Multimodal Biometric Databases: An Overview

Marcos Faundez-Zanuy
Escola Universitaria Politècnica de Mataró
&
Julian Fierrez-Aguilar, Javier Ortega-Garcia, Joaquin Gonzalez-Rodriguez
ATVS - Universidad Autónoma de Madrid

This overview is a summary and evaluation of all of the presentations on this subject at the IEEE 39th Annual International Carnahan Conference on Security Technology held in Las Palmas de Gran Canary, Spain, in October 2005, and serves as the report of major developments presented. AESS sponsors this conference which will next be held October 16-19, 2006, in Lexington, Kentucky, where the Carnahan Conference originated.

ABSTRACT

The interest on biometric recognition systems for person authentication has experienced an important growth in the last decade. One of the key factors of this success is the availability of biometric databases; these are of utmost importance to define common benchmarks that enable consistent comparison of competing recognition strategies. The design, acquisition, and collection of these databases are one of the most time- and resource-consuming tasks for the research community, especially in the case of multimodal databases including multiple biometric traits and acquisition sessions. In this paper, the most important multimodal biometric databases publicly available are summarized, and the contents of some new multimodal databases under development are outlined.

INTRODUCTION

Biometrics refers to automatic person recognition (either verification or identification) by means of physiological or behavioral traits, and plays an important role in security applications [1]. In the last years, an increasing number of efforts have been made in order to develop new algorithms, systems, and applications based on biometric authentication.

As a result, there is also an increasing need for technology assessment, evaluation, and benchmarking, which depend on the availability of biometric data. Biometric databases allow us to define evaluation protocols and strategies, so that the research community can follow common evaluation procedures. In this way, we can obtain comparative performance measures, often expressed in terms of False Acceptance and False Rejection rates (FAR and FRR) on DET and ROC plots [2-3]. The biometric databases used in performance evaluations enable consistent comparison between different algorithms thus validating the new approaches with respect to the state-of-the-art [4].

The more common type of performance evaluation is known as technology evaluation [5]. The goal of a technology evaluation is to compare competing recognition algorithms, regardless of the particularities of a specific scenario, or the operational conditions of the evaluation. The competing algorithms are tested on standardized data, which are collected through one or several biometric sensors. The performance on this database will depend upon both the acquisition environment and the population acquired. The evaluation can be carried out using offline processing of the data and, as far as the database is fixed, the results of technology tests are repeatable.

Evaluation protocols typically divide the subjects in the biometric database into development and evaluation sets. The

Author's Current Address:
M. Faundez-Zanuy, Escola Universitaria Politècnica de Mataró, Barcelona, Spain; J. Fierrez-Aguilar, J. Ortega-Garcia and J. Gonzalez-Rodriguez, ATVS - Universidad Autónoma de Madrid, Madrid, Spain.

Based on presentations at the 2005 Carnahan Conference on Security Technology.
0885/8985/06/ $17.00 © 2006 IEEE

development set is used for tuning the parameters of the recognition engines and the evaluation set is used to obtain the performance measures once the parameters are fixed. Within each set and for each particular subject in the database, training and testing subsets are also defined by separating the available biometric samples per subject. A variety of methods exist in order to split the available data into training and testing sets [6]. Biometric evaluation protocols include, for example, the Lausanne and BANCA protocols [7-8].

The collection of biometric databases is a continuous effort due to two major reasons. First, a specific biometric database can be used too extensively, so that the optimization efforts usually lead to an "overtraining" effect [6]. This effect can be identified when a given algorithm results in exceptionally good performance on just that particular dataset. At this point, the utility of that specific biometric database decreases, and new databases need to be collected. Second, the major reason of collecting new databases involves the incorporation of new biometric traits, sensors, or annotated acquisition conditions (such as noise level, image quality, and user interaction).

Unfortunately, the collection of biometric databases is confronted with several challenges. Technically, the collection and distribution of the databases is a time- and resource-consuming task, requiring experience and care both in the content design and the acquisition protocol. After the data collection, additional efforts are typically dedicated to supervision, annotation, error correction, labeling, and documentation. On the other hand, a set of legal requirements including consent forms to be signed by the donators and operational security measures as instructed by the data protection authorities have to be addressed. Finally, the distribution of the database involves intellectual property rights and maintenance issues.

In this paper, we provide an overview of the main existing and on-going multimodal biometric databases. We skip a detailed explanation of performance evaluation of biometric systems, the non-technical issues related to database collection, and the basics of the different biometric traits. For details on these topics we refer to the related literature [5].

BIOMETRIC DATABASES

The biometric databases containing only one single biometric trait or modality are called unimodal, while those including at least two traits from the same people are known as multimodal. It is widely assumed that multimodality provides lower vulnerability against hacker attacks [9]. Additionally, multimodal biometric systems can overcome the basic concern of failure-to-enroll (FTE) rate, i.e., the proportion of individuals in a general population for whom the system is unable to generate usable templates. FTE includes those subjects unable to produce the required biometric sample, those who generate a low-quality sample at enrolment, as well as those unable to reproduce their biometric feature in a consistent way. A multimodal biometric system typically weights with more importance the contribution of the more reliable trait [10-11]. Recent trends in multimodal biometrics include the use of user-dependent [12] and quality-based [13] weights.

The availability of multimodal biometric features corresponding to a large population of individuals, together with the desirable presence of biometric variability of each trait (multi-session, acquisition channel, and sensor, quality) makes multimodal database collection a complicated time-consuming process, in which a high degree of cooperation of the donators is needed. Furthermore, the legal issues regarding privacy and data protection in the case of collecting and storing multimodal signals are especially controversial [5]. For these reasons, nowadays, the number of existing public multimodal biometric databases is relatively small.

Due to the difficulties in multimodal database collection, some authors have assumed independence between different biometric traits and have performed their experiments on multimodal databases combining biometric signals from different unimodal databases, thus creating chimeric or virtual subjects [14]. The recent trend, as recommended by best practices, is to conduct the performance evaluations on real multimodal biometric data. The focus of this paper is, consequently, on this last type of multimodal databases.

Currently available multimodal databases have resulted from collaborative efforts in recent research projects. Examples of these joint efforts include European projects like M2VTS [7] or BANCA [8], and National projects like the French BIOMET [15] or the Spanish MCYT [4]. Other on-going efforts in multimodal database collection include the BIOSEC multimodal database [16], and the database activities of the BIOSECURE Network of Excellence [17].

Multimodal Biometric Databases can be broadly classified into two groups: 1) databases consisting of multimodal biometric samples; and 2) databases consisting of multimodal scores. In the first class, the collected data are biometric signals, such as fingerprint images or voice utterances. These signals may be used with a variety of different experimental protocols and algorithms, both for individual system development and for multimodal experiments at any fusion level (i.e., sensor, feature, score, or decision levels) [10]. The second class of multimodal databases consist of matching scores from the individual traits considered, and are intended exclusively for multimodal research based on score or decision fusion [10].

MULTIMODAL DATABASES CONSISTING OF BIOMETRIC SAMPLES

This section summarizes the most widely used existing multimodal databases of biometric signals. Table 1 summarizes the main characteristics.

BT-DAVID

The BT-DAVID database contains full-motion video, showing a full-face and a profile view of talking subjects, together with the associated synchronous audio [18]. BT-DAVID includes audio-visual material from more than 100 subjects including 30 clients recorded on 5 sessions spaced

Table 1. Summary of currently available multimodal databases
N/A= Not Available

Fingerprint	# users				327	96	330
	# sessions				3	172	1
	# repetitions/ session				N/A	N/A	12
	% male/female				50%	N/A	N/A
	# samples				N/A	N/A	79,200
	sensor				optical, capacitive	N/A	optical, capacitive
Face	# users	124	295	208	236		
	# sessions	5	4	12	2 (videocamera) 3 (infrared) 1 (3D)		
	# repetitions/ session	N/A	2	1	1 (videocamera) 1 (infrared) 5 (3D)		
	% male/female	50%	N/A	50%	50%		
	# samples	N/A	7,080	N/A	N/A		
	sensor	videocamera	videocamera	videocamera	videocamera, infrared & 3D		
Voice	# users	124	295	208	236	96	
	# sessions	5	4	12	2	172	
	# repetitions/ session	N/A	2	1	1	N/A	
	% male/female	50%	N/A	50%	50%	N/A	
	# samples	N/A	7,080	N/A	N/A	N/A	
	sensor	videocamera	videocamera	micro	videocamera	N/A	
Signature	# users				327	96	330
	# sessions				3	172	1
	# repetitions/ session				5 client + 5 impostor	N/A	25 client + 25 skilled forgeries
	% male/female				50%	N/A	N/A
	# samples				N/A	N/A	16,500
	sensor				digitizing tablet	N/A	digitizing tablet
Hand	# users				327	96	
	# sessions				3	172	
	# repetitions/ session				1, 1, and 3	N/A	
	% male/female				50%	N/A	
	# samples				509	N/A	
	sensor				document scanner	N/A	

over several months. The utterances include the English digit set, English alphabet E-set, vowel-consonant-vowel syllables, and phrases for the control of a video-conferencing session. The scenes include variable scene background complexity and illumination. Portions of the database include lip highlighting. Figure 1 shows some snapshots of this database.

XM2VTS

The XM2VTS database [7] (extended M2VTS) was acquired in the context of the M2VTS project (Multi-Modal Verification for Teleservices and Security applications), a part of the EU ACTS programme, which deals with access control by the use of multimodal identification based on face and voice. The database contains microphone speech and face image from 295 people. Every subject was recorded in four sessions over a period of four months. At each session, two head rotation shots and six speech shots (subjects reading three sentences twice) were recorded. Figure 2 shows an example of several acquisition scenarios for one person. The XM2VTS evaluation protocol specifies training, evaluation, and test sets, so algorithmic recognition performance can be assessed on the basis of comparable evaluation framework. A variety of subsets of the database are available for purchase from the University of Surrey. Up-to-date, the XM2VTS database has been distributed to more than 100 institutions.

BANCA

The BANCA database is a large, realistic and challenging multimodal database intended for training and testing multimodal verification systems [8]. The BANCA database

Fig. 1. Example of five acquisition conditions in the BT-DAVID database

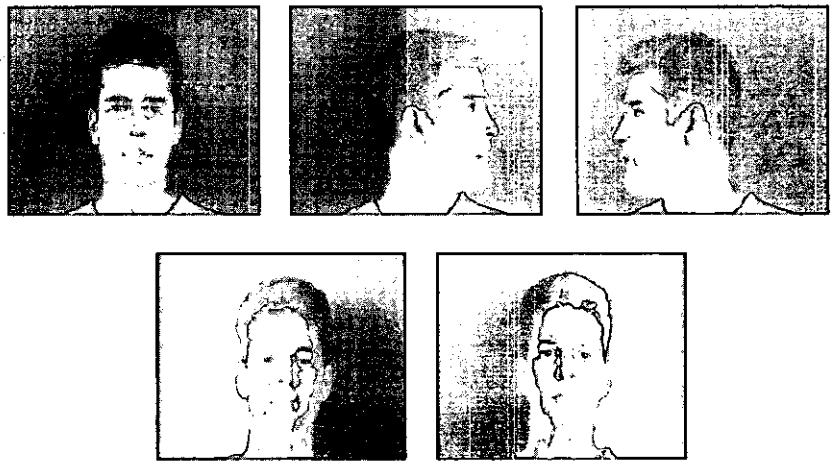

Fig. 2. Example of five acquisition conditions in the XM2VTS database: front and lateral views (top row), and front views with lighting variability (bottom row)

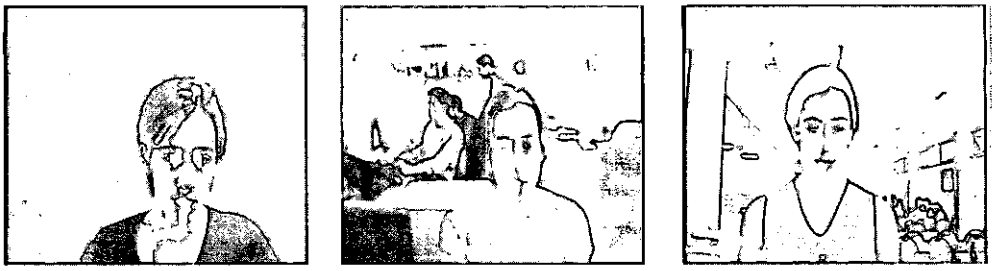

Fig. 3. Example of three acquisition scenarios in the BANCA database; From left to right: controlled, degraded, and adverse

was captured in four European languages and two modalities (face and voice). For recording, both high and low quality microphones and cameras were used. The subjects were recorded in three different scenarios: controlled, degraded, and adverse, over 12 different sessions, in a time span of three months.

Figure 3 shows an example of images of one person in these three scenarios. In total, 208 people were captured, with balanced gender distribution. For each recording the subject was instructed to utter a random 12-digit number along with a name, address, and date of birth (client or imposter data). Recordings took an average of 20 seconds. An associated BANCA evaluation protocol is also available.

BIOMET

Five different modalities are present in the BIOMET database [15]: audio, face image, hand image, fingerprint, and signature. For the face, besides images from a conventional digital camera, a camera using infrared illumination (designed to suppress the influence of the ambient light) is also used. Three different sessions have been realized, with three and five months spacing between them. The number of participants was

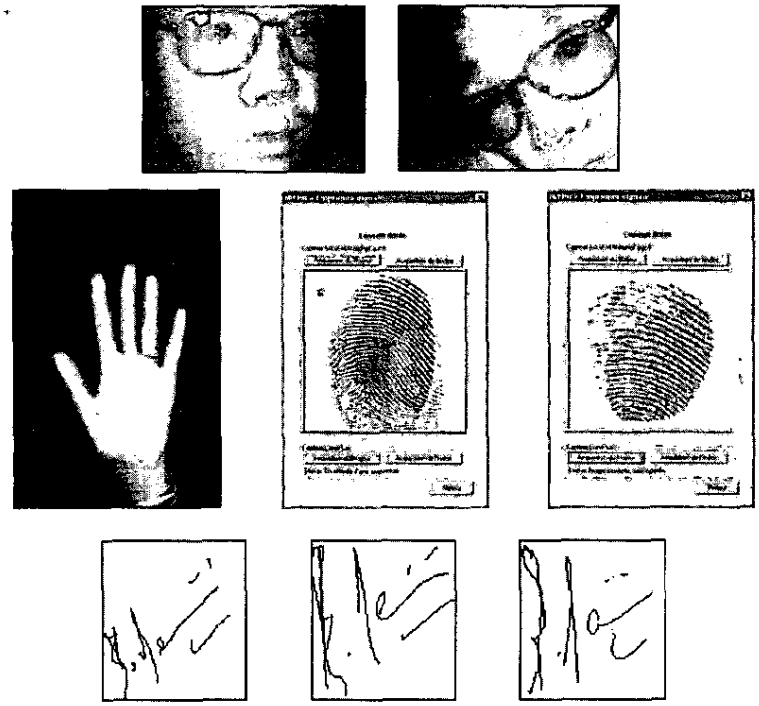

Fig. 4. Example of BIOMET acquisitions: infrared images (top row), hand and fingerprint (center row), and signature (bottom row, genuine and two forgeries)

130 for the first campaign, 106 for the second, and 91 for the final campaign. The proportion of females and males was balanced for all campaigns. 10% of the individuals were students (with a mean age of 20). The age of the rest varies from 35 up to 60 years. Figure 4 shows an example of several biometric traits acquired in the BIOMET database.

SMARTKOM

This is a multimodal database for the study of human–computer interaction created by SMARTKOM Consortium (Germany) and distributed by ELDA [19]. It has been recorded in public places (cinemas and restaurants) in the technical setup SMARTKOM Public, which is comparable to a traditional public phone booth but equipped with additional intelligent communication devices. This database includes the following traits: hand, signature, fingerprint, and voice of 96 users and 172 acquisitions. Figure 5 shows an example of SMARTKOM acquisition.

MCYT

The acquisition was conducted by a consortium of four Spanish academic institutions, namely: ATVS Research group (formerly at Universidad Politécnica de Madrid – UPM, currently at Universidad Autónoma de Madrid – UAM), Universidad de Valladolid (UVA), Universidad del País Vasco (EHU), and Escola Universitaria Politècnica de Mataró (EUPMT). The database consists of online signatures and fingerprints from 330 individuals [4]. For each individual, 12 samples of each finger are acquired using two different sensors (optical and capacitive). Therefore, $330 \times 12 \times 10 \times 2 = 79{,}200$ fingerprint samples are included in MCYT. Additionally, 25

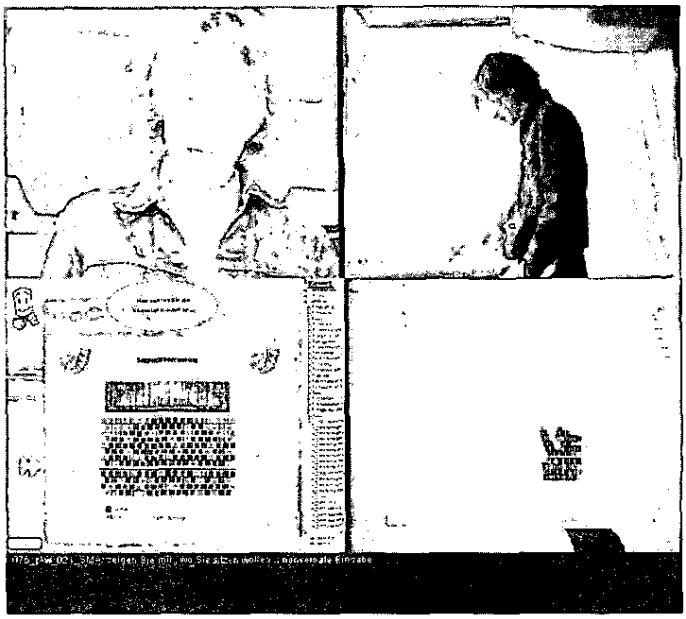

Fig. 5. Example of SMARTKOM acquisition. The left bottom square contains the screen output of the SMARTKOM system that the user sees projected on the flat interaction surface. The right bottom square contains the same picture overlaid with the output of the infrared camera that observes the interaction surface. The objects moved on the surface can be seen (e.g., pointing of fingers). The bottom object is the transcript of the current dialogue situation

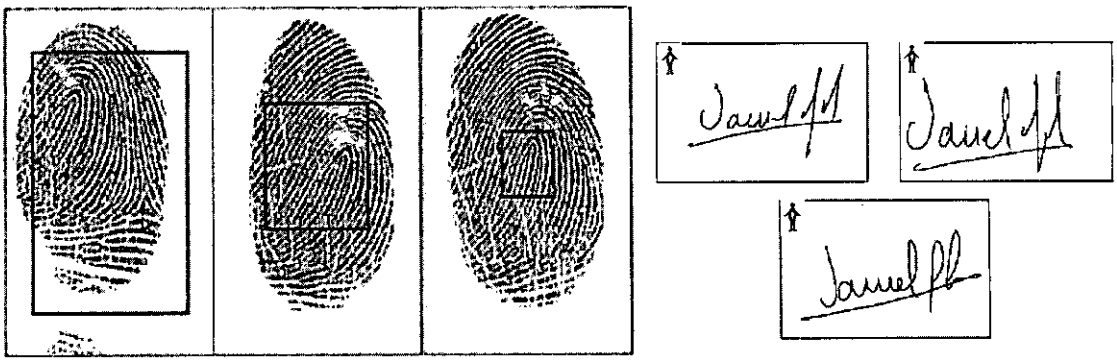

Fig. 6. Example of MCYT acquisitions. On the left, images of the same fingerprint employing the optical scanner with three different control levels according to the fingerprint core position. On the right, two genuine signatures (top) and one skilled forgery (bottom)

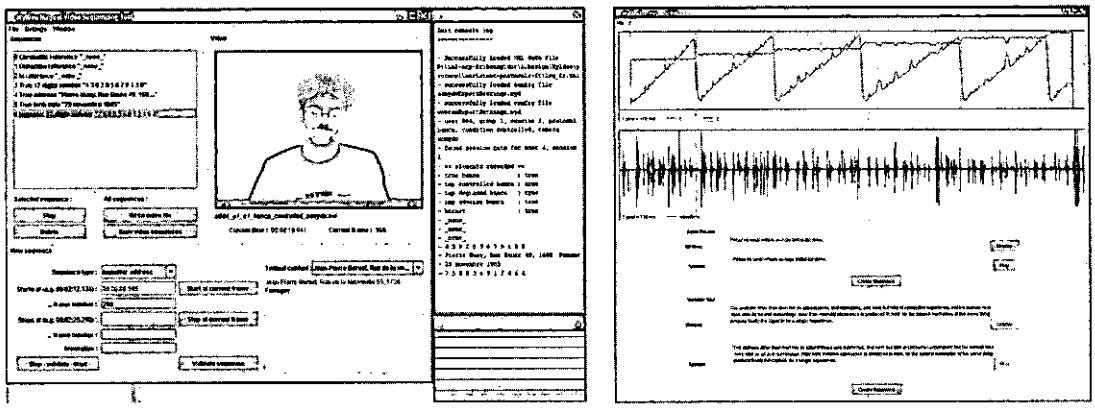

Fig. 7. Example of MYIDEA annotation tools: video annotation (left) and handwriting-voice annotation (right)

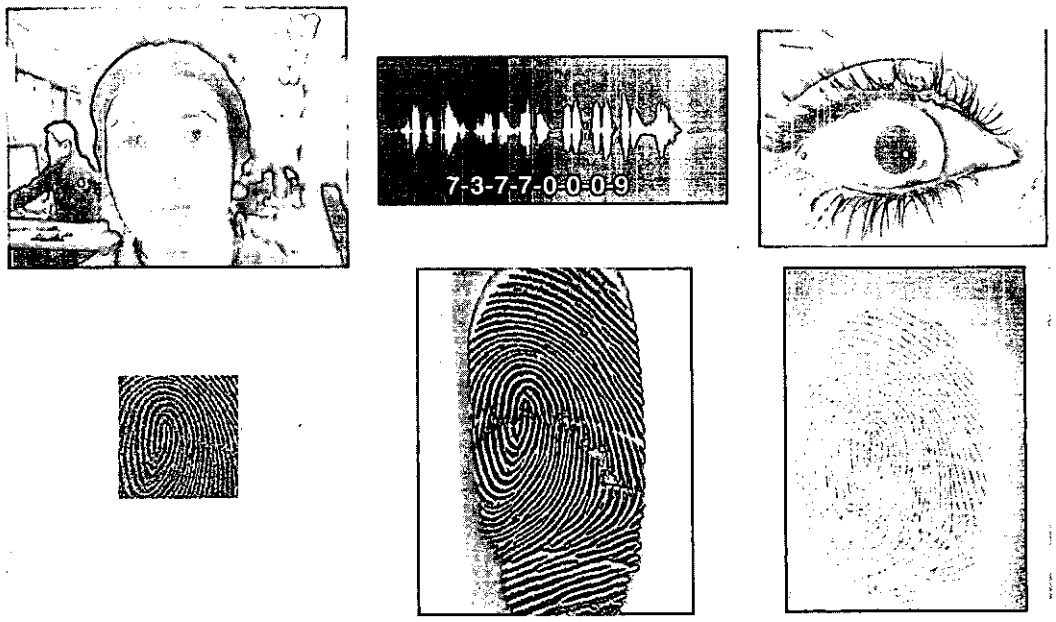

Fig. 8. Example of BIOSEC acquisitions. Top row from left to right: face, voice utterance, and iris image. Bottom row from left to right: fingerprint acquired with electric field, thermal and optical sensors

client signatures and 25 skilled forgeries (with natural dynamics) are obtained for each individual. Both on-line information (pen trajectory, pen pressure, and pen azimuth/ altitude versus time) and off-line information (image of the written signature) are included in the database. Therefore, 330 × (25 + 25) = 16,500 signature samples are contained in

Table 2. Summary of multimodal databases under development; N/A = Not Available

Trait		MYIDEA	BIOSEC	BIOSECUR-ID
Fingerprint	# users	104 aprox.	250	300 aprox.
	# sessions	3	4	4
	# repetitions/session	4 (x 10 fingers)	4 (x 4 fingers)	4 (x 4 fingers)
	% male/female	N/A	60/40	50%
	sensor	sweeping thermal, optical	CMOS electric field, sweeping thermal, optical	sweeping thermal, optical
Face	# users	104 aprox.	250	300 aprox.
	# sessions	3	4	4
	# repetitions/session	video input	4	4
	% male/female	N/A	60/40	50%
	sensor	handycam, webcam	webcam	webcam
Voice	# users	104 aprox.	250	300 aprox.
	# sessions	3	4	4
	# repetitions/session	several phrases	4	4
	% male/female	N/A	60/40	50%
	sensor	handycam, webcam, headset	Headset and webcam micro	headset micro
Signature	# users	104 aprox.		300 aprox.
	# sessions	3		4
	# repetitions/session	5		4
	% male/female	N/A		50%
	sensor	digitizing tablet		digitizing tablet
Iris	# users		250	300 aprox.
	# sessions		4	4
	# repetitions/session		4 (x 2 eyes)	4 (x 2 eyes)
	% male/female		60/40	50%
	sensor		High-quality iris camera	High-quality iris camera
Hand	# users	104 aprox.		300 aprox.
	# sessions	3		4
	# repetitions/session	4		4 (x 2 hands)
	% male/female	N/A		50%
	sensor	document scanner		document scanner
Keystroking	# users			300 aprox.
	# sessions			4
	# repetitions/session			4
	% male/female			50%
	sensor			keyboard
Handwriting	# users	104 aprox.		300 aprox.
	# sessions	3		4
	# repetitions/session	1		4
	% male/female	N/A		50%
	sensor	digitizing tablet		digitizing tablet

MCYT. Figure 6 shows example images from the MCYT database.

MULTIMODAL DATABASES CONSISTING OF BIOMETRIC SCORES

NIST

NIST Biometric Scores Set (BSSR1) is a set of raw output similarity scores from two 2002 face recognition systems and one 2004 fingerprint system, operating on frontal faces, and left and right index live-scan fingerprints, respectively [20]. The release includes true multimodal score data, i.e., similarity scores from comparisons of faces and fingerprints of the same people. This database is available upon request. The data are suited to the study of score-level fusion-based multimodal, multi-algorithmic, multisample and repeated-sample biometrics. The database contains three partitions: set 1 is comprised of face and fingerprint scores from the same set of 517 individuals. For each individual, the set contains one score from the comparison of two right index fingerprints, one score from the comparison of two left index fingerprints, and two scores (from two separate matchers) from the comparison of two frontal faces. Set 2 is comprised of fingerprint scores from one system run on images of 6,000 individuals. For each

individual, the set contains one score from the comparison of two left index fingerprints, and another from two right index fingerprints. Set 3 contains scores from two face systems run on images from 3,000 individuals. For each individual, the set contains one score from the comparison of face A with a later face, B, and a score from face A and another later face, C.

IDIAP

This score database is built on XM2VTS [7], respecting the standard Lausanne Protocols I and II (LP1 and LP2) [21]. LP1 has 8 baseline systems and LP2 has 5 baseline systems. The score database has two fusion protocols: 1) fusion of two experts with specific combinations in order to permit experiments on multimodal fusion, intramodal fusion with different feature sets, and intramodal fusion with the same feature; and 2) fusion with all the possible combinations across protocols.

MULTIMODAL BIOMETRIC DATABASES UNDER DEVELOPMENT

The acquisition of multimodal databases is a continuous effort, especially in the case of multimodal and multi-session databases, which typically are long lasting projects, involving several years of work. This section concentrates on current efforts in this regard from which public information is already available. The information on multimodal biometric databases under development is summarized in Table 2.

MYIDEA

The MYIDEA database is being acquired in the framework of collaboration between the University of Fribourg in Switzerland, the Engineering School of Fribourg in Switzerland, and the Groupe des Ecoles des Télécommunications in Paris. MYIDEA database includes face, audio, fingerprints, signature, handwriting, and hand geometry [22]. Further to the independent acquisition of each modality, two synchronized recordings are performed: face-voice and writing-voice. Video and handwriting-voice annotation tools are used in this case as pictured in Figure 7. The general specifications of MYIDEA are: target of 104 subjects, different quality of sensors, various realistic acquisition scenarios, and organization of the recordings to allow for open-set experimental scenarios. MYIDEA database is in close relationship with the database activities within the BIOSECURE project.

BIOSEC

BIOSEC is an Integrated Project of the 6th European Framework Programme [16]. The project is aimed at integrating biometrics and security to leverage trust and confidence in a wide spectrum of everyday applications. Over 20 partners from nine European countries participate in the project, including big companies, biometric HW/SW producers, prestigious universities, and SMEs. ATVS is in charge of the database activities carried out within BIOSEC, one of which is the design and acquisition of a new multimodal database. BIOSEC database includes face images, short speech utterances (low and high quality microphones), fingerprint images (3 different sensors) and iris images from 250 subjects acquired in 4 acquisition sessions. An initial subcorpus of 200 subjects acquired in 2 acquisition sessions is already available [23]. Example biometric signals from this subcorpus are depicted in Figure 8.

BIOSECUR-ID

BIOSECUR-ID is a joint project funded by the Spanish Ministerio de Ciencia Y Tecnología, following the successful MCYT [4] Project. Five Spanish academic partners participate in the project under the coordination of ATVS. One of the objectives of the project is to build a new multimodal database extending the BIOSEC database (both in terms of new sessions for the same subjects already acquired, and in terms of new biometric data and subjects). The new database will consist of the following biometric traits: face, fingerprint, voice, iris, written signature, handwriting, keystroking, palmprint, and hand geometry. Acquisition is being conducted as of late 2005 and will be completed by mid-2006. The database will be ready for research purposes by late 2006.

BIOSECURE

BIOSECURE is a Network of Excellence within the 6th European Framework Program (FP6) [17]. The project is aimed at coordinating the different research efforts focused on biometrics across Europe. Over 30 research institutions from over 15 countries participate in the network. ATVS is in charge of the database activities carried out within the network, one of which is the design and acquisition of a new multimodal database to be conducted during 2006. The new database will extend the efforts conducted in MYIDEA, BIOSEC, and BIOSECUR-ID.

CONCLUSION

In spite of the importance of the availability of common benchmarks for performance evaluation of multimodal biometric systems, the number of existing multimodal databases is quite reduced as compared to biometric databases containing only individual traits. This is a consequence of several factors, including the time- and resource-consuming task of biometric data acquisition, the high cooperation needed from the donators, and the legal issues regarding privacy and data protection.

In this paper, the most widely used existing multimodal biometric databases have been outlined. The databases have been divided into databases consisting of biometric samples, adequate for multimodal research at any fusion level (i.e., sensor, feature, score, or decision) and databases consisting of biometric scores, adequate for multimodal research at score or decision level. Finally, the contents of some relevant multimodal biometric databases under development have been summarized.

ACKNOWLEDGEMENTS

This work has been supported by the projects TIC-2003-08382-C05 and IST-2002-001766 (BioSec). The author J.F.-A. is supported by a FPI fellowship from Comunidad de Madrid and Fondo Social Europeo.

REFERENCES

[1] A.K. Jain, A. Ross and S. Prabhakar,
An Introduction to Biometric Recognition,
IEEE Trans. on Circuits and Systems for Video Technology, Vol. 14, No. 1, 2004, pp. 4-20.

[2] A.J. Mansfield and J.L. Wayman,
Best Practices in Testing and Reporting Performance of Biometric Devices,
National Physical Laboratory Report CMSC 14/02, August 2002.

[3] J. Ortega-Garcia, J. Bigun, D.A. Reynolds and J. Gonzalez-Rodriguez,
Increasing Security in DRM Systems through Biometric Authentication,
IEEE Signal Processing Magazine, Vol. 21, No. 2, 2004, pp. 50-62.

[4] Ortega-Garcia, J., Fierrez, J., Simon, D., Gonzalez, J., Faundez-Zanuy, M., Espinosa, V., Satue, A., Hernaez, I., Igarza, J.-J., Vivaracho, C., Escudero, D. and Moro, Q.-I.,
MCYT Baseline Corpus: A Multimodal Biometric Database,
IEE Proceedings Vision, Image and Signal Processing, Vol. 150, 2003, pp. 395-401.

[5] J. Wayman, A. Jain, D. Maltoni and D. Maio, eds.,
Biometric Systems: Technology, Design and Performance Evaluation,
Springer, 2005.

[6] A. Jain, R. Duin and J. Mao,
Statistical Pattern Recognition: A Review,
IEEE Trans. On Pattern Analysis and Machine Intelligence, Vol. 13, No. 3, 2000, pp.,252-264.

[7] K. Messer, J. Matas, J. Kittler and K. Jonsson,
XM2VTSDB: The Extended M2TVS Database,
In Proc. of IAPR Intl. Conf. on Audio- and Video-based Person Authentication, 1999.

[8] E. Bailly-Bailliere et al.,
The BANCA Database and Evaluation Protocol,
Lecture Notes in Computer Science, Vol. 2688, 2003, pp. 625-638.

[9] M. Faundez-Zanuy,
On the Vulnerability of Biometric Security Systems,
IEEE Aerospace and Electronic Systems Magazine,
Vol. 19, No. 6, 2004, pp. 3-8.

[10] A.K. Jain and A. Ross,
Multibiometric Systems,
Communications of the ACM, Vol. 47, No. 1, 2004, pp. 34-40.

[11] M. Faundez-Zanuy,
Data Fusion in Biometrics,
IEEE Aerospace and Electronic Systems Magazine,
Vol. 20, No. 1, 2005, pp. 34-38.

[12] J. Fierrez-Aguilar, D. Garcia-Romero, J. Ortega-Garcia and J. Gonzalez-Rodriguez,
Bayesian Adaptation for User-Dependent Multimodal Biometric Authentication,
Pattern Recognition, Vol. 38, No. 8, 2005, pp. 1317-1319.

[13] J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez and J. Bigun,
Discriminative Multimodal Biometric Authentication Based on Quality Measures,
Pattern Recognition, Vol. 38, No. 5, 2005, pp. 777-779.

[14] N. Poh and S. Bengio,
Can Chimeric Persons Be Used in Multimodal Biometric Authentication Experiments?,
in 2nd Intl. Workshop on Machine Learning and Multimodal Interaction, 2005.

[15] S. Garcia-Salicetti et al.,
BIOMET: A Multimodal Person Authentication Database Including Face, Voice, Fingerprint, Hand, and Signature Modalities,
Lecture Notes in Computer Science, Vol. 2688, 2003, pp. 845-853.

[16] BioSec, Biometrics and Security,
FP6 IP IST-2002-001766,
(http://www.biosec.org/).

[17] Biosecure, Biometrics for Secure Authentication,
FP6 NoE IST-2002-507634,
(http://www.biosecure.info/).

[18] C.C. Chibelushi, S. Gandon, J.S. Mason, F. Deravi and D. Johnston,
Design Issues for a Digital Integrated Audio-Visual Database,
in IEE Colloquium on Integrated Audio-Visual Processing for Recognition, Synthesis and Communication, November 1999, pp. 7/1–7/7.

[19] http://www.elda.otg/catalogue/en/speech/S0136.html.

[20] NIST image group's biometric scores, September 2004,
(http://www.nist.gov/biometricscores/).

[21] N. Poh and S. Bengio,
Database, Protocol and Tools for Evaluating Score-Level Fusion Algorithms in Biometric Authentication,
Pattern Recognition, Vol. 39, 2006, pp. 223-233.

[22] B. Dumas, J. Hennebert, A. Humm, R. Ingold, D. Petrovska, C. Pugin and D. Rotz,
MyIdea Sensors Specifications and Acquisition Protocol,
Computer Science Department Research Report DIUF-RR 2005.01,
University de Fribourg in Switzerland, January 2005.

[23] J. Fierrez-Aguilar,
Biometric Databases: Modalities, Privacy, and Size,
In 3rd BioSec Workshop, Helsinki, Finland, June 2005.