Combining Multiple Biometrics to Protect Privacy

Berrin Yanikoglu and Alisher Kholmatov
Sabanci University
Tuzla, Istanbul, 34956, Turkey
berrin@sabanciuniv.edu, alisher@su.sabanciuniv.edu

Abstract

As biometrics are gaining popularity, there is increased concern over the loss of privacy and potential misuse of biometric data held in central repositories. The association of fingerprints with criminals raises further concerns. On the other hand, the alternative suggestion of keeping biometric data in smart cards does not solve the problem, since forgers can always claim that their card is broken to avoid biometric verification altogether.

We propose a biometric authentication framework which uses two separate biometric features, combined to obtain a non-unique identifier of the individual, in order to address privacy concerns. As a particular example, we demonstrate a fingerprint verification system that uses two separate fingerprints of the same individual. A combined biometric ID composed of two fingerprints is stored in the central database, and imprints from both fingers are required in the verification process, lowering the risk of misuse and privacy loss. We demonstrate the performance of the proposed method on a small fingerprint database collected from 95 people.

1. Introduction

Biometric data is increasingly used in authentication and identification of individuals, replacing password-based security systems. Identification and authentication refers to two different tasks: finding the identity of a person given the biometric versus verifying the identity given the biometric data and the claimed identity.

There are two approaches to a biometric authentication system. In one alternative, enrolled users' biometric data are kept at a central repository and authentication is done by verifying the test data against the reference at the central repository. In the second alternative, a user carries a smart card containing his/her biometric data, and verification is done against the sample in the smart card. There are disadvantages associated with both of these two approaches. In particular there is increased concern over the loss of privacy and potential misuse of biometric data held in central repositories. Biometric data which can *uniquely* identify a person (e.g. fingerprints, iris patterns) can be used to track individuals, linking many separate databases (where the person has been, what he has purchased etc.). There is also fear that the central databases can be used for unintended purposes [2]. For instance, latent fingerprints can be used to search for information about a person in a central database, if such databases are compromised. The association of fingerprints with criminals raise further concerns for fingerprint databases in particular. Similarly, biometric data may reveal certain rare health problems, which may brings concern about possible discriminatory uses of central databases.

On the other hand, keeping biometric data in smart cards has its own disadvantages. In particular, forgers can claim that their card is broken and avoid biometric verification altogether. Since a smart card may become damaged legitimately, such a situation would need to be solved by non-biometric authentication or by resorting to a central database.

Tomko proposes the use of biometric data as an encryption key that would be used to encrypt/decrypt his/her PIN number (of which there can be many) [2, 3]. In this way, the fingerprint which uniquely identifies the person is not stored in the database, eliminating any privacy concerns. Indeed, this would be a good solution, however obtaining a unique encryption key from a biometric data, such as a fingerprint, is a challenge. Each impression of a fingerprint for instance is slightly different from another, due to many factors, cut marks, moisture, finger being pressed differently etc., making the task of key generation less than straightforward.

There are very few published research articles on the topic of privacy within the context of biometrics [1–4]; however public disapproval of the biometric technologies are increasing in many countries due to the threat of loss of privacy. In this paper we propose a biometric authentication framework to address these privacy concerns. In particular, two biometric features (e.g. fingerprints) are combined to

obtain a *non-unique* identifier of the individual and stored as such in a central database. While the *combined biometric ID* is not a unique identifier, relieving concerns of privacy, we show that it can still be used in authenticating a person's identity. As a particular example, we demonstrate a fingerprint verification system that uses two separate fingerprints of the same individual to form a combined biometric ID.

With the proposed method, a person can give two fingerprints for one application (e.g., passport application), and two other fingerprints for another one (e.g., bank), creating two separate biometric IDs. While the person can still be authenticated for either application, it is impossible to link the two databases. Similarly, it would be more difficult in this case to use latent fingerprints to search for a person, as one would need to try many such combinations of fingerprint pairs.

2. Proposed Method

Each person who enrolls into the system gives two fingerprints, A and B. The minutiae points of these two fingerprints are found and superimposed so that their center of mass are aligned. The obtained combined minutiae list becomes the biometric ID of the person and is stored in the central database. Note that the combined ID can be generated by many different fingerprint pairs, as such, it is *not* a unique identifier of the person.

The enrollment process is shown in Fig. 1, with the combined minutiae image being on the right. Note that in this figure we show the two parts of the combined fingerprint with separate markers for clarity; in fact they should all be marked the same, since they are indistinguishable in the combined list.

Figure 1. The combined fingerprint minutiae on the right is what is stored at the central database. The source finger of minutiae points are actually lost; they are marked here with special shapes for clarity.

When a person is to be authenticated, s/he gives two fingerprint impressions (A' and B'), *both* of which is used to verify his/her identity. First, one of the fingerprints, say A', is matched against the combined biometric ID, as shown

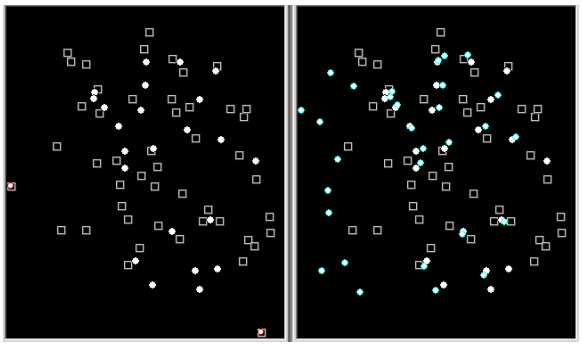

Figure 2. The combined minutiae list is on the left. The registration of the first fingerprint A', shown in blue circles, against the combined fingerprint is shown on the right. Circles and squares are used here for clarity. The corresponding fingerprints are shown in Fig. 3.

in Fig. 2. Note that even though the minutiae points are marked so as to indicate their source finger, they are not kept in the combined ID. The matching is done by finding the correspondence between the minutiae of the fingerprint and the combined minutiae list. Both the minutiae extraction and the point correspondence algorithm are non-essential to the proposed method and any previously developed minutiae detection or correspondence algorithms can be used.

After this first match step, the matched minutiae points are removed from the combined minutiae list, giving

$$A_M + B_M - A'_M$$

where A_M indicates the minutiae list of the fingerprint A, $+$ indicates concatenation and $-$ indicates deletion of *matched* points. Then, the second fingerprint B' is matched against these remaining minutiae points. The person is authenticated if the ratio of matched minutiae points to the remaining minutiae points left from the combined list plus those from B' is above a certain threshold:

$$score = 2 \times \frac{\left|(A_M + B_M - A'_M) \cap B'_M\right|}{\left|(A_M + B_M - A'_M) + B'_M\right|} \qquad (1)$$

In case A' matches A perfectly and B' matches B perfectly, the resulting score with this metric is 100. If A' was not successfully matched, it would be reflected in the final score since many minutiae points would be left unmatched, making the denominator large. If B' was not successfully matched, the numerator would be small.

Note that the match rate obtained in the first step is significantly higher than if we just matched the corresponding fingerprints A and A', since the combined ID contains about twice as many minutiae points. In particular, fingerprints

with few minutiae points match to several combined fingerprints with large sets of minutiae points. This makes it very difficult to search the combined database using a single fingerprint to find matching records (identification), which is the intended result. On the other hand, it does not reduce the effectiveness of the system: if minutiae from B are matched by A', it will show in the final score if it matters. If on the other hand A's and B's minutiae are nearby, then it does not matter whose minutiae are matched.

2.1. Experiments

We have demonstrated the concept of a combined biometric ID using fingerprints. Four fingerprints (two from one finger and two from another finger) are collected from each of the 96 people contributing to the database. Two of these fingerprints, one from each finger, are added to the reference set: they are used to form the combined ID for the person. The remaining two fingerprints, the second impressions of each finger, are added to the test set: they are used to authenticate the person.

Figure 3 shows a quadruple from the database: the top row is the reference set (A and B) and the bottom row is the test set (A' and B'), from left to right. Notice that the fingerprints have many missed minutiae, either due to labeling mistakes, or due to the shifts and deformations in the taking of the imprints.

Once the data is collected, the minutiae points are found and matching of the fingerprint pairs are done against the stored combined fingerprint, as explained in the previous section. In this work, the minutiae points are marked manually, but the matching is done automatically. However, note that manual labelling of the minutiae points is not essential: any reasonably successful minutiae detection and matching algorithm can be used. The automatic matching is done via a simple matching algorithm that aligned two point sets by finding the best alignment over all translations and rotations, allowing for some elastic deformation of the fingerprint (accepting two points as matching if they are within a small threshold in this alignment). Since the aim of this paper was to introduce the idea of a combined biometric ID, we only needed to show that the resulting combined ID is non-unique, but that it can still be used to authenticate a person. Hence, minutiae detection and matching were assumed to be given or were simply implemented.

Using the proposed method explained in Section 2 and the collected data, there was a 2.1% false accept rate (FRR). In other words, 2 out of 96 people in the database were not authorized using their second set of fingerprints (A' and B'). On the other hand when each of these fingerprint pairs were used as a forgery for all other people (for a total of 9120=96*95 data points), only 2.1% were falsely accepted (FAR). The 2.1% point is the equal error rate (EER) where

Figure 3. Sample quadruple fingerprints from the database. Top row shows fingerprints A and B; bottom row shows fingerprints A' and B', left to right.

FAR and FRR, which are inversely proportional, are equal.

In order to test how much error is introduced to the authentication scheme, by the use of two fingerprints instead of one, we have calculated the error rate of matching the fingerprints one by one, using the same minutiae detection and matching algorithms. The matching score used was the ratio of the number of matching points over the total number of points in the matched and the reference fingerprints. For instance, for the A set, it was:

$$score = 2 \times \frac{|A_M \cap A'_M|}{|A_M + A'_M|} \qquad (2)$$

In this task, the FRR was found to be 3.1%: in other words, only 6 fingerprints were falsely rejected out of 192 fingerprints (96x2). When each fingerprint was used as forgery for all the others, the FAR for this test was 2%. Hence, the combined biometric scheme introduced no aditional errors, in fact, it reduced the error rate. This should in fact be the case, since we are given more identifying information about the person, however the test have shown that the proposed combination scheme did not hinder verification.

The thresholds to decide where to authorize a fingerprint or fingerprints were set on the test set, for both tasks, in or-

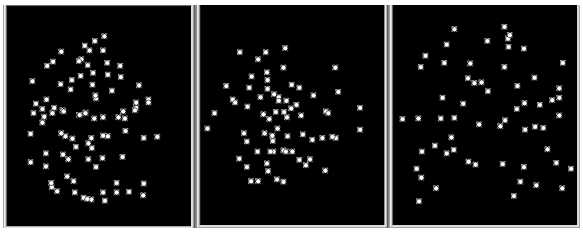

Figure 4. The combined minutiae from 3 different people.

der to give the EER. Since FAR and FRR are inversely proportional, this is a common practice and does not introduce undue advantage.

Most of the errors were due to fingerprints that had significant stretching between two instance, as these are not well matched using our simple matching algorithm. Other biggest source of error is fingerprints that have missing left or right parts, due to pressure being applied to one side of the finger while taking the imprint.

2.2. Summary and Conclusions

We have introduced the idea of combining biometrics such that the combined biometric would not be a unique identifier of the person, yet it could still be successfully used for authentication purposes.

We have demonstrated such a system using fingerprints and showed that the authentication error rate is very small (2.1% EER), even with very simple underlying algorithms for minutiae detection and matching. Given that there was actually a decrease in the verification error using the combined biometric, compared to our simple fingerprint verification system (labelled minutiae and simple alignment), we can say that the proposed scheme can be used to increase privacy without hindering the verification process.

We have not actually proven that the combined biometric cannot be used to track a person: it may be possible that a certain pattern of minutiae distribution appears only for a given person. However, the addition of minutiae points from the second fingerprint hides these patterns to the largest extent. In the future, one can further look into how to best combine two biometrics, (e.g. to disperse the minutiae points as much as possible etc.) so as to hide most unique features of a fingerprint. Three separate combined fingerprint minutiae are shown in Fig. 4 to give some idea.

We have collected our own data because we wanted to make sure to have four fingerprints from each user and to have relatively good fingerprints. In future, we will try the same tests with public fingerprint databases, as well as more sophisticated minutiae detection and matching algorithms.

References

[1] M. Crompton. Biometrics and privacy: The end of the world as we know it or the white knight of privacy? In *1st Biometrics Institute Conference*, 2003.

[2] G. Tomko. Biometrics as a privacy-enhancing technology: Friend or foe of privacy? In *Privacy Laws & Business 9th Privacy Commissioners/Data Protection Authorities Workshop*.

[3] G. Tomko. Privacy implications of biometrics – a solution in biometric encryption. In *Eighth Annual Conference on Computers, Freedom and Privacy*, 1998.

[4] J. Woodward. Biometrics: Privacy's foe or privacy's friend? In *Proceedings of the IEEE*, volume 85, 1997.