MULTIBIOMETRIC SYSTEMS

Ing. Martin DRAHANSKÝ, Doctoral Degree Programme (3)
Dept. of Intelligent Systems, FIT, BUT
E-mail: drahan@fit.vutbr.cz

Supervised by: Dr. František Zbořil

ABSTRACT

A biometric system which relies only on a single biometric attribute in making a personal identification is often not able to meet the desired performance requirements. Identification based on multiple biometrics represents a new solution. In this paper a multibiometric system is introduced. This system takes advantage of the capabilities of each individual biometric technology. It can be used to overcome some limitations or to extend the possibilities, which are laid on a single biometric system.

1 INTRODUCTION

In today's increasingly electronically wired information society, there are an increasing number of situations (e.g. accessing a multiuser computer account or entering a secured area) which require an individual (user) to be verified by an electronic device. Traditionally, a user can be verified, based on whether he possesses a certain *token* such as a smart card ("something you have") and/or whether he is in possession of a specific *knowledge* which only he himself is expected to know, such as a password ("something you know"). These approaches have a number of significant disadvantages. Tokens may be lost, stolen, forgotten, or misplaced. Passwords may be forgotten or compromised. All these approaches are unable to differentiate between an authorized user and an impostor who fraudulently acquires the "token" or "knowledge" of the authorized user [4]. Therefore, token- or knowledge-based authentication does not provide sufficient security in many critical applications, including access control and financial transactions.

Biometrics, which refer to the automatic identification of a person based on her physiological or behavioral characteristics (attributes), relies on "something what you are or you do" (e.g., putting the finger on a fingerprint scanner) to make a personal identification. It is inherently more reliable and has a higher discrimination capability than the token-based and/or knowledge-based approaches, because the physiological or behavioral characteristics are unique to each user. The user to be verified is required to be naturally physically present at the point-of-identification.

A *biometric system* is generally a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic indigenous from the user. In order to design a biometric system that is suitable for a

practical application, a number of issues need to be considered, including identification accuracy, population coverage, robustness, speed, size, cost, etc.

Nine different biometric characteristics (attributes) are either widely used or are under intensive evaluation, including *face*, *facial thermogram*, *fingerprint*, *hand geometry*, *hand veins*, *iris*, *retinal pattern*, *signature*, and *voice* [1;4] – see Fig. 1. All these biometric attributes have their own pros and cons in terms of the accuracy, user acceptance, and applicability.

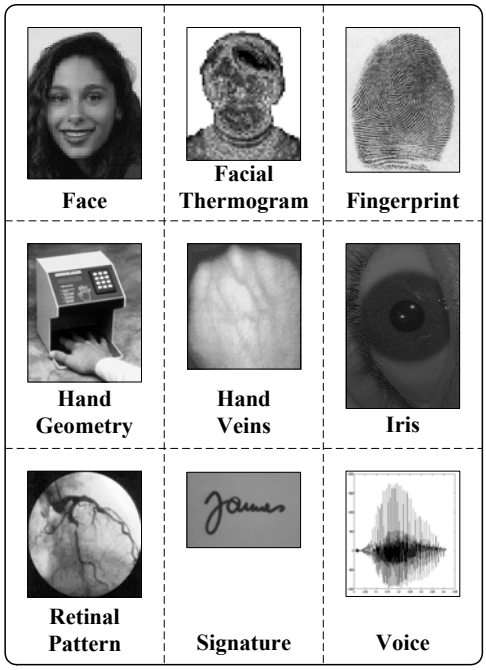

Fig. 1: *Nine types of biometric attributes*

2 MULTIBIOMETRICAL COMBINATION

A single biometric system that should operate effectively in different applications and environments is difficult to design. A multibiometric system which makes a personal identification based on multiple physiological or behavioral characteristics is mostly preferred (Fig. 2). Consider, for example, a network logon application where a biometric system is used for user authentication. If a user cannot provide good fingerprint images (e.g., due to dry finger, cuts, etc.) then other biometric characteristics may be better. Or, e.g., if the operating environment is "noisy" then voice is not a suitable biometric characteristic, etc.

Identification using multiple biometric attributes is essentially a sensor fusion problem, which utilizes information from multiple sensors (sources) to increase the fault-tolerance capability, to reduce uncertainty, to reduce noise, and to overcome the limitations of individual sensors [2;4]. A multibiometric approach can increase the reliability of the decisions made by a biometric system [3;4]. Multiple biometrics enable a user to be identified even if some of the biometric characteristics used by the system are not available and/or not suitable for automatic processing. By using multiple biometric characteristics, the system will be applicable to a larger target population. In addition, a multibiometric system is generally more robust to fraudulent technologies, because it is more difficult to forge multiple biometric attributes than to forge a single biometric attribute.

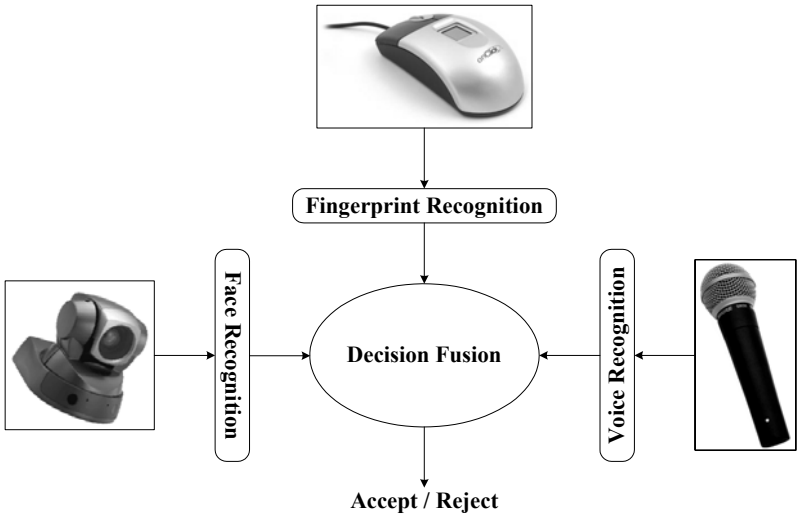

Fig. 2: *Integration of multiple biometric characteristics*

Let ***B*** denotes a given biometric system, and let $\Phi^1, \Phi^2, \ldots, \Phi^N$, denote the templates of the N users enrolled in ***B***, who are labeled by numerical indicators, *1*, *2*, ..., *N*. Assume, for simplicity, that each enrolled user has only one template (for each type of biometric characteristic) stored in the system. So the template for the i^{th} user, $\Phi^i = \{\Phi_1^i, \ldots, \Phi_M^i\}$, has M components, where $\Phi_1^i, \ldots, \Phi_M^i$ are the templates for different biometric attributes (e.g. fingerprint, face, etc.) and M is the number of used biometric attributes. Let (Φ^0, I) denotes the biometric characteristic and the identity ***I*** claimed by a user. Again Φ^0 has M components, $\Phi^0 = \{\Phi_1^0, \ldots, \Phi_M^0\}$, corresponding to the measurements of the individual biometric attributes. The claimed identity, ***I***, either belongs to category w_T or category w_F, where w_T indicates that the user claims a true identity (a genuine user) and w_F indicates that the user claims a false identity (an impostor). The biometric system ***B*** matches Φ^0 against Φ^I to determine which category, w_T or w_F, the claimed identity ***I*** falls in:

$$I \in \begin{cases} w_T, & \text{if } F(\Phi^0, \Phi^I) > \varepsilon \\ w_F, & \text{otherwise} \end{cases},$$

where $F(\Phi^0, \Phi^I)$ is a random variable representing the similarity between Φ^0 and Φ^I, and ε is a threshold. For a claimed identity ***I*** which can be in either w_T or w_F, the biometric system may determine whether ***I*** is in w_T or w_F.

2.1 DECISION FUSION

Let X_1, X_2, ..., X_M be the random variables used to indicate the similarity (differentiation) between an input and a template for M different biometric attributes. Let $p_j(X_j, w_i)$, where j =1, ..., M and i = T/F (True/False), be the class-conditional probability density functions of X_1, X_2, ..., X_M. Assume that X_1, X_2, ..., X_M are statistically independent. Then, the joint class-conditional probability density function of X_1, X_2, ..., X_M, has the following form:

$$p(X_1, \ldots, X_M \mid w_i) = \prod_{j=1}^{M} \left(X_j \mid w_i\right)$$

Depending on the practical requirement on verification accuracy, anyone of a number of

different statistical decision theory frameworks can be used. In biometrics, the performance requirement is usually specified in terms of the FAR (*False Acceptance Rate*) and FRR (*False Rejection Rate*) [1]. In this case, the decision fusion should establish a decision boundary which satisfies the FAR specification and minimizes the FRR. Let R^M denote the M-dimensional space spanned by $(X_1, X_2, \ldots, X_M)$; R_T^M and R_F^M denote the w_T-region and w_F-region, respectively ($R_T^M + R_F^M = R^M$); ε_0 denotes the pre-specified FAR. According to the Neyman-Pearson rule [4], a given observation, $X^0 = (X_1^0, \ldots, X_M^0)$, is classified as:

$$(X_1^0, \ldots, X_M^0) \in \begin{cases} w_T, & \dfrac{p(X_1^0, \ldots, X_M^0 \mid w_T)}{p(X_1^0, \ldots, X_M^0 \mid w_F)} > \lambda \\ w_F, & otherwise \end{cases}$$

where

$$\lambda = \frac{p(X_1, \ldots, X_M \mid w_T)}{p(X_1, \ldots, X_M \mid w_F)} \text{ and } \varepsilon_0 = \int_{R_T} p(X_1, \ldots, X_M \mid w_F) dX_1 \ldots dX_M$$

For a given biometric system, the class-conditional probability density functions are usually unknown. A critical issue in this decision fusion scheme is to estimate the class-conditional probability density function from a set of training samples. In biometrics, $p_j(X_j \mid w_T)$ is called the genuine probability density function and $p_j(X_j \mid w_F)$ is called the impostor probability density function [1;5;6]. Example of two genuine and impostor distributions from two different biometric attributes is shown in Fig. 3.

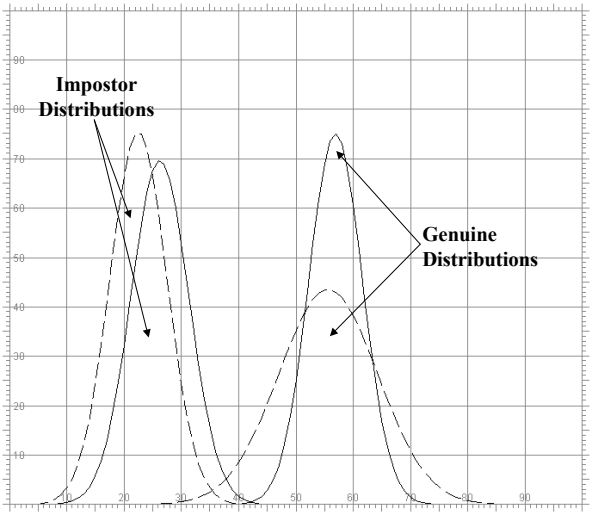

Fig. 3: *The impostor and genuine distributions for two different biometrics [4]*

2.2 IMPROVEMENT OF ACCURACY

A biometric system which relies only on a single biometric attribute in making a personal identification is often not able to meet the desired performance requirements. Identification based on multiple biometrics provides a solution. A decision made by multibiometrics is based on the integration of decisions made by individual biometric modules. If each module outputs a similarity, then a more accurate decision can be made at a rank level or at a measurement level by accumulating the confidence associated with each similarity value. All of the proposed algorithms for measurement level decision fusion algorithms [4;5] have been dem-

onstrated to be able to improve the accuracy over a single biometrics. For example, the EERs (*Equal Error Rate*) [1;4] of two biometric systems $\boldsymbol{B}_1$ and $\boldsymbol{B}_2$ with their genuine and impostor probability density functions shown in Figure 3 are 0.1% and 1.0%, respectively. By using the decision fusion algorithm with Neyman-Pearson rule, an ERR of 0.0058 % can be achieved! Note that the amount of improvement depends on the genuine and impostor distributions.

If the output of each module is only a category label, either w_T or w_F , which is not associated with any confidence value, then the integration of these multiple decisions can only be performed at an abstract level, at which a very limited number (at most $2 \cdot M$ where M is the number of biometric modules to be integrated) of decision rules can be used. Let P_{FR_i} and P_{FA_i} denote the FRR and FAR for $\boldsymbol{B}_i$, respectively, where $i = 1, \ldots, M$. There are only two acceptable decision rules that can be used to integrate two biometric modules:

- The AND rule – assign label w_T if both modules outputs w_T.
- The OR rule – assign label w_T if either module outputs label w_T.

An example: Let assume that $\boldsymbol{B}_1$ and $\boldsymbol{B}_2$ have an EER of 0.1 % and 1.0 %, respectively. If the AND rule is used, the rates are $\rightarrow$ FRR=1.099 % and FAR=0.001 %. If the OR rule is used, are FRR=0.001 % and FAR=1.099 %. Is 1.099 % FRR and 0.001 % FAR more accurate than 0.001 % FRR and 1.099 % FAR? The answer depends heavily on applications. If a 0.1 % FRR and 1.0 % FAR satisfies the accuracy requirement, then it is not necessary to combine $\boldsymbol{B}_1$ with $\boldsymbol{B}_2$. However, if the application requires rates around 1.099 % FRR and 0.001 % FAR or 0.001% FRR and 1.099 % FAR, then only the integrated system can satisfy the accuracy requirement (with the AND and OR rules).

3 CONCLUSION

A multimbiometric technique, which combines multiple biometric attributes (technologies) in making a personal identification, can be used to overcome the limitations. At each operating point, the accuracy of a biometric system is characterized by a pair of error rates, FAR and FRR. At a measurement level, integration of multiple biometric attributes can significantly improve the accuracy in a practical situation. At an abstract level, it depends on applications whether the improved accuracy is acceptable and required.

REFERENCES

[1] Drahanský, M.: Fingerabdruckerkennung mittels neuronaler Netze, Brno, Diploma Thesis, 2001

[2] Drahanský, M., Orság, F.: Biometric Security Systems: Fingerprint and Speech Technology, Tallahassee, USA, ISBN 0-9727412-0-8, p. 703 – 711

[3] N.N.: Can Multimodal Biometrics Improve Accuracy, 1999

[4] Jain, A., Hong, L., Kulkarni, Y.: A Multimodal Biometric System Using Fingerprint, Face and Speech, Michigan State University, 1998

[5] Marcialis, G.L., Roli, F., Loddo, P.: Fusion of Multiple Matchers for Fingerprint Verification, University of Cagliari, 2003

[6] Smith, R.E.: How Authentication Technologies Work, CISSP, Biometrics, 2003