SECURE FACE BIOMETRIC VERIFICATION IN THE RANDOMIZED RADON SPACE

M. A. Dabbah, S. S. Dlay and W. L. Woo

The University of Newcastle, Merz Court, Newcastle upon Tyne, NE1 7RU, United Kingdom

ABSTRACT

Biometrics has become a strong candidate to replace traditional authentication systems however biometric data in itself is vulnerable and requires protection. This paper presents a new method to protect face biometric data using one-way transformation in which original face images cannot be retrieved. The secure and reissuable templates are generated by utilizing the Radon transformed signatures of the face biometric and a multi-space random projection. Using an image-based statistical algorithm, authentication is conducted on the transformed templates without the need to reverse them back. Genuine and impostor distributions separation was also improved by 13.82% leading to a 41.35% reduction in the equal error rate.

Index Terms — cancellable biometric, face recognition, Radon transform, random projection.

1. INTRODUCTION

Although biometrics is a promising alternative to traditional authentication systems, there still are some improvements required such as better accuracy rates and the analysis of dynamic changes. One of the most challenging issues in is security. Biometrics is similar to any other data in terms of storage but very different in terms of usage. For example data cannot be securely stored using encryption and then used for authentication without being decrypted, which makes the biometric data vulnerable during the processing stage. Therefore, authentication must be conducted on the secure version of the data, which in turn will have an impact on the accuracy. In addition, due to the permanence of biometrics, compromised biometrics cannot be further used in an authentic manner by the genuine owners. Since the number of unique characteristics of the human body is limited, the number of biometric identities that someone could replace is indeed limited. For instance there is only one face biometric and it cannot be canceled nor replaced when compromised.

The first attempt to protect biometrics by cryptographic verification was for an iris based authentication scheme [1]. Error correction code was utilized to overcome the dynamical changes of biometrics. A voice biometric hardening key algorithm has been developed by extracting a distinguishable set of features from voice segments to generate a sharing table [2]. The fuzzy vault scheme [3] has also been proposed to protect biometrics cryptographically by a committed value that is infeasible for an attacker to learn. Later, the scheme was implemented on fingerprint biometrics [4]. The technique was evaluated at 20-30% false rejection rate without the alignment of fingerprint features in the fuzzy vault domain, which was later dealt with by Chung et al [5]. Another fingerprint based cryptographic key scheme has been developed using the uncertainty of the multiple-redundant lookup table of a random array mixing, [6]. A facial cryptographic user-dependant key generator was also introduced by binarizing the optimum distinguishable facial features extracted by linear dimensionality reduction techniques [7].

The first cancellable biometric technique was introduced using an intentional repeatable distortion of a biometrics signal based on chosen transforms [8, 9]. Another technique extracts the facial features by a linear space projection and then maps them onto a multiple random subspaces to obtain a quantized binary code (RMQ) [10]. Savvides et al [11] generate cancellable biometric by encrypting a training set of images to construct a minimum average correlation energy filter for face authentication. Zeng et al [12] presented a secured biometric key using lattice mapping. The biometric feature vector is mapped in the lattice space using a certain codeword. Recently another cancellable biometric technique [13] has been developed to protect face biometric though the usage of co-occurrence matrices and a high-order polynomial mapping.

In this paper we present a new secure biometric system for image-based authentication that generates an endless number of non-reversible cancellable templates from the same face image by using the Radon transform and multi-space random projection. The overall method is presented in Section 2, Section 3 outlines the eigenface algorithm while Section 4 focuses on the parameters for security analysis. The results are provided in Section 5 and the conclusion in Section 6.

2. THE RANDOMIZED RADON SIGNATURE (RRS)

The RRS is a pre-processing stage. As shown in figure 1 each face image is first transformed into its RRS format before being stored in the database or used for authentication through a linear feature extraction method. The database will contain the RRS templates and their
corresponding random subspaces used to generate them. The RRS transform is non-reversible which means that the original face images are not obtainable even when the templates, the transformation function and the random subspaces are available. In case a particular RRS template is compromised, different random subspaces will be used to generate different RRS template from the same original face image. This overcomes the limitation on the number of unique biometric characteristics of each individual i.e. for one face we can generate an endless number of RRS templates.

\[
\mathbf{f}_l = \kappa_l \mathbf{b}_l^T \mathbf{Q} 
\]

Similarly \(\mathbf{f}_l\) is constructed from the spatial domain of the face image \(\mathbf{b}_l\), where \(l\) is the index of the image column vector, \(\mathbf{Q}\) is a uniformly distributed random space that is independent of \(\mathbf{R}\), and \(\kappa_2\) is a constant offset. The random projection in equations (5) and (6) is a linear transformation that is based on the Johnson-Lindenstrauss lemma [15].

\[
(1 - \varepsilon) \| \mathbf{x} - \mathbf{y} \|^2 \leq \| \mathbf{f}(\mathbf{x}) - \mathbf{f}(\mathbf{y}) \|^2 \leq (1 + \varepsilon) \| \mathbf{x} - \mathbf{y} \|^2 
\]

It states that any \(n\) points in the \(p\)-dimensional Euclidean space \(E\) can be mapped to an \(O((ln\ n)/\varepsilon^2)\)-dimensional space, \(E'\) and \(f: E \rightarrow E'\), such that the distance between any two points, \(\mathbf{x}\) and \(\mathbf{y}\), is preserved within an arbitrary factor of \(\varepsilon\). This is due to the assumption that random subspaces are approximately orthogonal.

\[
\mathbf{t}_l = \mathbf{s}_l + \mathbf{f}_l = \kappa_l \mathbf{c}_l^T \mathbf{R} + \kappa_2 \mathbf{b}_l^T \mathbf{Q} 
\]

The final stage of the RRS template \(\{\mathbf{t}_l | l = 1,2,...,N\}\) formulation is the mixing operation of the \(M\)-dimensional vectors \(\mathbf{s}_l\) and \(\mathbf{f}_l\). Since \(\mathbf{R}\) is independent and different from \(\mathbf{Q}\), and neither \(\mathbf{b}_l\) nor \(\mathbf{c}_l\) are known, the RRS template \(\{\mathbf{t}_l | l = 1,2,...,N\}\) cannot be demixed nor reversed. Obviously the template does not resemble the facial shape nor contains any visual information.

In theory, these RRS templates can replace the original face images in any image-based authentication system that uses statistical linear feature extraction methods such as PCA, LDA etc. For the purpose of this paper, the RRS templates are evaluated using the eigenface algorithm [16].

### 3. Linear Feature Extraction

The eigenface algorithm is an image-based statistical approach for face features linear extraction [16]. Let \(\Gamma_1,\Gamma_2,...,\Gamma_L\) be the face images and \(L\) is the number of training images. Each face differs from the average face \(\boldsymbol{\Psi}\) by the vector \(\Phi_i = \Gamma_i - \boldsymbol{\Psi}\), where \(i\) corresponds to the \(i^{th}\) face image \(\Gamma_i\).

\[
\boldsymbol{\Psi} = \frac{1}{L} \sum_{l=1}^{L} \Gamma_l 
\]

A set of \(d'\) orthogonal vectors, \(\mathbf{u}_i\), are selected to describe the best distribution of the data. The \(k^{th}\) vector is chosen such that \(\lambda_k\) is a maximum subject to \(\delta_{lk}\).

\[
\lambda_k = \frac{1}{L} \sum_{l=1}^{L} (\mathbf{u}_i^T \Phi_i)^2 
\]

\[
\delta_{lk} = \begin{cases} 1 & \text{if } l = k \\ 0 & \text{otherwise} \end{cases} 
\]

The vector \(\mathbf{u}_i\) and the scalar \(\lambda_k\) are the eigenvector and the eigenvalue of covariance matrix, \(\mathbf{C}\). When a new face image is acquired for authentication, \(\Gamma_{new}\), it will be projected as shown in (13) into the eigenface space to
extract the weights, $\Omega^T = [\omega_1, \omega_2, \omega_3, \ldots, \omega_d']$, which are then used to find the minimum Euclidean distance, $\varepsilon_c$, with the corresponding face class $c$.

$$C = \frac{1}{T} \sum_{i=1}^{L} \Phi_i \Phi_i^T$$  \hfill (12)

$$\omega_k = u_k^T (\Psi_{\text{new}} - \Psi)$$ \hfill (13)

$$\varepsilon_c^2 = \| \Omega - \Omega_c \|^2$$ \hfill (14)

4. Security Analysis

As explained above the system equation (8) is not reversible due to the absence of original face images. Therefore, two different types of attacks will be considered in this section. The first is an exhaustive search attack (ESA) with the assumption that no information is available on the RRS templates except of the random subspaces, the transform function and the templates themselves.

Let $n$ be the number of binary bits contained in each template. The probability of ESA to succeed is defined by the length $n$, which is in the order of $1 \times 10^4$. Therefore the ESA probability of the RRS template given by $P_{ESA} = 2^{-n}$ is negligible, which indicates the immunity of the templates against such attacks.

An elegant attack can be conducted if some statistical information on the RRS templates is available. To analysis this type of risk the guessing entropy and its Shannon entropy lower-bound are used [17]. Let $T_c$ be a set of RRS templates of the same class $c = 1, 2, \ldots, K$. The number of registered templates per class in the database $m$ is determined by the system and fixed for all classes. However, because the ideal condition $e_B/e_W \rightarrow \infty$ when $e_W \rightarrow 0$ and $e_B \geq e_W$ does not exist for any functioning classifier, the lower-bound of the guessing entropy $G(T)$ tends to $G_c(T)$ (16), where $e_B$ and $e_W$ are the average distances between classes and within classes respectively. $H(T)$ is the Shannon entropy.

$$G(T) \geq \frac{1}{4} 2^{H(T)} + 1$$ \hfill (15)

$$G_c(T) \geq \frac{m}{4} K + 1$$ \hfill (16)

This leaves us with a lower-bound that is proportional to the number of registered classes and templates per class in the RRS database.

5. Experimental Results

The Olivetti Research Ltd (ORL) face database [18] has been used for this evaluation. It has 40 classes with 10 images each. Images were captured under no constraints on expressions but with limited side movement tolerated tilt, and stored in $112 \times 92$ pixels.

For comparison two separate eigenface projections are conducted with five enrolled training images or templates per class. Therefore the lower-bound of the guessing entropy (16) of the RRS templates is $G_c(T) \geq 51$ since $m=5$ and $K=40$. And since $n=8 \times 112 \times 92$ bits, the ESA success probability is almost zero $P_{ESA}=0$. The accuracy performance is evaluated using the false acceptance (FAR), false rejection (FRR) and equal error (EER) rates as indicators for a verification based procedure.

Investigating the genuine and impostor distributions of the original images and the RRS templates has shown in figure 2 a clearer separation with a reduced overlap that leads to a reduction of 41.35% in the EER.

Table 1: The best operation point of the original images and the RRS templates. $d'$ is number of eigenvector used.

<table>
<thead>
<tr>
<th></th>
<th>$D$</th>
<th>$\mu_c$</th>
<th>$\mu_i$</th>
<th>$d'$</th>
<th>EER [%]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original</td>
<td>2.46</td>
<td>8.49</td>
<td>17.95</td>
<td>19</td>
<td>12.0038</td>
</tr>
<tr>
<td>RRS</td>
<td>2.80</td>
<td>3.51</td>
<td>9.24</td>
<td>44</td>
<td>7.0397</td>
</tr>
</tbody>
</table>
Another way of evaluating the distribution separation is the measure $D$ [19], the higher the value of $D$ the better the performance. Using the mean $\mu_g$ and the standard deviation $\sigma_g$ of the genuine distribution and their equivalents $\mu_i$ and $\sigma_i$ of the impostor distribution, the measure shows an improvement of 13.82% for the RRS templates as shown in Table 1.

\[
D = \mu_g - \mu_i \sqrt{\frac{\sigma_g^2 + \sigma_i^2}{2}}
\]  

(17)

The relationship between the FAR and the FRR is illustrated by the receiver operating characteristic (ROC) curve shown in figure 3. The error rates of the RRS templates are less dependent on each other from that of the original images.

Figure 3: The ROC curves of the original images and the RRS templates.

6. CONCLUSION

In this work a new cancellable biometric technique was introduced. The RSS templates are non-reversible and can replace normal face images in current image-based statistical face authentication systems. By changing the multi-random spaces new issues of the same face biometric can be produced. Using the eigenface algorithm the evaluation has shown an improved separation of genuine and impostor distributions by 13.82%. This in turn has reduced the EER to 7.04% leading to a 58.65% accuracy enhancement for the RRS templates over the original face images.

6. ACKNOWLEDGMENT

The first author would like to thank the Institute of Engineering and Technology (IET) for their support through the Hudswell International Research Award for Excellence and the Universities UK for their support though the ORS Award Scheme.

7. REFERENCES