



HAL
open science

Computation EvaBio: A Tool for Performance Evaluation in Biometrics

Julien Mahier, Baptiste Hemery, Mohamad El-Abed, Mohamed El-Allam,
Mohamed Bouhaddaoui, Christophe Rosenberger

► **To cite this version:**

Julien Mahier, Baptiste Hemery, Mohamad El-Abed, Mohamed El-Allam, Mohamed Bouhaddaoui, et al.. Computation EvaBio: A Tool for Performance Evaluation in Biometrics. International Journal of Automated Identification Technology (IJAIT), 2011, pp.24. hal-00984026

HAL Id: hal-00984026

<https://hal.science/hal-00984026>

Submitted on 26 Apr 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Computation EvaBio: A Tool for Performance Evaluation in Biometrics

Julien Mahier, Baptiste Hemery, Mohamad El-Abed*, Mohamed T. El-Allam,
Mohamed Y. Bouhaddaoui, Christophe Rosenberger

GREYC Laboratory
ENSICAEN - University of Caen Basse Normandie - CNRS
6 Boulevard Maréchal Juin, 14000 Caen Cedex - France

Abstract

Performance evaluation is a key factor in biometrics. In order to assess the quality of a new biometric system, one has in general to compute the performance on a large dataset to have significant results. It is not always an easy task as the computation complexity could be important. Moreover, the use of existing datasets is not obvious as it is represented in different ways (datasets, directory of images) and contain multiple scenarios (single enrollment process, different numbers of samples for the template generation for each user, *etc.*). We propose in this paper a new distributed-based platform facilitating the computation on different datasets in biometrics. The architecture of the proposed platform is composed of a server distributing computation tasks on its available clients. Experimental results on two biometric datasets (PolyU finger knuckle print and AR face datasets) show the benefit of proposed computing platform.

Keywords:

Biometrics, Performance Evaluation, Benchmark, Distributed Computing

*Corresponding author

Email addresses: julien.mahier@ensicaen.fr (Julien Mahier),
baptiste.hemery@ensicaen.fr (Baptiste Hemery), mohamad.elabed@ensicaen.fr
(Mohamad El-Abed), christophe.rosenberger@ensicaen.fr (Christophe Rosenberger)

1. Introduction

The interest for biometric technologies has increased during the last few years. The application of biometrics in industrial domains becomes a reality. Apart from the traditional modalities such as fingerprints [1] or iris recognition [2], new modalities are studied such as keystroke dynamics [3], gait [4] or finger knuckle prints [5].

As there are many research works in biometrics, there is a strong need for comparing and benchmarking biometric algorithms. Several datasets are made available in order to ease this comparison process. However, a dataset can be used within several protocols, which sets up a benchmark, to establish the performance of an algorithm. This leads to an important complexity to correctly evaluate a biometric system. Moreover, there are some well-known performance metrics presented by the International Organization for Standardization ISO/IEC 19795-1 [6] for the evaluation process such as the ROC curve (Receiver Operating Characteristic) and the EER value (Equal Error Rate). The EPC (Expected Performance Curve) is also another performance metric presented in [7] towards the performance evaluation of biometric algorithms. It requires some datasets to be split in two parts, one dealing with development and the other one with experiment. However, it is still difficult to compare biometric algorithms. It is required that the used dataset is large enough to be significant, but this leads to a very long time consuming experiment. If we have a benchmark datasets of N individuals and M samples for each user, the definition of the FRR (False Rejection Rate) requires $(M - 1) \cdot N$ computations and for the FAR (False Acceptance Rate) $N(N - 1) \cdot M$ ones (for a single enrollment biometric system). In order to achieve a more accurate evaluation, we need to have a large dataset which exponentially grows the computation complexity. Some platforms dedicated to biometric algorithm evaluation exist (such as the online evaluation platform FVC-onGoing), but are generally specialized for only one kind of biometric modality and only one dataset.

31

32 We present in this paper a distributed-based computation platform called
33 EvaBio dedicated to the evaluation of biometric systems. The proposed plat-
34 form is modality-independent. Thus, it needs to be able to manage any biomet-
35 ric dataset. Moreover, this platform needs to be easy to use and efficient. Thus,
36 the required computation tasks can be easily distributed on several computers.

37

38 The outline of this paper is as follows: after the introduction, we present
39 in section 2 the existing platforms dedicated to the evaluation of biometric al-
40 gorithms. We also present the EvaBio platform we are working on in section
41 3 with a description of its computation capabilities and the scenarios genera-
42 tion for performance evaluation. Section 4 presents some experimental results.
43 Finally, we conclude and give the perspectives of this work in section 5.

44 **2. State of the art**

45 In comparison to traditional authentication systems (such as password-based
46 methods), biometric systems are less accurate and do not provide a 100% reliable
47 answer. Due to this inaccuracy, many efforts are done in the literature for the
48 performance evaluation of such systems. We provide first in this section, a brief
49 description of the used biometric performance metrics and some well known
50 benchmarks, followed by an overview of the well known platforms which aim to
51 evaluate monomodal and multimodal biometric systems.

52 *2.1. Biometric Performance Metrics*

53 The comparison of two biometric samples produces a similarity score. If the
54 score is higher than a predefined decision threshold, then the system accept the
55 claim user, otherwise the claim is rejected. Figure 1 illustrates the distribution
56 of the genuine and impostor scores. This figure shows that depending from fixed
57 decision threshold, we obtain different kind of errors: 1) genuine users who are
58 incorrectly rejected by the system, and 2) impostors who are considered as
59 genuine users.

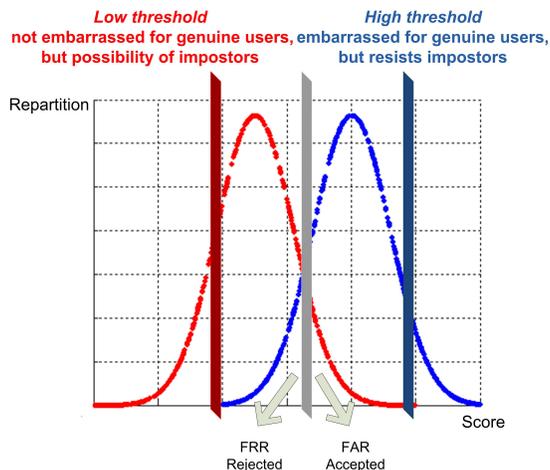


Figure 1: Distribution of genuine and impostor scores

60 In order to evaluate and compare the performance of biometric systems,
 61 the International Organization for Standardization ISO/IEC 19795-1 [6] defines
 62 several performance metrics such as:

- 63 • Failure-to-enroll rate (FTE): proportion of the user population for whom
 64 the biometric system fails to capture or extract usable information from
 65 biometric sample;
- 66 • Failure-to-acquire rate (FTA): proportion of verification or identification
 67 attempts for which a biometric system is unable to capture a sample or
 68 locate an image or signal of sufficient quality;
- 69 • False acceptance rate (FAR): proportion of impostors that are accepted
 70 by the biometric system;
- 71 • False rejection rate (FRR): proportion of authentic users that are incor-
 72 rectly denied;
- 73 • False-match-rate (FMR): the rate for incorrect positive matches by the
 74 matching algorithm for single template comparison attempts. FMR equals
 75 FAR when the biometric system uses one attempt by a user to match its

76 own stored template;

77 • False-non-match rate (FNMR): the rate for incorrect negative matches by
78 the matching algorithm for single template comparison attempts. FNMR
79 equals FRR when the biometric system uses one attempt by a user to
80 match its own stored template;

81 • Equal error rate (EER): it is the value where both errors rates, FAR and
82 FRR, are equals (*i.e.*, $FAR = FRR$). It constitutes a good indicator, and
83 the most used, to evaluate and compare biometric systems. In other words,
84 lower the EER, higher the accuracy of the system.

85 These performance metrics may be drawn to graphically visualize the preci-
86 sion of the target system. A well known curve is the ROC (Receiver Operating
87 Characteristic) curve which plots both types of errors (FAR and FRR) as
88 depicted in figure 2. This curve provides the performance of the tested system
89 among several decision thresholds. In addition to these metrics, usability met-
90 rics are computed within competitions and platforms such as the average enroll
91 time, average match time, average template size. These additional metrics are
92 important in order to have useful and usable systems.

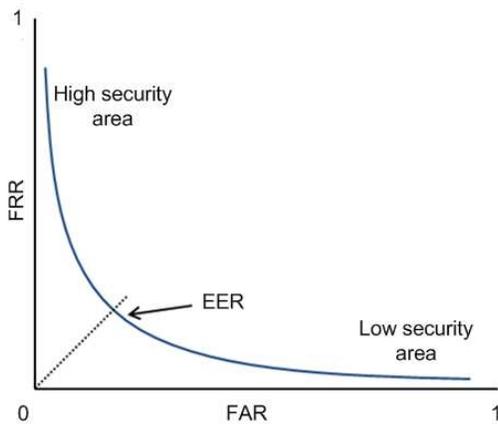


Figure 2: ROC curve

93 *2.2. Benchmarks*

94 In order to compute the performance metrics provided in the previous sec-
95 tion, we need biometrics benchmarks. Several benchmarks are publicly available
96 to researchers in order to evaluate their developed algorithms. Two categories of
97 datasets exist in the literature: 1) monomodal datasets such as PolyU FKP[8],
98 GREYC-Kesyroke [9], FACES94 [10], AR [11], FERET [12, 13], FRGC (Face
99 Recognition Grand Challenge) [14], *etc.*, and 2) multimodal datasets such as
100 XM2VTSDB [15], BANCA [16], BIOSECURE [17], *etc.* Figure 3 illustrates
101 an example of samples from AR, ENSIB and FACES94 datasets. A detailed
102 description of the used datasets (PolyU FKP and AR datasets) are given in
103 section 4.1.

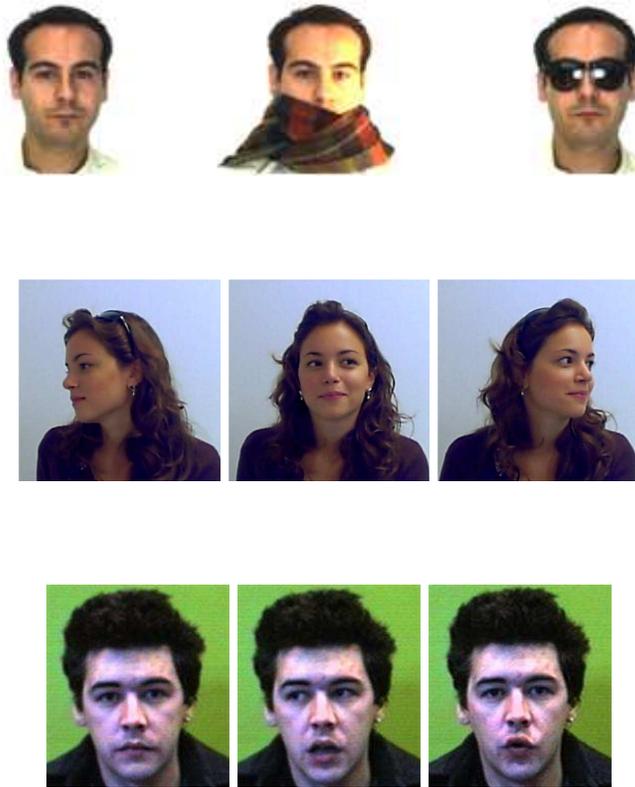


Figure 3: Biometric samples from the AR, ENSIB and FACES94 datasets

104 *2.3. Biometric Platforms*

105 *2.3.1. Fingerprint Verification Competition-onGoing (FVC-onGoing)*

106 FVC-onGoing is the evolution of the FVC international competitions held
107 on 2000, 2002, 2004 and 2006. It is a web-based automated evaluation for fin-
108 gerprint recognition algorithms available at [https://biolab.csr.unibo.it/
109 FVCOnGoing/](https://biolab.csr.unibo.it/FVCOnGoing/). The tests are done using sequestered datasets. The platform
110 uses several performance measures in terms of accuracy indications (such as the
111 EER value), enrollment and matching failures (such as the FTE value), usability
112 measures (such as the average enrollment time), and memory indicators (such
113 as the average template size).

114

115 The FVC-onGoing platform is a useful solution since the comparison process
116 is done using the same protocol, and the used evaluation metrics cover the main
117 criteria of having useful and usable systems. In addition, such kind of platforms
118 is important since the evaluation process is done by the online platform side.
119 This facilitates the tasks of other researchers that may do not have the required
120 materials (*e.g.*, a cluster computing) towards the evaluation of their developed
121 algorithms. However, FVC-onGoing is dedicated to the performance evaluation
122 of fingerprint algorithms. Hence, it could not be exploited for other types of
123 well used modalities such as face modality [18].

124 *2.3.2. BioSecure Reference and Evaluation framework*

125 BioSecure was a project of the 6th Framework Program of the European
126 Community. Its main objective was to build and provide a common evaluation
127 framework, which investigates and compares the biometrics-based identity au-
128 thentication methods. It provides twelve benchmarking reference systems freely
129 available at <http://share.int-evry.fr/svnview-eph/>: 2D face, 3D face, fin-
130 gerprint, hand, iris, signature, speech and talking-face reference systems.

131

132 These reference systems are made of replaceable modules (preprocessing, fea-
133 ture extraction, model building and matching) which allow developers and re-

134 searchers to investigate the improvement of a specific part of the tested system.
135 In this case, a researcher can evaluate and compare its matching algorithm just
136 by replacing the corresponding module in the reference system. An example
137 of the used performance measures is the distribution of genuine and impostor
138 comparison scores. BioSecure reference systems are useful since they cover sev-
139 eral kinds and the most used modalities. In addition, the structure of these
140 reference systems in allowing a researcher to test a specific part of a devel-
141 oped algorithm is a main advantage of these systems. However, in comparison
142 to the FVC-onGoing online platform, the computation is done on the side of
143 the developers which may do not have the specific materials dedicated to such
144 kinds of evaluation. Moreover, these reference systems are dependent from the
145 used modality and use a predefined dataset and protocol. This fact limits their
146 use if the researchers want to evaluate their developed algorithms using other
147 protocols or even other datasets.

148 2.3.3. *Biometric experimentation environment (BEE)*

149 The BEE distribution [14] is the test environment of the evaluation of face
150 recognitions systems in the Face Recognition Vendor Tests (FRVT2006). It is a
151 computational experimental environment which easily allows researchers to com-
152 pare their developed facial-based algorithms. The BEE distribution contains all
153 the data sets for performing and scoring the experiments. It also provide a PCA-
154 based method (known as BEE system) that has been optimized for large-scale
155 problems as a baseline algorithm, which applies the whitened cosine similarity
156 measure. An example of its use to compare face recognition systems in given in
157 [19]. The BEE framework returns three kinds of ROC curves as a performance
158 measure, corresponding to images collected within semesters, within a year, and
159 between semesters, respectively. The BEE system is a useful framework to com-
160 pare face recognition systems. However, BEE do not resolve the computation
161 complexity of performance metrics, which is considered as a main drawback in
162 biometrics research field. Towards resolving this problematic, we present in the
163 next section a distributed computation platform of performance metrics.

164 **3. Computation EvaBio platform**

165 *3.1. Proposed platform*

166 The Computation EvaBio Platform started its development in February
167 2009. Its goal is to provide a low cost, scalable, adaptable, modalities inde-
168 pendent and development tools independent platform dedicated to biometric
169 computation. The main idea is to use the unexploited calculation power of ex-
170 isting computer pool in a research laboratory.

171

172 The interest for the researcher is to focus only on his/her algorithm as-
173 suming small development constraints. The main constraint is to develop a
174 full autonomous application or script (without any interaction or IHM) dealing
175 with an atomic computation task. The global vision of the different calculation
176 steps is defined in the *Computation Task List*, within an XML file. Each task
177 defined in this file describes a computation task to be done on the laboratory
178 computers. The server is in charge of the repartition of the different computa-
179 tion tasks. Figure 4 shows the present architecture (v0.5). It is composed of
180 four parts, the server and the distribution process (presented by Mahier et al.
181 in [20]), the administration client and the computation task list generation, the
182 atomic algorithm creation and deployment, the dataset access and the different
183 biometrics dataset abstraction.

184 *3.2. Biometric datasets modeling*

185 We present in this section an original meta model suitable for any biometric
186 dataset, we choose to perform a modeling of four publicly available datasets. It
187 will allow us to be able to launch a performance evaluation scenario described
188 by this meta model. We choose to use the Merise method [21] for modeling
189 four existing biometric datasets. It is a modeling methodology for the develop-
190 ment of information systems, which is well suited for the dataset modeling. By
191 analysing existing benchmarks in biometrics (AR, Poly U FKP, FERET and
192 GREYC-Kesytroke, *etc.*), we can extract some tables that are general for all

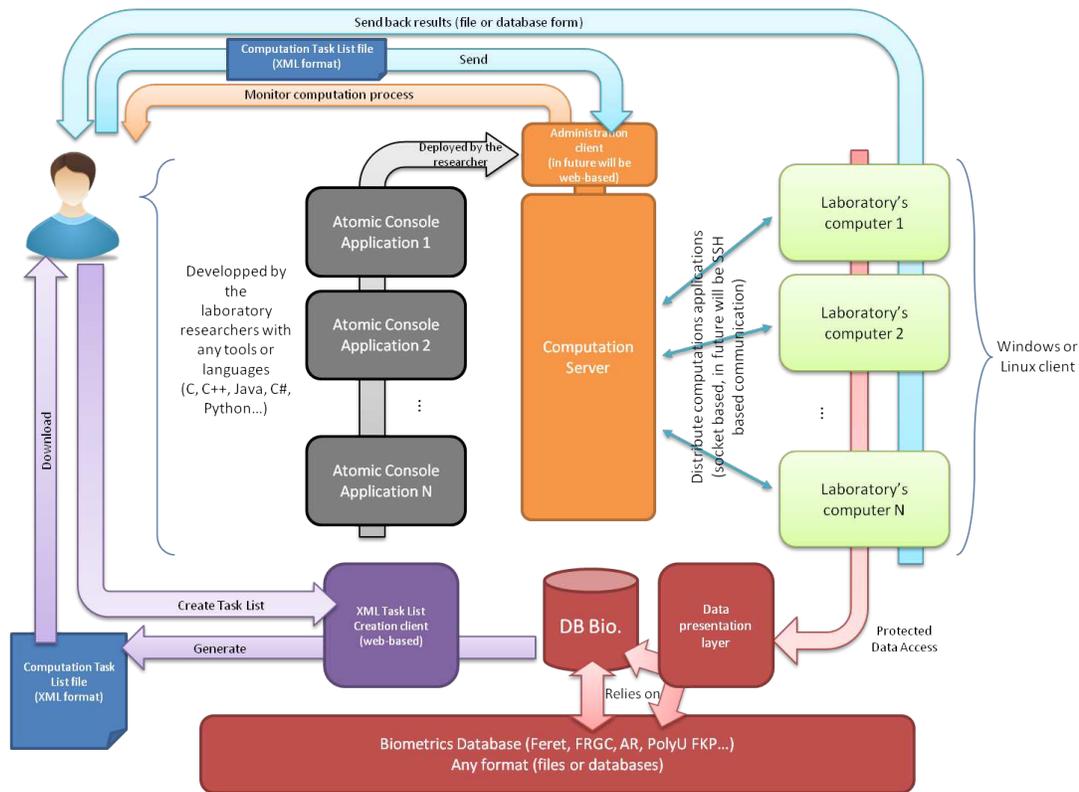


Figure 4: Computing EvaBio Platform Architecture

193 biometric datasets. We also had to add some tables specific in order to be able
 194 to manage several datasets. The obtained modeling can be seen at figure 5. The
 195 two top tables *Dataset* and *Modality* corresponds to specific tables we added
 196 to manage different biometric dataset. The *modalityDesc* field of the *Modality*
 197 corresponds to the used modality such as “face”, “keystroke” and so on. It
 198 is linked to the *Dataset* table, where we store the name of the dataset and a
 199 short description. Next, we find the *Individual* table which contains data about
 200 individuals present in a dataset. It is limited to an *individualNumber*, which
 201 reflects the number of the individual in the dataset, and its gender. We add an
 202 *externalID* as a foreign key to a table with more details about this individual,
 203 such as first name, last name or date of birth. This table is not included in the

204 model for anonymity reasons, but the externalID can still be used to retrieve the
205 same individual in several dataset, which can be useful for multi-modality bio-
206 metrics. Finally, an active field can be used to deactivate an individual if needed.

207

208 An individual is linked to several sessions, stored in the *Session* table, via
209 the *perform* table. The sessionID field is thus unique for each individual/session
210 number, and can be associated to a date. These tables are associated to the
211 table *BiometricData*, which contains information relative to the biometric sam-
212 ple. The data field is a link to the biometric sample and metaData can be
213 used to store an additional information about biometric data, such as the used
214 password for a keystroke dynamics biometric sample. The success field can be
215 necessary to compute failure to enroll rate. The addInformation field is a link
216 to additional data provided with some datasets, such as localization of eyes for
217 face ones. A biometric sample is also related to the *Sensor* table, so we can
218 manage several capture devices such as different keyboards or cameras.

219

220 Finally, we choose to add some specific information on each dataset in the
221 *Type* table. This table contains information about the type of data contained
222 in the dataset, such as the resolution of images, in an XML format. Thus, we
223 add the *XSL* table, which will contain the information about the XML format of
224 the *Type* table. In case we want to add a new biometric modality in this model,
225 we only have to add a new XSL entry and keep this model intact.

226 3.3. Use case

227 A researcher, named Paul, focus his work on a new face biometric algorithm.
228 He first has to implement his algorithm for one data sample from one person
229 (independently of the dataset and less coupled with the data format). To help
230 him to code accurately, the platform provides design application templates on
231 different languages. The different parameters of the algorithm will be passed
232 as application arguments. When Paul succeeds in developing his basic console
233 application, he will have to define the computation procedure, meaning to define

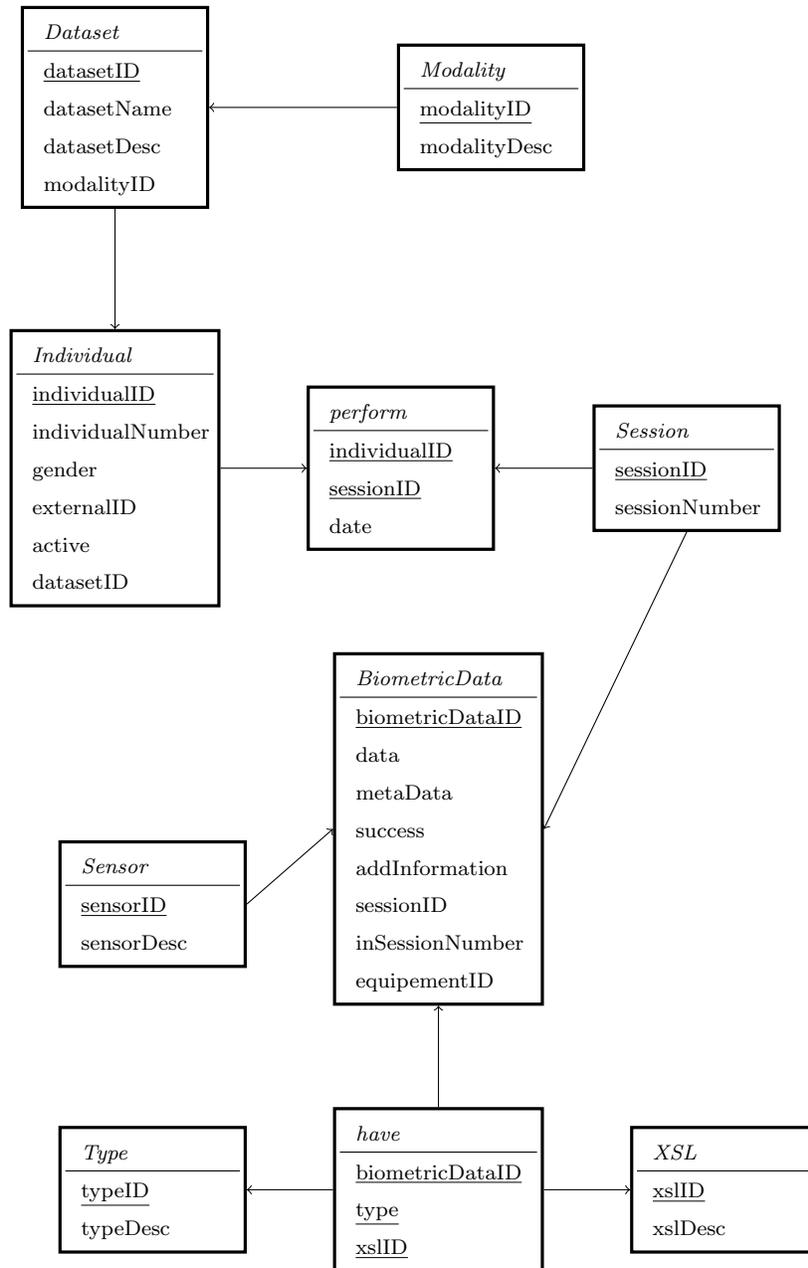


Figure 5: Meta-Model of a biometric dataset

234 the XML Computation Task List as depicted in table 1. This task list describes
 235 all the parameters of Paul's application will need to compute an atomic dataset.
 236 Finally, through the administration interface (see figure 6), Paul can launch its
 237 algorithm on all the predefined laboratory computers. The results are retrieved
 238 on a database or within a shared file on the network. Two weeks later, Paul
 239 need to replay some computations on another Biometric dataset. He just has
 240 to create the appropriate XML file and to launch the computation process.

```

<TaskPools>
  <TaskPool>
    <Task>
      <ExecutionCommand> ... </ ExecutionCommand>
      <ParameterList>
        <Parameter> ... </ Parameter>
      </ ParameterList>
    </ Task>
  </ TaskPool>
</ TaskPools>
  
```

Table 1: An XML Computation Task List description

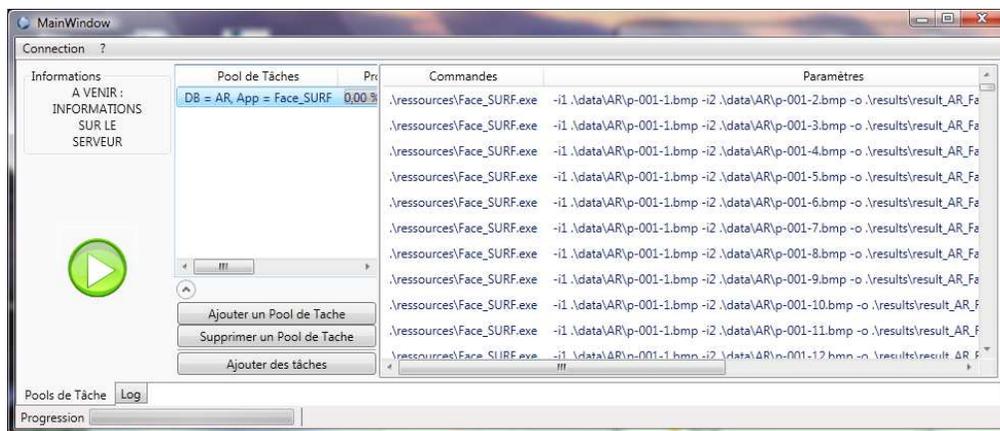


Figure 6: Administration interface

241 *3.4. Discussion*

242 The main interest of this solution is based on the biometric data definition
243 format (the meta-model). Given the abstraction of the biometric data, the
244 researcher focuses only on his algorithm and asks the platform to compute the
245 preselected computation tasks. The abstraction enables a pre-selection from
246 one part of a single dataset (for example only women and illumination altered
247 samples of the AR dataset) to multiple parts of multiple datasets (for example
248 only men of the AR and Feret datasets). The key point is on the tool which
249 allows the researcher to question the meta-biometric-dataset and generates the
250 XML task list. This tool will be presented in another paper.

251 **4. Results**

252 We present in this section some results of the computing EvaBio platform.
253 First, we present how an existing biometric dataset can be fitted into the pro-
254 posed model. Then, we present some results from the existing distributed com-
255 putation tool.

256 *4.1. Fitting existing datasets*

257 *4.1.1. PolyU FKP dataset*

258 The PolyU FKP images were collected from 165 volunteers (125 men and 40
259 women). Among them, 143 subjects were 20 to 30 years old and the others were
260 30 to 50. The images have been taken in two different sessions. In each session,
261 the subject has provided 6 images for the right index finger, for the right middle
262 finger, the left index finger and the left middle finger. There are therefore 48
263 pictures, from the 4 fingers from each person. In total, the dataset contains
264 7,920 images from 660 fingers. The interval average time between the first and
265 second session is 25 days. The maximum interval and minimum were 96 days
266 and 14 days respectively. The dataset consists of several files. Each file is writ-
267 ten in a folder named as “nnn.fingertype”: nnn represents the identity of the
268 person and fingertype can be left index, right index, left middle or right middle.

269 Each of these folders contains 12 pictures, from 01 to 06 belong to session 1 and
270 07 to 12 belong to the session 2. There is actually two datasets. The dataset
271 “FKP Database.zip” contains the original images and the “FKP ROI.zip” one
272 contains region of interest pictures [22]. However, the construction of the two
273 datasets is the same, and only the filename name changed, “ROI” being added
274 at the end of the filename for the ROI dataset. An example of these datasets
275 can be found in figure 7.

276

277 We present in figure 8 how the PolyU FKP dataset fits the meta-model.
278 We can see that the Poly U FKP fits well with this meta model. Some fields
279 cannot be completed such as the date where an individual performs a session.
280 Moreover, some fields have default value for publicly available datasets such as
281 the activate field of the *Individual* table, which is set to true. Apart from theses
282 fields, we can see that other fields are filled with data related to the biomet-
283 ric sample. Some specific data related to a dataset can also be stored in the
284 database. For example, the height and with of the images from the Poly U FKP
285 dataset can be stored in the XML field of the *Type* table.

286

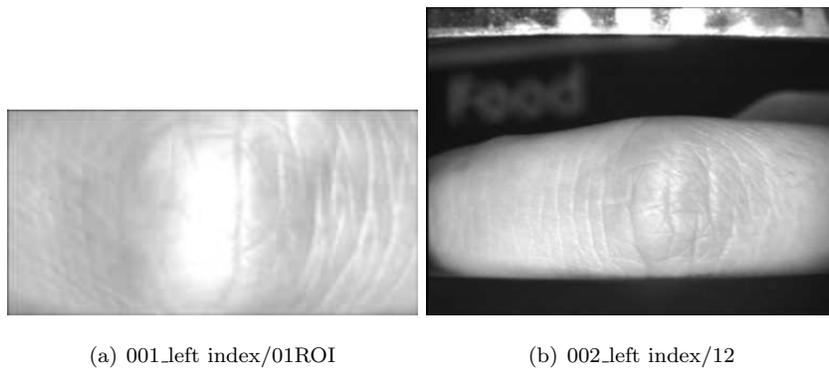


Figure 7: Two biometric samples from the PolyU FKP datasets

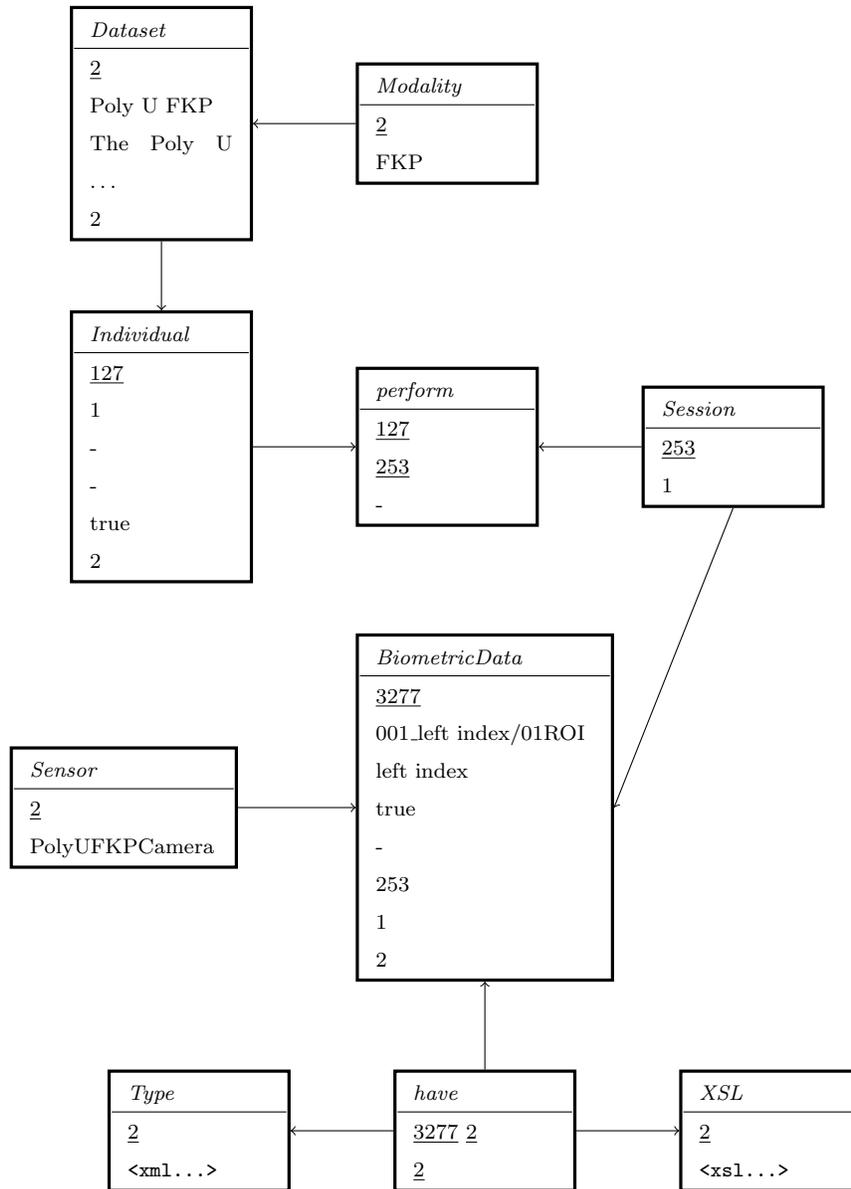


Figure 8: Application of the meta model to the FKP dataset

287 *4.1.2. AR face dataset*

288 The AR dataset contains over 4,000 color images, acquired with the same
 289 system, corresponding to 126 different faces (70 men and 56 women). The

290 images were taken from the front with various facial expressions, lighting con-
291 ditions varied, and sometimes with sunglasses or a scarf. Also, no restrictions
292 on clothing (clothes, glasses, *etc.*), makeup, and hair cut was imposed on par-
293 ticipants. Each person has participated in two sessions, separated by 14 days.
294 The same images were taken in both sessions. All image are in the same folder,
295 and only the file name enable distinguishing biometric data. The name of the
296 images is built this way “x-nnn-mm.jpg”: x can take the value m or f (male or
297 female), nnn identifies the person (can range from 001 to 070 for male and 001
298 to 056 for female) and mm identifies the session and the expression (01 to 26).
299 Examples of such images are presented in figure 9.

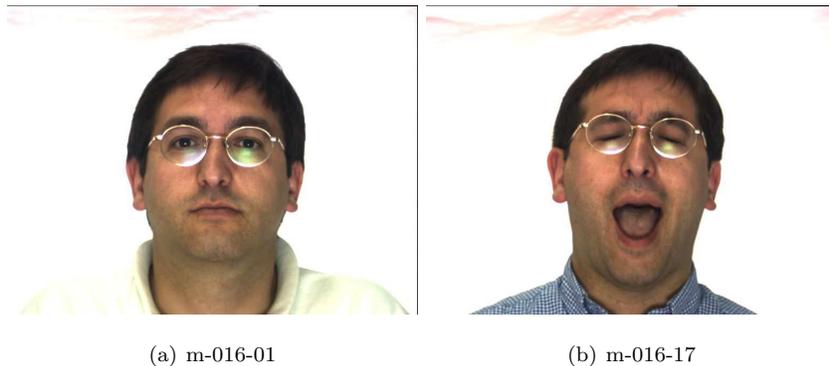


Figure 9: Two biometric samples from the AR face dataset

300 Similarly to the Poly U FKP dataset, we present in figure 10 how the meta-
301 model can be used to represent biometric data from the AR face dataset. We
302 can see that the AR face dataset fits well the meta-model. We still have some
303 fields that cannot be completed, but most of them are. We can also see that it
304 is simple to create requests on this database. For example, if we want only male
305 individuals from the AR dataset, we can create a SQL request containing two
306 conditions such as `Individual.gender=male` and `Dataset.datasetName=AR`.
307 Moreover, as the same model is applied, we can use the same SQL requests for
308 both datasets. This clearly shows the interest of this meta model.

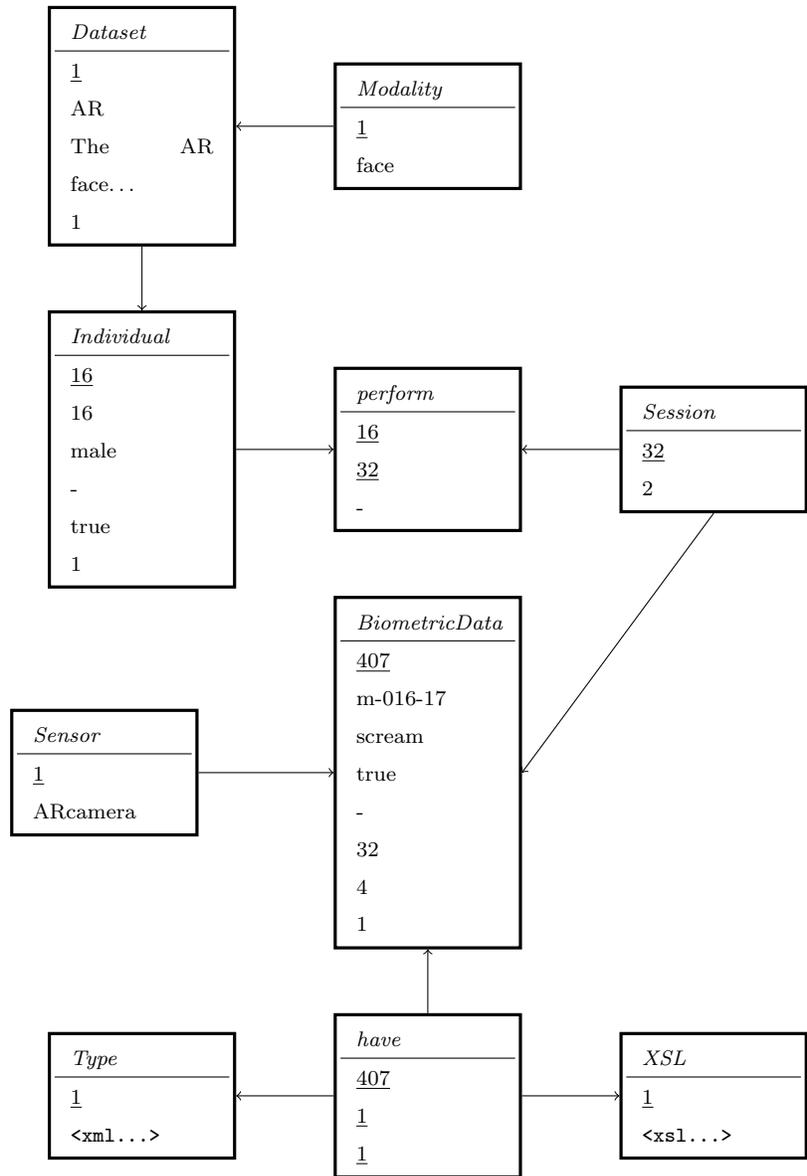


Figure 10: Application of the meta model to the AR dataset

309 4.2. Distributed computing

In order to show the efficiency of the distributed computing part of the EvaBio platform, we present the time gain provided by this platform using a

face verification algorithm based on SURF descriptor [23]. The used verification algorithm is a single-based enrollment. The comparison of two face images is considered as the comparison of two sets of keypoints detected from each image. Each SURF keypoint is characterized by a vector in 64 dimensions. The matching similarity principle is presented in previous works [24]. The matching between two images im_1 and im_2 corresponds to compute a similarity between two sets of features $X(im_1)$ and $X(im_2)$. We thus use the following matching method which is a modified version of a decision criterion first proposed by Lowe [25]. Given two keypoints $x \in X(im_1)$ and $y \in X(im_2)$, we say that x is associated to y iff:

$$d(x, y) = \min_{\{z \in X(im_2)\}} d(x, z) \text{ and } d(x, y) \leq C d(x, y') \quad (1)$$

where C is an arbitrary threshold, $d(\cdot, \cdot)$ denotes the Euclidean distance between the SIFT descriptors and y' denotes any point of $X(im_2)$ whose distance to x is minimal but greater than $d(x, y)$:

$$d(x, y') = \min_{\{z \in X(im_2), d(x, z) > d(x, y)\}} d(x, z) \quad (2)$$

310 In other words, x is associated to y if y is the closest point from x in $X(im_2)$
 311 according to the Euclidean distance between SIFT descriptors and if the second
 312 smallest value of this distance $d(x, y')$ is significantly greater than $d(x, y)$. The
 313 significance of the necessary gap between $d(x, y)$ and $d(x, y')$ is encoded by the
 314 constant C . Then, we consider that keypoint x is matched to y iff x is associated
 315 to y and y is associated to x . An example of a genuine and an impostor match-
 316 ing result is given in 11(a) and 11(b), respectively. The number of associations
 317 is used here as a similarity measure.

318

319 This experiment represents the computation required for 30 individuals from
 320 the AR face dataset, and thus, 900 task were present in an XML file. For a 26
 321 samples per individual, the definition of the FRR requires 750 comparisons and
 322 for the FAR 22620 ones. To do so, we used different numbers of clients to realize
 323 this computation tasks (some are present on the same computer). Results are

324 presented in table 2. For the two lines with local, the server and client were
 325 on the same computer, and thus does not require any network communication.
 326 For lines with a $n + n$, it means that two clients were used on n computer in
 327 order to benefit from the dual processor of computers. We can see that using
 328 two clients (line 1+1) on the same computer increases the performance. This is
 329 due to the fact that the computer used is a dual core processor and each task
 330 is single threaded. We can see that using as few as 3 computers is enough to
 331 clearly reduce the computation time.

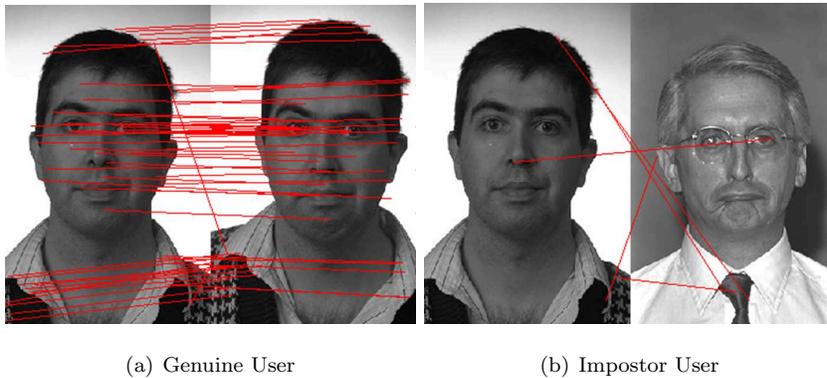


Figure 11: Face verification attempts using SURF descriptor: red lines correspond to a match between two associated keypoints

Number of clients	Time
1 (Local)	57m39s
1+1 (Local)	30m01s
1	70m27s
2	51m07s
3	32m19s
4	25m48s
4+4	14m07s

Table 2: Computation time results for different number of clients.

332 **5. Conclusion and perspectives**

333 We proposed in this paper a new platform dedicated to researchers and en-
334 gineers in the field of biometrics to develop new algorithms. The computing
335 EvaBio platform permits to launch on different clients some computation tasks
336 to quantify the performance of an algorithm in biometrics. A meta model has
337 also been proposed to characterize a dataset and to facilitate the creation of
338 benchmark and complex scenarios. This meta-model can be used to store the
339 data related to users and biometric sample acquisitions for any biometric modal-
340 ity. It aims to ease the relation between biometric samples and data related to
341 these samples. Thus, a single database, using this meta model, allow researchers
342 to have a single access point for each biometric benchmark stored in it.

343

344 We plan to use this model in a platform dedicated to performance evalu-
345 ation. This tool, containing a distributed computation tool, enables an easy
346 performance evaluation system. The perspective of this work is to create a tool
347 that will enable to easily create the XML file containing the difference compu-
348 tation tasks, used by the distributed computation tool. This tasks list creation
349 tool will rely on this meta-model to have a unique access point to all kind of
350 biometric datasets. We plan to provide this tool for the research community in
351 biometrics.

352 **Acknowledgements**

353 The authors would like to thank the French Research Ministry for their
354 financial support of this work.

355 **References**

- 356 [1] A. K. Jain, L. Hong, S. Pankanti, R. Bolle, An identity-authentication
357 system using fingerprints, Proceedings of the IEEE 85 (9) (1997) 1365–
358 1388.

- 359 [2] R. Wildes, J. Asmuth, G. Green, S. Hsu, R. Kolczynski, J. Matey,
360 S. McBride, A system for automated iris recognition, in: IEEE Workshop
361 on Applications of Computer Vision (WACV'94), 1994, pp. 121–128.
- 362 [3] R. Giot, M. El-Abed, C. Rosenberger, Keystroke dynamics with low con-
363 straints svm based passphrase enrollment, in: IEEE Third International
364 Conference on Biometrics : Theory, Applications and Systems (BTAS'09),
365 2009, pp. 1–6.
- 366 [4] S. Sarkar, P. J. Phillips, Z. Liu, I. R. Vega, P. Grother, K. W. Bowyer, The
367 humanID gait challenge problem: data sets, performance, and analysis,
368 IEEE Transactions on Pattern Analysis and Machine Intelligence 27 (2005)
369 162–177.
- 370 [5] A. Kumar, C. Ravikanth, Personal authentication using finger knuckle sur-
371 face, IEEE Transactions on Information Forensics and Security 4 (2009) 98
372 – 110.
- 373 [6] ISO/IEC 19795-1, Information technology – biometric performance testing
374 and reporting – part 1: Principles and framework (2006).
- 375 [7] S. Benjio, J. Mariethoz, M. Keller, The expected performance curve, in:
376 In Proceedings of the 22nd International Conference on Machine Learning,
377 2005, pp. 9 – 16.
- 378 [8] Polyu fkp database, [http://www.comp.polyu.edu.hk/~biometrics/FKP.](http://www.comp.polyu.edu.hk/~biometrics/FKP.htm)
379 [htm.](http://www.comp.polyu.edu.hk/~biometrics/FKP.htm)
- 380 [9] R. Giot, M. El-Abed, C. Rosenberger, Greyc keystroke : a benchmark
381 for keystroke dynamics biometric systems, in: IEEE Third International
382 Conference on Biometrics : Theory, Applications and Systems (BTAS),
383 2009.
- 384 [10] U. of Essex, Faces94 database, face recognition data (1994).
385 URL <http://cswww.essex.ac.uk/mv/allfaces/faces94.html>

- 386 [11] A. Martinez, R. Benavente, The ar face database, Tech. rep., CVC Techni-
387 cal Report 24 (1998).
- 388 [12] P. Phillips, H. Wechsler, J. Huang, P. Rauss, The FERET database and
389 evaluation procedure for face recognition algorithms, *Journal of Image and*
390 *Vision Computing* 16 (5) (1998) 295–306.
- 391 [13] J. P. Phillips, H. Moon, S. A. Rizvi, P. J. Rauss, The FERET evalua-
392 tion methodology for face-recognition algorithms, *IEEE Transactions on*
393 *Pattern Analysis and Machine Intelligence* 22 (2000) 1090–1104.
- 394 [14] P. Phillips, P. Flynn, T. Scruggs, K. Bowyer, J. Chang, K. Hoffman, J. Mar-
395 ques, J. Min, W. Worek, Overview of the face recognition grand challenge,
396 in: *Proceedings of the 2005 IEEE Computer Society Conference on Com-*
397 *puter Vision and Pattern Recognition (CVPR'05)*, Vol. 1, 2005, pp. 947–
398 954.
- 399 [15] K. Messer, J. Matas, J. Kittler, J. Luettin, G. Maitre, XM2VTSDB:
400 The Extended M2VTS Database, in: *Second International Conference*
401 *on Audio- and video-based Biometric Person Authentication (AVBPA'99)*,
402 1999, pp. 72–77.
- 403 [16] V. Popovici, J. Thiran, E. Bailly-Bailliere, S. Bengio, F. B. M. Hamouz,
404 J. Kittler, J. Mariethoz, J. Matas, K. M. B. Ruiz, F. Poiree, The BANCA
405 database and evaluation protocol, in: *4th International Conference on*
406 *Audio- and Video-Based Biometric Person Authentication*, Guildford, UK,
407 Vol. 2688, 2003, pp. 625–638.
- 408 [17] Biosecure Multimodal Biometric Database, <http://www.biosecure.info/>
409 (2008).
- 410 [18] P. N. Belhumeur, J. P. Hespanha, D. J. Kriegman, Eigenfaces vs. fisher-
411 faces: Recognition using class specific linear projection, *IEEE Transactions*
412 *on Pattern Analysis and Machine Intelligence (PAMI)* (1997) 711–720.

- 413 [19] J. Yang, C. Liu, Horizontal and vertical 2dpca-based discriminant analysis
414 for face verification on a large-scale database, *IEEE Trans. o 2 (4)* (2007)
415 781–792.
- 416 [20] J. Mahier, M. El-Abed, B. Hemery, C. Rosenberger, Toward a distributed
417 benchmarking tool for biometrics, in: In *IEEE International Conference*
418 *on High Performance Computing & Simulation (HPCS'11)*, 2011, pp. 1–6,
419 supplied as additional material [Article_hpbench.pdf](#).
- 420 [21] D. Avison, Merise: A european methodology for developing information
421 systems, *European Journal of Information Systems* 1 (3) (1991) 183–192.
- 422 [22] L. Zhang, L. Zhang, D. Zhang, Finger-knuckle-print: a new biometric iden-
423 tifier, in: *Proceedings of the IEEE International Conference on Image Pro-*
424 *cessing*, 2009, pp. 1981–1984.
- 425 [23] H. Bay, A. Ess, T. Tuytelaars, L. V. Gool, Surf: Speeded up robust features,
426 *Computer Vision and Image Understanding (CVIU)* 110 (2008) 346–359.
- 427 [24] B. Hemery, J.-J. Schwartzman, C. Rosenberger, Study on color spaces for
428 single image enrolment face authentication, in: *IAPR International Con-*
429 *ference on Pattern Recognition (ICPR)*, 2010, pp. 1249–1252.
- 430 [25] D. G. Lowe, Distinctive image features from scale-invariant keypoints, *Int.*
431 *J. Comput. Vision* 60 (2004) 91 – 110.