BIOMETRIC ACREDITATION ENTITIES
An Approach for Web Acreditation Services

B. Ruiz, L. Puente, D. Carrero
Universidad Carlos III de Madrid, Avda de la Universidad, 30, Leganés, Madrid, Spain

M. J. Poza
Universidad Francisco de Vitoria. Ctra. Pozuelo-Majadahonda Km. 1.800. Pozuelo de Alarcón, Madrid, Spain

Keywords: Biometrics, Authentication Devices, Emerging Technologies, Data Integration, Semantic Web Services, Ontologies.

Abstract: Identity verification is nowadays a crucial task for security applications. In the near future organizations dedicated to store individual biometric information will emerge in order to determine individual identity. Biometric authentication is currently information intensive. The volume and diversity of new data sources challenge current database technologies. Biometric identity heterogeneity arises when different data sources interoperate. New promising application fields such as the Semantic Web and Semantic Web Services can leverage the potential of biometric identity, even though heterogeneity continues rising. Semantic Web Services provide a platform to integrate the lattice of biometric identity data widely distributed both across the Internet and within individual organizations. In this paper, we present a framework for solving biometric identity heterogeneity based on Semantic Web Services. We use a multimodal fusion recognition scenario as a test-bed for evaluation.

1 INTRODUCTION

Nowadays, the most popular method to gain access to restricted physical areas is to show to the security agent the card that identifies the owner as a privileged person with enough rights go into the area. Personal cards usually have the owner's photography which is a biometrical sample of his face. On the other side to gain access to restricted virtual areas, the common use is to apply techniques such as PINs, passwords, digital signatures, etc.
Losing the personal card, forgetting the password or PIN or whatever data bearing in mind that performs personal identification is not only an inconvenient but also an outrage against the restricted area security.

Why not to putting these two methods together in order to get the advantages provided by each one?

Biometrics promises to offer a new alternative, portable, easy to use, free of memory, loss or theft problems (Puente et al, 2008). This technology allows the use of personal traits for individual identification, as human security agents do, but it also allows full automatic computer process.

In biometrics, knowledge area authentication usually means confirming that someone is who he/she says to be, basing it on his or her distinguishing traits. It is assumed that these traits are extracted from personal features. These features should have certain characteristics that permit computer processing, such as being measurable, repeatable by the owner, unrepeatable by others.

Since biometric identity technologies try to solve security problems dealing with private data, the challenge for the research community is to attain integrated solutions that address the entire problems from sensors and data acquisition to biometric data analysis preserving personal information.

Currently, in order to increase the accuracy of the biometric authentication result process, a technique called "Multimodal Fusion" is being used. It refers to simultaneous processes of various samples of different kind of traits (Kittler et al, 1998) (Jain et al, 2001). As a result of this, biometric information has grown exponentially and algorithms

Ruiz B., Puente L., Carrero D. and J. Poza M. (2008).
BIOMETRIC ACREDITATION ENTITIES - An Approach for Web Acreditation Services.
In *Proceedings of the International Conference on Signal Processing and Multimedia Applications*, pages 216-220
DOI: 10.5220/0001939902160220

for feature extraction, matching score or decision levels handle a tremendous amount of data. Furthermore, the recent years have provided an amount of duplicated efforts in building test databases such as face recognition databases (e.g. FERET, PIE or BANCA) (Bailly-Baillière et al, 2003) as well as a lack of uniform standards and granted open access to these databases, as discussed in (Ming et al, 2007).

Hence, the most critical need in biometric identity recognition is arguably to overcome semantic heterogeneity i.e. to identify elements in the different databases that represent the same or related biometric identities and to solve the differences in database structures or schemas, among the related elements. Such data integration is technically difficult for several reasons. First, the technologies which different databases are based on may differ and may not interoperate smoothly. Standards for cross-database communication allow the databases (and their users) to exchange information. Secondly, the precise naming conventions for many scientific concepts in fast developing fields such as biometrics are often inconsistent, and so mappings are required between different vocabularies.

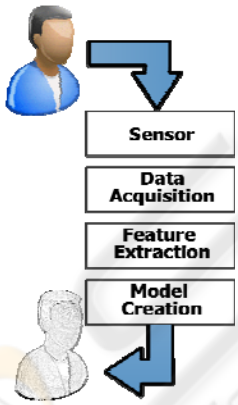

Figure 1: Model generation.

Therefore, in this paper we talk about the feasibility of taking advantages from a biometrics' technology framework preserving individual rights.

The remainder of this paper is organized as follows. Section 2 compiles a brief list of terms used along this paper. Section 3 introduces the current environment for the biometric works. Section 4 proposes a new environment for authentication purposes. Section 5 describes an experimentation environment. Section 6 compiles authors' conclusions.

2 USED TERMS

Before continuing talking about biometrics it is necessary to fix some terms that we are going to use along this paper.

A trait is defined as any physical, motor or psychomotor human characteristic capable of being used in biometric identification.

A user is any person to be recognized by the system, and whose traits are somehow stored in the database.

A donor is any person (user or not) whose trait is captured, voluntary or involuntary, by a sensor of the system.

A sample is defined in (Mansfield et al, 2002) as a biometric measure presented by the donor which eventually results in an image or signal.

Feature refers to a mathematical/measurable characteristic of the acquired sample. Sometimes it is the sample itself, other times it is the result of a more or less complicated mathematical process, in that case the process often captures a set of different features called feature vector. This process is known as "feature extraction".

3 CURRENT ENVIRONMENT

A typical biometric system presents a well defined structure (Mansfield et al, 2002) that includes two phases: enrolment and testing.

Enrolment faces the creation of a type of model representing the user in a univocal way. It starts storing a sample of one of the biometrical traits (data acquisition) from the sensor output data, the following process (feature extraction) tries to extract from this sample information that univocally characterizes the individual, avoiding to include the variable components of the trait and obtaining a set of feature vectors. At the end a (mathematical or not) model is obtained. Sometimes this transformation is trivial and the result model is the sample itself. Other times it is no so simple and at the end we obtain a mathematical expression with the set of its coefficients (see Figure 1).

On the other hand testing starts with the same steps of data acquisition and feature extraction obtaining a set of feature vectors (see Figure 2). But at the end it matches the vector feature set with the stored model of the individual. Model matching establishes a metric system in which a distance between the model and the sample is defined, the longer this distance the more probable is that the donor is not the model's user. The distance is

compared with a threshold (that leads to the decision) deciding if the donor is the user (acceptance) or not (rejection).

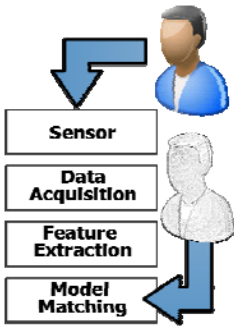

Figure 2: The testing process.

For the two phases (enrolment and testing) acquisition implies that one or more sensors acquire one or more samples of certain donor's biometric traits presented to the biometric systems (e.g. fingerprint, face, iris image) (Puente et al, 2008).

Two different tasks should be executed inside this environment. In the first one, called authentication, a donor declares to be a certain user (claimed user) and the system determines if it is true or not by checking if the donor's biometrical sample matches or not the user model.

In the second one, called identification, the donor does not inform about his/her identity, usually because he/she is an involuntary donor. Then it is necessary to look for the best accuracy models from all of the stored ones in the database and it will determine the probability of being any of the model users.

Nowadays user models are stored in a very local database. Multimodal fusion increases the complexity forcing to store no less than a model for each modality and for each user to be authorized. Furthermore the user has to place in every biometric database of the restricted areas he/she needs to access, no less than a biometric sample for each modality. It is not only an inconvenient but a problem of information protection, because this redundancy increases the probability that the biometric data stays in unauthorized hands, and makes practically impossible to remove this information from all databases.

Experimentation framework shows this problem in a more critical way. Currently, some entities have compiled databases of biometric samples. These samples were obtained from anonymous donors, who often give their authorization only for biometric experimentation. This database has been shared by researches and the usual support is a CD-ROM. In this environment it is impossible to control the use made with this information, or to remove certain samples from it.

4 EXPERIMENTAL RESULTS

Nowadays, several classification system (Dessimoz et al, 2006) and fusion techniques (Jain et al, 2005) exist in order to verify persons' identity.

The results obtained in identity verification using fusion of biometric data at score level from iris, signature and voice are shown in TABLE . The error rate of unimodal biometrics systems are 12.4%, 5.73% and 25% respectively.

Table 1: Rank of Methods Error Rate.

Fusion Method	Error Rate
3-3-1 N. Network with simple normalized data	1.58%
3-3-1 N.Network with normalization and sigmoid transformation	1.65%
Weighted Product with simple normalized data and Dynamic Score Selection	1.66%
Weighted Product with simple normalized data	1.67%
SVM with normalization and sigmoid transformation	1.68%

These results show the capability of recent fusion techniques to reduce the error rate in identity verification tasks. In this way, multimodal biometrics becomes one of the main tools in BAE.

5 PROPOSED ENVIRONMENT FOR AUTHENTICATION SERVICES

We propose not to share de data but the services.

A global solution will be based on the creation of specialized organizations offering authentication services. Of course, this Biometric Accreditation Entities (BAE) will obviously base their services on previously acquired biometric data. Then BAE could be created as specialized organizations dedicated to collect and store individual biometrical information and to offer identity accreditation services.

Throughout the Web BAEs will supply identity accreditation of their registered users just for user authorized organization.

The major limitation for BAE being useful is that all over the world we can find very different

techniques to capture biometric traits and therefore getting heterogeneous data formats.

The first option in order to face this problem is to create standards that normalize biometric data to be exchanged with BAE. In opposition to that, our proposal includes, as well as the BAE concept, the use of "Semantic Web Services" (SWS).

In this environment, BAE will provide a platform that allows data matching of acquired biometric samples, encapsulated in a semantic description bubble, against individual biometric models stored inside the BAE.

In addition to the above service, BAEs will also provide catalogues of the stored data. Not only does it allow determining where the models for a given user are located but also where the most accurate one for data acquisition process is.

Continuing in the development of this concept our future work will focus the creation of the semantic context by the definition of the ontology oriented to the purpose of making it possible.

The main application scenarios for authentication services are listed below. By one hand, military and defense scenarios can be described:

• Security in airports: BAE verification is a complementary way to improve traditional verification systems like passport, ID card and driving license.

• Frontiers control: BAE can offer support to the surveillance carried out by the security agents in order to identify and classify travelers in the entrance points to the countries.

• Access control to restricted areas: BAE offers second user verification behind the control made by security staff.

By the other hand, civil applications can be described too.

• Credit card payment: In order to complete an electronic transaction, BAE user verification is needed next to the user's financial data and signature.

• Documents accreditation: BAE may validate authorship of electronic documents by including a verification certificate about the author's identity. This system is similar to digital signature procedures.

• Control over employees: BAE may assist into the recognition tasks over employees. In the same way, BAE may improve the time control tasks over employees. Biometrics rules out in an effective manner some situations in which a person uses an identification card to prove other person's presence.

• Nurseries: BAE may verify parents' identity at the moment they pick their children.

In order to check the validity of donor's biometric data, biometric data acquisition have to be supervised by humans.

6 PROPOSED ENVIRONMENT FOR EXPERIMENTATION

Previously, we have mentioned that researchers on biometrics suffer the same problem related to the need of having access to biometrical databases.

In this context our proposal aim is similar to the one above for BAE: "not to share the data but the services".

In this case we promote the creation of a platform called "Biometrical Extended Experiment Platform" (BEEP), which is a virtual space where researchers can test their algorithm against a large multimodal database.

BEEP offers not only the database but the possibility of a true comparison with the published results of other colleges obtained in a similar, controlled and normalized environment.

It is BEEP's responsibility to ensure that only global results are at the end of a BEEP process, and that no individual information can be obtained.

As a continuation of this, our future work will define the algebraic context of BEEP in order to make it available for researchers, and to create its inside database.

7 CONCLUSIONS AND RELATED WORK

The creation of Biometric Accreditation Entities will be an alternative in the near future to the current digital certification organisms.

In this environment the heterogeneity of sample capture and data process should not become a barrier for the use of this identification technology.

In order to do that, Ontology and Semantic Web Services show their capabilities to offer a solution to the growing problem of the heterogeneous data.

On the other hand biometrical researching could be normalized by BEEP, offering a platform for making results' comparison.

Finally, our future work will focus on creating a completely adapted ontology and defining a standard for required services on SWS as well as determining an algebraic context for the biometrical experimentation process.

ACKNOWLEDGEMENTS

This work is founded by the Ministry of Science and Technology of Spain under the PIBES project of the Spanish Committee of Education & Science (TEC2006-12365-C02-01).

REFERENCES

Bailly-Baillière, E., Bengio, S. et al. 2003. The BANCA Database and Evaluation Protocol, in Springer LNCS-2688, 4th Int. Conf. Audio- and Video-Based Biometric Person Authentication, AVBPA'03. 2003, Springer-Verlag.

Berners-Lee, T., Hendler, J. and Lassila, O. 2001. The Semantic Web. Scientific American, May 2001, pp. 34-43.

Borst, W.N. 1997. Construction of Engineering Ontologies for Knowledge Sharing and Reuse. PhD Thesis. University of Twente. Enschede, The Netherlands.

Dessimoz, D., Champod, C., Richiardi, J. and Drygajlo, A. 2006. MBIOD. Multimodal Biometrics for Identity Documentation. State-of-the-art. Research Report. University of Lausanne. Available at: http://www.europeanbiometrics.info/images/resources/90_264_file.pdf.

Fensel, D. and Bussler, C. 2002. The Web Service Modeling Framework WSMF. Electronic Commerce Research and Applications, 1(2).

Gandon, F. and Sadeh, N. 2004. Semantic Web Technologies to Reconcile Privacy and Context Awareness. Web Semantics Journal, 1(3), 2004.

Gibbins, N., Harris, S. and Shadbolt, N. 2003. Agent-based Semantic Web Services. In Proc. of the 12th Int. World Wide Web Conference, May 2003.

Gómez, J. M., Rico-Almodóvar, M., García-Sánchez, F., Martínez-Bejar, R. and Bussler, C., 2004. GODO: Goal-driven Orchestration for Semantic Web Services. WSMO Implementation Workshop, September 2004.

Gruber, T. R. 1993. A translation approach to portable ontology specifications. Knowledge Acquisition vol. 5:199-220.

Hendler, J. 2001. Agents and the Semantic Web. IEEE Intelligent Systems, 16(2): 30-37, March/April 2001.

Jain, A., Nandakumar, K. and Ross, A. 2005. Score Normalization in Multibiometrics Systems. Pattern Recognition, vol. 38, pp. 2270-2285, Jan. 2005.

Jain, K., Bolle, R. et al.1999. Personal Identification in Networked Society. Kulwer Academic. 1999.

Jain, R. and Quian, J. 2001. Information Fusion in Biometrics. Proc. 3rd International Conference on Audio and Video Based Person Authentication (AVBPA) pp. 354-391, Sweden, 2001.

Kittler, J. Hatef, R. and Matas, J. G. 1998. On Combining Classifiers. IEEE Transactions on PAMI, vol. 12 (1998). Pp. 226-339.

Mansfield, J. and Wayman, J.L. 2002. Best Practices in Testing and Reporting Performance of Biometric Devices. National Physics Lab for Mathematics and Scientific Computing. 2002.

Ming, A. and Ma, H. 2007. An Algorithm Tested for the Biometrics Grid. Proceedings of the Second International Conference in Grid and Pervasive Computing (GPC07). Paris, France. 2007.

Puente, L., Poza, M.J., Ruiz, B. and Gómez, J.M. 2008. Biometric Authentication Devices and Semantic Web Services. An Approach for Multi Modal Fusion Framework , BIODEVICES 2008.

Web Ontology Working Group, 2004. OWL Web Ontology Language Guide.

OWL-S W3C Submission, 2004. OWL Web Ontology Language for Services. Available at: http://www.w3.org/Submission/2004/07/

SWSF W3C Submission, 2005. Semantic Web Service Framework. Available at: http://www.w3.org/Submission/2005/07/

WSMO W3C Submission, 2005. Web Service Modeling Ontology. Available at: http://www.w3.org/Submission/2005/06/

WSDL-S W3C Submission, 2005. Web Service Semantics. Available at: http://www.w3.org/Submission/2005/10/