GREYC Keystroke: a Benchmark for Keystroke Dynamics Biometric Systems

Romain Giot, Mohamad El-Abed, Christophe Rosenberger

GREYC Keystroke: a Benchmark for Keystroke Dynamics Biometric Systems

Romain Giot Mohamad El-Abed Christophe Rosenberger
GREYC Laboratory, ENSICAEN - Université de Caen, Basse-Normandie - CNRS
romain.giot@ensicaen.fr, {melabed,christophe.rosenberger}@greyc.ensicaen.fr

***Abstract*— Even if the market penetration rate of biometric technologies is still far below its potential, many biometric systems are used in our daily real-life. One of the main reasons to its low proliferation is the lack of a generic and complete approach that quantifies the performance of biometric systems taking into account individuals' perception among the process. Among all the existing biometric modalities, authentication systems based on keystroke dynamics are particularly interesting. Many researchers proposed in the last decades some algorithms to increase the efficiency of this approach. Nevertheless, none significant benchmark is available and commonly used in the state of the art to compare them by using a similar and rigorous protocol. We propose in this paper: a benchmark testing suite composed of a database and a software that are available for the scientific community for the evaluation of keystroke dynamics based systems. Performance evaluation of various keystroke dynamics methods tested on the database is available in [1].**

I. Introduction

Authentication systems allow entities to access to controlled resources. Traditionally, individuals are used to authenticate themselves on computers by using a classical couple of *login* and *password*. This scheme suffers of various problems decreasing its security [2]. *Strong authentication* has for objective to use multiple authenticators for security purposes. In this case: individuals are authenticated with the help of (i) what *they are*, or *what they are able to do*, (ii) what *they know*, (iii) and what *they own*.

Keystroke dynamics is one strong authentication method combining the two first authenticators. Its main interest is the fact that it is considered as *invisible*, because an individual already uses a password to connect on computers. Several kinds of keystroke dynamics systems exist in the literature and they are generally based on *very long texts*, *password* or *pass phrases*. The biometric template can be captured *statically* or *continuously* (i.e. at login phase or during computer usage). In this paper, we are interested on static authentication with passwords or pass phrases. We argue on the fact that most of the results presented in studies in the state of the art cannot be compared together due to various reasons presented in this paper. In order to contribute to solve this problem, we propose a benchmark testing suite to be used as a reference database in further keystroke dynamics studies.

ENSICAEN, 6 Boulevard Maréchal Juin, 14000 Caen Cedex - France

The document is organized as follows: in the first part, we present the *state of the art* of the general *evaluation* of biometric systems, common benchmark *databases* and *keystroke dynamics systems*. In the second part, we present the main reasons that explain why it is really *difficult to make a comparison* between the different implemented systems based on keystroke dynamics. The third part of this paper emphasises on some facts to solve these problems and present our *contribution*.

II. Evaluation Of Biometric Systems

A. General Methodologies

In order to compare different biometric systems (for the same modality or different ones), it is necessary to evaluate them. Many works have already been done on the evaluation of biometric systems [3], [4], and the purpose of this part is to present the general methodologies in the state of the art. For the evaluation of a biometric system, there are three main points to consider:

- the *performance*: it has for objective to measure various statistical figures on the performance of the system (*EER*, *FTE*, *FTA*, computation time, *ROC* curves, ... [4]);
- the *acceptability*: it gives some information, not on the performances in terms of errors of the system, but on the individuals' *perception* and *acceptance*;
- the *security*: it quantifies how the system is secure (i.e. if many *frauds* can be used by an impostor).

All these evaluation approaches have to be taken into account when comparing various biometrics systems. It seems strange to consider a system to be good if it has very low error rates (i.e. very good performance) while having a very low user acceptance (i.e. a high probability to be unused). Comparing biometric systems can be realized within three contexts [5] :

- the *technological evaluation*: the system is tested in an off-line way by using a well defined database. By this way, the results are always reproducible.
- the *scenario evaluation*: the tests are done in an implementation of the system (i.e. on-line) with a defined protocol. The results may not be reproducible.
- the *operational evaluation*: the tests are done with a real panel of individuals in an operational way. The results

are not reproducible, but give a good representation of the usability of the system.

The first evaluation context needs a benchmark database to compute the performance of a biometric system, we focus on this point in the next section.

B. Biometric Databases

Most of the biometric modalities have common public benchmark databases [6]. The aim of these databases is to allow researchers to work on the same data, which allows them to compare their algorithms in the same context. Creating a database is not an easy task because it requires a lot of *time*, *energy* and sometimes some *specific materials*. That is why such common databases are interesting, because researchers who cannot create one (for various reasons), can download one and work on it. By this way, more researchers are able to work on the subject and improve it. Two kinds of database can be found:

- the *real* databases: which consist of real collected data, and are difficult and time consuming to build;
- *synthetic* databases: which are constituted of artificial data simulating real biometric data, and are quick and easy to create. Very few biometric modalities are concerned [7].

The most commonly used databases are *FERET* [8], *UBIRIS* [9], *SFinGe* [7] based databases, *XM2VTSDB* [10], *BANCA* [11], *BIOSECURE* [12]. The aim of *FERET* is to quantify facial recognition performances. Data were collected on 1199 individuals during several sessions between 1993 and 1996. *UBIRIS* are two databases created to quantify the performances of iris recognition. For the first version, 1877 images were collected in two sessions in 2004. *SFinGe* is a tool for the generation of synthetic fingerprint images. The software is able to generate 100,000 realistic templates in about one day on a single computer. *XM2VTSDB* is a multi-modal database which aim is to test and evaluate vocal and facial (2D and 3D) recognition. 295 individuals participated during four months (one session per month) to the creation of the database. *BANCA* is also a multi-modal database captured in four languages (French, Italian, English and Spanish) for voice and face modalities. 12 sessions during 3 months involving 208 individuals were necessary. *BIOSECURE* is a multi-modal database where 11 universities were involved in its creation. The included modalities are face, voice, iris, fingerprint, hand geometry and signature dynamics. The data were collected during 2 sessions in different acquisition conditions (controlled, uncontrolled) and divided into three datasets (internet, desktop and mobile dataset).

In addition to these benchmarks, several competitions have also been created for the main modalities (i.e. *FVC* for the fingerprint, *FRVT* for the face recognition, *ICE* for the iris) [13], [14]. The main objective of these competitions is to compare biometric algorithms using a predefined database. We can see that they are large databases for the main modalities, but there exists none available to our knowledge for the keystroke dynamics. In the next section, we focus on keystroke dynamics based biometric systems.

III. Keystroke Dynamics

We discuss in this section the performance of keystroke dynamics algorithms from the state of the art. The first research work in this domain was realized in 1980 with the report of the *Rand Corporation* [15]. This study proves that individuals could be differentiated by considering their way of typing. Seven secretaries were asked to type three different long texts, and the comparison was done using *statistical methods*. A lot of studies have already be done on keystroke dynamics, in order to improve its performance [16], [17], [18], [19], [20], [21], [22].

1) Differences on the Acquisition Protocols: Most of the studies in the literature have used different protocols for their data acquisition, which is totally understandable due to the existence of different kinds of keystroke dynamics systems (static, continuous, dynamic) which of course necessitate different acquisition protocols. It is known that the performance of the algorithms can be dependant of the used database [22]. By using their own databases, researchers do not give a good overview of the global performance of their methods, but an overview in a specific case: the one represented by their database. In the keystroke dynamics research field, there is an important diversity of protocols used to collect the data. They differ on the *number of individuals* participating to the study, the *acknowledgement* of the password (which impacts on the speed typing, hesitation, and *FTA*), the use of *different computers* (which impacts on the timing accuracy), *different keyboards* (which impacts on the way of typing) or not, the *quantity* of collected data, the *duration* of the collection of the whole database, the *control* of the acquisition process (i.e. acquisition done behind the researcher who controls if it is done with respect to the protocol or made at home where none verification is possible), the use of *different* or *identical* passwords (which impacts on the quality of impostors' data) and so on. Table I illustrates some differences in the protocol of different studies by presenting the following information: duration of the protocol, number of individuals involved in the database and if it is a controlled acquisition.

2) Differences on the Objective Analysis: Many performance metrics can be used to analyse a biometric system. Most of the papers have used such kind of information to evaluate their algorithms and present their performances, but, most of the time, not all the information are presented. Distance-based algorithms and classification-based ones have not the same kind of output: a score which is continuous value or a class which is discrete value.The most important thing is when the *EER*, *FAR* and *FRR* values are presented in an article, they are computed with a database (which is also not available) with a certain number of templates used for the enrolment. It seems really impossible to compare a study using twenty vectors for the enrolment process with another using only five. In addition to the enrollment size, the degree of expertise of the volunteers has an impact on the illustrated performance results. The same argument can also be used when comparing research works using a global threshold, with others using per-user threshold. Table I presents the

number of vectors used for creating the enrolled template and the use of a global or individual threshold for some protocols of the literature.

3) User Acceptance: Usability is an important factor to be taken into account in order to evaluate a biometric system. It seems difficult in a research environment to systematically do such a thing, especially when a subjective evaluation has already been done on the modality in previous researches. But, by changing the procedures of acquisition and verification, several parameters may have been changed concerning, for example, the memory use or computational time, and, these modifications can alter the user's perception of the system (so, the user can consider the system more or less usable due to these modifications).

4) The Laboratory Environment: The problem of the laboratory environment is inherent to most of keystroke dynamics studies. Except very few studies, none realistic databases are used: the databases are not extracted from a real use. This can be easily understandable because individuals will not be agree to use their own passwords and share it with others playing impostors. For this reason, most of the passwords are *artificial* one generated differently all along the literature (i.e. dictionary words, aleatory combination of letters, numbers and symbols, and so on) and the individuals do not necessarily master their typing (because they do not daily use them, and, they do not choose them). In some controlled environment, individuals are in a quiet room without any inconveniences which do not fit the reality where we can authenticate on our machines and talking with other people or being in a noisy room. In an uncontrolled environment, nothing proves that all the typing patterns of a user have been done by this user with respect of the protocol.

IV. Contribution

Different databases of different quality have been used for all the research work. It is known that the results of the experiments can be highly dependent on the used database. The main interests of using a common database are to avoid researchers to take too much time for creating it, and to easily compare the performance of different algorithms with the same input data.

Hosseinzadeh and Krishnan have presented in [22] very interesting information on the way of creating a good keystroke dynamics database supposed to be used with specific confidence intervals. They applied their method for creating the database used in their paper, but, sadly, did not make it available. In [5], we argue that to create a good behavioural biometric database the number of required sessions have to be superior or equal to three, that these sessions must be spaced in time, the population must be large and diversified. These requirements were not always fit in previous researches.

A. Overview Of GREYC-Keystroke

GREYC-Keystroke is a software we developed allowing the creation of a keystroke dynamics database and is downloadable at the following address: `http://www.ecole.ensicaen.fr/~rosenber/keystroke.html`. A screen capture of the application is available in Fig. 1. We developed this application in order to create our own keystroke dynamics database, and share it in order to allow other researchers to create their own databases. The idea is that researchers who used this software to create a new database are requested to send us an anonymous version in order to make it available for everybody. The data are stored in an sqlite file which allows quickly and easily the extraction of specific information, thanks to SQL (Structured Query Language) queries. Database tables are presented in Fig. 2.

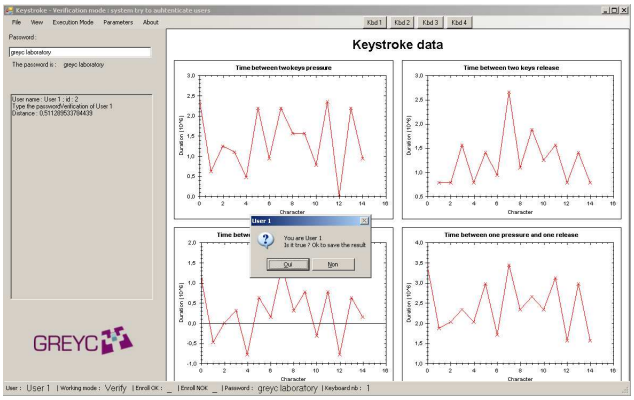

Fig. 1. Screenshot of the database collecting tool

The functionalities of the software application are the followings:

- possibility to *change the attended password*, the default one is "greyc laboratory". Each user is able to type different passwords, a model is created for each one;
- possibility to *add a new user* to the database. The individuals are stored in the table called $individuals$;
- possibility for the user to *train* himself to type the password, the data are not saved, but timing information are displayed on screen with curves representing extracted features;
- possibility to *show the mean vector* of one user (useful to visually compare with mean vector of other individuals, or with the typing of the actual user);
- *capturing the typing information* of a user. *Raw* and *extracted data* are added to the database and stored in the table $keystroke\_datas$ and $keystroke\_typing$;
- during the capture process, the *number of typing mistakes* is counted and added to the database. This information gives the *FTA* of the database and can be useful for the evaluation and is computed with the information in the tables $keystroke\_typing$;
- when a user has five captured vectors, he can try a *verification*. The method used is presented in [19] and returns a matching score compared to a threshold (hard-coded in the application, which can be incorrect for another password or database). The following equation

TABLE I

SUMMARY OF THE PROTOCOLS USED FOR DIFFERENT STUDIES IN THE STATE OF THE ART. THE INFORMATION PRESENTED ARE THE AUTHORS, THE TOTAL ACQUISITION TIME OF THE DATABASE, THE NUMBER OF INVOLVED INDIVIDUALS,IF IT IS A CONTROLLED ACQUISITION OR NOT, GLOBAL OR ADAPTIVE THRESHOLD AND THE *FAR* AND *FRR* OF THE SYSTEM. "??" INDICATES THAT NO INFORMATION IS PROVIDED IN THE ARTICLE.

Paper	**Duration**	**Individuals**	**Enrollment**	**Acquisition**	**Global threshold**	***FAR***	***FRR***
Obaidat and Sadoun [17]	8 weeks	15	112	no	no	0%	0%
Bleha *et al.* [16]	8 weeks	36	30	yes	yes	2.8%	8.1%
Rodriguez *et al.* [20]	4 sessions	20	30	??	no	3.6%	3.6%
Hocquet *et al.* [19]	??	38	??	??	no	1.7%	2.1%
Revett *et al.* [21]	14 days	30	10	??	no	0.15%	0.2%
Hosseinzadeh and Krishnan [22]	??	41	30	no	no	4.3%	4.8%

represents the way to compute the score:

$$score \;=\; 1 \;-\; \frac{1}{n}\sum_{i=1}^{n} exp\left(-\frac{|v_i - \mu_i|}{\sigma_i}\right) \qquad (1)$$

with μ and σ respectively the mean and standard deviation vectors of size n of the enrolled timing vectors of the claimed user, and v the test vector. The EER of this method, is about 10% with the database;

- it is also possible to indicate the *change of keyboard* in order to test typing evolution depending of this parameter (this information is not taken into account during the verification process of the application);
- as in most of static keystroke dynamics studies, *typing correction is not allowed*, when a user does a mistake, he has to type again the password.

Both raw and extracted features are saved in the database. For any keystroke capture, the captured data are the (i) code of the key, (ii) the type of event (press or release), and (iii) the time of the event. All this information is stored in the $keystroke\_datas$ table in the fields $rawPress$ and $rawRelease$, for respectively press and release events, for each keystroke typing of an entire and correctly typed password. The data are saved following this scheme: code of the key, followed by a space, followed by the timestamp of the event, followed by a new line and so on, for each events. The interest of storing these raw data, is to permit other researchers to create their own feature extracted data if our data does not fit their requirements.The extracted data features stored in the database are the timing differences between two events of these kinds: press/press, release/release, press/release and release/press, an additional vector resulting of the concatenation of the previous ones and the total typing timing of the password. They are stored in the fields $ppTime$, $rrTime$, $prTime$, $rpTime$ and $vector$ of the table $keystroke\_datas$ and $time\_to\_type$ of the table $keystroke\_typing$. As the ordering is based on time and not key code, these data do not match exactly to duration and latencies of keys.

B. Overview of the Database α

1) Presentation: We have created a meaningful keystroke dynamics database with the help of *GREYC-Keystroke* software which is also downloadable on our website. We have

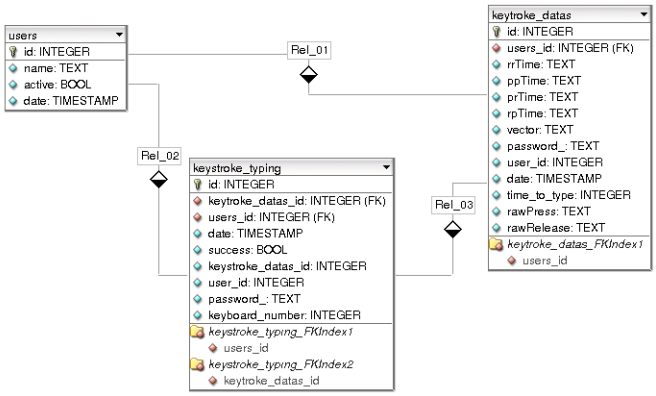

Fig. 2. Keystroke database representation

respected constraints presented in [5] on the way of creating good behavioural biometrics databases (in term of number of sessions, duration between each session, number of individuals and so on). Most of the population composing the database is composed of researchers in computer science, secretaries, students in computer science or in chemistry. There are different kinds of typists: fast, slow, two fingers, all the fingers, etc.

Our idea is to make it publicly available in order to be used as a reference database for testing keystroke dynamics algorithms and facilitate the comparison of previous and future keystroke dynamics authentication methods. For the moment, 133 individuals have participated to the capture process by typing between 5 and 107 times the password "greyc laboratory" between 03/18/2009 and 07/05/2009. We have 7555 available captures, and the average number of acquisitions per user is 51 with 100 of them having more than 60 templates. Most of the individuals participated at least to 5 sessions.

Referring to the information presented in Table I, we can say that it is a quite huge database, collected on a reasonable period. The individuals were asked to participate to one session every week (few of them have done two sessions within a week due to time constraints). We can see that a very few of them, really participate on all the sessions by considering the number of available templates. Two keyboards (the original keyboard of the laptop, and an

usb one plugged on the laptop) were used to verify if the model is only dependent on a user or if it is dependent on both user and keyboard. That is why, during each session, individuals were asked to type six times on each keyboard the password by alternating a typing from a keyboard to another. By using the first keyboard, then the second, then the first and so on, the individuals were obliged to move their hand (and sometimes, keyboard, computer or chair) before typing the next password which avoids the problem of mechanical typing of too similar patterns.

During the first session, the individuals were able to train themselves on the typing of the password on the two keyboards as long as they wanted, because it is not their usual password and do not already have typing habits and pattern for it. For the following sessions, they were not authorized to train, but have to directly register their typing events.

2) Analysis: As we have already done in a previous study [23], we have proposed to volunteers to answer questions about their feeling on such systems [1]. 100 volunteers have answered to it, their age and gender are presented in the Fig. 3. Even if all the database is not represented, it gives a good overview of it.

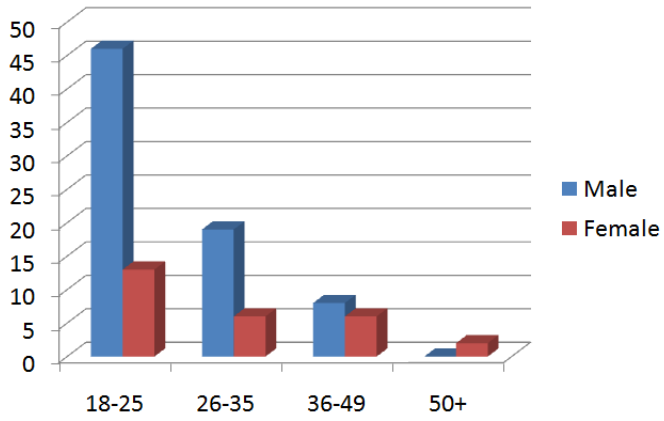

Fig. 3. Diversity of the population who answered the questionnaire (100 out of 133).

In the case of the static keystroke dynamics authentication, there is a quite huge number of failures during acquisitions. These failures are due to the fact that no mistake is allowed while typing the password: a typing mistake imposes to type the password from scratch. It is an interesting thing to analyse the reasons of these mistakes. The number of errors during acquisition is very important for this modality. Fig. 4 presents the quantity of captures done by each user by separating the correct (in red) and the erroneous ones (in yellow). The number of mistakes is quite huge for most of the volunteers. Its average rate is about 20%: one input out of five is incorrect due to typing mistakes.

These mistakes are due to several reasons :

[1]The lack of space does not allow us to give more information about this questionnaire

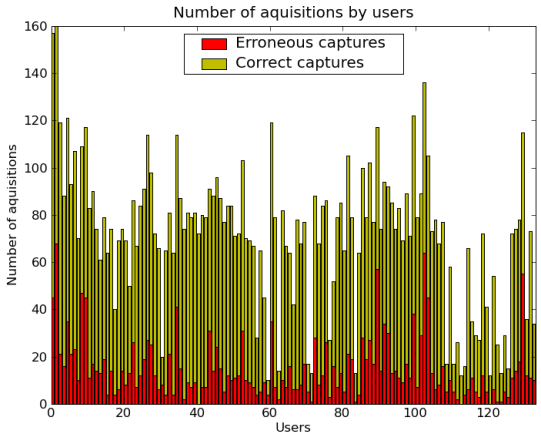

Fig. 4. Number of acquisitions for each user. Correct and erroneous acquisitions are both represented

- the password is quite long to type (17 characters) and its typing mistakes increase by using more than 8 characters [22];
- user is not used with keyboard and have a lot of hesitation while typing;
- user wants to type faster than he is able to do it;
- user forgets the password;
- user is disturbed by the environment;
- user has to type a predefined password.

Usually, we type our own passwords faster than the imposed one. We have tested if this error rate of acquiring process is dependant of user's typing speed, but it seems that there is no correlation. Fig. 5 represents the acquisition error rates (during the acquisition of the database) depending on the typing speed of users. As we can see, the experiment shows no dependency between these factors. In all intervals, we have high error rates.

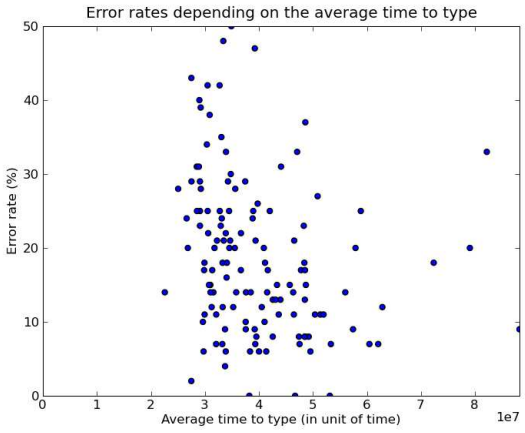

Fig. 5. Acquisition error rate depending on the mean typing speed of each users

V. Conclusions And Future Works

In this paper, we have shown that even if there are existing and used metrics to compare biometrics systems, it is not an easy task to compare studies for the keystroke dynamics modality. This is partially due to the fact that there are not enough details in the papers of literature. Another part of the problem, is that there is not enough public keystroke dynamics database to test the algorithms. Some databases were used in several papers [24], [25], but not used by other researchers or made publicly available. Our contribution is the spreading of a keystroke dynamics database and a tool allowing the creation of such kind of database. The sharing of these tools will allow researchers to work with the same data and give more credibility in the comparisons of the different methods.

Many things have to be tested in the keystroke dynamics world. Most of them necessitate a new database designed for testing these facts (i.e. dependency to keyboard, computer operating system, knowledge of the password, size of the password, content of the password). These databases can be done by merging different databases from different researchers (if the acquisition protocols are equivalent) or by creating new ones with the help of *GREYC-Keystroke* software. Each new database corresponding to a specific problematic with a specific protocol. It could also be interesting to make an evaluation of the most popular existing methods of static keystroke dynamics authentication by using our database and compare the results with our own methods.

VI. Acknowledgments

The authors would like to thank the "Basse-Normandie Region" and the French Research Ministry for their financial support of this work. We would like also to thank all the individuals who have participated to the definition of the keystroke dynamics database.

References

[1] R. Giot, M. El-Abed, and R. Christophe, "Keystroke dynamics with low constraints svm based passphrase enrollment," in *IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS 2009)*, 2009.

[2] A. Conklin, G. Dietrich, and D. Walz, "Password-based authentication: A system perspective," in *Proceedings of the 37th Hawaii International Conference on System Sciences, Hawaii*, 2004.

[3] M. Theofanos, B. Stanton, and C. A. Wolfson, *Usability & Biometrics: Ensuring Successful Biometric Systems*. National Institute of Standards and Technology (NIST), 2008.

[4] ISO, "Biometric performance testing and reporting," ISO/IEC 1975-1:2006(E), Tech. Rep., 2006.

[5] F. Cherifi, B. Hemery, R. Giot, M. Pasquet, and C. Rosenberger, *Behavioral Biometrics for Human Identification: Intelligent Applications*. IGI Global, 2009, ch. Performance Evaluation Of Behavioral Biometric Systems, pp. 21+.

[6] P. Flynn, *Handbook of biometrics*. Springer, 2007, ch. Biometrics databases, pp. 529–548.

[7] R. Cappelli, D. Maio, and D. Maltoni, "Synthetic fingerprint-database generation," in *Pattern Recognition, 2002. Proceedings. 16th International Conference on*, vol. 3, 2002.

[8] P. Phillips, H. Moon, S. Rizvi, and P. Rauss, "The feret evaluation methodology for face-recognition algorithms," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, no. 10, pp. 1090–1104, 2000.

[9] H. Proença and L. Alexandre, "Ubiris: A noisy iris image database," *Lecture Notes in Computer Science*, vol. 3617, p. 970, 2005.

[10] K. Messer, J. Matas, J. Kittler, J. Luettin, and G. Maitre, "Xm2vtsdb: The extended m2vts database," in *Second International Conference on Audio and Video-based Biometric Person Authentication*, vol. 964, 1999, pp. 965–966.

[11] E. Bailly-Bailliere, S. Bengio, F. Bimbot, M. Hamouz, J. Kittler, J. Mariethoz, J. Matas, K. Messer, V. Popovici, F. Poree *et al.*, "The banca database and evaluation protocol," *Lecture Notes in Computer Science*, pp. 625–638, 2003.

[12] J. Fierrez, "The biosecure multimodal biometric database," in *Biosecure Research Project Workshop*.

[13] D. Maio, D. Maltoni, R. Cappelli, J. Wayman, and A. Jain, "FVC 2004: Third fingerprint verification competition," *Lecture Notes in Computer Science*, pp. 1–7, 2004.

[14] P. Phillips, W. Scruggs, A. O'Toole, P. Flynn, K. Bowyer, C. Schott, and M. Sharpe, "FRVT 2006 and ICE 2006 large-scale results," *National Institute of Standards and Technology, NISTIR*, vol. 7408, 2007.

[15] R. Gaines, W. Lisowski, S. Press, and N. Shapiro, "Authentication by keystroke timing: some preliminary results," Rand Corporation, Tech. Rep., 1980.

[16] S. Bleha, C. Slivinsky, and B. Hussien, "Computer-access security systems using keystroke dynamics," *IEEE Transactions On Pattern Analysis And Machine Intelligence*, vol. 12 (12), pp. 1216–1222, 1990.

[17] M. Obaidat and B. Sadoun, "Verification of computer users using keystroke dynamics," *Systems, Man and Cybernetics, Part B, IEEE Transactions on*, vol. 27, no. 2, pp. 261–269, 1997.

[18] S. Cho and S. Hwang, "Artificial rhythms and cues for keystroke dynamics based authentication," in *IAPR International Conference on Biometrics*, vol. 5, 2006, pp. 626–632.

[19] S. Hocquet, J.-Y. Ramel, and H. Cardot, "User classification for keystroke dynamics authentication," in *The Sixth International Conference on Biometrics (ICB2007)*, 2007, pp. 531–539.

[20] R. Rodrigues, G. Yared, C. do NCosta, J. Yabu-Uti, F. Violaro, and L. Ling, "Biometric access control through numerical keyboards based on keystroke dynamics," *Lecture notes in computer science*, vol. 3832, p. 640, 2006.

[21] K. Revett, S. de Magalhaes, and H. Santos, "On the use of rough sets for user authentication via keystroke dynamics," *Lecture notes in computer science*, vol. 4874, p. 145, 2007.

[22] D. Hosseinzadeh and S. Krishnan, "Gaussian mixture modeling of keystroke patterns for biometric applications," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, vol. 38, no. 6, pp. 816–826, 2008.

[23] R. Giot, M. El-Abed, and C. Rosenberger, "Keystroke dynamics authentication for collaborative systems," in *The IEEE International Symposium on Collaborative Technologies and Systems (CTS)*, 2009, pp. 172–179.

[24] J. R. M. Filho and E. O. Freire, "On the equalization of keystroke timing histograms," *Pattern Recognition Letters*, vol. 27, p. 1440–1446, 2006.

[25] E. Yu and S. Cho, "Keystroke dynamics identity verification—its problems and practical solutions," *Computers & Security*, vol. 23, no. 5, pp. 428–440, 2004.