Study on Synthetic Face Database for Performance Evaluation

Kazuhiko Sumi, Chang Liu, and Takashi Matsuyama

Graduate School of Informatics, Kyoto University, Kyoto 606–8501, Japan,
sumi@vision.kueee.kyoto-u.ac.jp,
WWW home page: http://vision.kuee.kyoto-u.ac.jp/

Abstract. We have analyzed the vulnerability and threat of the biometric evaluation database and proposed the method to generate a synthetic database from a real database. Our method is characterized by finding nearest neighbor triples or pairs in the feature space of biometric samples, and by crossing over those triples and pairs to generate synthetic samples. The advantages of our method is that we can keep the statistical distribution of the original database, thus, the evaluation result is expected to be the same as original real database. The proposed database, which does not have privacy problem, can be circulated freely among biometric vendors and testers. We have implemented this idea on a face image database using active appearance model. The synthesized image database has the same distance distribution with the original database, which suggests it will deriver the same accuracy with the original one.

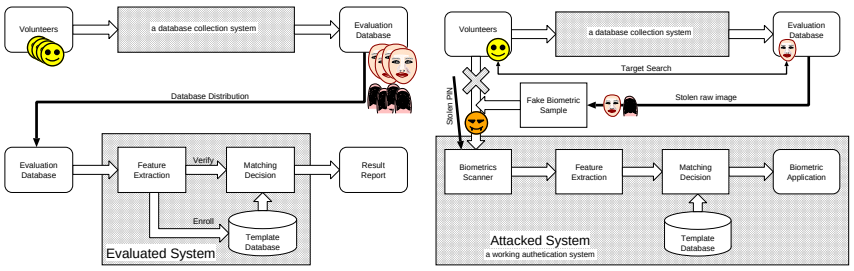
1 Introduction

Evaluation of biometric authentication systems, especially accuracy evaluation, requires a large-scale biometric database[1]. As biometric authentication systems become practical, number of volunteers required for evaluation becoming large[2]. This implies possibility of leakage of the individual data. Once, the individual data is leaked, there are several scenarios of database abuse and possible social threat. We analyze such social threat and propose a synthetic database as an alternative solution for privacy protection. In the field of fingerprint, an image synthesis tool SFINGE[3] has been developed. It has been applied in the public benchmarking such as FVC2004[4], and proven to have correlation with a real database. However, initial conditions, such as ridge orientation map and locations of fiducial points, should be given a priori. Moreover, this method cannot be applied to other biometrics, whose development process are not modeled well.

In this paper, we propose a method to generate synthetic biometric samples from real biometric examples. We try to maintain the same recognition difficulty as the original database, in order to use the synthetic database for evaluation purpose. Our idea is to find closest triples and pairs in the original database and to cross between those triples and pairs for generation of synthetic samples. As a case study, we apply this idea on a face databese.

2 Threat analysis of biometric evaluation database

Various types of vulnerability have been alerted in biometric authentication systems. It is much easier to steal personal data from evaluation database than to steal them from templates, because evaluation database has raw images and it is not secured in a safe place.



(a) System (b) Vulnerability

Fig. 1. Schematic diagram of database collection and evaluation of a biometric authentication system and its vulnerability

Figure. 1(a) shows the schematic diagram of database collection and evaluation procedure. In this figure, database which has volunteer's individual biometric data in a raw format is transferred from database developper to an evaluater.

The first scenario is to produce a fake biometric example from stolen database. A fake biometric sample, such as a fake fingerprint, an iris and a fake facemask, can be produced from the raw image. This fake example can be used to attack a biometric authentication system under operation shown in Figure 1(b) Suppose the attacker steal the template database DB_B of biometric evaluation system B. If the attacker knows the PIN N_j of the person $P_j, (P_j \in DB_B)$, a fake biometric, which produces the same impression as T_j, is produced from T_j, then it can be used to attack a 1-to-1 authentication system A and obtain the access permit of the owner j. Even if the PIN is not known, but it is certain to be enrolled in the specific system A, the fake example can be used to obtain access permit to the system, if the system allows 1-to-N authentication scheme.

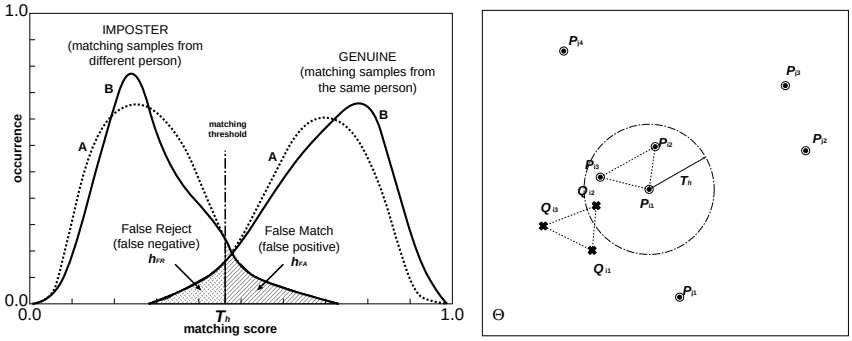
To prevent those privacy invasion, protecting the database is desirable. However, hiding raw image is impossible, because the evaluation usually includes feature extraction algorithm as well as matching and classifying algorithms. The input of the algorithm must be a raw image. So, we propose a synthetic biometric database in the next section.

3 Requirement of synthetic biometric database

A synthetic biometric database consists of virtual individual biometric examples is one of the solution. However, to satisfy accurate evaluation of biometric authentication systems, the database should have the following characteristics:

1. (precision requirement) The evaluation results derived from a synthetic biometric database should be equal to the one from the real database.
2. (universality requirement) The precision requirement should be satisfied for all of authentication algorithms to be evaluated.
3. (privacy requirement) Each biometric data in the synthetic database should not represent any real person.

The precision requirement can be resolved in the following way.



(a) Distribution (b) Critical samples

Fig. 2. Similarity distributions of synthetic database B and real database A (a), and relationships of critical samples in a real database and the corresponding synthetic database (b)

Suppose group A is a real database corrected from existing individuals consist of M_A examples. Using algorithm Θ, an biometric raw example $a_i, (a_i \in A, 1 \leq i \leq M_A)$ is projected to $\theta(a_i)$ in a future space. If we obtain a similarity distribution like Figure. 2(a)A, it means that the distribution of h_{FA} at threshold T_h is the number of impostor samples closer than T_h in the feature space Θ. Another group B is a synthetic database derived from A consists of M_B examples. ($M_B = M_A$ in this case) Using algorithm θ, a biometric raw example $b_i, (b_i \in B, 1 \leq i \leq B_A)$ is projected to $\theta(b_i)$ in a future space. If we like to have the same false rejection rate (FRR) and false accept rate (FAR) at threshold T_h, the number of pairs, which are closer than T_h in the feature

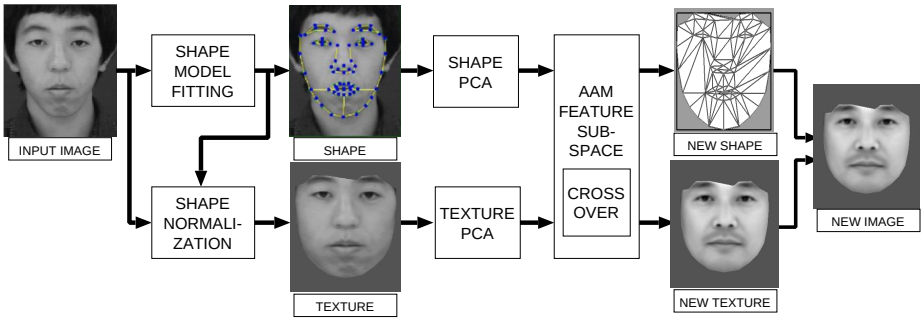


Fig. 3. Schematic diagram of face image deformation based on facial parts regions

space Θ should be the same with the case of A. This suggests that we should be careful not to change the distance of samples, whose distance is less than T_h, but we don't have to be careful about the distance of samples, whose distance is larger than T_h. Figure.2(b)shows an example of such a deformation. Suppose P are the biometric samples. For a arbitrary index i, select samples closer than the threshold T_h in the feature space Θ. In this figure, they are P_{i1}, P_{i2}, and P_{i3}. If we generate synthetic examples Q_{i1}, Q_{i2}, and Q_{i3}, and the distance between Q_{i1} and Q_{i2}, Q_{i1} and Q_{i3}, and Q_{i2} and Q_{i3} are equal to the original distance between P_{i1} and P_{i2}, P_{i1} and P_{i3}, and P_{i2} and P_{i3}, respectively, the synthetic samples satisfy with the three requirements explained in this section.

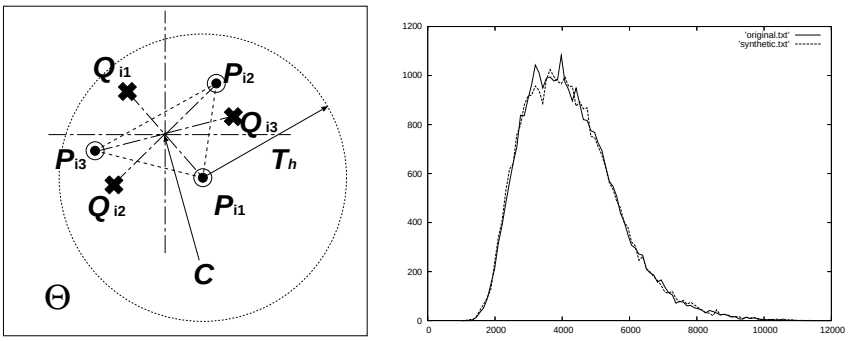
In the above deformation, we should consider isolated samples which have only one neighbor or no neighbors within the threshold T_h. In case of doubles, we rotate the pair of samples around its center. In case of standalone, we move the sample along a certain displacement, which has a fixed length and a random direction.

4 A case study using active appearance model

According to the idea in Section. 3, we have synthesized a face database from a real face database. The real faces are from HOIP face database contains 300 subjects of various age (from 20 to 60) and gender (150 males and 150 females), in a illumination controlled environment.

In this study, we deform the faces in PCA subspaces represented by active appearance model[5], and then reconstruct face images. Deformation is performed in the PCA subspaces of active appearance model (AAM), which consists of shape subspace and texture subspace. In the subspace, all the samples are grouped into triples, pairs, and singles according to the distance to the nearest neighbors. Then cross-over operation is performed to generate new samples. Finally, those synthetic samples are back projected and images of synthetic samples are generated.

Regards to the details of deformation, triples are detected in each PCA subspace Θ of AAM feature space. Then the center of the triples P_{i1}, P_{i2}, and P_{i3} are calculates as C. The synthetic face samples Q_{i1}, Q_{i2}, and Q_{i3} are placed at the symmetrical position of P_{i1}, P_{i2}, and P_{i3}, respectively. The relationships of P_{i1}, P_{i2}, P_{i3}, Q_{i1}, Q_{i2}, Q_{i3}, and C are shown in Figure. 4(a). In case of not finding a triple around the focused sample, a pair is detected instead. If there are no sample in a given distance T_h, the sample is regarded as a singlar sample. Random displacement is given for such a singlar sample.



(a) Closest triples (b) Distance distribution

Fig. 4. Selection of the closest triples and its deformation (a) and the distribution of distance between arbitrary two samples in the original database and in the synthetic database (b)

Examples of synthetic faces are shown in Figure. 5. In the figure, upper row is the real faces and the lower row is the synthesized images. As we can see, the pair (upper and lower) of images is apparently different person but has similar impression. The distances between three samples are same within the PCA feature space.

To confirm the precision requirement described in Section 3, we compared the distribution of distance between arbitrary samples both in original database and in synthetic database. Figure.fig-deformation2(b) shows the distribution of distance. The original database and the synthetic database shows the quite similar distribution. It suggests that evaluation using these two database will derive the same accuracy results.

5 Discussion and future direction

At this moment, we have not completed the way to satisfy the universality requirement yet. The synthetic database, whose distances are same with the

Fig. 5. The real face image (upper) and the synthetic face image (lower) using our proposed method

original database measured in PCA sub-space of AAM, may not be equal-distant in other feature space, such as simple eigenfaces and banch graph matching. Never the less, AAM, which employs both geometric (shape) and photometric (texture) features, is the most promissing approach for 2D image.

Another discussion is how to deal with intra-personal variations. Some of the face recognition algorithms require multiple images with different appearances for enrollment. Also, we need intra-personal variations to evaluate false non-match rate of an algorithm. So, we have to synthesize multiple appearances for a synthesized person. The method to generate multiple appearances for a person depends on the variation of the original images. If the variation of the original images are arbitrary, we have to use the common intra-personal variation space, which is introduced by Moghaddam[6]. First, we will build the intra-personal variation space using the original images, then apply it to the synthetic image and generate multiple views. If the variation of the original images are taken systematically and changes are parameterized, we can use the changed images and apply same deformation to the images.

6 Summary

In this paper, we have analyzed the vulnerability and threat of the biometric evaluation database and proposed a new method to generate synthetic database based on real database. Our method is characterized by finding nearest neighbor triples or pairs in the feature space of biometric samples, and by crossing over those triples and pairs to generate synthetic samples. The advantages of our method is that we can keep the statistical distribution of the original database, thus, the evaluation result is expected to be the same as original real database. The proposed database, which does not have privacy problem, can be circulated freely among biometric vendors and testers. We have implemented this idea on a face image database using active appearance model. The proposed database, which does not have privacy problem, can be circulated freely among biometric vendors and testers. We hope that this technique will accelerate the development practical biometric authentication systems.

Acknowledgments

This research is supported in part by the Informatics Research Center for Development of Knowledge Society Infrastructure, 21st. Century COE program and by contracts 13224051 and 14380161 of the Ministry of Education, Culture, Sports, Science and Technology, Japan. This research is also supported in part by the research contracts with Japan Automatic Identification Systems Association.

References

1. Wilson, C.L.: Large scale usa patriot act biometric testing. In: Proc. International Meeting of Biometrics Expert. (2004) http://www.biometricscatalog.-org/document_area/view_document.asp?pk={5E0CA69A-B4AC-4FE9-9624-6ED3450E9CCF}.
2. Wayman, J.: Technical Testing and Evaluation of Biometric Identification Devices, in, A. Jain, etal(ed): Biometrics: Personal Identification in a Networked Society. Kluwer Academic Press, Higham, MA, USA (1999)
3. Cappelli, R., Erol, A., Maio, D., Maltoni, D.: Synthetic fingerprint-image generation. In: Proc. International Conference on Pattern Recognition. (2000)
4. Maio, D., Maltoni, D., Cappelli, R., Wayman, J., Jain, A.K.: Fvc2004: Third fingerprint verificatin competition. In: Proc. International Conference on Biometric Authentication. (2000) 1–7
5. Cootes, T., Walker, K., Taylor, C.: View-based active appearance models. In: AFGR00. (2000) 227–232
6. Moghaddam, B., Jebara, T., Pentland, A.S.: Baysian face recognition. PR **33** (2000) 1171–1782