Using keystroke dynamics for gender identification in social network environment

FAIRHURST, M. and DA COSTA ABREU, Marjory <http://orcid.org/0000-0001-7461-7570>

Published version

FAIRHURST, M. and DA COSTA ABREU, Marjory (2012). Using keystroke dynamics for gender identification in social network environment. In: 4th International Conference on Imaging for Crime Detection and Prevention 2011 (ICDP 2011). IET.

Copyright and re-use policy

Using keystroke dynamics for gender identification in social network environment

Michael Fairhurst and Márjory Da Costa-Abreu

School of Engineering and Digital Arts, University of Kent, Canterbury, Kent CT2 7NT, UK.
E-mail: {M.C.Fairhurst, M.C.D.C.Abreu}@kent.ac.uk

Keywords: Social network security, keystroke dynamics, trait prediction.

Abstract

Social networking is now a very widely adopted and highly pervasive communication medium, especially among younger people. However, while offering exceptional opportunities to share and interact these media also introduce the risk of transactions with individuals who deliberately conceal their identity or, importantly, can easily misrepresent their personal characteristics. This paper introduces an approach to addressing such risks by using a form of biometric data accessible from routine interaction mechanisms to predict important user characteristics, thereby directly increasing trust and reliability with respect to the claims made to message receivers by those who communicate with them.

1 Introduction

Online social networks (such as *Facebook, MySpace and Orkut*), which once were intended to serve a small and specialised community only (e.g university students), are now powerful online tools connecting and sharing information among a large and diverse body of people and groups ([29], [18] and [5]). It is the reach, power and anonymity of such media which is both what provides their attraction but also which also creates opportunities for exploitation and endangerment of a subset of users. Some interesting facts about online social networks [31] include the following:

- 61% of 13-17 year old teenagers have a personal profile on social networking sites.
- 44% of teenagers with profiles have been contacted by a stranger, compared with 16% of those who do not have a profile.
- 50% of people who use social networks access it every day.
- The average *Facebook* user, as an example, has 130 friends.
- Social network websites host over 900 million objects, such as pages, groups, community pages, and events, with which users can engage.
- The average person with a profile is linked in with 80 groups, community pages, and events.
- More than 30 billion pieces of content are created each month.
- Only 3% of teenagers reported being contacted by a stranger online to an adult.
- Each week, *MySpace* deletes 25000 profiles for people who do not meet the 14-year-old age requirement.
- Between 2007 and 2009, *MySpace* deleted 90000 accounts that belonged to registered sex offenders.

As it is clear from such statistics, young people especially can put themselves in potentially dangerous situations as social network users, where they run the risk of coming into contact, for example, with child predators who trawl social networking sites ([30] and [16]).

Approaches to alleviating such problems can, however, be found, such as software which captures and stores all keystroke activity [1], [2], but such approaches have the disadvantage that they depend on an adult or a responsible individual subsequently analysing the data.

We propose an alternative and potentially much more powerful approach, which is to detect and interpret more information about the person generating incoming data based entirely on data which can be extracted form available patterns of activity. Specifically, we investigate the use of information available from the captured input stream (keyboard activity at the sender) to identify the user at the sending end or, more likely, to predict relevant characteristics of the sender short of full identification but nevertheless relevant to an assessment of the risk involved in engaging with that sender.

In order to do this we use the concepts of keystroke dynamics (extracting information about the nature and pattern of keyboard activity from the user) as a biometric information carrier. While other biometric modalities could

[1] Keystroke Spy (http://www.keystrokespysoftware.com/)
[2] SPECTOR PRO (http://www.spectorsoft.com/)

Paper	Technique	Enrolment word	Users	FAR	FRR	Forgeries?
[14]	KNN with Mahalanobis	User name and 4-number-PIN	33	0.17%	13.30%	No
[3]	Probabilistic Bayes	User and uni name	22	0.50%	3.10%	No
[4]	Kohonen and MLP	User name	46	4.20%	4.20%	Yes
[22]	KNN	phrases	N/A	15.40%	15.40%	No
[2]	1-NN simple distance	Fixed text of 683 char	44	0.01%	4.00%	No
[26]	Rough set theory	Pass-phrase	100	0.00%	0.00%	No
[23]	Hidden Markov Models	Four fixed words	47	12.70%	12.70%	No
[6]	Degree of Disorder	User name	18	1.90%	23.91%	No
[13]	Hidden Markov Models	User name and password	58	2.54%	2.45%	No
[27]	Probabilistic neural networks	Login Id/password	50	3.90%	3.90%	Yes
[19]	Extended p-norm	Password	16	0.79%	1.60%	Yes
[32]	Markov and fuzzy	N/A	40	8.60%	8.60%	No
[28]	Vote	Texts	37	24.22%	24.22%	No
[15]	KNN with hybrid-score	Password	46	0.58%	-	Yes
[12]	Artificial rhythms	Password	25	1.50%	1.50%	Yes
[10]	SVM	Greyc Laboratory	133	6.96%	6.96%	No
[21]	KNN (mobile application)	Six passwords	40	14%	14%	No

Table 1. Relevant literature related to identity prediction based on keystroke dynamics

be employed, and perhaps with greater accuracy, most are clearly less suitable, either because they require the obvious cooperation of the user and/or additional equipment or operational overhead (for example, providing a fingerprint sample), or because they are easily circumvented (e,g, voice characteristics).

While highest security is likely to be achieved if full user identification is possible, this is a scenario likely to be unrealistic in practice, but the principle can still be used to predict properties of the user relevant to this application, and keyboard dynamics provide a means of exploiting information available automatically from most interaction events.

2 State of the art

Keystroke dynamics (also known as keyboard dynamics) is the study of the unique timing patterns embedded in an individual's typing and most often developed in a way characteristic of that individual, hence the use of keyboard dynamics as a biometrics-based identification modality. Processing of such data typically includes extracting keystroke timing features such as the duration of a key press and the time elapsed between successive key presses [9].

Keystroke-based user identification compares current user activity against stored samples of similar activity usually captured during enrolment (known also as a user *profile*) ([22] and [2]). Most applications aim at detecting significant differences in computer use in order to reduce inappropriate user authorisations to access and change valuable data, depending on the degree of certainty of negative identification ([23] and [27]).

Keystroke-related data can be collected without the aid of special tools or additional hardware but, nevertheless, user authentication through keystroke characteristics remains a difficult task because, as with all behavioural biometrics, typing dynamics are prone to a higher degree of variability than physiological biometrics, even without considering the psychological and physiological state of the individual under observation. Thus, the variability between two immediately consecutive samples can occur even if the subject providing the samples strives to maintain a uniform way of typing ([7], [15], [12] and [10]).

Physiological characteristics tend to be more robust in this respect, although some modalities such as voice patterns and handwriting generally offer a manageable level of uniformity. On the other hand, in the act of typing on a keyboard, it is very challenging to maintain significant control over, for example, the number of milliseconds for which a key is depressed.

The main features typically used for user verification/identification based on their keystroke dynamics are:

- Latency between consecutive keystroke and
- Duration of the keystroke (hold time)

Most keystroke-based authentication systems use fixed-text models, in the sense that they use exactly the same static piece of text for authentication as was used during model construction. There have been fewer approaches that use models based on free text (text that is not prescribed to the user), and unsurprisingly these do not perform as well as fixed-text models. The length of the required training text varies between different studies; some require a few words or full pages of text, which can create better-performing models. Table 1 briefly summarises relevant details of some of the principal studies reported in the literature.

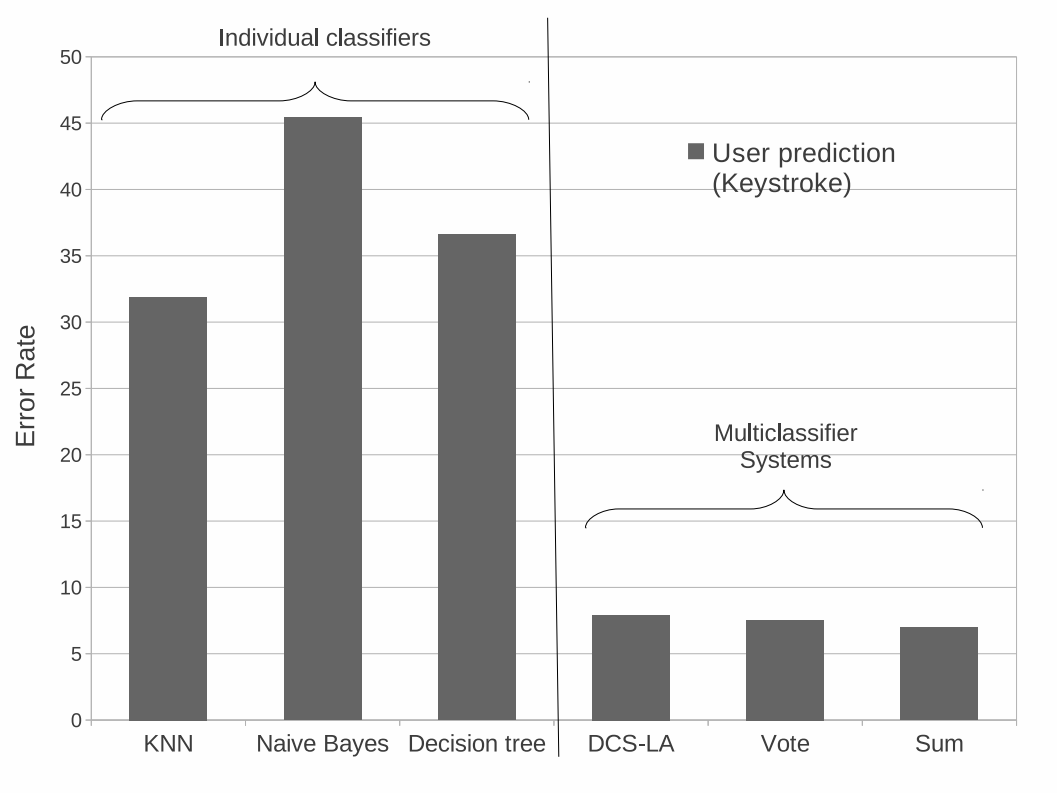

Figure 1. Results for the keystroke database performing identity prediction

3 Case study

In this paper we report an initial case study which considers different strategies for the deployment of keyboard dynamics in seeking to provide information to message recipients about the message sender. We will show some results which demonstrate how optimal configurations can already provide encouraging levels of performance, pointing to the desirability of developing this approach as a means of establishing practical tools to improve trust and confidence in social network transactions.

Our initial investigation is based on the largest publicly available keystroke dynamics database: the GREYC-Keystroke [11]. This dataset contains samples collected from 133 individuals who were asked to type between 5 and 107 times the password "greyc laboratory" over a period of three months. There are 7555 available captures, and the average number of acquisitions per user is 51 with 100 users providing more than 60 templates. Most of the individuals participated in at least 5 sessions. The extracted data features stored in the database are the timing differences between two events of the following categories: press/press, release/release, press/release and release/press.

Since one aim of our work (see below) is to investigate the prediction of user gender from the keystroke data, we have also used the gender information which is available in this database. There are 98 male and 35 female users in the GREYC-keystroke database. Within the constraints of the available data, we will consider two scenarios in our practical study, and then discuss the implications of the results reported.

As we wish in this preliminary study to principally to demonstrate the potential of our application, we have selected three very simple classifiers (K-Nearest Neighbours (KNN) [1], Decision Trees [25] and Naive Bayesian Learning (Naive Bayes) [8]) and also explored classifier combination using three well-known fusion techniques (Dynamic Classifier Selection based on local accuracy class (DCS-LA) [33], Majority Voting and Sum [17]. A 10-fold-cross-validation method [20] was used to evaluate classifier performance.

3.1 Predicting identity from keystroke data

We first consider a scenario in which we aim to predict individual identity from the keystroke data, constituting a typical biometrics-based authentication task.

Figure 1 presents the results of our experiments in the form of error rates (alternatively accuracy (= 100% - error rate) can be considered) using the GREYC-Keystroke database with a selection of individual classifiers as well as using multiclassifier approaches based on a number of fusion techniques in order to perform identity prediction. Although it is seen that, when using the very simple individual classifiers shown here, the identification error rates

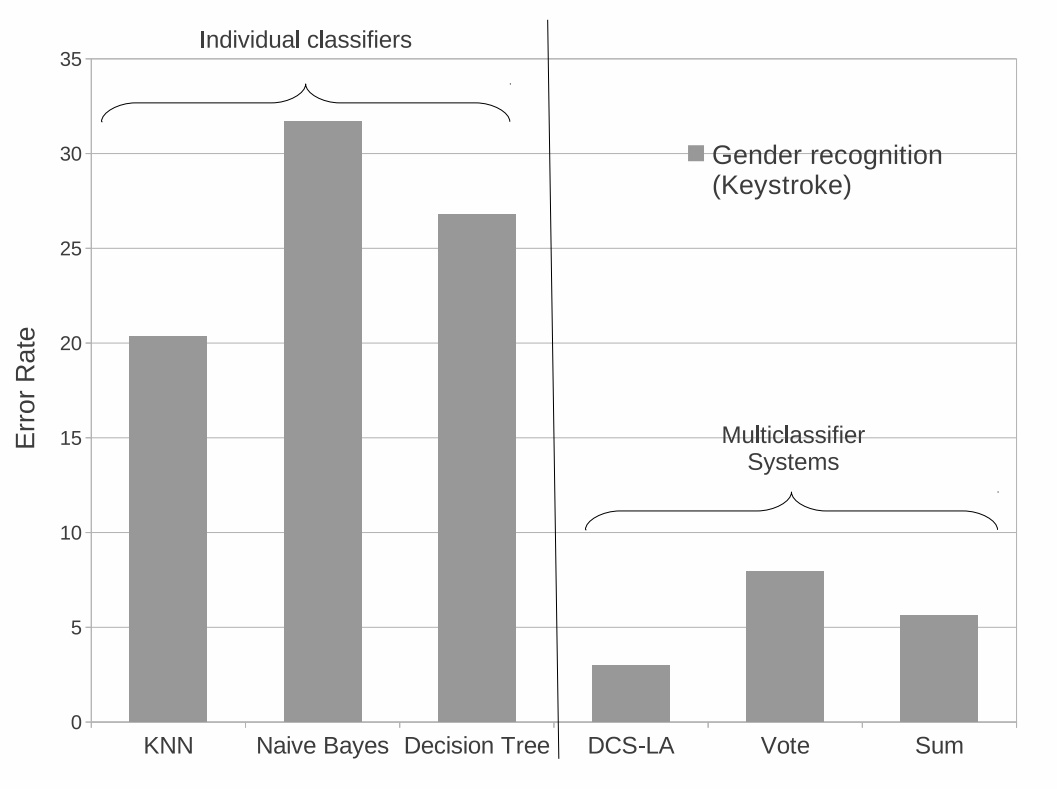

Figure 2. Results for the keystroke database performing gender prediction

obtained are generally rather higher than those recorded for comparison in Table 1, when even basic multiclassifier techniques are adopted, even the simplest (such as Vote or Sum approaches) generate a very significant drop in the error rate. It should be noted also that the database we have adopted is the largest of those publicly available, and hence represents a much better test of the processing algorithms than many of the others for which results are reported in the literature. Indeed, even the worst performance returned by our chosen fusion techniques is better than any recorded in Table 1.

It is clear that security applications could benefit greatly from an ability automatically to recognise the individual accessing a website or software package just by analysing the keystroke pattern generated. In current social networking environments, of course, this scenario would be impractical, both because it requires genuine samples donated by each individual user, and because the nature of the environment remains vulnerable to concealment of real identity. However, it does offer opportunities to consider developing in the future a new operational configuration which employs some form of more rigorous and perhaps supervised or controlled enrolment.

3.2 Predicting gender from keystroke data

Another possible scenario, however, is to attempt to predict, not specific user identity, but instead some personal characteristic which is less specific in its nature but which nevertheless can provide information of relevance in the application context. So called "soft biometric" information is an ideal example of such characteristics. Soft biometrics are characteristics which are not unique to an individual but which are nevertheless directly related to individuals, with typical examples including gender, age, handedness, and so on. As an example of how such information might be used, and given that demographic labels are provided for database samples, we have conducted experiments which use the available samples to predict the gender of the typer solely from the keystroke dynamics. Figure 2 presents the gender prediction results of our experiments, once again, in the form of error rates (alternatively accuracy (= 100% - error rate) can be considered) using the same individual classifiers and fusion techniques as described in Section 3.1.

These results are extremely encouraging, and show that, provided the choice of classifier is appropriate and its operational configurations optimised (and the adoption of multiclassifier configurations again shows particular promise in this respect) the gender of the typer can be predicted with a high degree of accuracy. It is easy to see how this facility might be very useful in the context of protecting individuals on social networking sites, where this type of capability can be used to detect fraudulent claims of gender on the part of those adopting a false identity in order to gain the trust and confidence of the recipient. Al-

though, of course, knowing gender alone is not necessarily a conclusive piece of evidence, it is one important piece of information which can be tested in order to build up a more reliable picture of the claimed profile of a system user.

4 Further potential of this approach

We have seen how it is possible to use biometric user data inherent in a network transaction to predict the identity of the user (although only if a reliable and robust externally supervised enrolment process is introduced) or, without such a procedure, how other characteristics of the message sender might be predicted, offering the opportunity to obtain information of relevance in assessing the degree of trust to place in the credentials of the message sender. We have used gender prediction as one obvious example of this, but it is important to emphasise that other similarly relevant factors may also be predictable.

Individual Classifiers	Err Mean±Stan Dev
MLP	6.39±2.10
Jrip	7.22±2.42
SVM	7.99±2.31
Decision Tree	9.37±2.43
KNN	9.98±2.37

Table 2. Error mean and standard deviation of some individual classifiers using the handwritten signature data from the Biosecure database

A good example of a further user characteristic of real potential relevance here would be the age of the sender. While the keystroke dynamics database we have used does not include age information in its demographic tags (and we are not therefore able to report experiments with this actual database), we can show that it is possible to predict age from other biometric samples, and we include a brief example indicative of what might be achieved. As an example, therefore, we consider the prediction of age according to three age bands ($< \mathbf{25}$, $\mathbf{25 - 60}$ and $> \mathbf{60}$ years) based on the analysis of handwritten signature samples (these representing another behavioural biometric sharing some parallels with the manual operations required in keystroke operation). Here we use the BioSecure database (see [24]), which does report subject age, with Table 2 showing the prediction accuracy for a variety of classifier configurations. Although not directly comparable to the keystroke analysis, this is nevertheless a further indicator of how behavioural data generated in a network-based transaction can readily be used to reveal characteristics of the message sender, providing further evidence of the potential of our approach.

5 Conclusion

While the advantages of social networking systems are readily apparent, it is well known that they also introduce the potential for uncontrolled data exchange, the creation of liaisons which rely on assumptions which may not always turn our to be accurate, and a high degree of trust from parties who contribute to the social transactions facilitated. While much of this traffic is low risk, there are also an increasing number of instances of exploitation and misuse which arise largely because of the vulnerability of such systems to what is effectively identity fraud in varying degrees. This paper has presented some very preliminary results and analysis to promote the idea of fundamental biometric technologies playing a significant role in increasing the trust and confidence of users in social networking transactions, at least from the point of view of providing warnings about aspects of identity or individual characteristics which are susceptible to analysis on the basis of data which can be extracted from input data generated by network users.

Although much work remains to be done if this approach is to be taken further, and while there are clearly further barriers to overcome, the results presented here provide considerable optimism that this type of approach may offer some viable options to increase the extent to which users can be protected against some of the fraudulent or misleading attempts to conceal personal characteristics, thereby providing a step forward in making the social networking environment safer and more secure.

References

[1] A. Arya. An optimal algorithm for approximate nearest neighbors searching fixed dimensions. *Journal of ACM*, 45(6):891–923, 1998.

[2] F. Bergadano, D. Gunetti, and C. Picardi. User authentication through keystroke dynamics. *ACM Transactions on Information and System Security (TISSEC)*, 5(4):367–397, 2002.

[3] S. Bleha, C. Slivinsky, and B. Hussien. Computer-access security systems using keystroke dynamics. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 12(12):1217–1222, December 1990.

[4] M. Brown and S.J. Rogers. User identification via keystroke characteristics of typed names using neural networks. *International Journal of Man-Machine Studies*, 39(6):999–1014, 1993.

[5] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham. A semantic web based framework for social network access control. In *The 14th ACM symposium on Access control models and technologies*, SACMAT 2009, pages 177–186, New York, NY, USA, 2009. ACM.

[6] M. Choraś and P. Mroczkowski. Keystroke dynamics for biometrics identification. In *The 8th international conference on Adaptive and Natural Computing Algorithms, Part II*, ICANNGA 2007, pages 424–431, Berlin, Heidelberg, 2007. Springer-Verlag.

[7] D. Chudá and M. Ďurfina. Multifactor authentication based on keystroke dynamics. In *The International Conference on Computer Systems and Technologies and Workshop for PhD Students in Computing*, CompSysTech 2009, pages 1–6, New York, NY, USA, 2009. ACM.

[8] C. Elkan. Boosting and naive bayesian learning. Technical report, Department of Computer Science and Engineering, University of California, San Diego, 1997.

[9] C. Epp, M. Lippold, and R.L. Mandryk. Identifying emotional states using keystroke dynamics. In *The 2011 annual conference on Human factors in computing systems*, CHI 2011, pages 715–724, New York, NY, USA, 2011. ACM.

[10] R. Giot, M. EI-Abed, and C. Rosenberger. Keystroke dynamics with low constraints svm based passphrase enrollment. In *The 3rd IEEE international conference on Biometrics: Theory, applications and systems*, BTAS 2009, pages 425–430, Piscataway, NJ, USA, 2009. IEEE Press.

[11] R. Giot, M. El-Abed, and C. Rosenberger. Greyc keystroke: A benchmark for keystroke dynamics biometric systems. In *The IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems*, BTAS 2009, pages 1–6, September 2009.

[12] S.-s. Hwang, H.-j. Lee, and S. Cho. Improving authentication accuracy using artificial rhythms and cues for keystroke dynamics-based authentication. *Expert Systems with Applications: An International Journal*, 36(7):10649–10656, 2009.

[13] C.-H. Jiang, S. Shieh, and J.-C. Liu. Keystroke statistical learning model for web authentication. In *The 2nd ACM symposium on Information, computer and communications security*, ASIACCS 2007, pages 359–361, New York, NY, USA, 2007. ACM.

[14] R. Joyce and G. Gupta. Identity authentication based on keystroke latencies. *Magazine - Communications of the ACM*, 33:168–176, February 1990.

[15] P. Kang and S. Cho. A hybrid novelty score and its use in keystroke dynamics-based user authentication. *Pattern Recognition*, 42(11):3115–3127, 2009.

[16] S. Kisilevich and F. Mansmann. Analysis of privacy in online social networks of runet. In *The 3rd international conference on Security of information and networks*, SIN 2010, pages 46–55, New York, NY, USA, 2010. ACM.

[17] L.I. Kuncheva. *Combining Pattern Classifiers: Methods and Algorithms*. Wiley-Interscience, 2004.

[18] N. Lavesson and H. Johnson. Measuring profile distance in online social networks. In *The International Conference on Web Intelligence, Mining and Semantics*, WIMS 2011, pages 1–12, New York, NY, USA, 2011. ACM.

[19] J.-W. Lee, S.-S. Choi, and B.-R. Moon. An evolutionary keystroke authentication based on ellipsoidal hypothesis space. In *The 9th annual conference on Genetic and evolutionary computation*, GECCO 2007, pages 2090–2097, New York, NY, USA, 2007. ACM.

[20] F. Leisch, L.C. Jain, and K. Hornik. Cross-validation with active pattern selection for neural-network classifiers. *IEEE Transactions on Neural Networks*, 9(1):35–41, January 1998.

[21] E. Maiorana, P. Campisi, N. González-Carballo, and A. Neri. Keystroke dynamics authentication for mobile phones. In *The 2011 ACM Symposium on Applied Computing*, SAC 2011, pages 21–26, New York, NY, USA, 2011. ACM.

[22] F. Monrose and A. Rubin. Authentication via keystroke dynamics. In *The 4th ACM conference on Computer and communications security*, CCS 1997, pages 48–56, New York, NY, USA, 1997. ACM.

[23] J.R. Montalv ao Filho and E.O. Freire. On the equalization of keystroke timing histograms. *Pattern Recognition Letters*, 27(13):1440–1446, 2006.

[24] J. Ortega-Garcia, J. Fierrez, F. Alonso-Fernandez, J. Galbally, M.R. Freire, J. Gonzalez-Rodriguez, C. Garcia-Mateo, J.-L. Alba-Castro, E. Gonzalez-Agulla, E. Otero-Muras, S. Garcia-Salicetti, L. Allano, B. Ly-Van, B. Dorizzi, J. Kittler, T. Bourlai, N. Poh, F. Deravi, M.W.R. Ng, M.C. Fairhurst, J. Hennebert, A. Humm, M. Tistarelli, L. Brodo, J. Richiardi, A. Drygajlo, H. Ganster, F.M. Sukno, S.-K. Pavani, A. Frangi, L. Akarun, and A. Savran. The multiscenario multienvironment biosecure multimodal database (bmdb). *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 32:1097–1111, 2010.

[25] J.R. Quinlan. *C4.5: programs for machine learning*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 1993.

[26] K. Revett, S.T. de Magalhaes, and H. Santos. Data mining a keystroke dynamics based biometrics database using rough sets. In *The portuguese conference on Artificial intelligence*, epia 2005, pages 188–191, December 2005.

[27] K. Revett, F. Gorunescu, M. Gorunescu, M. Ene, S.T. de Magalhaes, and H.M. D. Santos. A machine learning approach to keystroke dynamics based user authentication. *International Journal of Electronic Security and Digital Forensics*, 1(1):55–70, 2007.

[28] M. Rybnik, M. Tabedzki, and K. Saeed. A keystroke dynamics based system for user identification. In *The 7th Computer Information Systems and Industrial Management Applications*, CISIM 2008, pages 225–230, June 2008.

[29] J. Schrammel, C. Köffel, and M. Tscheligi. How much do you tell?: information disclosure behaviour indifferent types of online communities. In *The 4th international conference on Communities and technologies*, pages 275–284, New York, NY, USA, 2009. ACM.

[30] J. Schrammel, C. Köffel, and M. Tscheligi. Personality traits, usage patterns and information disclosure in online communities. In *The 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology*, BCS-HCI 2009, pages 169–174, Swinton, UK, UK, 2009. British Computer Society.

[31] A.C. Squicciarini, M. Shehab, and F. Paci. Collective privacy management in social networks. In *The 18th international conference on World wide web*, WWW 2009, pages 521–530, New York, NY, USA, 2009. ACM.

[32] D. Tran, W. Ma, G. Chetty, and D. Sharma. Fuzzy and markov models for keystroke biometrics authentication. In *The 7th WSEAS International Conference on Simulation, Modelling and Optimization*, SMO 2007, pages 89–94, Stevens Point, Wisconsin, USA, 2007. World Scientific and Engineering Academy and Society (WSEAS).

[33] K. Woods, W.P. Kegelmeyer Jr., and K. Bowyer. Combination of multiple classifiers using local accuracy estimates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 19(4):405–410, 1997.