Data Fusion in Biometrics

Marcos Faundez-Zanuy
Escola Universitaria Politècnica de Mataró

ABSTRACT

Any biometric system has drawbacks and cannot warranty 100% identification rates, nor 0% False Acceptance and Rejection Ratios. One way to overcome the limitations is through a combination of different biometric systems. In addition, a multimodal biometric recognition is more difficult to fool than a single biometric system, because it is more unlikely to defeat two or three biometric systems than one. This paper summarizes the different data fusion levels, and how it must be performed in order to improve the results of each combined system on its own.

INTRODUCTION

All biometric systems have some weaknesses [1], so it is difficult to obtain a biometric system that accomplishes the four most desirable points for a biometric-based security system:

- **Universality:**
  All the persons should have the selected biometric identifier.

- **Distinctiveness:**
  Two persons with a biometric characteristic too close to be confused should not exist.

- **Permanence:**
  The biometric identifier should remain the same for long periods of time, enabling the user authentication years after the registration of the user in the database.

- **Collectability:**
  The biometric should be measurable quantitatively.

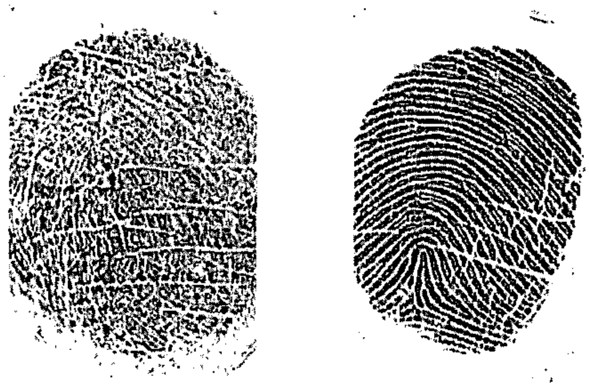

Fig. 1. Fingerprint of a 75-year-old and a typical fingerprint

Although for most users and operational environments there are not great problems, several scenarios and users difficult to manage exist. Table 1 summarizes some drawbacks of the well-known biometric systems. This list skips those situations where the user is not collaborative enough, or some unavoidable environment changes take place (different illumination, ambient noise, etc.). Obviously in these situations, data fusion can also facilitate the recognition process.

Another problem is a hacker trying to illegally access a biometric system relying on a single biometric characteristic. A single biometric system can be fooled in several ways, as described in [2]. The combination of different systems can improve the security level of only one system. For example, in a biometric system consisting of a fingerprint and voice analysis it is more difficult to imitate the fingerprint and voice of a given user, than just using one biometric characteristic, or if a person presents low-quality fingerprints, he can be recognized by means of his voice. Figure 1 shows the fingerprint of a 75-year-old acquired with the best effort to obtain the highest possible quality, and a typical fingerprint with enough quality.

This work was supported by the Spanish Grant CICYT TIC-2003-08382-C05-02.

Authors' Current Addresses:
M. Faundez-Zanuy, Escola Universitaria Politècnica de Mataró, Avda. Puig i Cadafalch 101-111, 08303 Mataro (Barcelona) Spain.

Manuscript received December 28, 2003; revised February 2004.

Table 1. Drawbacks of the Main Biometric System

Biometric Technology	Weaknesses
Fingerprint	Certain users do not have fingerprints (elder people, some Asian populations [1], manual workers with acid, cement, etc.)
	Some fingerprint scanners cannot acquire fingerprints that are too oily, dry, wet, warm, etc.
	Temporal or permanent damages can make fingerprint recognition impossible.
Face	Changes in hairstyle, makeup, facial hair, etc.
	Addition or removal of glasses, hats, scarves, etc.
	Dramatic variations of weight, skin color change due to sun exposure, etc.
Iris	Eye trauma is rarely present, but still possible. Although this system is quite robust, it is not popular – nor are the sensors widely-introduced.
Voice	Illness can modify the voice (cold, flu, aphonia, etc.)
	Acquisition devices and environments can vary significantly, for instance, in mobile phone access. This degrades the recognition rates.
Hand Geometry	Weight increases or decreases, injuries, swelling, water retention, etc., can make recognition impossible.
	Some users can be unable to locate the hand geometry due to paralysis, arthrosis, etc.

The key point to overcome these drawbacks, or at least to mitigate them, is using a combination of different informations. This is done by live beings in order to improve our knowledge of the surrounding world. Some examples are:

- The combination of the information sensed by two ears lets us identify the arrival direction of the sound, two eyes let us identify the depth of the scene, and obtain a three-dimension image.

- Simultaneously touching and looking at an object yields more information than just using only one sense.

- In democracy, the final decision of who the governor is consists of the combination of millions of people's decisions.

A similar strategy can be adopted to improve a biometric system. Figure 2 shows the scheme of a general biometric system. Four main parts corresponding to different data fusion levels can be identified.

In all cases, the system can be classified as [3]:

- **Unimodal biometric system:**
  it relies on a single biometric characteristic.

- **Multimodal biometric system:**
  It uses multiple biometric characteristics, like voice plus fingerprint; or face plus iris.

Usually the unimodal systems are easier to install, the computational burden is typically smaller, they are easier to use, and cheaper because just one sensor (or several sensors of the same kind) are needed. On the other hand, a multimodal system can overcome the limitations of a single biometric characteristic.

DATA FUSION LEVELS

Considering the main blocks plotted in Figure 2, the following levels can be defined:

- **1. Sensor level:**
  In this level, the digital input signal is the result of sensing the same biometric characteristic with two or more sensors. Thus, it is related to unimodal biometrics. Figure 3 shows an example of sensor fusion that consists of sensing a speech signal simultaneously with two different microphones. The combination of the input signals can provide noise cancellation, blind source separation [4], etc.

Another example is face recognition using multiple cameras that are used to acquire frontal and profile images in order to obtain a three-dimensional face model, which is used for feature extraction.

Although this fusion level is useful in several scenarios, it is not the most usual one.

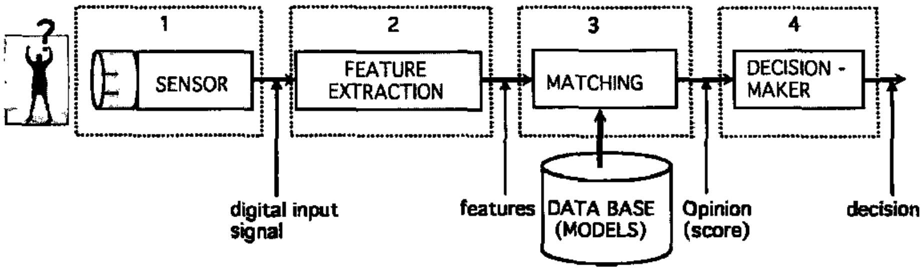

Fig. 2 General scheme of a biometric system

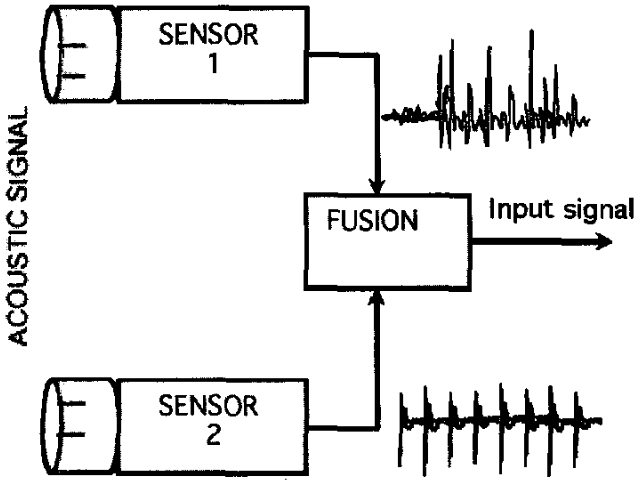

Fig. 3. Example of sensor fusion for speech signals. This block should replace block number 1 in Figure 2

- **2. Feature level:**
  This level can apply to the extraction of different features over a single biometric signal (unimodal system) and the combination of feature levels extracted from different biometric characteristics (multimodal system). An example of a unimodal system is the combination of instantaneous and transitional information for speaker recognition [5].

Figure 4 shows an example that consists of a combination of face and fingerprint at the feature level.

This combination strategy is usually done by a concatenation of the feature vectors extracted by each feature extractor. This yields an extended size vector set.

Some drawbacks of this fusion approach are:

- There is little control over the contribution of each vector component on the final result, and the augmented feature space can imply a more difficult classifier design, the need for more training and testing data, etc.

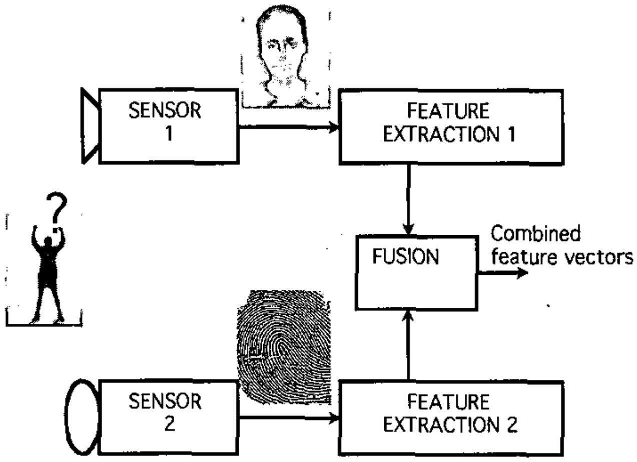

Fig. 4 Example of feature fusion. This block should replace block numbers 1 and 2 in Figure 2

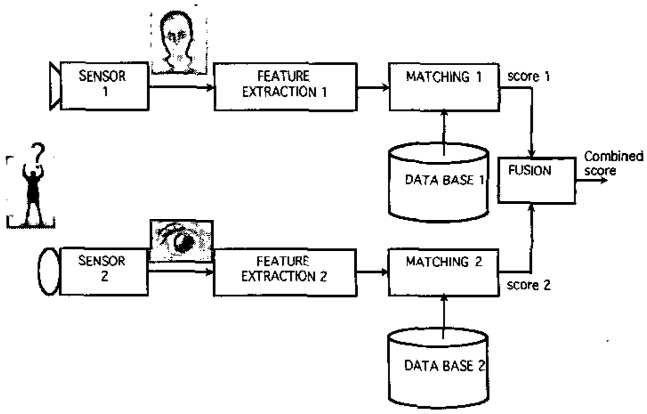

Fig. 5 Example of opinion fusion. This block should replace block numbers 1, 2, and 3 in Figure 2

- Both feature extractors should provide identical vector rates. This is not a problem for the combination of speech and fingerprint, because one vector per acquisition is obtained. However,

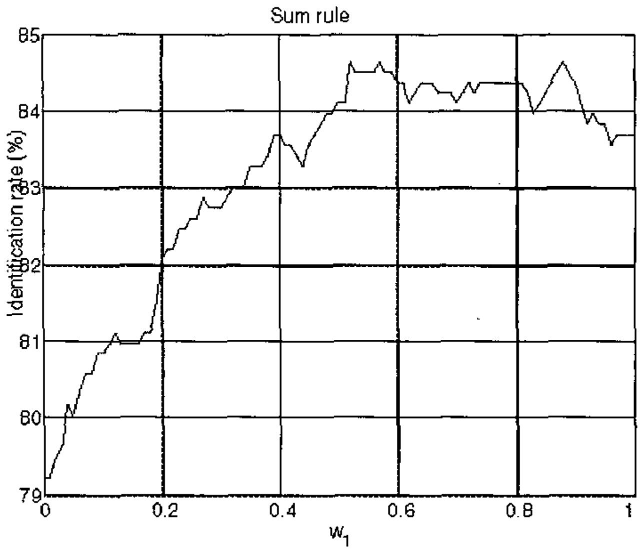

Fig. 6. Example of trained rule for opinion fusion. It combines two different speaker recognition classifiers

it can be a problem for combining voice with another biometric characteristic, due to the high number of vectors that depend on the test sentence length.

Although it is a common belief that the earlier the combination is done, the better result is achieved, state-of-the-art data fusion relies mainly on the opinion and decision levels.

- **3. Opinion level:**
  This kind of fusion is also known as confidence level. It consists of the combination of the scores provided by each matcher. The matcher just provides a distance measure or a similarity measure between the input features and the models stored on the database.

It is possible to combine several classifiers working with the same biometric characteristic (unimodal systems) or to combine different ones. Figure 5 shows an example of multimodal combination of face and iris.

Before opinion fusion, normalization must be done. For instance, if the measures of the first classifier are similarity measures that lie on the [0, 1] range, and the measures of the second classifier are distance measures that range on [0, 100] two normalizations must be done:

- 1) The similarity measures must be converted into distance measures (or vice versa).
- 2) The location and scale parameters of the similarity scores from the individual classifiers must be shifted to a common range. For instance, see [6] for detailed formulation.

After the normalization procedure, several combination schemes can be applied [7].

The combination strategies can be classified into three main groups:

- **Fixed rules:** All the classifiers have the same relevance. An example is the sum of the outputs of the classifiers;
- **Trained rules:** Some classifiers should have more relevance on the final result. This is achieved by means of some weighting factors computed using a training sequence. (Figure 6 shows an example of a trained rule that consists of the combination of two different classifiers for speech recognition. It is interesting to observe that for $\omega_1 = 1$) (83.8% identification rate) just the first classifier is considered, while for $\omega_t = 0$) (79.2% identification rate) just the second classifier has relevance. For intermediate values, higher identification rates are achieved (84.8%)); and
- **Adaptive rules:** The relevance of each classifier depends on the instant time. This is interesting for variable environments. (For instance, a system that combines speech and face can detect those situations where the background noise increases and then reduce the speech classifier weight. Similarly, the face classifier weight is decreased when the illumination degrades or there is no evidence that a frontal face is present).

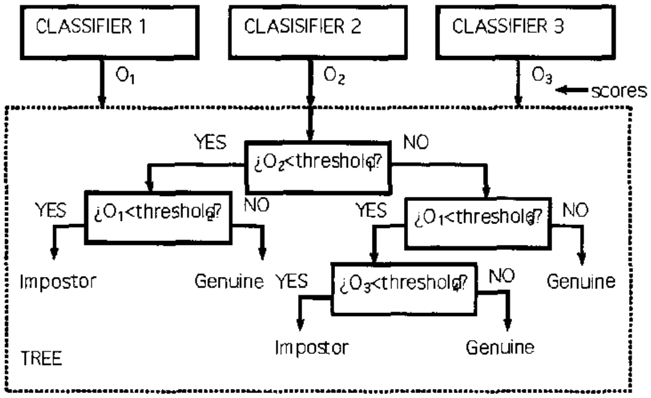

Fig. 7. Example of opinion fusion using classifier trees

The most popular combination schemes are: Weighted sum, Weighted product, and decision trees (based on if-then-else

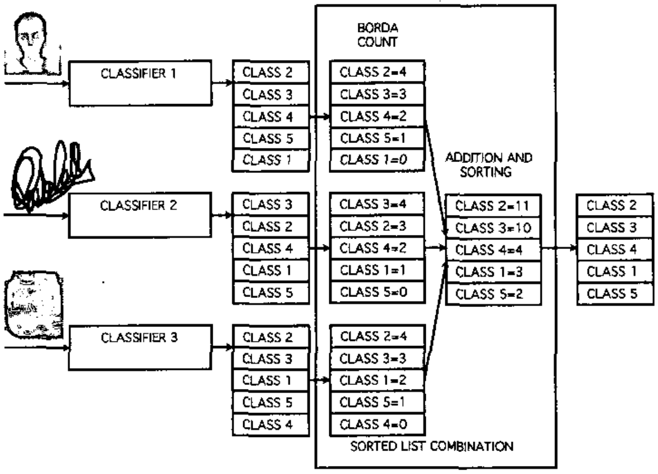

Fig. 8. Example of decision level fusion. It combines face, signature, and fingerprint by means of the Borda count

sentences). Figure 7 shows an example of data fusion using a decision tree.

- **4. Decision level:**
  At this level, each classifier provides a decision. On verification applications, it is an accepted / rejected decision. On identification systems, it is the identified person or a ranked list with the most probable person on its top. In this last case, the Borda count method [8] can be used for combining the classifiers' outputs. This approach overcomes the scores normalization that was mandatory for the opinion fusion level. Figure 8 shows an example of the Borda count. The Borda count assigns a score that is equal to the number of classes ranked below the given class.

One problem that appears with decision level fusion is the possibility of ties. For verification applications, at least three classifiers are needed (at least two will agree and there is no tie), but for identification scenarios, the number of classifiers should be higher than the number of classes. This is not a realistic situation, so this combination level is usually applied to verification scenarios.

An important combination scheme at the decision level is the serial and parallel combination, also known as "AND" and "OR" combinations. Figure 9 shows the block diagram. In the first case, a positive verification must be achieved in both systems, while access is achieved in the second one if the user is accepted by one of the systems.

The AND combination improves the False Acceptance Ratio (FAR) while the OR combination improves the False Rejection Ratio (FRR). Simultaneously combining serial and parallel systems, it is possible to improve both rates. For instance, [9] reports the combination of two different biometric systems offering three trials in each one (similar to the PIN keystroke on ATM cashiers). In this case, if each system on its own yields a 1% False Acceptance Ratio (FAR) and 1% False Rejection Ratio (FRR), the combined system yields FAR = 0.0882% and FRR = 0.0002%.

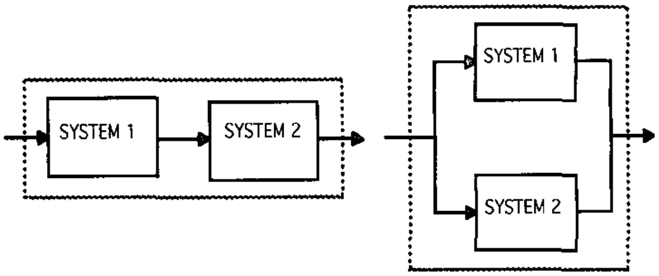

Fig. 9. Serial and parallel decision level combinations

REFERENCES

[1] S. Nanavati, M. Thieme and R. Nanavati, 2002,
Biometrics: Identity in a networked world,
Ed. John Wiley 2002.

[2] M. Faundez-Zanuy, 2004,
On the vulnerability of biometric security systems,
To appear in ***IEEE Aerospace and Electronic Systems Magazine***, 2004.

[3] A. Jain, R. Bolle and S. Pankanti, 1999,
Biometrics: personal identification in networked society,
Kluwer Academic Publishers, 1999.

[4] A. Hyvärinen, J. Karhunen and E. Oja, 2001,
Independent component analysis,
Ed. John Wiley & Sons, 2001.

[5] F.K. Soong and A.E. Rosenberg, June 1988,
On the use of instantaneous and transitional spectral information in speaker recognition,
IEEE Trans. On Acoustics, speech and signal processing,
Vol. 36, pp. 871-879, June 1988.

[6] C. Sanderson, September 2002,
Information fusion and person verification using speech & face information,
IDIAP Research Report 02-33, pp. 1-37, September 2002.

[7] J. Kittler, M. Hatef, R.P.W. Duin and J. Matas, March 1998,
On combining classifiers,
IEEE Trans. On pattern analysis and machine intelligence,
Vol. 20, No. 3, pp. 226-239, March 1998.

[8] T. K. Ho, J.J. Hull and S.N. Srihari, January 1994,
Decision combination in multiple classifier systems,
IEEE Trans. On Pattern analysis and machine intelligence,
Vol. 16, No. 1, pp.66-75, January 1994.

[9] M. Willems and P. Forret, December 1997,
Layered Biometric Verification, White paper,
Keyware Technologies, December 1997.