Mutual dependency of features in multimodal biometric systems

Wencheng Yang, Jiankun Hu, Song Wang and Chi Chen

Multimodal biometric systems have many advantages over single-modal biometric systems, e.g. higher recognition accuracy and security level. However, for most existing multimodal biometric systems, experiments are conducted using the unreal multimodal databases in which no samples of different biometric modules are from the same person. For example, a fingerprint sample of person A and a biometric face sample of person B will be combined to form a sample of the joint fingerprint module and face module. A multimodal biometric system is designed and tested, which is made up of two common biometrics, face and fingerprint, using a real multimodal database (a sample of the joint fingerprint module and face module is formed from the fingerprint and face of the same person) and two unreal multimodal databases. From the experimental results it is observed that there is a large discrepancy between the system performances evaluated with the real and unreal multimodal databases. This indicates that ignoring the influence of feature dependency, which has been a common practice in evaluating multimodal biometrics systems, can produce misleading system performance evaluation results.

Introduction: Single-modal biometric systems that use only one biometric trait for recognition often suffer from issues such as biometric data variation, lack of distinctiveness, low recognition accuracy and spoof attacks [1]. To overcome these problems, multimodal biometric systems that fuse multiple biometric features from two or more sources, e.g. fingerprint, finger-vein, iris and face, are built. Compared with single-modal biometric systems, multimodal biometric systems tend to improve recognition accuracy, security and system reliability. However, most existing multimodal biometric systems, see, e.g. [2–4], are designed by processing biometric features independently without taking into account the features’ mutual dependency in different modules. In these experiments, ‘unreal’ multimodal databases are used, in which samples of multimodal biometric modules which are supposed to be constructed from different biometric modules of the same subject are constructed from different persons. Such an ‘unreal’ multimodal database ignores the mutual dependency of features. A simple example of this mutual dependency is an intuitive observation that a tall person tends to have bigger hands than a short person. Experimental results generated using this type of ‘unreal’ multimodal databases cannot reflect real situations, and consequently may misguide the implementation of multi-biometric systems in real applications. To show the existence of feature dependency and verify its influence on system performance, in this Letter we design a face and fingerprint-based multi-biometric system and test it on the ‘real’ and ‘unreal’ multimodal databases.

Multimodal biometric system: In this Section, we design a multimodal biometric system to substantiate the impact of feature dependency on system performance. The designed multi-biometric system includes two modules, namely, face module and fingerprint module.

In the face module, each face image is first rotated and cropped into a standard size of 128 x 128 pixels according to the eye coordinates. Then the Gabor filter and linear discriminate analysis-based technique is used to extract the face feature [5]. For each face image, a real-valued vector containing 99 real values is generated. This real-valued vector is further transformed into a binary string \( P_1 \) by utilising the biobashing technique [6]. The overall processing flow of face feature extraction is shown in Fig. 1.

![Fig. 1 Overall processing flow of face feature extraction](image)

To calculate the similarity score between a face template \( T_2 \) and a face query \( Q_1 \), the feature set \( P_1^T \) extracted from the template \( T_2 \) and the feature set \( P_1^Q \) extracted from the query \( Q_1 \) are compared and the similarity score between them is calculated as follows:

\[
S_1 = 1 - \frac{\text{hamdist}(P_1^T, P_1^Q) \text{len}(P_1^T)} {\text{len}(P_1^T)}
\]

where \( \text{hamdist}(P_1^T, P_1^Q) \) is the Hamming distance between \( P_1^T \) and \( P_1^Q \) and \( \text{len}(P_1^T) \) is the binary length of the \( P_1^T \).

In the fingerprint module, given a fingerprint image, a set of minutiae \( M = (m_{0}, m_{1}, m_{2}, ..., m_{NT-1}) \) are extracted by a commercial software package called VeriFinger 4.0 from Neurotechnology [7]. Each minutia \( m_{n} \) is represented by a vector \((x_{n}, y_{n}, \theta_{n})\), where \( x_{n} \) and \( y_{n} \) are the x, y coordinates and \( \theta_{n} \) is the orientation of \( m_{n} \). To avoid global registration, a polar coordinate-based structure is constructed, centred at each minutia [8]. For example, if minutia \( m_{0} \) is chosen as the centre point of the polar coordinate, other minutiae in the range of \( R \) around \( m_{0} \) are translated and rotated with respect to the vector \((x_{0}, y_{0}, \theta_{0})\). The value of \((x_{n}, y_{n}, \theta_{n})\) is deemed as \((0, 0, 0)\) and any other minutia \( m_{n} \) can be transformed and represented as \((\rho_{n}, \alpha_{n}, \beta_{n})\) in a polar coordinate system, where \( \rho_{n} \in (0, R) \) is the radial distance, \( \alpha_{n} \in [0, 2\pi) \) is the radial angle and \( \beta_{n} \in [0, 2\pi) \) is the relative orientation of minutia \( m_{n} \). To tolerate some feature uncertainty caused by non-linear distortion, the polar coordinate space is further quantised into many grids of step sizes \((x_{s}, y_{s}, \theta_{s})\) where \( x_{s} \) is the step size of \( \rho_{n} \), \( y_{s} \) is the step size of \( \alpha_{n} \) and \( \theta_{s} \) is the step size of \( \beta_{n} \). In this way, the polar coordinate space centred at minutia \( m_{0} \) can be divided into a three-dimensional (3D) cube containing \( |R|x_{s}|y_{s}|\theta_{s}|x_{s}|y_{s}|\theta_{s}| \) cells. Then, each cell of the 3D cube is examined and number ‘1’ is used to index a cell if at least one minutia falls into it; otherwise, ‘0’ is used to index that cell. By concatenating the index number of each cell, the polar coordinate-based structure centred at minutia \( m_{0} \) can be represented by a vector \( P_2(m_{0}) \), which contains only os and ls. At the end of this process, for each fingerprint image, a vector set \( \{ P_2(m_{n}) \}_{n=0}^{NT-1} \) is obtained, where \( N \) is the number of minutiae in the fingerprint image. The overall processing flow of fingerprint feature extraction is shown in Fig. 2.

![Fig. 2 Overall processing flow of fingerprint feature extraction](image)

To calculate the similarity score between a fingerprint template \( T_2 \) and a fingerprint query \( Q_2 \), each vector \( P_2^T(m_{n}) \) from the vector set \( \{ P_2^T(m_{n}) \}_{n=0}^{NT-1} \) extracted from template \( T_2 \) is compared with each vector \( P_2^Q(m_{n}) \in \{ P_2^Q(m_{n}) \}_{n=0}^{NT-1} \) extracted from query \( Q_2 \), where \( NT \) and \( NQ \) are the number of minutiae in \( T_2 \) and \( Q_2 \), respectively. The similarity score between \( P_2^T(m_{n}) \) and \( P_2^Q(m_{n}) \) is calculated as follows:

\[
S_2 = \frac { \sqrt { \sum_{k=1}^{NQ} (P_2^Q(m_{n}) - P_2^T(m_{n})) (P_2^Q(m_{n}) - P_2^T(m_{n})) } } { \sqrt { \sum_{k=1}^{NT} (P_2^T(m_{n}) - P_2^T(m_{n}))^2 } } \]

(2)

On the completion of the above comparisons, a score matrix in the size of \( NT \times NQ \) can be generated and the maximum score in the matrix is chosen as the final matching score \( S_2 \) between \( T_2 \) and \( Q_2 \).

The final score \( S_2 \) of the multi-biometric system is calculated based on score \( S_1 \) from the face modal and score \( S_2 \) from the fingerprint modal, that is

\[
S = \frac { \text{norm}(S_1) + \text{norm}(S_2) } { 2 } \]

(3)

where \( \text{norm}(\cdot) \) represents the score normalisation process, which converts the score value into the range of \([0, 1]\). If the final matching score \( S \) is greater than a preset threshold, then the authentication is considered to be successful, and vice versa.

ELECTRONICS LETTERS 5th February 2015 Vol. 51 No. 3 pp. 234–235
Experiments: We chose a subset of the ‘real’ Multimodal Biosecure Database [9], in which all the combined biometric samples are extracted from the same user. The database DS2 contains biometric samples collected from a total of 210 users and each user contributed six modalities, namely, audio–video, face, fingerprint, hand, iris and signature, in two sessions which were generated in a 1 month interval. Our tests included the first 100 users from the database DS2. Four high-definition face images and the first two fingerprint images from each of the 100 users were chosen from each session, so there are altogether 800 face images and 400 fingerprint images that were employed in our experiments. By applying the algorithms described in the previous Section, biometric features were extracted from the face and fingerprint images, respectively. For the face module, the first four images of each user were used for training and the remaining four images were used for testing. We combined the 5th, 6th, 7th and 8th face images with the 1st, 2nd, 3rd and 4th fingerprint images to form four multimodal pairs for each user. The 1st pair acted as the template and the other three pairs as the query. Three cases are designed to verify the influence of feature dependency on system performance.

Case 1: The combined face and fingerprint samples for both template and query combinations are from the same user. These combinations constitute a ‘real’ multimodal database, which represents a real-life situation.

Case 2: The combined face and fingerprint samples for both template and query combinations are from different users. These combinations form the ‘unreal’ multimodal database A, which is used in the experiments by most existing multi-biometric systems.

Case 3: The combined face and fingerprint samples for template combinations are from the same user but the query combinations for impostor tests are from different users. These combinations represent the ‘unreal’ multimodal database B.

The performance of the designed multi-biometric system is evaluated by the false accept rate (FAR) and false reject rate (FRR). The results of the three cases are shown in Fig. 3, from which we can see that the performances of case 1 (using the ‘real’ multimodal database) and case 2 (using ‘unreal’ multimodal database A) are quite different. For example, when the FAR is set to 0.1%, the FRR is 0.78% for case 1 and 1.66% for case 2, which means that the FRR has increased by about 113%. Case 3 (‘unreal’ multimodal database B) may also happen in real life but it is more like a kind of attack (random attempt using different feature combinations). We can see from Fig. 3 that case 3 also shows performances different from case 2. When FAR = 0.1%, the FRR is 0.73% in case 3, which is also quite different from the FRR of 1.66% in case 2.

Conclusion: We have evaluated a multimodal biometric system based on ‘real’ and ‘unreal’ multimodal databases. Our experimental results verify the existence of feature dependency in multi-biometric systems and also show that most existing multimodal biometric systems that utilize ‘unreal’ multimodal databases for testing do not reflect actual system performance in real situations where a multimodal template should consist of multimodal biometrics from the same person. Our investigation manifests the importance of taking into account the features’ mutual dependency when designing and testing a multimodal biometric system.

Acknowledgment: The work in this Letter was supported by the Australian Research Council (ARC) Linkage Project LP120100595.

This is an open access article published by the IET under the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0/)

1 December 2014
doi: 10.1049/el.2014.4182

One or more of the Figures in this Letter are available in colour online.

Wencheng Yang and Jiankun Hu (School of Engineering and Information Technology, University of New South Wales, Canberra 2600, Australia)
E-mail: J.Hu@adfa.edu.au

Song Wang (School of Engineering and Mathematical Sciences, LaTrobe University, Melbourne 3086, Australia)

Chi Chen (State Key Laboratory of Information Security, Institute of Information Engineering, CAS, Beijing, People’s Republic of China)

References

1 Ross, A., Nandakumar, K., and Jain, A.K.: ‘Introduction to multibiometrics’, in Jain A.K., Flynn P., and Ross A.A. (Eds.): ‘Handbook of biometrics’, (Springer, 2008)

2 Nandakumar, K., and Jain, A.K.: ‘Multimetric template security using fuzzy vault’, 2nd IEEE Int. Conf. on Biometrics: Theory, Applications and Systems, 2008

3 Nagar, A., Nandakumar, K., and Jain, A.K.: ‘Multimetric cryptosystems based on feature-level fusion’, IEEE Trans. Inf. Forensics Sec., 2012, 7, (1), pp. 255–268

4 Karthi, G., and Azhlarasans, M.: ‘Hybrid multimodal template protection technique using fuzzy extractor and random projection’, Int. J. Res. Comput Commun Technol., 2013, 2, (7), pp. 381–386

5 Vitomir, Š., and Nikola, P.: ‘The complete Gabo-fisher classifier for robust face recognition’, EURASIP J. Adv. Signal Process., 2010, p. 26

6 Jia, T.B., Lang, D.N.C., and Goh, A.: ‘Biohashing: two factor authentication featuring fingerprint data and tokenised random number’, Pattern Recognit., 2004, 37, (11), pp. 2245–2255

7 Neuro Technology: ‘VeriFinger SDK 2010 Version’. Available at URL: http://www.neurotechnology.com/verifinger.html, November 2014

8 Ahmad, T., Hu, J., and Wang, S.: ‘Pair-polar coordinate-based cancelable fingerprint templates’, Pattern Recognit., 2011, 44, (10), pp. 2555–2564

9 Ortega-Garcia, J., Fierrez, J., Alonso-Fernandez, F., Galbally, J., Freire, M.R., Gonzalez-Rodriguez, J., Garcia-Mateo, C., Alba-Castro, J.-L., Gonzalez-Aguila, E., and Otero-Muras, E.: ‘The multiscenario multi-environment biocure multimodal database (Bmdb)’, IEEE Trans. Pattern Anal. Mach. Intell., 2010, 32, (6), pp. 1097–1111