Letters

Combine crossing matching scores with conventional matching scores for bimodal biometrics and face and palmprint recognition experiments

Yong Xu a,b,*, Qi Zhu a, David Zhang c

a Bio-Computing Research Center, Shenzhen Graduate School, Harbin Institute of Technology, Shenzhen, China
b Key Laboratory of Network Oriented Intelligent Computation, China
b Bio-Computing Research Centre, Department of Computing, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong, China

1. Introduction

In the past years biometrics has attracted increasing attention [1–7]. A variety of studies have shown that multi-biometrics almost always outperforms single biometrics in authentication accuracy [8–15]. This is mainly because multi-biometrics can exploit more information of the subject to authenticate the identity than single biometrics.

Bimodal biometrics not only includes the basic components of multi-biometrics but also can be viewed as the simplest multi-biometrics [16,17]. There have been a number of studies on bimodal biometrics [17–20]. Previous personal authentication methods often fuse the two biometrics traits in three ways [21–25]. In the first way, the method usually first extracts the features from every sample of the two biometrics traits, respectively. Then the method calculates the matching scores between each test sample and training sample of the first trait. This matching score is referred to as the first matching score. The method also calculates the matching scores between each test sample and training sample of the second trait and refers to it as the second matching score. The method then combines these two scores to perform personal authentication. The method is the so-called matching scores level fusion method. In the second way, the method first fuses two biometrics traits in the feature level, then extracts features from the obtained data and performs personal authentication [14,15]. In the third way, the method first performs authentication for the first and second traits and then combines their authentication results to obtain the final authentication result. The method is indeed so-called decision level fusion method [16].

In real-world applications, there is a special kind of bimodal biometrics system that includes two similar biometrics traits. The biometrics system including visible light and infrared face images [26–30], and the biometrics system including palmprint images captured at two bands [31,32] are two examples of this kind of bimodal biometrics. Though the above examples are special, no ‘special’ methods have been proposed for them. We note that in this special kind of bimodal biometrics, the first and second biometrics traits of the same subject are very similar whereas the first and second biometrics traits from different subjects are not. As a result, we propose to exploit the similarity between the two biometrics traits for personal authentication. That is, we propose to integrate the crossing matching score between the two traits with the first and second matching scores for personal authentication. The proposed method has the following advantages: first, as it is a weighted matching score level fusion method, it not only can convey more information of the two biometrics traits than the decision level fusion but also can properly set the influence of the three kinds of matching scores.
by virtue of the weight coefficients. Second, the crossing matching score allows the similarity between the two traits of the same subject to be exploited for personal authentication. As a result, the proposed method can exploit more information for authentication than the conventional weighted matching score level fusion, which always fuses only two matching scores from two biometrics traits. This paper has the following contributions. It defines, for the first time, a matching score for two similar biometrics traits such as visible light and infrared face images of the same subject and the palm images captured at two bands and proposes a weighted score level fusion method for the corresponding biometrics system. The experimental results have shown that the proposed fusion method can obtain a higher accuracy than conventional score level fusion methods.

The rest of the paper is organized as follows: Section 2 presents the proposed method. Section 3 shows the rationale of the method. Section 4 shows the experimental results. Finally Section 5 offers the conclusion of the paper.

2. The proposed method

In this section we formally present the proposed method. Let \( x_j^1 \) and \( y_j^1 (1 \leq j \leq M, 1 \leq i \leq n) \) denote the i-th sample vectors of the first and second biometrics traits of the j-th subject, respectively. Suppose that all \( x_j^1 \) and \( y_j^1 \) are training samples. Let \( t^1 \) and \( t^2 \) denote testing samples and be the sample vectors of the first and second biometrics traits of an ‘unknown’ subject, respectively. We assume that all these sample vectors are column vectors.

The proposed method consists of four steps. The first three steps calculate the first, second and crossing matching scores, respectively. The fourth step combines these three matching scores to perform personal authentication.

The first step of the proposed method works as follows. First, it assumes that \( t^1 \) can be approximately expressed as a linear combination of all of \( x_j^1 \), i.e.

\[
 t^1 = a_1 x_1^1 + \ldots + a_n x_n^1 + \ldots + a_{nM} x_M^1
 \]  
(1)

We can rewrite Eq. (1) as \( t^1 = Xa \), where \( X = [x_1^1 \ldots x_M^1] \).

\[
 A = (X'X + \gamma I)^{-1}X't^1
 \]  
(2)

where \( I \) is the identity matrix and \( \gamma \) is a small positive constant.

The first step calculates the first matching score using

\[
 s_j^1 = \| t^1 - \sum_{i=1}^{n} \hat{a}_{j-i+n+1} x_i^1 \|, 1 \leq j \leq M
 \]  
(3)

where \( \hat{a}_{j-i+n+1} \) is the \( (j-i)+n+i \)-th entry of \( \hat{A} \). \( s_j^1 \) is actually a distance metric between \( t^1 \) and the training samples of the first trait of the j-th subject \( (1 \leq j \leq M) \). The smaller \( s_j^1 \) is, the greater the probability that the testing sample is from the j-th subject is.

The second step of the proposed methods works in a similar way as the first step. First, it assumes that \( t^2 \) can be approximately expressed as a linear combination of all of \( y_j^1 \), i.e.

\[
 t^2 = b_1 y_1^1 + \ldots + b_n y_n^1 + \ldots + b_{nM} y_M^1
 \]  
(4)

We can rewrite Eq. (4) as \( t^2 = Yb \), where \( Y = [y_1^1 \ldots y_M^1] \).

\[
 B = (Y'Y + \gamma I)^{-1}Y't^2
 \]  
(5)

The second step calculates the second matching score using

\[
 s_j^2 = \| t^2 - \sum_{i=1}^{n} \hat{b}_{j-i+n+1} y_i^1 \|, 1 \leq j \leq M
 \]  
(6)

where \( \hat{b}_{j-i+n+1} \) is the \( (j-i)+n+i \)-th entry of \( \hat{B} \). \( s_j^2 \) is a distance metric between \( t^2 \) and the training sample of the second trait of the j-th subject \( (1 \leq j \leq M) \). Actually, the first and second matching scores are calculated in the same way as the deviation of the global version of the method proposed in [33].

The third step of the proposed method calculates the crossing matching score using

\[
 s_j^3 = n - \sum_{i=1}^{n} (t^1_i y_j^1 / \| t^1_i \|) \| t^2_i \| / \| y_j^1 \|, 1 \leq j \leq M
 \]

(7)

In Eq. (7), \( (t^1)^T y_j^1 / \| t^1_i \| \) denotes the similarity between the testing sample of the second trait and the i-th training sample of the first trait of the j-th subject. It is clear that for the biometrics trait in the form of images, the similarity is in the range of 0 to 1. As a result, \( \sum_{i=1}^{n} (t^1_i y_j^1 / \| t^1_i \|) \| t^2_i \| / \| y_j^1 \| \) is in the range of 0 to n. Eq. (7) has the following rationale: first, it must be a non-negative value. Second, it is easy to know that the lower the \( s_j^3 \) is, the larger the similarity between the training samples of the first trait of the j-th subject and the testing sample of the second trait. Moreover, if \( s_j^3 \) is small, then the training samples of the first (or second) trait of the j-th subject will be similar to the testing sample. As a result, \( s_j^1 \), \( s_j^2 \) and \( s_j^3 \) are compatible and we can use the weighted sum of them to perform classification.

The fourth step first normalizes the first, second and the crossing matching scores of the same testing sample using

\[
 s_j^4 = \frac{s_j^1 - \min(s_j^1)}{\max(s_j^1) - \min(s_j^1)}, 1 \leq j \leq M
 \]

(8)

\[
 \max(s_j^1) \) and \( \min(s_j^1) \) denote the maximum and minimum values of \( s_j^1 \), respectively. This step then combines the three normalized matching scores using

\[
 s = w_1 s_j^1 + w_2 s_j^2 + (1 - w_1 - w_2) s_j^3, j = 1, \ldots, M
 \]

(9)

Weight coefficients \( w_1 \), \( w_2 \) and \( 1-w_1-w_2 \) enable the three kinds of matching scores to have different influences on the ultimate personal authentication. \( s \) is referred to as final matching score. \( w_1 \), \( w_2 \) and \( 1-w_1-w_2 \) are referred to as weight coefficients of the first, second and crossing matching scores, respectively. If \( k = \arg \min(s_j^3) \), then the fourth step makes the decision that the testing sample is from the k-th subject.

Fig. 1 summarizes the main steps of the proposed method.

3. Characteristics and rationale of the proposed method

In this section, we will show the characteristics and rationale of the proposed method. As a matching score level fusion method, our method is very suitable for the bimodal biometrics systems that have two similar traits. As we know, a conventional matching score level fusion method first calculates the matching scores of the two traits and then exploits the sum of the first and the second matching scores for personal authentication, respectively. However, our method combines the crossing matching score with the first and the second matching scores for personal authentication. If the two traits are similar, the crossing matching score will contain useful information for personal authentication. Actually because in the focused issues the two traits of the same subject are similar, the testing sample of the second trait will be similar.

---

**The main steps of the proposed method**

1. Calculate the first matching score using Eq.(3).
2. Calculate the second matching score using Eq.(6).
3. Calculate the crossing matching score using Eq.(7).
4. Use Eq.(8) and Eq.(9) to calculate the final matching score and perform personal authentication.

---

**Fig. 1.** Summary of the main steps of the proposed method.
to the training sample of the first trait of the same subject. As a
result, the corresponding crossing matching score will be small.
However, the testing sample of the second trait of a subject will
be very dissimilar to the training sample of the first trait of
another subject, so the corresponding crossing matching score
will be great. It is clear that for all of the three kinds of matching
scores, a small score means a high similarity, and thus it is
reasonable for the proposed method to use the weighted sum of
them to classify the testing sample.

In order to show the difference between the crossing matching
score and the first and the second matching scores, we define
genuine scores and imposter scores and use figures to show them.
Genuine scores are defined as the matching scores between a testing
sample and the training samples from the same subject. Imposter
scores are defined as the matching scores between a testing sample
and the training samples from different subjects. The visible light
and near infrared face images are used as the first and the second
biometrics traits, respectively. Figs. 2–4 show the distributions of
the genuine and imposter scores of the face image dataset shown in
Section 4.2, respectively. In these figures, the horizontal and vertical
coordinates show the value and the probability of the matching
score, respectively. Figs. 2 and 3 show that the genuine scores and
imposter scores of each of the first and second matching scores have
very different distributions. Thus, the first and second matching
scores are very useful for authenticating different subjects. Fig. 4
shows that the crossing matching score is not as powerful as the
first and the second matching scores for personal authentication.
Nevertheless, as the distributions of the genuine scores and impos-
ter scores in Fig. 4 are somewhat different, the crossing matching
score is also useful for personal authentication.

It is intuitive that the first and second matching scores play a
more important role than the crossing matching score, so we suggest
that two large weight coefficients be assigned to the first and second
matching scores and a small weight coefficient be assigned to the
crossing matching score. Our experimental results also support this
suggestion. Moreover, if in a real-world bimodal biometrics issue, the
first and second traits lead to two very different authentication
accuracies, then we can assign a greater weight coefficient to the
matching score corresponding to a higher accuracy.

We note that Shao and Brady defined the cross correlation for
the object retrieval [34]. Shao and Brady used the cross correla-
tion to evaluate the similarity between regions from different
images [34]. Shao and Brady found that the regions selected from
images of the same object are more similar to each of other than
regions selected from images of different objects. Thus, they used
the correlation as the similarity metric between regions selected
from different images. They considered that two images contain
the same object, if some regions selected from the first image are
highly correlated to some regions selected from the second image.

The crossing matching score defined in Section 2 has clear
difference to the cross correlation and is used in a very different
way. Specifically, the crossing matching score must be combined
with two other kinds of matching scores for personal authentica-
tion. However, only the cross correlation defined in [34] was used
for the object retrieval. Actually, the crossing matching score
provides only complementary information of the similarity
between the testing sample and the training samples and the
main information of the similarity is provided by the first and
second matching scores defined in Section 2. On the other hand,
for the object retrieval issue in [34], the cross correlation contains
all available information of the similarity.

4. Experimental results

In this section, we use two datasets to test our method. We
also performed experiments on the conventional weighted
matching score level fusion of the two biometrics traits. The
4.1. Experiments on the PolyU multispectral palmprint dataset

We first conducted experiments on the PolyU multispectral palmprint dataset. This dataset was collected from 250 subjects (55 women and 195 men) using the palmprint acquisition device developed by PolyU [35]. Every subject provided palmprint images of both the left and right palms. Since there were four illuminations, i.e. red, green, blue and near infrared illuminations, there were four kinds of multispectral palmprint images, i.e. red, green, blue and near infrared palmprint images. These multispectral palmprint images were collected in two separate sessions. In each session, every palm provided 6 palmprint images at each spectral band. As a result, for each spectral band, the database contained 6,000 images from 500 different palms. In the following experiments, we only use the images from the first session. The first three images of each band images of a palm were used as training samples and the remaining images were used as testing samples. The resolution of the palmprint image was 352 × 288. The 128 × 128 region of interest (ROI) domain was extracted from each palmprint image using the method proposed in [32]. The ROI images were resized to 32 × 32. Fig. 5 shows some ROI images. The ROI images were further converted into one-dimensional sample vectors. Before carrying out the proposed method, we normalized every sample vector as a unit vector in advance.

Tables 1–4 show the experimental results of our method and the conventional weighted matching score level fusion on the green and near infrared palmprint images.

4.2. Experiments on visible light and near infrared face images

We created a face recognition system that simultaneously captures and uses visible light and infrared face images for personal authentication. We used it to capture face images from 119 subjects under different lighting conditions. For example, upon the condition that both the left and the right lamps were on, each subject provided 2 to 19 visible light and infrared face images. Fig. 6 shows some visible light and near infrared face images. We used these images to conduct experiments. As one subject provided only 2 visible light and infrared face images, we exploited only the remaining 118 subjects. Each of these subjects had at least

Fig. 5. Four ROI images of a same palm. The first, second, third and fourth ROI images were extracted from the blue, green, near infrared and red palmprint images, respectively. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article).
5 visible light and infrared face images. We took the first two visible light and infrared face images of each subject as training samples and used the remaining images as testing samples. The visible light and infrared face images were treated as the first and the second biometrics traits, respectively. As shown in Table 5, the lowest classification error rate of our method is smaller than the conventional weighted matching score level fusion. Fig. 7 shows three visible light face images (shown in the first column) that were erroneously and correctly classified by the conventional weighted matching score level fusion and our method. In each row, the second image is one of the visible light face images of the subject that the first image was erroneously classified as.

In order to further explore the performance of our method, we also conducted an experiment in which different subjects provide different numbers of training samples. We used all available samples of the subject to conduct the experiment. The last three samples of each subject were taken as testing samples whereas the others were used as training samples. Eqs. (3), (6) and (7) were revised into the subject that has the maximum classification error rate of our method is smaller than the conventional weighted matching score level fusion.

### Table 4

<table>
<thead>
<tr>
<th>Number of erroneously classified palms</th>
<th>Classification error rate</th>
<th>( w_1 (w_j) )</th>
<th>( w_2 (w_j) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our method</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>52</td>
<td>3.47%</td>
<td>0.5</td>
<td>0.3</td>
</tr>
<tr>
<td>52</td>
<td>3.47%</td>
<td>0.6</td>
<td>0.3</td>
</tr>
<tr>
<td>50</td>
<td>3.33%</td>
<td>0.6</td>
<td>0.25</td>
</tr>
<tr>
<td>49</td>
<td>3.27%</td>
<td>0.6</td>
<td>0.2</td>
</tr>
<tr>
<td>The conventional weighted matching score level fusion</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>3.73%</td>
<td>0.4</td>
<td>0.6</td>
</tr>
<tr>
<td>56</td>
<td>3.73%</td>
<td>0.5</td>
<td>0.5</td>
</tr>
<tr>
<td>55</td>
<td>3.67%</td>
<td>0.6</td>
<td>0.4</td>
</tr>
</tbody>
</table>

### Table 5

<table>
<thead>
<tr>
<th>Number of erroneously classified testing samples</th>
<th>Classification error rate</th>
<th>( w_1 (w_j) )</th>
<th>( w_2 (w_j) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our method</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>58</td>
<td>16.38%</td>
<td>0.6</td>
<td>0.35</td>
</tr>
<tr>
<td>58</td>
<td>16.38%</td>
<td>0.6</td>
<td>0.30</td>
</tr>
<tr>
<td>The conventional weighted matching score level fusion</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>80</td>
<td>22.60%</td>
<td>0.4</td>
<td>0.6</td>
</tr>
<tr>
<td>65</td>
<td>18.36%</td>
<td>0.5</td>
<td>0.5</td>
</tr>
<tr>
<td>63</td>
<td>17.80%</td>
<td>0.6</td>
<td>0.4</td>
</tr>
<tr>
<td>65</td>
<td>18.36%</td>
<td>0.7</td>
<td>0.3</td>
</tr>
</tbody>
</table>

### Table 6

<table>
<thead>
<tr>
<th>Number of erroneously classified testing samples</th>
<th>Classification error rate</th>
<th>( w_1 (w_j) )</th>
<th>( w_2 (w_j) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our method</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>12.99%</td>
<td>0.6</td>
<td>0.38</td>
</tr>
<tr>
<td>47</td>
<td>13.28%</td>
<td>0.5</td>
<td>0.48</td>
</tr>
<tr>
<td>48</td>
<td>13.56%</td>
<td>0.49</td>
<td>0.49</td>
</tr>
<tr>
<td>The conventional weighted matching score level fusion</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>62</td>
<td>17.51%</td>
<td>0.3</td>
<td>0.7</td>
</tr>
<tr>
<td>57</td>
<td>16.10%</td>
<td>0.35</td>
<td>0.65</td>
</tr>
<tr>
<td>48</td>
<td>13.56%</td>
<td>0.4</td>
<td>0.6</td>
</tr>
</tbody>
</table>

Fig. 7. Three visible light face images (shown in the first column) that were erroneously and correctly classified by the conventional weighted matching score level fusion and our method. In each row, the second image is one of the visible light face images of the subject that the first image was erroneously classified as.
traits can be integrated with the conventional matching scores for similar and those of different subjects have relatively great similarity. Our idea is to combine the crossing matching score with the first and the second traits of the same subject can reflect the similarity. On the other hand, the first trait from a subject will be very dissimilar to the second trait from another subject and the crossing matching score can also reflect the dissimilarity. This means that the crossing matching score is also helpful for personal authentication. As a result, it is reasonable for our proposed method to combine the crossing matching score with the first and the second matching scores for the focused bimodal biometrics. Our paper makes important contributions to both the methodologies and applications of biometrics.

We note that Poh et al. also studied the issue of “cross matching” [36]. What they explored is the so-called cross-device matching in which the acquisition device used to prepare a template (during enrollment) is different from the one used to acquire a query sample. Differing from this, we do not take the device into account and study the issue of exploiting two looking similar biometrics traits for personal authentication. Our idea is that since the two biometrics traits of the same subject are very similar and those of different subjects have relatively great difference, the crossing matching score of the two biometrics traits can be integrated with the conventional matching scores for personal authentication. The cost sensitive evaluation presented in [36] is very important for applications of the biometrics system, so in the future we will also perform the cost sensitive evaluation for further improving our method. For example, it is worth studying the issue of devising a means to automatically determine optimal weights for our method for obtaining a higher accuracy.

Acknowledgements

This article is partly supported by Program for New Century Excellent Talents in University (Nos. NCET-08-0156 and NCET-08-0155), NSFC under Grant nos. 61071179, 60803090, 60902099 and 61010137 as well as the Fundamental Research Funds for the Central Universities (HIT.NSRIF. 2009130).

References


Yong Xu was born in Sichuan, China, in 1972. He received his B.S. degree, M.S. degree in 1994 and 1997, respectively. He received the Ph.D degree in Pattern recognition and Intelligence System at NUST (China) in 2005. Now he works at Shenzhen graduate school, Harbin Institute of Technology. His current interests include feature extraction, biometrics, face recognition, machine learning, image processing and video analysis.
Qi Zhu obtained his Master degree in 2009 from Shenzhen graduate school, Harbin Institute of Technology. He is working for his Ph.D degree at Shenzhen graduate school, Harbin Institute of Technology. His current interests include pattern recognition and biometrics.

David Zhang graduated in computer science from Peking University (1974). He received his MSc in computer science in 1982 and Ph.D in 1985 from the Harbin Institute of Technology (HIT). From 1986 to 1988, he was a postdoctoral fellow at Tsinghua University and then an associate professor at the Academia Sinica, Beijing. In 1994, he received his second Ph.D in electrical and computer engineering from the University of Waterloo, Ontario, Canada. Currently, he is a chair professor at the Hong Kong Polytechnic University, where he is the founding director of the Biometrics Technology Centre (UGC/CRC) supported by the Hong Kong SAR government in 1998. He also serves as visiting chair professor in Tsinghua University, and adjunct professor at Shanghai Jiao Tong University, Beihang University, HIT and the University of Waterloo. He is the founder and editor-in-chief of the International Journal of Image and Graphics (IJIG); book editor of the Springer International Series on Biometrics (SISB); organizer of the International Conference on Biometrics 2004 and 2006 (ICBA 2004 and ICB 2006); associate editor of more than 10 international journals, including IEEE Transactions on SMC-A/SMC-C/Pattern Recognition; chair of IEEE/CIS Technical Committee on Intelligent System Application; and the author of more than 10 books and 160 journal papers. Professor Zhang is a Croucher senior research fellow, distinguished speaker of the IEEE Computer Society, and fellow of the International Association of Pattern Recognition (IAPR).