) imposter attempts for *Essex Faces 94* and 7800 (780×10) for *ORL database*. For the genuine population, each image of each subject is matched against all other images of the same subject, leading to 29,070 (190 attempts o f each subject $\times$ 153) for *Essex Faces 94* while 1800 (45 attempts of each subject $\times$ 40) for *ORL database*. Note that since only face images are found in the scene in both databases, thus face detection is not required for this database. Generally speaking, all wavelet bases with smooth, compactly support orthogonal can be chosen, and hence a wavelet base with Daubechies Filter 7 in level 1 is selected for WFMT generation.

Following are the abbreviations used for brevity in this paper:

- *wfmt*: denoting wavelet Fourier-Mellin transform configuration;
- *wfmtd*-l_b: denoting 2^{l_b} discretisation, where l_b is the bit length.

The experimental data are acquired for $l_b = 20$, 40, 60 and 80 in all cases while for the dissimilarity matching, Euclidean distance metric is adopted for *wfmt* whereas Hamming distance is used in *wfmtd*-l_b.

From Fig. 5, genuine populations for *wfmtd*-l_b centralized at Hamming distance of 0, particularly for $l_b = 40$, 60 and 80 while imposter populations centered at $l_b/2$ for *Essex Faces 94*, indicate that

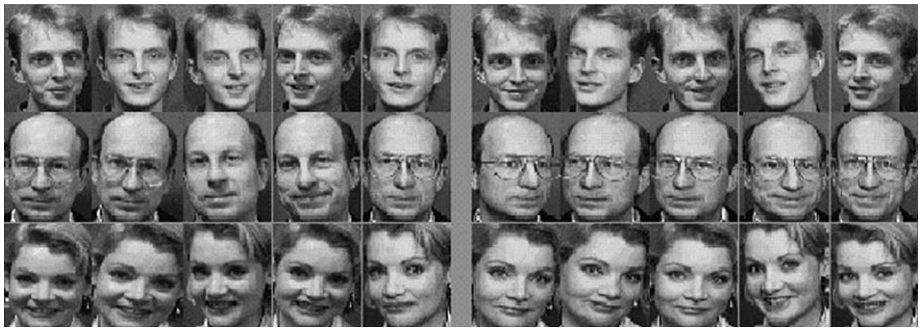


Figure 3 Face samples from *ORL Face Database*.

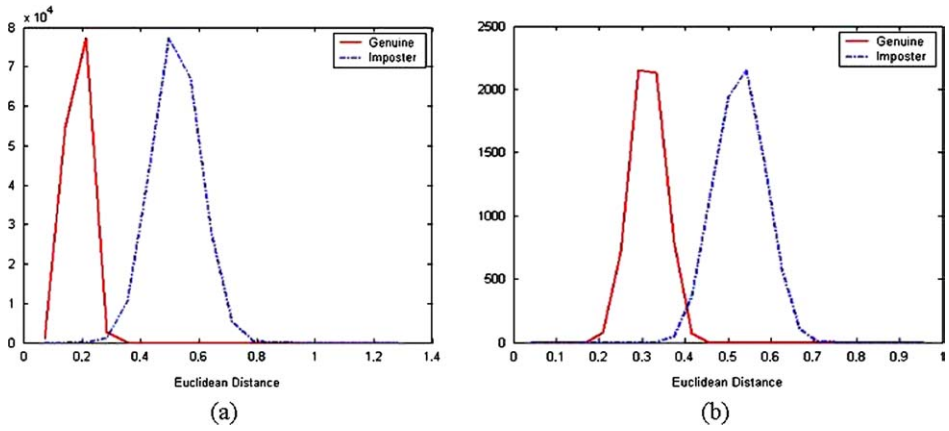


Figure 4 Genuine and imposter population distribution for *wfmt* from (a) *Essex Faces 94* and (b) *ORL Face Database*.

zero (or very small) bit different of two face images from a user and about 50% bit different from different face images. For *ORL database*, they also had shown centralization of near 0 for genuine population and $l_b/2$ for imposter populations despite *ORL database* being more challenging than *Essex Faces 94*. Besides, clear separation of genuine/imposter population is tremendously important from the security viewpoint as it implies that both zero False Acceptance (the probability that a biometric system fails to reject an impostor) as well as False Rejection (the probability that a biometric system fails to verify the legitimate) claimed identity of an enrollee. Compared to the conventional biometrics approach, for *wfmt* as shown in Fig. 4, it is extremely difficult or impossible to obtain a clear separation of genuine/imposter population (Daugman, 2002). This indicates that *wfmtd-*l_b outweighs *wfmt* by minimizing the intra-class distance and maximizing the inter-class distance. Both observations vindicate the robustness *of FaceHash*, $\boldsymbol{b}$ to resist the variations among the same users and otherwise for the different users as discussed in 'Verification (key retrieval)' section.

Security analysis

The security of $H : 2^{l_b} \times \Re^M \rightarrow Z_q$, where q is a prime number, transformation should be evaluated in terms of key-factor:

- *Independence*, such as evaluation of $H(\boldsymbol{r}_\perp, \Gamma)$ in the absence of $\boldsymbol{r}_\perp$ or Γ.
- *Non-recovery* of $\boldsymbol{r}_\perp$ or Γ given specific value of $\Gamma(\boldsymbol{r}_\perp, \Gamma)$ and the other factor.With the benchmark being cryptographic hashing

$$h(\boldsymbol{r}, k) : 2^l \times \underset{l'}{\forall} 2^{l'} \rightarrow 2^l$$

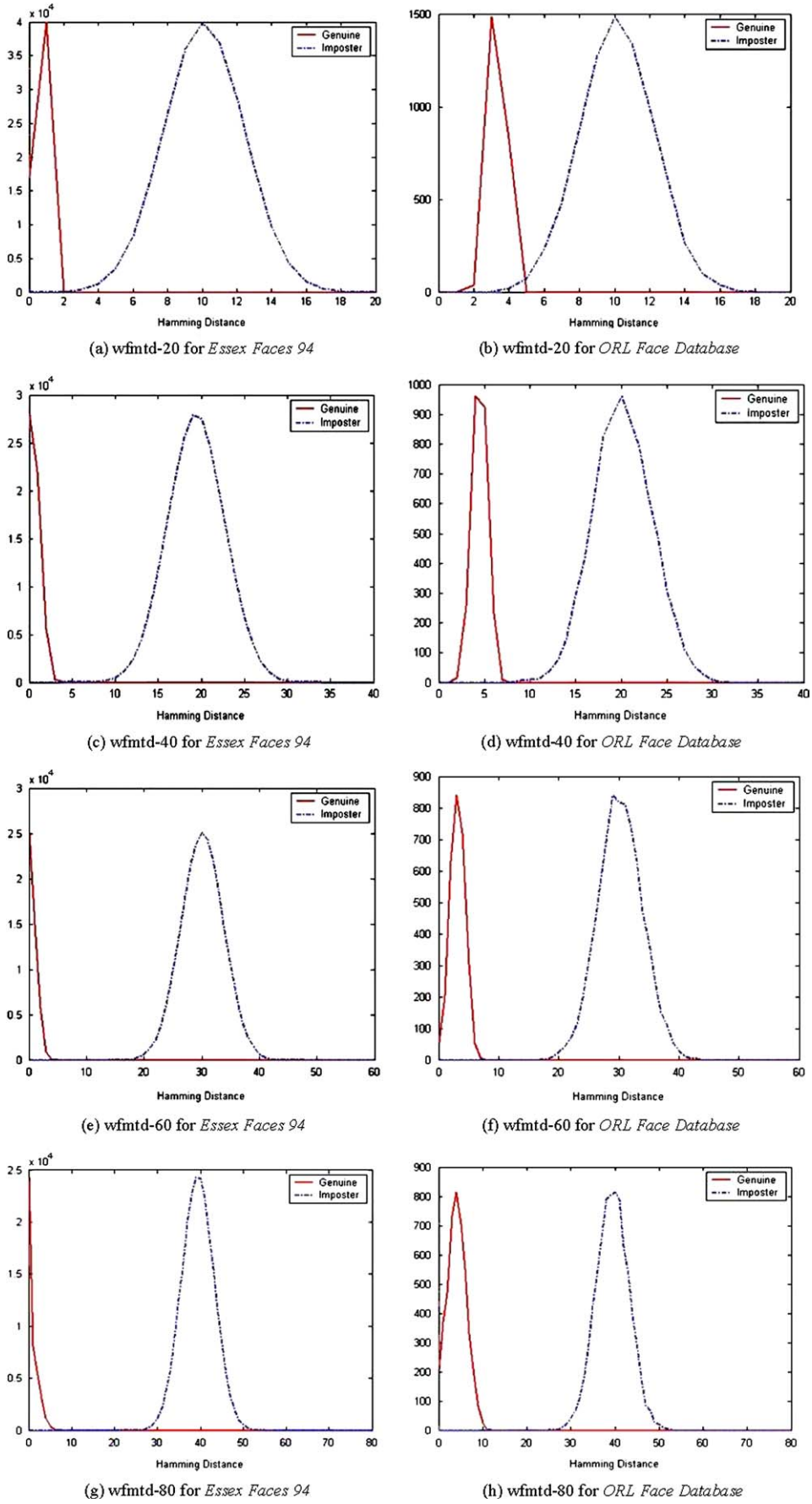
and secret knowledge $\boldsymbol{k}$, where $a = h(\mathbf{r}, k)$ cannot be computed without both $\langle \boldsymbol{r}, k \rangle$ factors, so that adversarial deduction is no more probable than random guessing of order $1/2^l$.$\langle \boldsymbol{r}, k \rangle$ is also protected by the target-collision resistance of h, so that deduction of $\boldsymbol{r}$ or k from output $a = h(\boldsymbol{r}, k)$ and one of the factors is no more probable than $1/2^l$.

Key-factor independence

Non-possession of $\boldsymbol{r}_\perp$ means that tokenised $\varsigma(\boldsymbol{r}_\perp)$ is unavailable to an adversary; thereby previously intercepted (or fabricated) Γ is simply not useful. This prevents meaningful deduction of $H(\boldsymbol{r}_\perp, \Gamma)$, with random guessing being of probability q^{-1} in this case. Possession of $\boldsymbol{r}$ is more useful as it leads to adversarial knowledge of $H^0 : \{h_i^0 = H(x_i^0), | i = 1, \ldots, l_s\}$ from token, $\chi = \{H^0, Y^0\}$ which suggests an analytic strategy whereby random $\boldsymbol{b} \in 2^{l_b}$ bit string are tested for suitability with respect condition $h(h(\Gamma)) = H^0$. The collision probability is $l_s 2^{-l_b}$ in this case, hence the motivation to minimize l_s, and to maximize l_b. Note that the l_b is restricted to not more than dimension of log-polar frequency domain, M, though M is a huge number ($M = 64 \times 64$ used in this paper).

The operational security of our scheme is enhanced via token-side access control and encryption of χ, with respective session key $\langle j', j \rangle = h(i', i)$ for domain or platform serialization i'. This necessitates prior token-side storage of $\psi = E_{j'}(\chi)$, with the following operational sequence:

1. Compute $\langle j', j \rangle$ from token i
2. Transmit j to retrieve ψ from token



(a) wfmtd-20 for *Essex Faces 94*

(b) wfmtd-20 for *ORL Face Database*

(c) wfmtd-40 for *Essex Faces 94*

(d) wfmtd-40 for *ORL Face Database*

(e) wfmtd-60 for *Essex Faces 94*

(f) wfmtd-60 for *ORL Face Database*

(g) wfmtd-80 for *Essex Faces 94*

(h) wfmtd-80 for *ORL Face Database*

Figure 5 Genuine and imposter population distribution for *wfmtd*-l_b for $1_b = 20$, 40, 60 and 80.

3. Decrypt $\chi = D_{j'}(\psi)$

prior to the computations of 'Verification (key retrieval)' section, successful completion of which is restricted to domain/platform *i*.

Key-factor non-recovery

Knowledge of $\Gamma(\boldsymbol{r}_\perp, \Gamma)$ and Γ does not in any way jeopardize $\boldsymbol{r}_\perp$, due to non-recovery of:

- Any $\boldsymbol{b} \in 2^{l_b}$ from Γ
- Any $\boldsymbol{r}_\perp \in \Re^M$ from $\boldsymbol{b}$ or Γ

thereby resulting in $\boldsymbol{r}_\perp$ deduction being no less probable than the $1/2^{l_b}$ of random guessing. The other scenario of $\boldsymbol{r}_\perp$ and Γ compromise (consequent to which H^0 is also divulged) allows analytic strategy based on the testing of random $\Gamma \in \Re^M$ for suitability with respect condition $H^0 : \{h_i^0 = H(x_i^0), |i = 1, \ldots, l_s\}$. Probability of recovery in this case is $l_s 2^{-l_b}$.

Key-factor protection is enhanced via adoption of measures previously discussed:

- Minimize the l_s, and maximize the l_b
- Access control and encryption of χ

Concluding remarks

This paper described an error-tolerant biometrics feature discretisation methodology—*FaceHashing* that leads to the cryptographic key computation based on face biometrics with uniquely tokenised pseudo random number. The *FaceHashing* has significant functional advantages over solely biometrics or token usage, such as extremely clear separation of the genuine and the imposter populations and thereby introduce an error free decision. $H(\boldsymbol{r}_\perp, \Gamma)$ is furthermore highly secure with respect to independence and non-recovery of the $\langle \boldsymbol{r}_\perp, \Gamma \rangle$ key-factor, with immunity against biometric interception or fabrication. The key is constructed to resist cryptanalysis even against an adversary who captures the user device or the feature descriptor. Our security analysis suggests that our technique is viable for use in practice.

References

Albert Bodo. Method for producing a digital signature with aids of a biometric feature. German Patent DE 42 43 908 A1; 1994.

Andrew TBJ, David NCL. Integrated wavelet and Fourier-Mellin invariant feature in fingerprint verification system. ACM SIGMM 2003 multimedia biometrics method and application workshop, CA, USA; 2003. p. 82–8.

Daugman John. Biometric decision landscapes, Technical Report, No. 482, Cambridge University Computer Laboratory; 2002.

Davida GI, Frankel Y, Matt BJ. On enabling secure applications through offline biometric identification. Proceedings of the 1998 IEEE symposium on security and privacy; 1998. p. 148–57.

Goh A, Ngo David CL. Computation of cryptographic keys from face biometrics. Lecture notes in computer science, vol. 2828. Springer-Verlag; 2003. p. 1–13.

Harmon LD. The recognition of faces. Sci Am 1973; 229.

Mallat S. A wavelet tour of signal processing. San Diego: Academic Press; 1998.

Monrose F, Reiter MK, Li Q, Wetzel S. Cryptographic key generation from voice. IEEE symposium security & privacy; 2001. p. 202–13.

Monrose F, Reiter MK, Wetzel S. Password hardening based on keystroke dynamics. Proceedings of the sixth ACM conference on computer and communications security; 1999. p. 73–82.

Nastar C, Moghaddam B, Pentland A. Flexible images: matching and recognition using learned deformations. Comput Vision Image Understanding 1997;65(2):179–91.

Smith Richard E. Internet cryptography: Addison-Wesley; 1997.

Peyravian M, Matyas SM, Roginsky A, Zunic N. Generating user-based cryptographic keys and random numbers. Comput Secur 1999;18(7):619–26.

Reddy BS, Chatterji BN. An FFT-based technique for translation, rotation and scale-invariant image registration. IEEE Trans Image Process 1996;5(8):1266–71.

Shamir A. How to share a secret. Commun ACM 1979;22:612–3.

Soutar C, Roberge D, Stoianov A, Gilroy R, Vijaya Kumar BVK. Biometric encryption. In: Nichols RK, editor. ICSA guide to cryptography. New York: McGraw-Hill; 1999. p. 649–75.

Andrew Teoh Beng Jin obtained his BEng (Electronic) in 1999 and PhD degree in 2003 from National University of Malaysia. He is currently a lecturer in 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.

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 PhD 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.

Alwyn Goh is an experienced and well-published researcher in biometrics, cryptography and information security. His work is recognized 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.