MULTIMODAL BIOMETRIC SYSTEMS OVERVIEW

Eugen LUPU Petre G. POP
Technical University of Cluj-Napoca
phone: +40-264-401-266; fax: +40-264-556-244
Email: Eugen.Lupu@com.utcluj.ro

Abstract: Biometric systems allow automatic person recognition based on physical or behavioral features which belong to a certain person. Each biometric feature has its limits and no biometric system is perfect so unimodal biometric systems raise a variety of problems. To over fulfilling some of the mentioned inconvenient and limitations and to increase the level of security the multimodal biometric systems are used. This paper discusses the main features of the multimodal biometric system: architecture, level of fusion, methodology used for integrating the multiple verifiers and normalization techniques. The main applications of the multimodal biometric systems are also presented.

Key words: *biometric, authentication, multimodal, security, access control, fusion. normalization*

I. INTRODUCTION

In the age of universal electronic connectivity, "the electronic world" (e-world), with all its possibilities: e-mail, e-commerce, e-banking, virtual shops, e-government etc. has increased the number of activities which are related to the Internet.

The development and the spreading of the Internet have determined the apparition of some problems and obstacles such as: viruses, computer theft, hackers, unauthorized access etc. that affect the productivity and the prosperity of corporations and individual persons. Thus, security became more and more important and necessary. One solution for the systems' security is authentication, meaning the verification of the message and of the user. Anyhow, in the e-world, the necessity of personal identification is increasing, and the authentication of the user represents a challenge that must stop the advanced technologies of fraud met in nowadays complex society.

Identity, in the e-world context, represents the answer to the question "who am I?" Usually the identity confirmation is done through two factors namely: ***what I have*** (document, passport, key) and ***what I know*** (code, password, PIN). The raised problem of these two factors is that they may be lost, forgotten or counterfeit, and thus the safety of the frontiers, buildings and finances is discredited. Exceeding these drawbacks of identity confirmation, another factor is added: ***what I am (what I do)***, which in biometrics terms means digital representations of the face shape, fingerprints, hand geometry, iris, signature or voiceprint etc.

Due to the fact that biometric verifiers cannot be easily counterfeit, borrowed or unsuitably kept, they are seen as more secure for the person's verification than the traditional methods.

Usually a classification of the biometric features is made: physiological (fingerprint, face shape, iris, retina etc.) and behavioral (voice, gait, writing style etc.). In practice, all biometric verifiers may be considered combinations of physiological and behavioral characteristics due to the interaction mode between the user and the system, which puts its mark over the characteristic. Any physiological or behavioral feature may be used as a biometric verifier as long as it satisfies the following requirements [1]:

- **Universality** – every person must own this characteristic;
- **Distinctiveness** – two persons possessing the same characteristic do not exist
- **Permanence** – the characteristic must be invariant for a time period as long as possible;
- **Collectablility** – indicates the fact that biometric may be quantitatively measured;

For practical systems, there are some additional requirements that must be fulfilled such as [1]:

- **Performance** – which refers to the accuracy of the tangible recognition, speed, robustness, as well as the prerequisites for touching a certain level of performance;
- **Acceptability** – indicates the degree in which the given biometric characteristic is accepted by the users;
- **Resistance to circumvention** – indicates the facility through which a system can avoid fraud.

Biometric systems

Actually, biometric systems are recognition systems based on a model, which captures biometric features from a person and extracts a set of specific vectors that are compared with

Manuscript received September 1, 2008; revised October 5, 2008

a set of models from a database.

A common biometric system has four important elements fig.1. :

- Sensor module acquires the biometric data of an individual. An example is a fingerprint sensor that captures fingerprint impressions of a user.
- Feature extraction module in which the acquired data is processed to extract feature values. For example, the position and orientation of minutiae points in a fingerprint image would be extracted in the feature extraction module of a fingerprint system.
- Matching module in which the feature values are compared with those in the template by generating a matching score. For example, in this module, the number of matching minutiae points between the query and the template will be computed and treated as a matching score.
- Decision module in which the user's identity is established or a claimed identity is either accepted or rejected based on the matching score generated in the matching module.

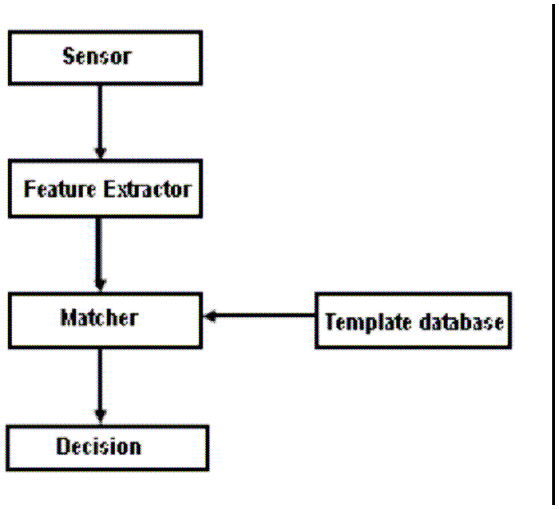

Figure 1. A biometric authentication system

Depending on the application context, a biometric system can operate in the *verification* mode or in the *identification* one.

First, biometric recognition implies the **enrolment of the user** in the system for creating the reference model in the database.

In verification mode, the assignation of the test model to the asserted person may be accepted or rejected; therefore only one comparison is made between the test model and the reference of the user that claims it. The verification problem may be presented consequently: being given a biometric vector X_Q and the asserted identity I, establish if (I, X_Q) belongs to the classes B1 or B2, where B1 indicates the fact that the demand is true, meaning that the vector X_Q is authentic of the user I, and B2 indicates a false demand, that is the vector X_Q belongs to an impostor. For taking the decision, the vector X_Q is compared with X_I, which represents the model of the user, I [1]. So:

$$(I, X_Q) \in \begin{cases} B_1 \text{ if } S(X_Q, XI) \geq p \\ B_2 \text{ otherwise,} \end{cases} \quad (1)$$

Where S is a measure of the similarity between the biometric vectors X_Q and X_I, and p is a predefined threshold. $S(X_Q, X_I)$ defines the similitude degree or the similarity score between the biometric vectors of the user and of the one who asserts the identity [3].

In identification mode, the system recognizes whom the tested biometric feature belongs to, meaning that it compares the test model with the reference models from the database (fig.1). From the formal point of view, the identification may be defined like this: being given a biometric vector X_Q, determine the user's identity I_k, $k \in \{1,2\ldots N+1\}$ (to) whom the vector belongs to. The identities I_1, $I_2 \ldots I_N$ belong to the user's enrolment in the system, and I_{N+1} indicates the situation of the rejection of the test vector.

$$X_Q \in \begin{cases} I_k \text{ if } \max\{S(X_Q, X_{I\,k})\} \geq p, \; k=1,2,..N \\ I_{N+1} \text{ otherwise,} \end{cases} \quad (2)$$

Where X_{Ik} is the biometric model corresponding to the identity I_k and p is a predefined threshold [3].

In some application, a **screening task** is required to verify if some persons (suspects) are registered in the biometric database.

The features and the taxonomy of the biometric systems

The global performance of a biometric system is appreciated taken into account different factors like: precision, speed and storage of the data, easiness of utilization and costs, factors that affect the system's efficiency. The architecture of the biometric recognition systems depends on the application.

Any user, before he/she can be tested by the system, must be enlisted, meaning that he/she must pass through a stage where the biometric characteristics of that system are captured.

The biometric recognition systems can operate in *positive* or *negative* mode.

An application of positive recognition establishes if the person that claims his/her identity is indeed that person. The purpose of positive recognition is to prevent the situation when more users use the same identity. In this case, false acceptance favors fraud. The *negative* recognition proves that the user is not who he/she claims to be. The goal of negative identification is to prevent the situation when a person has more than one identity. For instance, the user X received certain facilities (rights in a system), but now he/she pretends to be someone else, the user Y, in order to profit by his/her rights too (double permission). The system will establish that "the user Y" is not who he/she claims to be. The traditional methods of authentication using passwords, PIN, keys can function for positive recognition, but the negative recognition can be realized only through

biometric methods.

A biometric system may be classified taking into account a number of characteristics and their dependency of the application. All biometric applications can be classified in different categories based on their features, thus [1]:

- **Cooperating versus non-cooperating** – is adverted to the behavior of the impostor in interaction with the system. For instance, in a system with positive recognition, it is in the interest of the impostor to cooperate with the system in order to be accepted as a valid user. On the other hand, in a system with negative recognition, it's in the interest of the impostor not to collaborate with the system in order not to be recognized.
- **Habituated versus non-habituated** – indicates the frequency in which the registered users are the subjects of the biometric recognition;
- **Overt** – if the user is informed that he/she is the subject of recognition, the application is considered visible, and if the user doesn't know that he is being supervised, the application is covert. Most commercial applications of the biometry are overt, but the government, surveillance and forensic applications are usually covert;
- **Assisted versus unassisted** – indicates the way that the process of the biometric data acquisition takes place, that is establishing whether the application is guided or not by a human. Usually the non-cooperating applications require assisted utilization;
- **Public or private** – this dichotomy is adverted to the system's users who are the customers and the employees of a company, which the biometric system serves;
- **Standard versus non-standard** environment – is adverted to the medium conditions in which the system operates, a controlled or not environment (such as temperature, pressure, humidity, luminance etc.);
- **Open versus closed** – shows how (is use) the biometric prototype of a person for one or more applications is used. It must be specified that most popular commercial applications have the following attributes: cooperating, visible, closed and private, frequently used, controlled enrolment and unassisted, operating in a standard environment.

Different biometric verifiers are used in different applications. Each biometric characteristic has its strong points and weak points, and the typical choice depends on the application.

When a biometric factor is chosen for a certain application, the following questions must be taken into account:

- the application require verification or identification?
- which are the utilization modes of the application?

(the application is assisted or unassisted, the utilization is frequently used or not, the application is hidden or visible, the subjects are cooperating or non–cooperating etc.);

- Which are the storing requirements for the application?
- Which are the biometric characteristics, accepted by the users?

II. MULTIMODAL BIOMETRICS

Unimodal biometrics limitations

The unimodal biometric verification systems are more reliable than classical authentication systems. Unimodal biometric systems perform person recognition based on a single source of biometric information. Such systems are often affected by the following limitations and problems:

- The lack of universality of some characteristics (for instance, in the case of fingerprints, approximately 4% of people cannot enlist because of weak fingerprints, and this percent increases at 7% in the case of the iris);
- Noisy signals captured from the sensors due to the incorrect usage by the clients and due to the environmental conditions (humidity, dirt, dust etc.);

The lack of the safety of the used sensors;

- The limitation of the discrimination of biometric systems due to a high in-class and low inter-class variability;
- The recognition performances of the systems are upper limited at a certain level;
- Unacceptable error rates for the unimodal biometric systems;
- The lack of permanence and variability in time of the biometric characteristics;
- The fraud possibility through voluntarily or involuntarily cloning (of) a biometric characteristic.

Due to these practical problems, the error rates associated with unimodal biometric systems are quite high and they are made unacceptable for deployment in security critical applications. The state-of-the-art error rates associated with fingerprint, face, hand shape and voice biometric systems shown in the table below are dependent on a number of test conditions.

All the information previously mentioned may be synthesized in fact that ***each biometric feature has its limits and no biometric system is perfect.***

Multimodal systems

To over fulfill the mentioned problems and limitations the multimodal systems are used, leading to the improvement of the system's performances, and the increase of the number of enlisted population in the systems and discouragement of fraud.

Multimodal biometric systems that have been proposed in references may be classified using four parameters:

-architecture;
- sources that provide multiple evidence;
- level of fusion ;
- methodology used for integrating the multiple verifiers.

Biometrics	FAR	FRR	Test Parameters	Reference
Face	1 %	10 %	Varied lightning, indoor/outdoor	FRVT (2002)
Fingerprint	1 %	0.1 %	US Government operational data	FpVTE (2003)
	2 %	2 %	Rotation and exaggerated skin distortion	FVC (2004)
Hand shape	2 %	0.1 %	With rings and improper placement	(2005)
Iris	0.0001 %	0.2 %	Best conditions	NIST (2005)
	0.94%	0.95 %	Indoor environment	ITIRT (2005)
Voice	2 %	10 %	Text independent, multilingual	NIST (2004)

FAR= False Acceptance Rate; FRR= False Rejection Rate; Face Recognition Vendor Tests (FRVT); Fingerprint Verification Competition (FVC); National Institute of Standards and Technology (NIST)

Table 1. State-of-the-art error rates associated with fingerprint, face, hand shape, iris and voice biometric systems

The application scenario plays an important role in making the design decisions which influence the performance of the system.The sequence in which different biometrics are acquired and processed defines the architecture of a multimodal biometric system, which is, in general, either of parallel or cascade/serial nature. Functioning in parallel implies the processing types operating independently with their outcomes fusing according to a predefined scheme, while functioning in serial implies the sequential processing of functions with the result from one modality affecting the next.

There are advantages and disadvantages in both types of architecture: serial systems seem to be more user friendly as they are subject to less recognition time in comparison to parallel systems; still, they require complex algorithms in order to achieve the control of the sequence of operations. Therefore a cascaded multimodal biometrics system is recommended for applications that are less security critical (e.g. bank ATMs), while parallel architecture is recommended for applications requiring a high level of security (e.g. access to military installations or sites). The third possibility exists (hierarchical construction), that of combining parallel and serial architecture, by designing a system that preserves the advantages offered by the two.

In multimodal biometric systems different biometric ***sources of evidence*** are used to overcome the limitations of unimodal systems. Multimodal biometric systems may be:
- **Multi-sensor** system for the same biometric (e.g. optical, capacitive, based on chip fingerprint sensor etc.);
- Multi-method system – this uses multiple methods to compare the test arrays with the references (e.g. multiple fingerprint matchers based on minutiae or filtering, multiple face matchers like PCA and LDA);
- Multi-characteristic system – (e.g. it uses the fingerprints from several fingers, left and right iris images);
- Multi-capture/instance system – it acquires samples from the same biometric characteristic (e.g. the same fingerprint will be sampled for more than one time);
- Multi-verifier system – it uses more than one biometric verifier (fingerprint, face, hand, voice etc.).

In the table below the biometric features that are suited to be used in multiple biometric traits systems are presented.

Biometric features
Voice, Face, Lips movement
Fingerprint, Face
Fingerprint, Face, Voice
Fingerprint, Face, Hand geometry
Fingerprint, Voice, Hand geometry
Voice, Hand geometry
Facial theromogram, Face
Iris, Face
Palm print, Hand geometry
Ear form, Voice
Voice, Lips movement

Table 2. Biometric features suited to fusion

Theoretically, in the multimodal biometric systems it is possible that the **fusion** occurs at any level (sensors, feature extraction, parameters matching or decision module).G generally, the fusions at the first two levels are difficult to achieve (e.g., fusion at the feature level in practice is difficult to be employed because: the feature sets of the various modalities may be not compatible (eigen-coefficients of face and minutiae set of finger), and most commercial biometric systems do not provide access to the feature sets which they use in their products) and (at) the decision level is considered to be rigid due to the availability of limited information. Generally, the fusion at the matching score level is preferred, as it is relatively easy to access and combine the scores presented by the different modalities.

Fusion methods

Fusion in the context of biometrics can take the following forms:
-Single biometric multiple representation;
- Single biometric multiple matchers;
- Multiple biometric fusion.
Here are five fusion methods, among which the first three are considered classical and the last are subject to

innovation, their employing the importance of individual matchers in analyzing their contributions [8].

The notations used are: n_m^i for the normalized value for the matcher m (m=1,2,…M, M representing the number of distinct matchers) and the user I (i=1,2,…I, I representing the number of registered individuals). f_i is the fused score.

Simple sum (SS): Summing the scores for an individual:

$$f_i = \sum_{m=1}^{M} n_i^m, \quad (3)$$

Min Score (MIS): Extracts the minimum from the scores of an individual:

$$f_i = min(n_i^1, n_i^2, \ldots\ldots n_i^M), \quad (4)$$

Max Score (MAS)*:* Extracts the maximum from the scores of an individual:

$$f_i = max(n_i^1, n_i^2, \ldots\ldots n_i^M), \quad (5)$$

Matcher Weighting (MW). Fusion based on MW uses the Equal Error Rate (EER). If the EER of a matcher m is e^m, m=1,2,…M, then the weight w^m connected to the matcher m is calculated as it follows:

$$w^m = \frac{\frac{1}{e^m}}{\sum_{m=1}^{M} \frac{1}{e^m}} \quad (6)$$

It is important to consider that $0 \le w^m \le 1$, and $\sum_{m=1}^{M} w^m = 1$ and that the relationship between weights and their corresponding errors is of inverse proportionality, thus higher weights correspond to more accurate matchers (EER is used in order to spam the data available to the integrator above, despite the fact that the accuracy of a matcher may not be well estimated by the EER alone). The fused score (MW) is given by:

$$f_i = \sum_{m=1}^{M} w^m n_i^m, \quad (7)$$

User Weighting (UW): It applies weights to individual matchers, offering distinct solutions for distinct users; the fused score is to be calculated as it follows:

$$f_i = \sum_{m=1}^{M} w_i^m n_i^m, \quad (8)$$

w_i^m representing the weight of a matcher m for user i.

Normalization techniques

The matching scores output given by the different modalities are heterogeneous, therefore score normalization is needed so that the scores can be brought to a common domain before combining them. For instance, if one matcher is in the range [200, 2000] and another one in [0,1], the lack of normalization in the fusion of scores leads to the elimination of the contribution of the second matcher. Here are the most frequently used methods [7]. Let s be a raw matcher from the complete set of scores for that matcher, and n the corresponding normalized score.

Min-Max (MM): It maps the raw scores in the [0,1] range, max(S) and min(S) being the end points of the score range, generally provided by vendors:

$$n = \frac{s - min(S)}{max(S) - min(S)} \quad (9)$$

Z-score(ZS): By using this method, the scores are transformed to a distribution with mean of 0 and standard deviation of 1. *mean() and std()* represent the mean and standard deviation operators:

$$n = \frac{s - mean(S)}{std(S)} \quad (10)$$

Tanh (TH): The method consists of one of the robust statistical techniques [6], maps the scores to the [0,1] range:

$$n = \frac{1}{2}\left[tanh\left(0.01 \frac{s - mean(S)}{std(S)}\right) + 1 \right] \quad (11)$$

Adaptive (AD): The overlap of genuine and impostor distributions results into errors of individual biometric matchers, this region giving its center *c* and its width *w*. An adaptive normalization procedure that increases the level of separation of genuine and impostor distributions is used, while mapping scores to [0,1]. It is formulated as

$$n_{AD} = f(n_{MM}) \quad (12)$$

where *f()* represents the mapping function used on the MM normalized scores; these functions may be two-quadratics, logistic quadratic-line-quadratic [8].

Soft biometrics

Any trait that provides some information about the identity of a person, but does not provide sufficient evidence to exactly determine the identity can be referred to as ***soft biometric trait.*** A solution to reduce the error rates of the biometric system is based on incorporating soft verifiers of human identity like gender, skin color, hair color, ethnicity, height, weighty, eye color etc. into a (primary) biometric verification system. For this purpose, both primary (fingerprint, hand form, face form, iris, etc) and soft biometric information are employed to verify the account holder's identity. If information about the person's gender, height, ethnicity and eye color are available in addition to the posteriori matching probabilities given by the primary biometric information matcher, then a proper combination of these sources of information will lead to a correct and much faster identification of the test user.

Demographic attributes like gender, ethnicity, age, eye color, skin color, and other distinguishing physical marks such as scars can be extracted from the face images used in a face recognition system. Gender, accent, and perceptual age

of the speaker can be inferred in a voice recognition system. Eye color can be easily found from iris images [7].

III.MULTIMODAL BIOMETRICS APPLICATIONS

The application characteristics that drive the need for multimodal biometrics are: the risk and viability of spoofing, universal enrolment requirements, accuracy/ integrity requirements suitability in usage environment, transaction time flexibility.

The target applications of the multimodal biometrics may be classified in three categories depending on the potential of the solution provided by the systems:

- strong potential (for multimodal solutions): physical access, civil ID, criminal ID;
- moderate potential: network/PC access, Kiosk/ATM;
- modest potential: retail/POS, surveillance, eCommerce, telephony.

The FTE rate can be successfully reduced by using multimodality in the case of an identity documents application. The number of non-enroll able people is significantly reduced by the sequential use of multiple modalities which permits an equal treatment of individuals who do not have a certain biometric trait.)

There is a list of factors to be taken into account when designing a multimodal biometric system: (1) the nature and the number of traits (2) the level at which the information provided by the biometric traits is to be integrated (3) the method chosen to integrate the information (4) the relationship between costs and performance.

The performance that can be gained by using state-of-the-art commercial off-the-shelf (COTS) for biometric systems is currently under study on a large number of individuals.

IV. CONCLUSION

Biometric authentication will never be totally secure, but it is still one of the most reliable current security methods. The accuracy of biometric systems is affected by factors such as non-universality, noisy input, lack of invariant representation and non-distinctiveness. Integrating multiple cues may lead to overcoming some of these disadvantages. Better methods to combine information from multiple sources have been the subject of extensive research. The early levels of processing (sensor and feature levels) make information fusion difficult, while the decision level lacks sufficient information content. Consequently, the matching score level is preferred by researchers, this being the compromise between ease in fusion and information content. Biometrics systems are not yet used at a wide scale due to the unsatisfactory performance in comparison to the requirements, therefore improving the system performance is the most important research challenge.

REFERENCES

[1]D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar *Handbook of Fingerprint Recognition*, Springer Verlag, NY, 2003

[2] A.K. Jain, A. Ross, S. Prabhkar, "An introduction to biometric recognition*" IEEE Transactions on Circuits and Systems for Video Technology, Special issue on Image and video-based biometrics,* ***vol.14****, No.1. Jan. 2004*

[3] Arun Ross and Anil K. Jain, *"Multimodal Biometrics: an overview"*, Appeared in Proc. of 12th European Signal Processing Conference (EUSIPCO), (Vienna, Austria), pp. 1221-1224, September 2004.

[4] K.Delac, M. Grgic "A survey of biometric recognition methods" *46th International Symposium Electronics in Marine, ELMAR-2004*, 16-18 June 2004, Zadar, Croatia

[5]A. Ross, A.K. Jain, "Information Fusion in Biometrics", *Pattern Recognition Letters, September 2003*

[6]A.K. Jain "Multimodal biometrics Systems" 2004, *http://biometrics.cse.msu.edu*

[7] A.K. Jain, S. C. Dass and K. Nandakumar, " Soft Biometric Traits for Personal Recognition Systems", *in Proceedings of International Conference on Biometric Authentication (ICBA), LNCS 3072*, pp. 731-738, Hong Kong, July 2004.

[8] Jain A., Mink A., Uludag U., Indovina M., "*Multimodal Biometric Authentication Methods: A COTS Approach*", Proceedings of Workshop on Multimodal User Authentication, December, 2003

[9] A. K. Jain, S. C. Dass and K. Nandakumar, " Can soft biometric traits assist user recognition?", *in Proceedings of SPIE Vol. 5404, Biometric Technology for Human Identification*, pp. 561-572, Orlando, FL, April 2004.

[10] A. Ross, A. K. Jain, and J. Qian, "Information fusion in biometrics," in *Proceedings AVBPA'01*, Halmstad, Sweden, Jun 2001, pp. 354–359.

[11] Michael Thieme, Director of Special Projects International Biometric Group *"Multimodal Biometric Systems: Applications and Usage Scenarios"*, IEEE Workshop on Multimodal Sentient Computing: Sensors, Algorithms, and Systems, Minneapolis, Minnesota, USA Friday, June 22, 2007

[12] Anil K. Jain and Arun Ross, *"Learning User-Specific Parameters in a Multibiometric System"*Proc.International Conference on Image Processing (ICIP), Rochester, New York, September 22-25, 2002.

[13] A. Jain, K. Nandakumar, A. Ross, *"Score Normalization in Multimodal Biometric Systems",* Pattern Recognition, 2005.

[14] Robert Snelick, Umut Uludag, Alan Mink, Michael Indovina and Anil Jain, "*Large Scale Evaluation of Multimodal Biometric Authentication Using Stat of-the-Art Systems",* IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 27, No. 3, Mar 2005, pp 450-455

[15] A. K. Jain, K. Nandakumar, X. Lu, and U. Park, " Integrating Faces, Fingerprints, and Soft Biometric Traits for User Recognition", *in Proceedings of Biometric Authentication Workshop, in conjunction with ECCV2004, LNCS 3087*, pp. 259-269, Prague, May 2004.

[16] European Biometrics Portal*, "Biometrics in Europe",* Trend Report, Brussels, June 2006