BiosecurID: a Multimodal Biometric Database

J. Galbally[1], J. Fierrez[1], J. Ortega-Garcia[1], M. R. Freire[1],
F. Alonso-Fernandez[1], J. A. Siguenza[1], J. Garrido-Salas[1], E. Anguiano-Rey[1],
G. Gonzalez-de-Rivera[1], R. Ribalda[1], M. Faundez-Zanuy[2], J. A. Ortega[3],
V. Cardeñoso-Payo[4], A. Viloria[4], C. E. Vivaracho[4], Q. I. Moro[4],
J. J. Igarza[5], J. Sanchez[5], I. Hernaez[5], and C. Orrite-Uruñuela[6]

[1] Universidad Autonoma de Madrid, EPS, Biometric Recognition Group–ATVS,
C/ Francisco Tomas y Valiente 11, 28049 Madrid, SPAIN
javier.galbally@uam.es

[2] Escuela Universitaria Politecnica de Mataro,
Avda. Puig i Cadafalch 101-111, 08303 Mataro, Barcelona, SPAIN

[3] Universidad Politecnica de Cataluña, Esc. Univ. de Ing. Tec. Industrial de Terrassa,
C/ Colom 1, 08222 Terrassa, Barcelona, SPAIN

[4] Universidad de Valladolid, Edif. de Tecnicas de la Inf. y las Telecom.,
Campus Miguel Delibes s/n, 47011 Valladolid, SPAIN

[5] Universidad del Pais Vasco, Escuela Superior de Ingenieros,
C/ Alameda de Urquijo s/n, 48013 Bilbao, SPAIN

[6] Universidad de Zaragoza, Computer Vision Lab Group, Edif. Ada Byron,
C/ Maria de Luna 1, 50015 Zaragoza, SPAIN

Abstract. A new multimodal biometric database, acquired in the framework of the BiosecurID project funded by the Spanish MEC, is presented together with a brief description of the acquisition setup and protocol. The database includes 7 unimodal biometric traits, namely: speech, iris, face (photographs and talking faces), signature and handwriting (on-line and off-line), fingerprints (acquired with two different sensors), hand (palmprint and contour-geometry) and keystroking. The database comprises 400 subjects and presents features such as: realistic acquisition scenario, balanced gender and population distributions, availability of information about particular demographic groups (age, gender, handedness), acquisition of skilled forgeries, and compatibility with other existing databases. All these characteristics make it very useful in research and development of multimodal biometric systems.

1 Introduction

Authentication methods based on biometric technology [1], which guarantees that the means of identification cannot be stolen, lost or forgotten, are being increasingly demanded in security environments and applications like access control and electronic transactions. Big efforts have been undertaken in the biometric community to increase the security systems reliability by combining existing

unimodal expert recognizers in order to implement multimodal authentication systems [2, 3] which fit the market requirements. Nevertheless, in real-world circumstances, error rates achieved with state-of-the-art technology have slowed down their generalized application. In order to overcome the difference in performance between laboratory experiments and practical implementations, there is an urgent need for the collection of realistic multimodal biometric data which permit to infer valid results from controlled experimental conditions to the final application.

In the present contribution we describe the BiosecurID Multimodal Database acquired within the BiosecurID project [4] supported by the Spanish MEC, and conducted by a consortium of 6 Spanish Universities, Universidad Autonoma de Madrid (UAM), Universidad Politecnica de Madrid (UPM), Universidad Politecnica de Catalu na (UPC, Campus of Terrasa and Campus of Mataro), Universidad de Zaragoza (UniZar), Universidad de Valladolid (UVA), and Universidad del Pais Vasco (UPV). The main objective of the project was the acquisition of a realistic multimodal and multisession database, statistically representative of the potential users of future biometric applications.

Although several multimodal biometric databases are already available for research purposes [5, 6], none of them can match the BiosecurID database in terms of number of users, number of biometric traits and number of temporal separated acquisition sessions. The data collected in the project are especially useful for the development and testing of automatic recognition systems due to some design characteristics such as: realistic acquisition scenario, balanced gender and population distributions, availability of information about particular demographic groups (age, gender, handedness, visual aid), acquisition of skilled forgeries (pin utterance, signature, and keystroking), and compatibility with other existing databases. All these important design features were fixed in order to comply with the main objective of the project, that is, to obtain comparable performance results between laboratory tests and real-world biometric applications.

2 Other Existing Multimodal Biometric Databases

Some of the oldest and most widely used biometric databases are **XM2VTS** [7] containing microphone speech and face images of 295 people captured in 4 different sessions, and **MCYT** [8] database including fingerprints and signature of 330 subjects. More recent databases include **BIOMET** [9], **BANCA** [10], **MYIDEA** [11], **MBioID** [12], and **M3** [13]. Other current initiatives in multimodal database collection closely related to the BiosecurID database are the following:

- **BIOSEC** [14]. It was acquired under FP6 EU BioSec Integrated Project, and comprises fingerprint images acquired with three different sensors, frontal face images from a webcam, iris images, and voice utterances (captured both with a webcam and a close-talk headset), of 250 subjects.

– **BIOSECURE** [15]. One of the Biosecure NoE objectives is the acquisition of a multimodal database which will extend the efforts conducted in MYIDEA, BIOSEC, and BiosecurID. The database considers three acquisition scenarios, namely:
  - Unsupervised internet acquisition (internet dataset), including voice, and face (still images and talking faces).
  - Supervised office-like scenario (desktop dataset), including voice, fingerprints, face (still images and talking faces), iris, signature and hand.
  - Acquisition in a mobile device (mobile dataset), including signature, fingerprints, voice, and face (images and video).

  All datasets include 2 sessions, with the biggest dataset (internet) comprising over 1000 subjects, and about 700 users the other two. Around 400 of these donors are common to the whole database.

3 BiosecurID Database

The database was collected in 6 different sites, in an office-like uncontrolled environment (in order to simulate a realistic scenario), and was designed to comply with three main characteristics which make it unique in the current multimodal biometric databases field, namely:

1. **Number of subjects**: a total of 400 users were acquired.
2. **Number of unimodal biometric traits**: speech, iris, face (photographs and talking faces), signature and handwriting (on-line and off-line), fingerprints, hand (palmprint and contour-geometry) and keystroking.
3. **Number of sessions**: 4 sessions distributed in a 4 month time span. Thus, three different levels of temporal variability are taken into account: *i*) within the same session (the samples of a same biometric trait are not acquired consecutively), *ii*) within weeks (between two consecutive sessions), and *iii*) within months (between non-consecutive sessions).

Furthermore, the database was designed to be compatible with other existing databases. Thus, the devices and protocol used in the acquisition of some of the traits present in the BiosecurID database (optical/thermal fingerprints, face, speech and iris), were chosen to be interoperable with the Biosec database, with 250 subjects. Moreover, both databases (Biosec and BiosecurID) have some subjects in common, which will allow real long term (2 year) temporal variability studies.

The BiosecurID database is also thought to represent in a realistic way the population distribution where biometric systems will be deployed. Thus, all sites were asked to acquire 30% of the subjects between 18 and 25 years of age, 20% between 25 and 35, 20% between 35 and 45, and the remaining 30% of the users above 45 years of age. Moreover, the gender distribution was forced to be balanced and only a 10% difference was permitted between male and female acquired subjects.

Fig. 1. Example setup used in the acquisition of the BiosecurID database.

All relevant non-biometric data of each subject is stored in an independent file so that experiments regarding specific demographic groups can be easily carried out. The available information in these files includes: age, gender, handedness, manual worker (yes/no), and vision aids (glasses, contact lenses, none). The "manual worker" group includes all users having eroded fingerprints, and the use of glasses, contact lenses or none of them refers to regular use.

3.1 Acquisition Environment

Each of the 6 acquisition sites prepared an acquisition kiosk following some very general indications about the environmental conditions, regarding illumination (neutral lighting with no preponderant focuses), noise (indoor conditions with no excessive background noise), and pose of the contributor (frontal while sitting in a non-revolving chair). This relaxed environmental conditions allow a desirable variability between the samples acquired in the different sites which simulates the changing working conditions of a real-world biometric application. In Fig. 1 we show the acquisition kiosk prepared in one of the sites.

During the acquisition procedure a human operator gave the necessary instructions to the contributors so that the acquisition protocol was followed. In spite of this guidance, and of the usage of a specifically designed acquisition software, some human and software errors occurred. In order to ensure that the BiosecurID database complies with the acquisition protocol, all biometric samples were manually verified by a human expert.

Table 1. Acquisition devices used for the BiosecurID database.

Modality	Model	Main Features
Speech	Plantronics DSP 400	Noise cancelling. 10Hz - 10KHz
Fingerprints	Biometrika FX2000	Optical. 569 dpi.
Fingerprints	Yubee (Atmel)	Thermal Sweeping. 500 dpi.
Iris	LG Iris Access 3000	640 × 480 pixels. Infrared illumin.
Hand	Scanner EPSON Perfection 4990	4800 × 9600 dpi. 48 bits color depth.
Face	Philips ToUcam Pro II	CCD. 640 × 480 pixels.
Writing/Signature	Wacom Intuos3 A4/Inking pen	5080 dpi. 1024 pressure levels.
Keystroking	Labtec Standard Keyboard SE	Standard

3.2 Acquisition Devices

In Table 1 we show a list with all the devices used in the database acquisition and its most relevant features. All of them were connected to a standard PC in which an acquisition software specifically designed following the database protocol was installed. This programme centralized the functioning and launching of all the devices, as well as the naming and storage of the captured samples and management of the database, thus minimizing eventual acquisition errors.

3.3 Acquisition Protocol

Biometric data are personal data and thus have to be protected according to the directives of the country where it is collected [7]. At the start of the first session a consent form was signed by each subject in which the donors were properly informed about how the personal information will be used, that these data will only be transmitted to other institutions for research purposes and for a limited period of time, and that they have the right to access their data in order to correct, or delete it. The acquisition procedure started only once this consent form was fully understood and signed by the donor. In Table 2 we we summarize the biometric data captured for each user, which consist of:

Speech. 10 short sentences in Spanish (the ones used in the Ahumada database [16], and the same 10 for each donor) distributed along the four sessions ($4+2+2+2$) are recorded at 44KHz stereo with 16 bits (PCM with no compression). In addition to the short sentences, 4 utterances of a user-specific PIN of 8 digits were also recorded, and an utterance of other 3 users' PINs to simulate informed forgeries in which an impostor has access to the number of a client. The forged users in each session were $n - 3S + 2$, $n - 3S + 1$, and $n - 3S$, where n is the ID number inside the database of the current donor, and $S = \{1, 2, 3, 4\}$ is the session number. The 8 digits were always pronounced digit-by-digit in a single continuous and fluent utterance.

[7] Directive 95/96/EC of the European Parliament and the Council of 24 October 1995.

Table 2. Number of samples available for each user in the BiosecurID database.

Modality	Samples	Total Samples
Speech	10 short sentences 4×4 PIN 3×4 PIN forgeries	**38**
Fingerprints	$4 \times 4 \times 4$ optical $4 \times 4 \times 4$ thermal	**128**
Iris	$2 \times 4 \times 4$	**32**
Hand	$2 \times 4 \times 4$	**32**
Face	4×4 still faces 1×4 talking faces	**20**
Writing	1×4 lower-case text 1×4 upper-case words 1×4 number sequence	**12**
Signature	4×4 genuine signatures 3×4 skilled forgeries	**28**
Keystroking	4×4 genuine name 3×4 skilled forgeries	**28**

Fingerprints. 4 samples (BMP format with no compression) with 2 different sensors (see Table 1) of the index and middle fingers of both hands, interleaving fingers between consecutive acquisitions in order to achieve intravariability among images of the same fingerprint.

Iris. 4 samples (BMP with no compression) of each iris, changing eyes between consecutive captures. Glasses are removed for the acquisition, while the use of contact lenses is saved in the non-biometric data file.

Hand. 4 images (JPG format) of each hand, alternating hands between consecutive acquisitions. The scanner used in the acquisition was isolated from external illumination using a box with just a little slot to insert the hand, and covered with a black opaque cloth.

Face. 4 frontal images (BMP not compressed), with no specific background conditions (except that no moving objects are permitted). One video sequence of five seconds saying the 8 digit PIN corresponding to the captured donor. Both the audio (PCM 8 bit) and video (29 frames per second) are captured with the webcam (see Table 1).

Handwriting. A Spanish text (the same for all subjects) handwritten in lowercase with no corrections or crossing outs permitted. The 10 digits, written separately and sequentially from 1 to 9 and last the 0. 16 Spanish separate words

in upper-case. All the writing was captured using an inking pen so that both on-line (following the SVC [17] format) and off-line versions of the data are available. The lower-case text is collected in a different sheet of paper with no guiding lines, while the upper-case words and the number sequence were stored in a template-like page with boxes for each separate piece of writing.

Signature. 4 genuine signatures per session (2 at the start and 2 at the end) and 1 forgery of each of the precedent three donors (the same three in all the sessions). In order to consider an incremental level of skill in the forgeries, four different scenarios are considered, namely: *i*) the forger only sees the written signature once and tries to imitate it right away (session 1), *ii*) the user sees the written signature and trains for a minute before making the forgery (session 2), *iii*) the donor is able to see the dynamics of the signing process 3 times, trains for a minute and then makes the forgery (session 3), and *iv*) the dynamics of the signature are shown as many times as the donor requests, he is allowed to train for a minute and then signes (session 4). Again both the on-line (SVC format) and off-line versions of the signature are captured using an inking pen. This trait is compatible with the publicly available MCYT database (330 subjects) [8].

Keystroking. 4 repetitions of the donor's name and surname (2 in the middle of the session and two at the end) keystroked in a natural and continuous manner. No mistakes are permitted (i.e., pressing the backspace), if the user gets it wrong, he is asked to start the sequence again. The names of 3 different donors are also captured as forgeries (the same three donors as in the speech forgeries), again with no mistakes permitted when keying the name. Samples are stored in plain text files with the total number of keystrokes in the first line, then all the events (SCAN code + D=press/U=release) with the miliseconds elapsed from the last event in the subsequent lines.

Examples of typical images in BiosecurID database are depicted in Fig. 2 (different traits corresponding to different random subjects). Voice utterances are shown as waveforms, while keystroking samples do not appear.

4 Conclusions

In the present contribution a short overview of the existing multimodal biometric databases has been presented, together with the description of the acquisition protocol and contents of the new BiosecurID database, comprising speech, iris, face (photographs and talking faces), signature and handwriting (on-line and off-line), fingerprints (acquired with two different sensors), hand (palmprint and contour-geometry) and keystroking of 400 subjects.

The distribution details of the BiosecurID Multimodal Biometric DB will shortly be available at http://atvs.ii.uam.es.

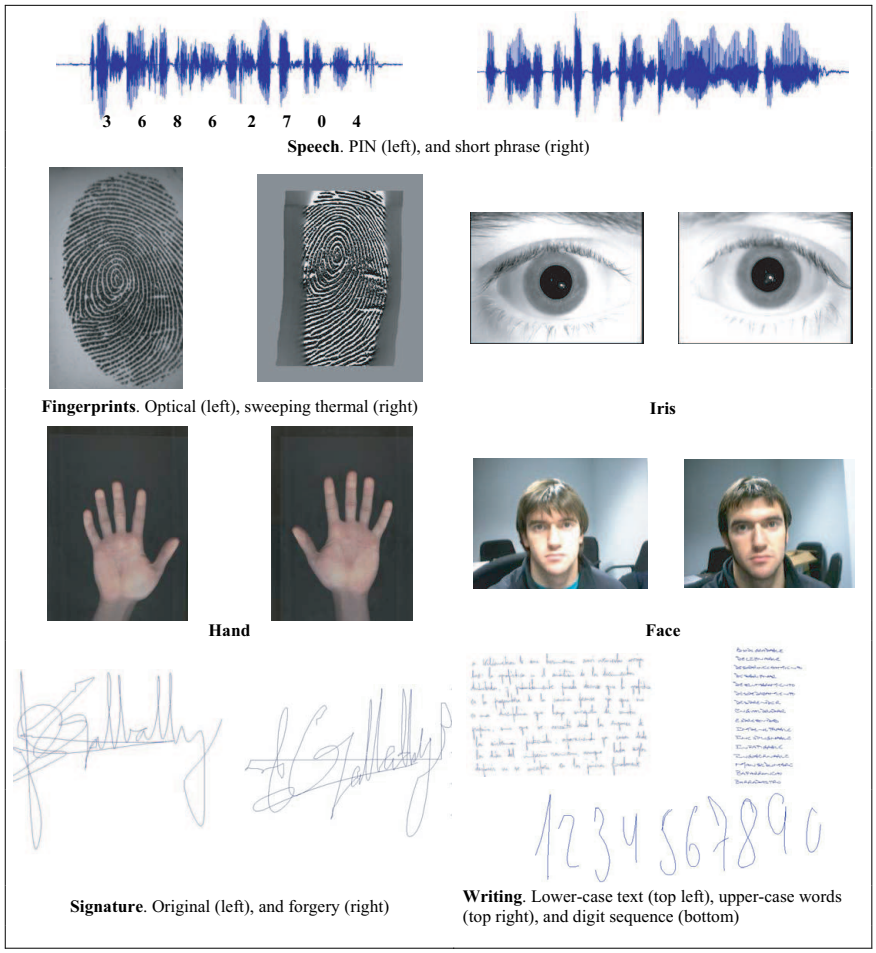

Fig. 2. Example setup used in the acquisition of the BiosecurID database.

Acknowledgements

This work has been supported by Spanish MEC under project TIC2003-08382-C05-01. The author J. G. is also supported by a FPU Fellowship from the Spanish MEC, J. F. is supported by a Marie Curie Fellowship from the European Commission, and M. R. F. and F. A.-F. are supported by a FPI Fellowship from CAM. The authors would like to thank the valuable development work of Javier Garrido-Tomas and Borja Fernandez-Tomas.

References

1. Jain, A.K., Ross, A., Pankanti, S.: Biometrics: a tool for information security. IEEE Trans. on Information Forensics and Security **1** (2006) 125–143

2. Fierrez-Aguilar, J., Ortega-Garcia, J., et al.: Discriminative multimodal biometric authentication based on quality measures. Pattern Recognition **38** (2005) 777–779
3. Ross, A., et al.: Handbook of Multibiometrics. Springer (2006)
4. BiosecurID: Seguridad Multimodal basada en Autenticacion Biometrica mediante Fusion de Expertos Unimodales, MCYT TIC2003-08382-C05.
5. Faundez-Zanuy, M., Fierrez, J., et al.: Multimodal biometric databases: An overview. IEEE AES Magazine **21** (2006) 29–37
6. Flynn, P.J.: Biometric Databases. In: Handbook of Biometrics. Springer (2007)
7. Messer, K., Matas, J., et al.: XM2VTSDB: The extended M2VTS database. In: Proc. of IAPR AVBPA. (1999)
8. Ortega-Garcia, J., Fierrez, J., et al.: MCYT baseline corpus: a bimodal biometric database. IEE Proc. VISP **150** (2003) 391–401
9. Garcia-Salicetti, S., Beumier, C., et al.: BIOMET: A multimodal person authentication database including face, voice, fingerprint, hand and signature modalities. In: Proc. of IAPR AVBPA, Springer LNCS-2688 (2003) 845–853
10. Bailly-Bailliere, E., Bengio, S., et al.: The BANCA database and evaluation protocol. In: Proc. of IAPR AVBPA, Springer LNCS-2688 (2003) 625–638
11. Dumas, B., Hennebert, J., et al.: MyIdea - Sensors specifications and acquisition protocol. Computer Science Department Research Report DIUF-RR 2005.01, University de Fribourg in Switzerland (2005)
12. Dessimoz, D., Richiardi, J., et al.: Multimodal biometrics for identity documents (MBioID). Forensic Science International **167** (2007) 154–159
13. Meng, H., Ching, P.C., et al.: The multi-biometric, multi-device and multilingual (M3) corpus. In: Proc. MMUA Workshop. (2006)
14. Fierrez, J., Ortega-Garcia, J., et al.: Biosec baseline corpus: a multimodal biometric database. Pattern Recognition **40** (2007) 1389–1392
15. Biosecure: (2007) Biometrics for Secure Authentication, FP6 NoE IST-2002-507634. (http://www.biosecure.info/).
16. Ortega-Garcia, J., Gonzalez-Rodriguez, J., Marrero-Aguilar, V.: Ahumada: A large speech corpus in spanish for speaker characterization and identification. Speech Communication **31** (2000) 255–264
17. Yeung, D.Y., Chang, H., et al.: SVC2004: First International Signature Verification Competition. In: Proc. ICBA. LNCS-3072, Springer (2004) 16–22