Front. Comput. Sci., 2015, 9(3): 392–401
DOI 10.1007/s11704-014-4070-1

RESEARCH ARTICLE

A hybrid biometric identification framework for high security applications

Xuzhou LI[1,2], Yilong YIN (✉)[1], Yanbin NING[1], Gongping YANG[1], Lei PAN[1]

1 School of Computer Science and Technology, Shandong University, Jinan 250101, China
2 Key Laboratory of Information Security and Intelligent Control of Shandong Province, Shandong Youth University of Political Science, Jinan 250103, China

Abstract Research on biometrics for high security applications has not attracted as much attention as civilian or forensic applications. Limited research and deficient analysis so far has led to a lack of general solutions and leaves this as a challenging issue. This work provides a systematic analysis and identification of the problems to be solved in order to meet the performance requirements for high security applications, a double low problem. A hybrid ensemble framework is proposed to solve this problem. Setting an adequately high threshold for each matcher can guarantee a zero false acceptance rate (FAR) and then use the hybrid ensemble framework makes the false reject rate (FRR) as low as possible. Three experiments are performed to verify the effectiveness and generalization of the framework. First, two fingerprint verification algorithms are fused. In this test only 10.55% of fingerprints are falsely rejected with zero false acceptance rate, this is significantly lower than other state of the art methods. Second, in face verification, the framework also results in a large reduction in incorrect classification. Finally, assessing the performance of the framework on a combination of face and gait verification using a heterogeneous database show this framework can achieve both 0% false rejection and 0% false acceptance simultaneously.

Keywords biometric verification, hybrid ensemble framework, high security applications

Received February 21, 2014; accepted July 2, 2014

E-mail: ylyin@sdu.edu.cn

1 Introduction

Biometrics are metrics recording physiological and behavioral characteristics of a person, they are being increasingly adopted for person verification applications [1]. Of the large variety of biometric verification applications, civilian and forensic applications are the most representative. Civilian applications cover a wide range of application fields including commerce, medicine, immigration, and office work. Most civilian applications [2] emphasize the need for equally simultaneously low false acceptance rate (FAR) and false reject rate (FRR), this leads to the pursuit of low equal error rate (EER). Forensic applications [3,4], such as criminal verification, belong to another representative kind of biometric verification applications. Forensic applications use the biometric traits found at a crime scene to detect criminals or to verify the identity of a suspect. Forensic applications have quite different performance requirements to civilian applications. In forensic applications, biometric traits are acquired from object surfaces that are inadvertently touched or handled by a person, so they are usually of low quality and have incomplete information. These kinds of biometric traits are called latent data [5]. Most forensic applications require biometric verification systems to efficiently deal with such latent data [6]. Low FRR is a critical design issue for forensic applications, that is, the police do not want to miss a criminal even at the risk of manually examining a large number of possibly incorrect candidates that the biometric system has identified.

Beside civilian and forensic applications, there is another very important kind of biometric verification applications, high security applications such as ATM verification and access control of nuclear power stations [7]. High security applications also cover a wide range of application fields such as access control of military installation areas, government secrets, and commercial trade secrets. In such high security applications, a disaster may occur if an impostor is falsely accepted, so the overwhelming performance requirement is extremely low FAR. The performance of a verification system is not good enough in this kind of application, so, a verification module is often used to control access. The FAR of the verification module is close to zero, while the FRR is often high. Figure summarizes the main performance requirements of the three kinds of applications [7].

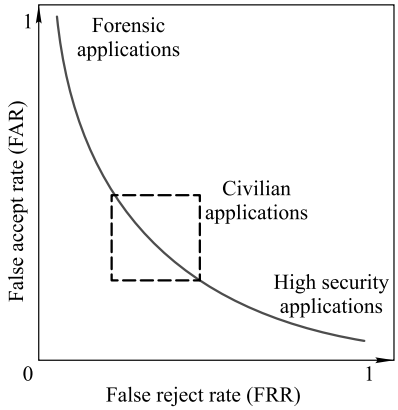

Fig. 1 Main performance requirements for three kinds of biometric verification application

Most research has concentrated on civilian applications and forensic applications, and many effective solutions have been proposed. However, high security applications have not attracted as much attention as civilian or forensic applications. Previous work [8,9] briefly introduced high security applications and elucidated the extremely low FAR requirement without proposing any feasible solutions. Research described in [10] and [11] gave an effective fusion method for high security fingerprint verification applications. An iris verification system based on random secret integration was proposed in [12] for high security uses. Many simulated fusion works have been done, but those methods cannot be applied as a general solution for other biometrics or multimodal problems. None of the previous research has provided enough systematic analysis of the performance requirements for high security applications, and special characteristics of the performance requirements have not been well explored. Limited research leads to a lack of general solutions and leaves this issue to remain a challenging one. In this paper, we provide a systematic analysis of the performance requirements for high security applications, and name the problem to be solved in order to meet these requirements as a double low problem. Based on our analysis, a hybrid ensemble framework that sequentially combines a serial ensemble and rank-level parallel ensemble orderly is proposed. Here, the rank-level parallel ensemble only achieves successful verification if the identities identified by multiple fingerprint matching algorithms are the same.

Our approach represents a significant extension of our earlier and much work [13]. The main differences between this work and our earlier work are as follows. First, we use multiple matchers in the serial fusion part, this means that the parallel fusion part works only if all the matchers cannot recognize the input sample, whereas in [13], there are only two matchers in the serial fusion section. Second, we apply the proposed framework on fingerprint, gait, and face scenarios to verify the generality of the framework. Whereas [13] only focuses on fingerprint identification.

The main contributions of this paper are as follows:

1) We provide a systematic analysis of the unique characteristics of performance requirements for high security applications and name the problem to be solved in order to meet the special performance requirements defined as the double low problem.

2) The proposed hybrid ensemble framework can integrate different base identifiers, and can be used to solve high security applications, so it is general to some degree.

3) Our framework can achieve better performance that only using a serial ensemble method or only using a parallel ensemble.

Section 2 gives a systematic analysis of performance requirements for high security applications. Section 3 introduces the proposed hybrid ensemble framework. In Section 4, three applications of the hybrid ensemble framework in fingerprint model, face model, fusion of face and gait model, and the experimental results of each one are presented. Finally, concluding comments are presented in Section 5.

2 Problem analyses

High security applications, such as ATM verification, access control of nuclear power stations and Internet transactions [10,12], have special performance requirements for biometric verification systems. In such applications, if a genuine user is mistakenly rejected, it only causes inconvenience. However, if an impostor is falsely accepted, it may be a disaster. It means that the false acceptation is far more serious than the

false rejection. In other words, extremely low FAR is required first of all in high security applications. But in a biometrics system, if we lower the FAR with fixed EER, the FRR will become higher. At the same time, it is not desirable to abandon the requirement of low FRR to pursue an extremely low FAR. For example, in bank ATM verification, a false acceptance of an impostor could mean a disastrous loss of money, while a high FRR might lead to the loss of valuable customers. So we can conclude that extremely low FAR and as low as possible FRR are desired simultaneously in high security applications. We call this problem the double low problem.

Most efforts in the biometric verification domain pursue low EER, which puts equal emphasis on FAR and FRR. A low EER usually denotes a biometric verification system that has very high performance [14,15]. In order to achieve low ERR, researchers have proposed effective solutions, such as, fusion of multiple biometrics. However, these solutions are curative and mostly applicable to specific algorithms or systems, and cannot be used in a generic scenario.

A system with low EER might not be suitable for high security applications. To illustrate the problem, the performance of a real minutiae-based fingerprint system that we use is introduced. The EER of the system is 2.7%, which is fairly low, while its FRR can reach 15.8% when FAR is zero in FVC2002DB2. This means nearly 16 in 100 genuine users will be falsely rejected on average under the zero FAR condition. Such a high FRR cannot meet the demands of high security application well since low FAR and low FRR are desired simultaneously in high security applications.

So, it is difficult to meet the special performance demand of high security applications by simply reducing EER. Admittedly, in the FVC2002 [16] report, many methods achieve low EER with simultaneously low FAR and FRR, but they cannot guarantee zero FAR requirements and are also unfit for solving the double low problem. Therefore, new schemes should be developed. Many fusion or ensemble methods have been proposed to offer high performance, and, the ensemble or fusion of various biometric verification algorithms are becoming a natural way to meet the requirements of high security applications.

According to the above analysis, we propose a general hybrid ensemble framework that can handle the double low problem effectively. The framework is described in detail in the next section.

3 Hybrid ensemble framework

The proposed hybrid ensemble framework consists of two parts. The first part is a serial ensemble in which multiple biometric matchers are used in sequence. The second part is a parallel ensemble in which all biometric matchers used in the serial ensemble are joined using rank-level fusion wherein user identification is decided according to its rank in two or more matchers to give a final result. The structure of the framework is shown in Fig. 2, where we suppose that N matchers are used in the hybrid ensemble framework.

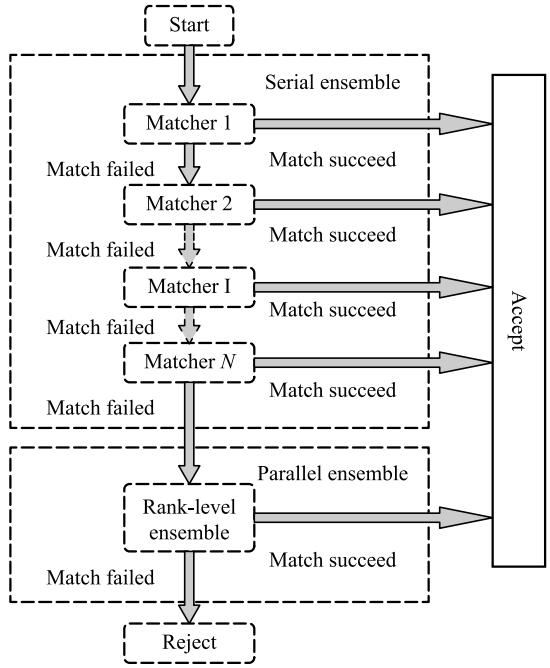

Fig. 2 The architecture diagram of the hybrid ensemble framework. The two parts of the framework are the serial ensemble and the parallel ensemble

As shown in Fig. 2, in the serial ensemble, multiple matchers are used in sequence. In a traditional verification algorithm, a threshold is set in the first place and if the maximum matching score of the query is higher than the threshold, the query is accepted. In our framework, in order to guarantee extremely low FAR for high security applications, a stricter, higher threshold is set for each matcher. If verification is successful at a matcher, the required service access will be accepted and the process will terminate. Otherwise, if the verification of one matcher fails, the next matcher will be started. The same procedure will continue until the last matcher.

If no matcher in the serial ensemble can successfully identify the query subject, the process enters the parallel ensemble in which rank-level fusion is performed using all the prior matchers. Rank-level fusion [17,18] is a parallel ensemble that is used when the output of a matcher is the rank of the candidates in a template database. Unlike a verification system, an identification system can output a rank or a candidate

list instead of a match score or a Boolean value. Fusion at the rank level has a high potential for efficient integration of multiple biometric matcher outputs [19]. In other words, the similarity in this case is not explicitly coded into a score but is implicitly coded in the ranking. Rank 1 template is more similar to the query subject than Rank 2 template, and so forth. The goal of a rank-level ensemble is to combine ranks assigned by various matchers to derive an integrated rank for each query. There are three rules usually used to combine ranks assigned by different matchers, namely, the highest rank rule, the Borda count rule, and the logistic regression rule [20]. However, these three rank level ensemble rules are relatively loose and they are unsuitable for applications of high security because the demands of double low are very strict. Therefore in this paper, we use far more rigorous rank level ensemble rules that will be described in detail in Section 4 for different modal biometrics. If the rank-level ensemble fails to identify the subject we reject the query subject.

In the serial ensemble, only if verifications in the foregoing i matchers are unsuccessful, the $(i+1)$th matcher is used. And most users can be recognized successfully in the serial ensemble, in other words, only a small number of users will use the parallel ensemble. So the proposed framework will not take much more time compared with the individual matcher.

4 Experiment results

To evaluate the proposed hybrid ensemble framework, three experiments are performed. These use the fingerprint model, face model and a fusion of face and gait model data. Our results are discussed in the following three subsections.

4.1 Fingerprint model

In this part, the proposed hybrid ensemble framework is used on two popular fingerprint matching algorithms. First, we briefly introduce the two algorithms. Then, the hybrid ensemble framework using these two algorithms is presented. And the experiments are described in detail.

4.1.1 Minutiae-based matching algorithm

The Minutiae-based matching algorithm [21], and its process is shown in Fig. 3. Local structures are used for matching and also provide correspondence for aligning the global structure of the minutiae. So, the global structure of minutiae reliably determines the uniqueness of a fingerprint. On the whole, the local and global structures of minutiae together provide a solid basis for reliable and robust minutiae matching.

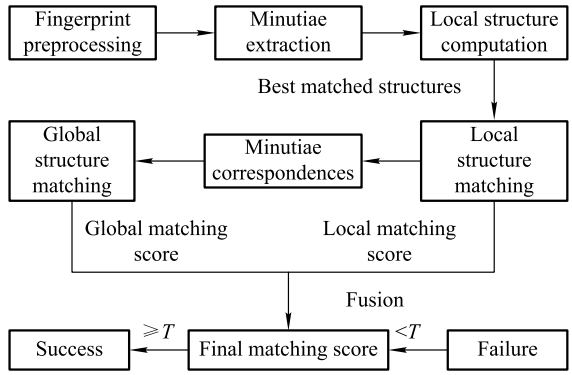

Fig. 3 The flowchart of the minutiae-based fingerprint matching algorithm [13]

4.1.2 Ridge-based matching algorithm

The ridge-based algorithm [22] is shown in Fig. 4. In the method, the relations between ridges and minutiae are established. In the alignment stage, a set of N initial substructure pairs is found, and for each of the N initial substructure pairs, ridge matching is performed. Finally, the maximum of the N scores is used as the final matching score.

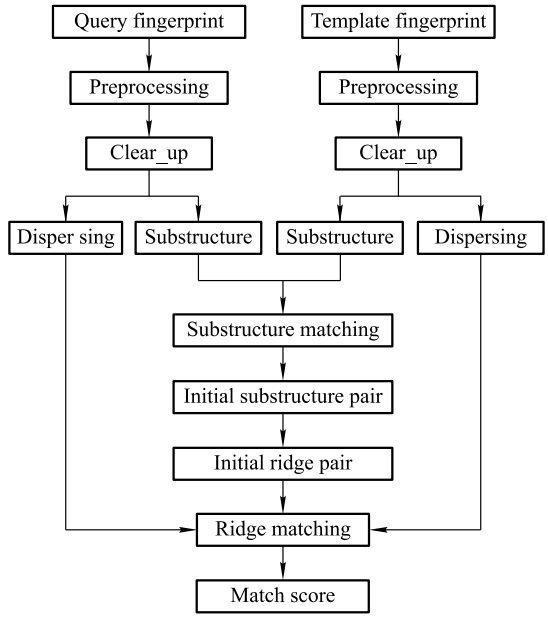

Fig. 4 Flowchart of the ridge-based fingerprint matching algorithm

4.1.3 Hybrid ensemble framework

The hybrid ensemble framework applies the proposed hybrid ensemble framework to the above two fingerprint matching algorithms. First, minutiae-based matching algorithm and ridge-based algorithm are used in order. T1 and T2 denote thresholds for the two fingerprint matching algorithms and S1 and S2 denote the maximum scores computed by the two

fingerprint matching algorithms. If either of the two matchers successfully identifies the query, the verification process will terminate and service access will be granted. Otherwise, the rank-level parallel ensemble will be executed. The ensemble rule is that the verification is successful only if the identified identities corresponding to the first rank of both the two fingerprint matching algorithms are the same. If the above constraint is not satisfied, the system will reject the query.

4.1.4 Experiments

Experiments are performed on four fingerprint databases, FVC2002DB1, FVC2002DB2, FVC2002DB3, and FVC2002DB4 [16]. The introduction of databases is given in Table 1. For each database, one image of each finger is selected to constitute the template database and the remaining images constitute the query database.

For comparison, we not only report the experimental results of the hybrid ensemble framework (HEF), but also show the experimental results of the two individual fingerprint matching algorithms and two other ensemble methods, which are briefly described below.

Table 1 FVC2002 fingerprint databases

Database	Sensor type	Image size	Resolution/dpi
DB1	Optical	388×374	500
DB2	Optical	296×560	569
DB3	Capacitive	300×300	500
DB4	SFinGe v2.51	288×384	500

The two individual algorithms are the minutiae-based matching algorithm and the ridge-based matching algorithm, called individual method 1(IM1) and individual method 2 (IM2) in our experiments, respectively.

The two other ensemble methods are the serial ensemble of the minutiae-based matching algorithm and the ridge-based matching algorithm, and the rank-level parallel ensemble of these two methods. They are called ensemble method 1 (EM1) and ensemble method 2 (EM2) in this paper, respectively.

In HEF we first use the minutiae-based matching algorithm and ridge-based matching algorithm in the serial ensemble, and then, for those users not recognized, the rank-level parallel ensemble.

The same thresholds T1 and T2 for the minutiae-based matching algorithm and the ridge-based matching algorithm are used in this experiment. We select zero FAR as a datum mark to compare the performance of the five methods, so thresholds T1 and T2 are the minima under zero FAR. That is, with the increase in threshold, FAR reduces. But, once FAR reaches zero, FAR will be unchanged with further increase in threshold. So, on the premise of guarantee of zero FAR, a minimal threshold should be used.

The results of the experiments are shown in Table 2. On average, 28.03% (IM1) and 59.23% (IM2) of fingerprints are falsely rejected with zero FAR. And an average of 22.1% (EM1) and 15.05% (EM2) of fingerprints are falsely rejected respectively with zero FAR. However, using the hybrid ensemble framework, only 10.55% of the fingerprints are falsely rejected with zero FAR. The FFR value of IM2 on FVC2002DB3 is far too high; this is mainly caused by the low quality images in this database, yet our hybrid ensemble framework achieves the lowest FRR of the five methods on this database demonstrating its effectiveness.

Table 2 The FRR of five methods under the constraint FAR=0

Database	FRR /%				
	IM1	IM2	EM1	EM2	HEF
FVC2002DB1	22.9	56.1	17.6	12.1	8.3
FVC2002DB2	15.8	47.4	12.0	6.7	5.0
FVC2002DB3	45.6	72.4	34.4	24.7	18.6
FVC2002DB4	27.8	61	24.4	16.7	10.3
Average	28.03	59.23	22.1	15.05	10.55

The performance of the HEF is better than that of EM1, indicating that adding the parallel ensemble part can improve the performance. HEF also outperforms EM2. This may be attributed to the fact that some samples can be identified in the serial ensemble of the HEF, but cannot be identified by the parallel ensemble EM2. In detail, a sample, with one high matching score and one low matching score, can be identified in the serial ensemble of the HEF. But it cannot be identified by EM2, since there is a big difference in rank values of two matching scores.

4.2 On face modal

In this part, the proposed framework is used on face verification. First, we briefly introduce two face verification algorithms that we use. Then, we present the HEF of these algorithms. Finally, we describe our experiments.

4.2.1 Eigenface for face verification

The first face verification method is the eigenface method [23, 24]. Principle component analysis (PCA) is used to extract features, as shown in Fig. 5.

4.2.2 LBP-based face verification

Face identification based on local binary pattern (LBP) is

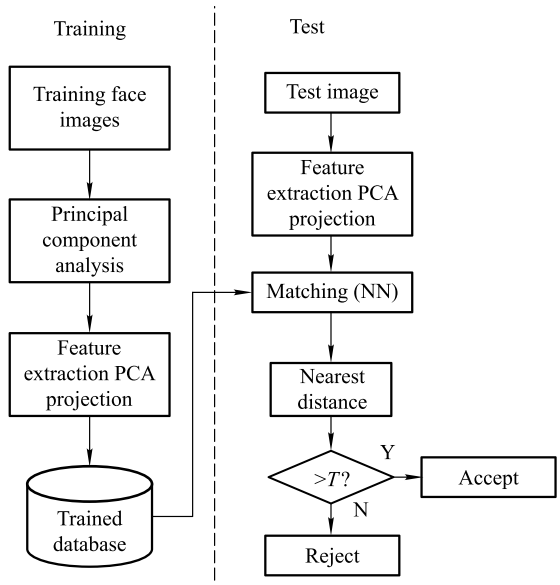

Fig. 5 Flowchart of the eigenface algorithm

proposed in [25,26], and its extension, uniform LBP, is adopted in this paper. A single image is first divided into small regions, as shown in Fig. 6(b), and then LBP features in Fig. 6(a) are extracted from each region. In uniform LBP at most two bitwise transitions are applied from 0 to 1, or vice versa, and the neighborhood is shown in Fig. 6(d). The weighted Chi-squared distance is used as a dissimilarity measure:

$$\chi^2_\omega(S, M) = \sum_{j,i} \omega_j \frac{(S_{i,j} - M_{i,j})^2}{(S_{i,j} + M_{i,j})}.$$

Fig. 6(c) shows the weight matrix.

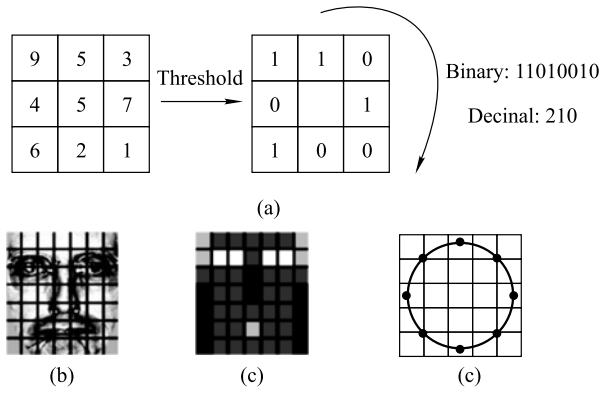

Fig. 6 The weight matrix. (a) The basic LBP operator; (b) An example of a face image divided into 7×7 windows [25]; (c) The weights of the regions, black squares indicate weight 0.0, dark grey 1.0, light gray 2.0 and white 4.0 [25]. (d) The circular (8,2) neighborhood. The pixel values are bilinear interpolated whenever the sampling point is not in the center of a pixel

4.2.3 Hybrid ensemble framework

The hybrid ensemble framework applies the proposed hybrid ensemble framework to the above two face verification algorithms. Firstly, eigenface and LBP-based algorithms are used in sequence. T1 and T2 denote thresholds for the two individual algorithms and S1 and S2 denote the maximum scores. A score is the minimum distance between the query image and enrolled images computed by the algorithm. If either of the two matchers successfully identifies the query face image, the verification process will terminate and service access will be granted. Otherwise, the rank-level parallel ensemble will be executed. The ensemble rule is that the verification is successful only when the identified identities corresponding to the first rank of both the two face verification algorithms are the same. If the above constraint is not satisfied, the system will reject the query.

4.2.4 Experiments

To assess the viability of our framework, we performed experiments on four face databases, namely the ORL Database [27], Yale Database [28], FacePix (30) Database [29, 30], and CAS PEAL R1 Database [31]. We only use a subset containing 61 images (with rotation angles between $-30°$ and $+30°$) of pose variations set with an ambient light source. For CAS PEAL R1, we choose a subset containing 367 people with six images from the expression sub database per person. Samples in FacePix (30) and CAS PEAL R1 are cropped to 100×100 size. For the other two databases we keep the original image size.

In the experiment on ORL, Yale, and CAS PEAL R1 face databases, three images of each subject are randomly selected from the database for training and the remaining images used for testing. On FacePix (30), seven images are selected for training and the remaining images for testing.

In the hybrid ensemble framework of eigen-based face verification and LBP-based face verification, eigen and LBP are first performed in the serial ensemble, and then, if unrecognized, in the rank-level parallel ensemble of eigen and LBP.

For comparison, we provide the experimental results of the two individual face verification algorithms. Table 3 shows the results of the correct classification rate (CCR) with zero FAR. The column FAR=0 is the situation of setting a threshold make FAR equal to zero. Under this constraint, the performance of a system with larger CCR and smaller FRR is better. From Table 3, we can see that setting FAR=0 causes decrease large reduction in CCR, indicating lower performance.

Table 4 summarizes the CCR of our approach with FAR=0. The third column is our framework. We can see that there is a large improvement in CCR when using our hybrid ensemble framework indicating the FRR undergoes a large reduc-

tion. As the CCR increases, more users are recognized correctly, and fewer users will be mistakenly rejected, so FRR decreases.

Table 3 The CCR /% of two face verification methods

Database	Eigenface		LBP	
	NN	FAR=0	NN	FAR=0
ORL	72.8	53.93	85	57.14
Yale	77.5	60.8	97.5	62.5
CAS_PEL	84.8	35.73	99.2	74.29
FacePix(0)	76.0	22.59	98.6	92.41

Table 4 The CCR /% of hybrid ensemble for face verification

Database	Eigenface	LBP-based method	Hybrid ensemble framework
ORL	53.93	57.14	73.93
Yale	60.8	62.5	76.67
CAS_PEAL	35.73	74.29	84.31
FacePix(30)	22.59	92.41	94.69

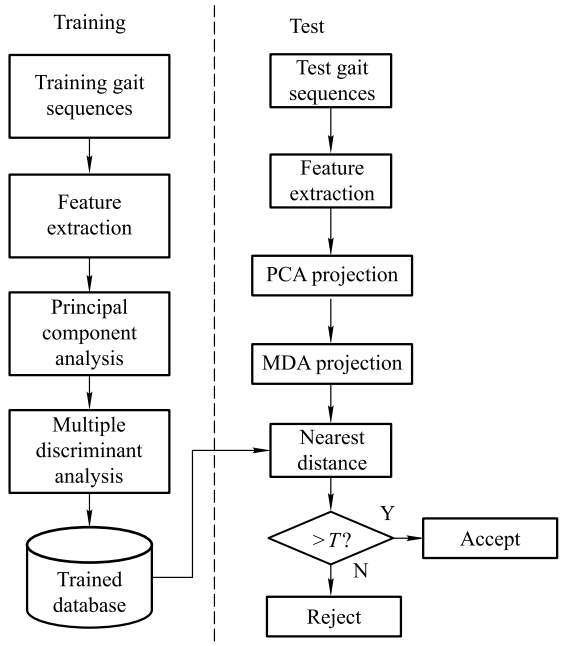

Fig. 7 Flowchart of the gait verification algorithm

4.3 On multi-modal face and gait data

In this section, the hybrid ensemble framework will be applied to fuse face and gait data. Eigenface is used as the base method of face verification here just as we used in Section 4.2. We now briefly introduce the two gait verification algorithms, and then present our framework and experiments.

4.3.1 Gait verification algorithm

We use the gait verification algorithm described in [32]. We extract the distance information between the pixels on the outermost contour and the centroid of the silhouette. Then we use PCA and multiple discriminate analysis (MDA) training to simultaneously reduce the dimensionality of the feature vectors and optimize the class separation ability of different gait image sequences. The process of the gait verification algorithm is shown in Fig. 7.

4.3.2 Hybrid ensemble framework

The hybrid ensemble framework applied to the above face and gait verification algorithms also adopt the hybrid ensemble framework as described in Section 3. In the serial ensemble part of the hybrid ensemble framework, we use the face and gait verification algorithm in sequence. Tf and Tg are the thresholds for face and gait verification algorithms, respectively, to guarantee a near zero FAR. If neither algorithm can achieve a successful verification, we enter the parallel ensemble. In the parallel ensemble, a special strict rank-level ensemble is applied. We use an n-Rank ($n = 7$) method referencing the first seven identities according to their matching scores. Note that here a matching score is reciprocal to the calculated distance between the query subject and the trained samples in the training set. For a query subject, we get two ranks R1 and R2. R1 is the result of face recognition and R2 is the result of gait recognition. In each rank, there are seven ordered numbers that are the IDs of subjects. The order of the number represents similarity from high to low. If a subject ID appears in the two ranks and the position of it in R1 is n and in R2 is m, the final score of the query is $n+m$. The query subject is classified by the identity with the minimum final score. If two identities have the same final score, we choose the one who has lower rank in the face verification algorithm considering that face verification is usually more accurate than gait verification. If no same identities exist in the two ranks, the verification fails.

4.3.3 Experiments

Because there is no homologous database containing both face and gait biometrics, in our experiment we construct a heterogeneous face and gait database using the CAS PEAL R1 Database and the CASIA gait database [33]. For face verification, we choose a sub database of 100 people with six images per person from the CAS PEAL R1 Database. No illumination or view angel variances are included in the images. For gait verification, we also construct a sub database of 100 people chosen from the CASIA gait database. The sub database is only selected from the view angle 90° of normal walking. Every subject in this gait database has six normal

sequences. In our experiments, we chose three face samples and gait samples of each subject to form the training set, and the remaining samples form the testing set.

Experiments are performed with three different methods: the hybrid ensemble framework fusing face and gait verification algorithms, the individual face verification algorithm, and the individual gait verification algorithm.

In the hybrid ensemble framework of face and gait, face identification and gait identification are first performed in serial ensemble, and then unrecognized users, will be recognized in parallel ensemble. In order to show the verification of our hybrid ensemble framework, we record the successfully identified number of samples during each step of the hybrid ensemble framework, as shown in Fig. 8. As we analyzed in Section 2, under the rigid requirements of zero FAR, some samples that could be successfully identified are falsely rejected by an individual matcher, this also happens under the serial ensemble of multiple matchers. However, after the parallel ensemble, all queries are successfully identified.

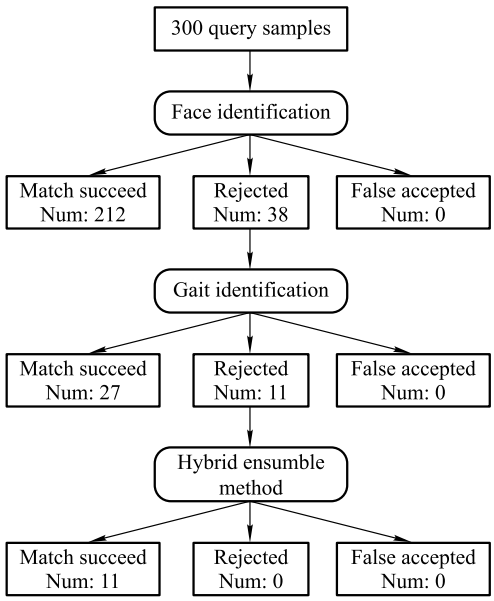

Fig. 8 Recognition number of samples during each step of the hybrid ensemble framework

The compared experimental results are shown in Table 5. The same threshold is set to the same biometric in different experiments to guarantee zero FAR. Here, we provide a comparison of CCR, FAR, and FRR. Rather than single face and gait verification, which respectively have 11% and 26% FRR under zero FAR, we can see that the hybrid ensemble framework achieves 0% FRR when FAR is 0%, which perfectly satisfies the double low requirement for high security applications.

Table 5 The results of hybrid ensemble for face and gait verification

Methods	CCR/%	FRR/%	FAR/%
Face verification	87.33	11	0
Gait verification	71.67	26	0
Hybrid ensemble framework	100.00	0	0

5 Discussion and conclusions

In this paper, we provide a systematic analysis of the special performance requirements of high security applications and define double low problem. Our proposed a hybrid ensemble framework is a general solution that can be applied to the ensemble of various biometric verification algorithms of a biometric system. By setting a sufficiently high threshold to guarantee zero or close to zero FAR and using our framework to reduce the FRR as much as possible we can see strong results on three representative tasks exhibiting the hybrid ensemble frameworks strength. Our hybrid approach significantly outperforms traditional verification methods. We also observe that the advantages of this hybrid ensemble framework are more distinct when it is applied to verification algorithms of different biometric traits like face and gait. This is because different biometric traits are independent, and thus the performance of their verification algorithms is also independent, so different biometric traits are more complementary than different algorithms of the same biometric trait, and thus can get better performance in a hybrid ensemble framework.

In our experiments, we did not compare our experimental results with other recent ensemble methods or individual methods that also show excellent performance. That is because these methods pursue low EER and are not applicable as a general framework to improve existing and fixed systems, whereas our work focuses on improving existing and fixed systems in dealing with the double low problem of high security applications. Since no previous work has tested FRR with zero FAR, a comparison with them has little significance.

It should be noted that the performance of the individual algorithms used in this paper is relatively common. That is because ordinary individual algorithms with high performance are so complicated that they are unsuitable for ensemble use, and even using common (low performance) individual algorithms we verify that our hybrid ensemble framework can achieve good performance: this is very valuable.

Acknowledgements The authors would like to thank Qing Zhang for the help in writing and the Institute of Automation, Chinese Academy of Sci-

ences for CASIA Gait Database and the Chinese National Hi-Tech Program and ISVISION Tech. Co. Ltd for the sponsor to the CAS-PEAL-R1 face database. We would like to thank the CUbiC of Arizona State University for FacePix (30) database. This work was supported in part by the National Natural Science Foundation of China (Grant No. 61070097), Shandong Natural Science Funds for Distinguished Young Scholar under (JQ201316), Program for New Century Excellent Talents in University of Ministry of Education of China (NCET-11-0315), and Program of Shandong Province Higher Educational Science and Technology (J13LN23).

References

1. Jain A K, Ross A, Pankanti S. Biometrics. A tool for information security. IEEE Transactions on Information Forensics and Security, 2006, 1(2): 125–143
2. Tabor Z, Karpisz D, Wojnar L, Kowalski P. An automatic recognition of the frontal sinus in X-ray images of skull. IEEE Transactions on Biomedical Engineering, 2009, 56(2): 361–368
3. Jain A K, Klare B, Park U. Face recognition: some challenges in forensics. In: Proceedings of the 2011 IEEE International Conference on Automatic Face and Gesture Recognition and Workshops. 2011, 726–733
4. Jain A K, Feng J J. Latent fingerprint matching. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2011, 33(1): 88–100
5. Yoon S, Feng J J, Jain A K. On latent fingerprint enhancement. In: Proceedings of SPIE, Biometric Technology for Human Verification VII. 2010, 7–17
6. Nakajima K, Mizukami Y, Tanaka K, Tamura T. Footprint-based personal recognition. IEEE Transactions on Biomedical Engineering, 2000, 47(11): 1534–1537
7. Prabhakar S, Pankanti S, Jain A K. Biometric recognition: security and privacy concerns. IEEE Security Privacy, 2003, 1(2): 33–42
8. Ratha N K, Connell J H, Bolle R M. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 2001, 40(3): 614–634
9. Liu S, Silverman M. A practical guide to biometric security technology. IT Professional, 2001, 3(1): 27–32
10. Marcialis G, Roli F. High security fingerprint verification by perceptron-based fusion of multiple matchers. Multiple Classifier Systems, 2004, 3077: 364–373
11. Jain A K, Prabhakar S, Chen S Y. Combining multiple matchers for a high security fingerprint verification system. Pattern Recognition Letter, 1999, 20(11–13): 1371–1379
12. Siew C C, Beng J A T, Chek L D N. High security iris verification system based on random secret integration. Computer Vision and Image Understanding, 2006, 102(2): 169–177
13. Yin Y L, Ning Y B, Yang Z G. A hybrid fusion method of fingerprint identification for high security applications. In: Proceedings of the 17th IEEE International Conference on Image Processing. 2010, 3101–3104
14. Feng J J. Combining minutiae descriptors for fingerprint matching. Pattern Recognition, 2008, 41(1): 342–352
15. Maltoni D, Maio D, Jain A K, Prabhakar, S. Handbook of fingerprint recognition. New York: Springer-Verlag, 2009, 224–231
16. Maio D, Maltoni D, Cappelli R, Wayman J L, Jain A K. FVC2002: Fingerprint verification competition. In: Proceedings of the 2002 International Conference Pattern Recognition. 2002, 744–747
17. Monwar M M, Gavrilova M L. FES: A system for combining face, ear and signature biometrics using rank level fusion. In: Proceedings of the 5th International Conference on Information Technology: New Generations. 2008, 922–927
18. Monwar M M, Gavrilova M L. Multimodal biometric system using rank-level fusion approach. IEEE Transaction on Systems, Man, and Cybernetics, Part B: Cybernetics, Part B-Cybernetics, 2009, 39(4): 867–878
19. Bhatnagar J, Kumar A, Saggar N. A novel approach to improve biometric recognition using rank level fusion. In: Proceedings of the 2007 IEEE Conference on Computer Vision and Pattern Recognition. 2007, 2978–2983
20. Ross A A, Nandakumar K, Jain A K. Handbook of multibiometrics. New York: Springer-Verlag, 2006, 59–82
21. Jiang X D, Yau W Y. Fingerprint minutiae matching based on the local and global structures. In: Proceedings of the 15th International Conference on Pattern Recognition. 2000, 1038–1041
22. Feng J J, Ou Y Z Y, Cai A N. Fingerprint matching using ridges. Pattern Recognition, 2006, 39(11): 2131–2140
23. Turk M A, Pentland A P. Face recognition using eigenfaces. In: Proceedings of IEEE Conference on Computer Vision and Pattern Recognition. 1991, 586–591
24. Turk M A, Pentland A P. Eigenfaces for recognition. Journal of Cognitive Neuroscience, 1991, 3(1): 71–86
25. Ahonen T, Hadid A, Pietikäinen M. Face recognition with local binary patterns. In: Proceedings of the 8th European Conference of Computer Vision. 2004, 469–481
26. Ahonen T, Hadid A, Pietikäinen M. Face description with local binary patterns: application to face recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2006, 28(12): 2037–2041
27. Samaria F. Face Recognition Using Hidden Markov Models. PhD thesis, University of Cambridge, 1994
28. Belhumeur N, Hespanha P, Kriegman J. Eigenfaces vs. fisherfaces: recognition using class specific linear projection. IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(7) (1997) 711–720
29. Black J A, Gargesha M, Kahol K, Panchanathan S. A framework for performance evaluation of face recognition algorithms. In: Proceedings of the International Conference on ITCOM, Internet Multimedia Systems II. 2002, 163–174
30. Little G, Krishna S, Black J. A methodology for evaluating robustness of face recognition algorithms with respect to variations in pose angle and illumination angle. In: Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing. 2005, 89–92
31. Gao W, Cao B, Shan S G, Chen X L, Zhou D L, Zhang X H, Zhao D B. The CAS-PEAL large-scale Chinese face database and baseline evaluations. IEEE Transactions on Systems, Man, and Cybernetics, Part a-Systems Humans, 2008, 38(1): 149–161
32. Liu L L, Yin Y L, Qin W. Gait recognition based on outermost contour. In: Proceedings of the 5th International Conference on Rough Sets and Knowledge Technology. 2010, 395–402
33. Yu S Q, Tan D L, Tan T N. A framework for evaluating the effect of view angle, clothing and carrying condition on gait recognition. In: Proceedings of the 18th International Conference on Pattern Recognition. 2006, 441–444

Xuzhou Li received his BS of computer science and technology from Shandong Institute of Light Industry, China in 2002, and MS of software engineering from Qilu Software College, Shandong University, China in 2006. Li has been working at Shandong Youth College, China since 2002. Now he is also a candidate for PhD of computer science and technology in Shandong University, China now. His research interest is biometrics.

Yilong Yin is now the director of MLA Group and a professor of Shandong University, China. He received his PhD of mechanics in 2000 from Jilin University, China. From 2000 to 2002, he worked as a post-doctoral fellow in the Department of Electronic Science and Engineering, Nanjing University, China. His research interests include machine learning, data mining, computational medicine and biometrics.

Yanbin Ning received his BS of computer science and technology from Software College, Shandong University, China in 2009, from where he also received his MS in 2012. Now he works in China Citic Bank Corporation Limited. His research interest is in biometrics.

Gongping Yang received his PhD in computer science and technology from Shandong University, China in 2007. From 2003 to 2007, he was an professor in the School of Computer Science and Technology, Shandong University, China. His research interests are machine learning and applications, medical image process and analysis, and pattern recognition.

Lei Pan received his BS in computer science and technology from the School of Computer Science and Technology, Shandong University, China in 2009, where he also received his MS in 2012. Now he works in China Citic Bank Corporation Limited. His research interests include face recognition and machine learning.