Authentication with Keystroke Dynamics on Touchscreen Keypads - Effect of different N-Graph Combinations

Matthias Trojahn
Mobile-Devices & Auto-ID Technologies
Volkswagen AG
Wolfsburg, Germany
matthias.trojahn@volkswagen.de

Florian Arndt
Client Design & Management
Volkswagen AG
Wolfsburg, Germany
florian.arndt1@volkswagen.de

Frank Ortmeier
Computer Systems in Engineering
Otto-von-Guericke University
Magdeburg, Germany
frank.ortmeier@ovgu.de

***Abstract*—The security and access protection on mobile devices have become an important topic due to the increasing amount of personal and sensitive data stored on these devices. The traditional security techniques based on PIN (*Personal Identification Number*)-input are insufficient and do not correspond to the present password standards. An authentication with usage of keystroke behavior could increase the security and a lot of research has been published based on traditional PC keypads. Keystroke behavior on touchscreen keypads, as they are nowadays installed on smartphones, enables adding additional features for the authentication. For example, pressure, size or exact coordinates of keystroke can be used. The focus of this paper is that several time differences (e.g. digraph) are examined and checked for suitability for a keystroke authentication. For that, data of 152 subjects were classified. With additional features of the touchscreen, an error rate of false rejected persons of only 4.59% and false accepted persons of only 4.19% could be reached.**

***Keywords*—keystroke authentication; n-graph; mobile devices; capacitive display**

I. INTRODUCTION

Smartphones are not only used to phone or write a SMS (*Short Message Service*), especially, with the introduction of the iPhone in the year 2007. This also increases the number of security relevant data and information which are stored on the smartphone or provided through applications. This could be private online banking data, passwords or confidential company documents, e.g., extracted from E-Mail attachments [1], [2]. In addition, personal data (e.g., GPS (*Global Positioning System*) data) have an increasingly important significance [3].

For this reason, the security on smartphones established itself as an important topic, especially the access protection [4], [5]. The challenge is to protect and to avoid economic damage for the enterprise data and assets [6]. However, traditional PIN authentication can easily be defeated and does not conform to present password standards [7]. The standard goes for a two-factor-authentication. In this case, in addition to the password, a possession of a person (e.g., bank card, token) [7] are required.

Greater security can be achieved by another (biometric) authentication factor, such as keystroke dynamics. Components are on the one hand an item that the person knows (password) and on the other an element that is the person himself/herself (keystroke) [8]. Other biometric methods are possible but are not discussed in this paper.

Keystroke has the advantage that no additional hardware is needed because the standard keyboard of the device can be used. However, special software is required for reading the typing behavior. This is, in terms of sustainability, an advantage over other authentication methods which need additional hardware, such as card reader for user ID's [9]. Furthermore, by the lack of additional hardware, the ease of use in keystroke dynamics as an authentication method is less affected [10]. For the optimal case, the user does not notice the procedure because the password entry and the keystroke is checked automatically by the software.

Through the use of a biometric modality additional personal information are stored. Especially, the methods for face recognition cannot be used every time because of religious or cultural reasons [11]. A further complication is that the storage of this data includes an agreement by the user (e.g., German Federal Privacy Act 4a [12]). Saving the typing behavior is seen by many people, however, as less critical, which is a further advantage of the process [1].

In this study, we will discuss keystroke dynamics on touchscreen devices and examine it by an experiment. It will be shown which features or feature combination is suitable for authentication. In addition, we added the pressure and size during typing to see whether it is improving the authentication. The pressure is also used in handwriting recognition [13]. For this purpose, different combinations of properties of typing habits are selected and examined for their suitability for authentication.

In this paper, we will first describe in Section 2 some basic backgrounds regarding biometric authentication and then the hypotheses. In Section 3, the experimental design will be explained. After this, the results are shown and discussed in Section 4. In the last Section, we will give a conclusion with some implications and future work.

II. THEORETICAL BACKGROUND

In this section, we will describe some basics about biometric authentication. Then, we present our hypotheses.

 ISBN: 978-1-61208-313-1

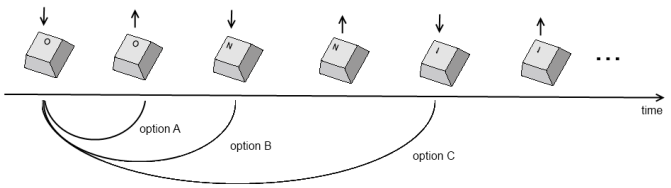

Fig. 1: Events between pressing different keys

A. Biometric Authentication

Keystroke dynamics is a biometric characteristic of a person which describes the rhythm how a person is typing on a keyboard [14]. It can be used like other biometric methods to identify a person. Basically, the rhythm is a characteristic which can be calculated by different aspects, but, in most cases, at least the time differences were used [15].

As seen in Figure 1, different time differences can be used for authentication. In general, two different types of events can be recorded: The first represents the length of time a key is pressed which is time between pressing and releasing a key (residence time) (option A). On the other hand, the time period can be calculated by the striking of keys (the release is here ignored). The time difference between two keystrokes, defined by the two press events, is also called movement time (option B). Both variants of the time period can be called digraph [16]. Furthermore, combinations of more than two keystrokes can be used. A time difference between n key events is called n-graph [15]. In addition to the use of digraphs in many publications, the combination of three key presses are also utilized-the trigraph (option C) [17]. In general, all the values for $n > 1$ are possible in order to determine the time differences. The higher the values the smaller the information which can be extracted by the input because an average over n events is used.

In this paper, the term digraph is used for a better understanding only for the movement time between two keystrokes. We use the residence time to denote the duration of time a key is pressed.

All these features are used to determine a person uniquely. Various classifiers are used to compare these characteristics. As classifiers, in most cases, a statistical classifier (such as distance measures) [18] or neural networks [19], [20] are used.

The authentication process will be measured using different error rates (mismatches). Two possible errors can be distinguished: First, the false acceptance rate (FAR), which indicates the proportion of falsely accepted people:

$$FAR = \frac{number\ of\ false\ acceptances}{number\ of\ impostor\ identification\ attempts} \quad (1)$$

On the other side is the false rejection rate (FRR), which represents how many users are rejected by the system although they are the right person:

$$FRR = \frac{number\ of\ false\ rejections}{number\ of\ enrollee\ identification\ attempts} \quad (2)$$

The last value is the Equal Error Rate (EER) which represents the point where FAR and FRR are the same [21].

The keystroke dynamics on conventional keyboards have been part of numerous scientific papers. The residence time [22], [23], [24] as well as the movement time [14], [25], [26] have been examined as a feature for typing behavior. Besides these features, the number of input errors can be used as well [2]. The time characteristics and the error rate are the most widely used features that can be extracted by computer keyboards [27].

Even the typing behavior for authentication on mobile phone keypads has been investigated [1], [2]. Here, devices were used which have 12 hardware buttons.

In the survey paper of Banerjee [28] a good overview was given about different experiments and their results. Here, only a set of these studies will be presented.

Basically, all publications are related to the keyboard of a computer or to a mobile device with 12 keys. The error rates are influenced by the number of subjects, the classifier and the features. The first study about keystroke dynamics on computer keyboards were done by Umpress et al. (FAR: 11.7%, FRR: 5.8%) [18] and Joyce (FAR: 0.3%, FRR: 16.4% with 33 subjects) [29] and used only digraphs and a statistical classifier. Later on Ord and Furnell [30] used a neuronal network for 14 subjects and get a result of 9.9% for the FAR and 30.0% for the FRR.

Also on the mobile device (12-key layout) good results were published by Clarke et al. [31] with an EER of 15.2% and Zahid et al. [2] had a FAR of 11% and a FRR of 9.22%. Both experiments used neuronal network and had 25 respectively 30 subjects.

One of the first studies with a touchscreen device was done by Saevanee [32] who used the pressure of the fingertip. With the ten subjects he achieved an accuracy rate of 99%.

In addition to the pressure feature, the size of the fingertip was used by Trojahn and Ortmeier [33]. They analyzed the typing behavior of 35 subjects (FAR: 9.53%, FRR: 5.88%).

B. Hypotheses

The existing publications are mainly dealing with the computer or 12-key mobile phone keyboard. On touchscreen keyboards which are now installed in nearly every smartphone, besides the well-known features, other possibilities for typing behavior can be read. Examples for this are the pressure or the size of the fingertip during typing. These can be used in combination with the time values for authentication [34].

For this, we want to prove that an authentication with a touchscreen keyboard is possible. We identified therefore the following hypotheses:

H1: If an authentication is done with a touchscreen keyboard using n-graph the same error rates can be achieved compared with the existing keystroke dynamics studies.

H2: If the model is extended with additional features (pressure and size of the finger) the error rates can be reduced.

III. Experimental Design

The subjects were asked to enter a predefined, 17-digit passphrase ten times in a row on a smartphone. A Samsung Galaxy Nexus has been used as a test device. A soft keyboard was implemented to deactivate uppercase and the alignment changes. In addition, an application was designed to read the keystroke. Other descriptive data were also queried about the

 ISBN: 978-1-61208-313-1

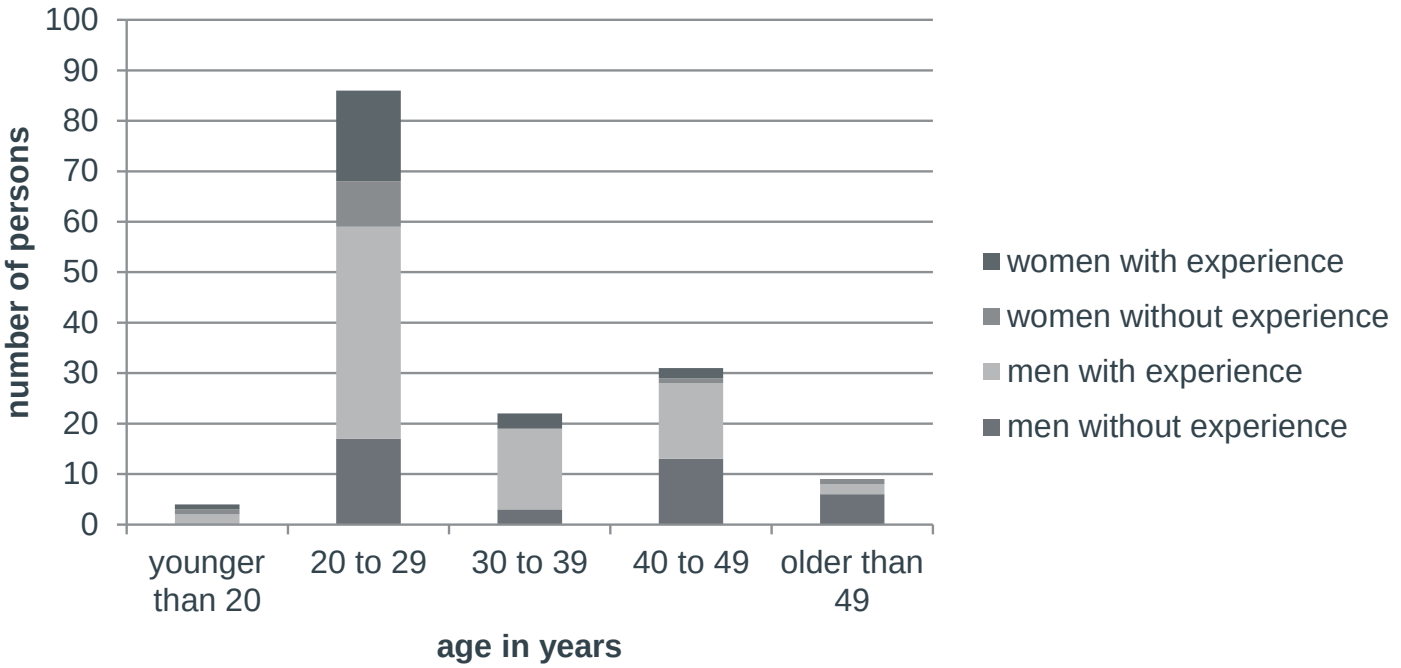

Fig. 2: Experience structure in combination with age and sex

self-written application and stored on the mobile device in a file.

In the experiment, 101 out of the 152 participants already had prior experience with a touchscreen keyboard. Out of these 101 persons, 62% had experience with the Android operating system. On average, the subjects use their smartphone 1.7 hours per day. The experiment lasted 15 to 20 minutes per subject. More detailed information of the data set can be found in Figure 2.

In order to avoid the user familiarity with the device affect the results of the test, the subjects had time to practice with the equipment and get used to the keyboard. In addition, they had to enter a test text before the real test started. All ten repetitions of the password had to be entered correctly. Otherwise, this entry attempt was rejected and the user had to enter the same password a second time. Afterwards, the data set was divided into test and evaluation data. Every third input of a test person had been assigned to the evaluation data and the remaining part to the training data. This means that per subject seven inputs are used for the training data and three were used as evaluation data. This mutual selection was continued for further inputs and was done to reduce the fault which is created the rising learning curve.

The recorded raw data include all interactions (events) with the keyboard: Press and release buttons and movements on the screen. For each event, the date and the code of the pressed key are stored as well.

In the present study, different combinations of button presses and different n-graph (digraph and trigraph) for their suitability for authentication are examined. First, the individual features are calculated and in the later course fused to represent the ability of combinations (no weights between the features).

Since at each authentication attempt, the tip pattern shows up slight differences and entry errors are made, it is important to smooth the differences. Therefore, a classification method (statistical classifier using K-Means) was used with brute force to filter the best solutions. Two filters were implemented in front of the classifier. At first, the data were divided into test and evaluation data (ratio 7:3). After this, for each feature the two largest values were extracted and from the rest an average value was calculated for the model. The individual evaluation data were compared to this average. The value has to be within a specified tolerance of the average. At the end, it was decided based on the individual values and a predefined threshold value, whether it is a person or not.

IV. Results and Discussion

For the first evaluation of the recorded data, the single features have been extracted. In addition, the residence time of the keystroke, the digraph and trigraph were calculated. The following figures show the extracted data for five randomly selected subjects for better representation (analogue [35], [31]). Figure 3 shows the data of the digraph and Figure 4 represents the data of the retention time.

The amount of data which can be extracted depends on the number of letters and on which feature is selected. For the residence time there can be extracted one more than for the digraph. That means for a 17 letter key phrase 16 values can be extracted.

In Figure 3 it can be seen that for the randomly selected subjects the average duration is in most cases more constant over the time. The same applies for the whole record. However, there are considerable differences among the people, even in the general speed and then between single digraphs of one subject. The differences between individuals can be explained on the basis of experience. So the fifth person, for example, has a lot of experience while subject number four has no experience. This explains also the high values for each digraph

 ISBN: 978-1-61208-313-1

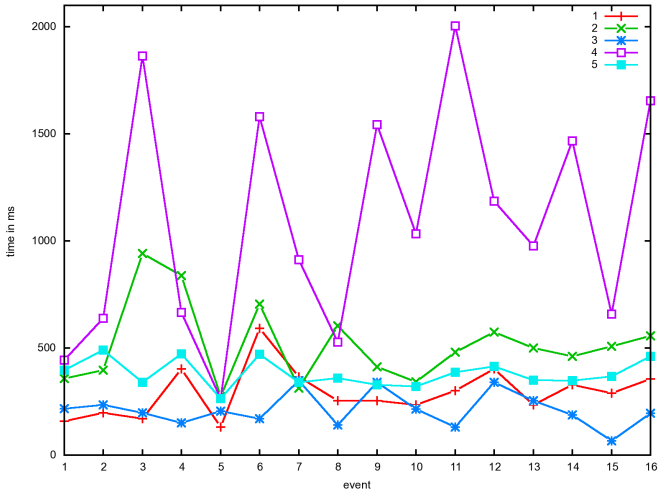

Fig. 3: Digraph for five different users

for the fourth person. The slight movement time for all subjects at fifth time event is explained by the fact that the password has the same letter twice in a row. In this situation the person does not need to search next letter. The described features of the typing behavior of the five randomly chosen test subjects can be observed in all subjects of the experiment in similar ways.

The rhythm of the residence time (Figure 4), however, is less constant between individuals and also between different attempts by one person. Furthermore, the residence time tends to be less than the movement time. A person needs more time to press the next key than to hold a key. Also the differences in experience of a touchscreen are less noticeable at the residence.

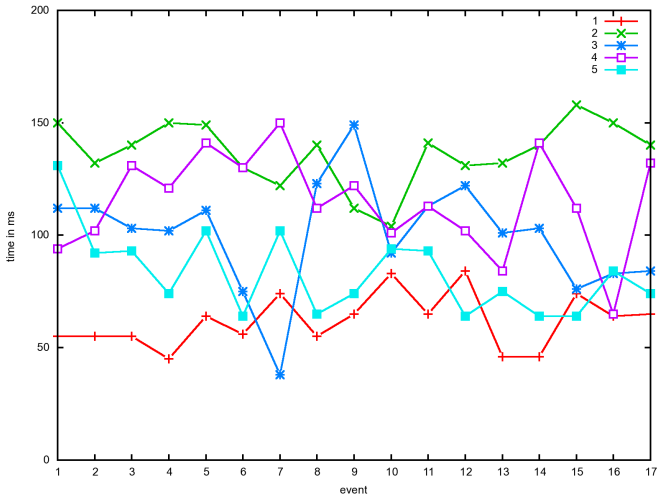

Fig. 4: Residence time for five different subjects

Table I shows the results of the classification as average values of all 152 subjects with the statistical process with several different combinations of the extracted features.

To simplify the comparison, the results shown in Table I are generated by comparing the sum of the error rates for each feature selection. This approach was already selected to determine the best error ratio for the individual characteristics and allows obtaining the respective minima. A comparison of the first two lines indicates that the assumption that the residence time is more suitable than the digraph is correct. With the feature digraph, for example, one of nine people is incorrectly accepted and only every 15th attempt to authenticate someone is falsely rejected. The feature of the trigraph is even less appropriate and gives worse results than the feature over two keystrokes.

TABLE I: Results for different feature combinations

FAR (in %)	FRR (in %)	Selection of features
8.03	12.3	residence time
12.66	11.64	digraph (two different keys)
13.63	33.33	trigraph (three different keys)
9.28	6.72	residence time + digraph
10.01	10.98	residence time + trigraph
10.02	13.77	digraph + trigraph
6.61	8.03	residence time + digraph + trigraph

Better results can be achieved with combinations of features. Then the sum of the lowest error rate is achieved with the combination of residence time digraph. This combination was, therefore, continued to be used in order to merge with add-on features.

Very good results have been achieved with the additional features of the pressure, the size of the key presses, the exact coordinates while pressing and releasing the finger. A combination of residence time and digraph and additional features (e.g., pressure and size) can provided a FAR of 4.19% and a FRR of 4.59%. This means that an authentication on the basis of these characteristics, only every 24th person is falsely accepted and only every 22th attempt is falsely rejected. In comparison to the general password approach where each attempt is successful it is an improvement. Altogether this means, the traditional feature (duration, digraph and trigraph) can be improved with the new features.

V. Conclusion

This section will give a summary and will describe some limitations as well as some future work.

A. Summary and Implications

Due to the increasing number of sensitive, personal information on mobile devices, the security and access control settings on these devices are becoming an increasingly important issue. A higher security is, however, in accordance with normal additional hardware less user friendly, for example, by stringent password standards (more letter or alphanumeric).

Based on the study, it was shown that an authentication using the keystroke is possible on touchscreens and enhances the security. Furthermore, the study has shown an attack on the authentication. Each subject used the same password (so it was known by everyone) in this situation only the behavior was important. It showed the same impact as they were already achieved in previous scientific publications with conventional keyboards (see Table 1). By adding further features of the typing behavior the error ratio can be reduced more.

In most combinations of features the calculated FRR was smaller than the FAR. In particular, in the best case when using the pressure and the size of the keystrokes, in addition, the

 ISBN: 978-1-61208-313-1

FRR was particularly low. This is desirable in mobile devices, since the ease of use is desired [36] to ensure acceptance of the procedure. If the correct user is rejected too often incorrectly, the method is not usable.

B. Limitation and Future Work

Like most studies, some limitations exist in our study that should be mentioned at this point.

The experiment was conducted in a controlled environment, which reduces many outside influences in the observation. These include stress and negative emotions to the subject, during the authentication process on their smartphone, which may affect the keystroke dynamics [37]. Even movements and orientation of the phone can affect the typing and should be observed in further studies [38]. This includes whether the person is sitting, lying or standing.

The presented method for authentication of mobile devices can be applied to all devices with a touchscreen. Thereby, it is possible to use the method for mobile devices such as the smart grid environment [39], [40]. Examples of this would be that a technician who is equipped with a mobile device (stores sensitive data) secures his device against unauthorized access in case of theft. For this, a two-factor authentication using the keystroke would be a useful and user-friendly solution that can be used without any additional hardware and thus lower costs.

Future research could aim to achieve a further reducing of the error rates by including the factors that the user no longer perceives the additional authentication. In addition, it could be tested how much influence a rhythm during typing has [41], like using own pauses or music melodies during typing. This could greatly increase the usability and acceptance of the process.

REFERENCES

[1] A. Buchoux and N. L. Clarke, "Deployment of keystroke analysis on a smartphone," in *Proceedings of the 6th Australian Information Security & Management Conference*, 2008.

[2] S. Zahid, M. Shahzad, S. A. Khayam, and M. Farooq, "Keystroke-based user identification on smart phones," in *Proceedings of the 12th International Symposium on Recent Advances in Intrusion Detection*, ser. RAID '09. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 224–243.

[3] C. Bettini, X. S. Wang, and S. Jajodia, "Protecting privacy against location-based personal identification," in *In 2nd VLDB Workshop SDM*, 2005, pp. 185–199.

[4] X. Ni, Z. Yang, X. Bai, A. Champion, and D. Xuan, "Diffuser: Differentiated user access control on smartphones," in *Mobile Adhoc and Sensor Systems, 2009. MASS '09. IEEE 6th International Conference*, 2009, pp. 1012–1017.

[5] I. Muslukhov, "Survey: Data protection in smartphones against physical threats," 2012.

[6] P. M. Milligan and D. Hutcheson, "Business risks and security assessment for mobile devices," in *Proceedings of the 8th Conference on 8th WSEAS Int. Conference on Mathematics and Computers in Business and Economics - Volume 8*, ser. MCBE'07. Stevens Point, Wisconsin, USA: World Scientific and Engineering Academy and Society (WSEAS), 2007, pp. 189–193.

[7] T.-Y. Chang, C.-J. Tsai, and J.-H. Lin, "A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices," in *Journal of Systems and Software*, vol. 85, no. 5, 2012, pp. 1157–1165.

[8] C. Vielhauer, *Biometric User Authentication for IT Security: From Fundamentals to Handwriting*, ser. Advances in information security. Springer-Verlag, 2006.

[9] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," in *Future Generation Computer Systems*, vol. 28. Elsevier Science Publishers B. V, 2000, pp. 583–592.

[10] S. Sonkamble, R. Thool, and B. Sonkamble, "Survey of biometric recognition systems and their applications," in *Journal of Theoretical and Applied Information Technology*, 2010.

[11] A. Esposito, "Debunking some myths about biometric authentication," in *arXiv preprint arXiv:1203.0333*, 2012.

[12] S. Simitis, "Bundesdatenschutzgesetz: Bdsg," Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Baden-Baden, Tech. Rep., 2011.

[13] A. Makrushin, T. Scheidat, and C. Vielhauer, "Handwriting biometrics: feature selection based improvements in authentication and hash generation accuracy," in *Proceedings of the COST 2101 European conference on Biometrics and ID management*, ser. BioID'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 37–48.

[14] F. Monrose and A. D. Rubin, "Authentication via keystroke dynamics," in *Proceedings of the 4th ACM conference on Computer and communications security*, ser. CCS '97. New York, NY, USA: ACM, 1997, pp. 48–56.

[15] R. Moskovitch, C. Feher, A. Messerman, N. Kirschnick, T. Mustafic, A. Camtepe, B. Löhlein, U. Heister, S. Möller, L. Rokach, and Y. Elovici, "Identity theft, computers and behavioral biometrics," in *Proceedings of the 2009 IEEE international conference on Intelligence and security informatics*, ser. ISI'09. Piscataway, NJ, USA: IEEE Press, 2009, pp. 155–160.

[16] C. Epp, M. Lippold, and R. L. Mandryk, "Identifying emotional states using keystroke dynamics," in *Proceedings of the 2011 annual conference on Human factors in computing systems*, ser. CHI '11. New York, NY, USA: ACM, 2011, pp. 715–724.

[17] M. Choraś and P. Mroczkowski, "Keystroke dynamics for biometrics identification," in *Proceedings of the 8th international conference on Adaptive and Natural Computing Algorithms, Part II*, ser. ICANNGA '07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 424–431.

[18] D. Umphress and G. Williams, "Identity verification through keyboard characteristics," in *International Journal of Man-Machine Studies*, vol. 23, 1985, pp. 263–273.

[19] F. A. Alsulaiman, J. Cha, and A. Saddik, "User identification based on handwritten signatures with haptic information," in *Proceedings of the 6th international conference on Haptics: Perception, Devices and Scenarios*, ser. EuroHaptics '08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 114–121.

[20] M. Faundez-zanuy, "Study of a committee of neural networks for biometric hand-geometry recognition," in *Neural Networks*, 2005, pp. 1180 – 1187.

[21] S. Karatzouni and N. L. Clarke, "Keystroke analysis for thumb-based keyboards on mobile devices," in *New Approaches for Security, Privacy and Trust in Complex Environments, Proceedings of the IFIP TC-11 22nd International Information Security Conference (SEC 2007), 14-16 May 2007, Sandton, South Africa*, ser. IFIP, H. S. Venter, M. M. Eloff, L. Labuschagne, J. H. P. Eloff, and R. v. Solms, Eds., vol. 232. Springer, 2007, pp. 253–263.

[22] S. Cho, C. Han, D. H. Han, and H.-I. Kim, "Web-based keystroke dynamics identity verification using neural network," in *Journal of Organizational Computing and Electronic Commerce*, vol. 10, no. 4, 2000, pp. 295–307.

[23] D.-T. Lin, "Computer-access authentication with neural network based keystroke identity verification," in *Neural Networks,1997., International Conference on*, vol. 1, 1997, pp. 174 –178.

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

[25] M. Obaidat and D. Macchiarolo, "An online neural network system for computer access security," in *Industrial Electronics, IEEE Transactions on*, vol. 40, no. 2, 1993, pp. 235–242.

[26] S. Haider, A. Abbas, and A. Zaidi, "A multi-technique approach for user identification through keystroke dynamics," in *Systems, Man, and Cybernetics, 2000 IEEE International Conference on*, vol. 2, 2000, pp. 1336 –1341.

[27] D. Shanmugapriya and G. Padmavathi, "A survey of biometric keystroke

 ISBN: 978-1-61208-313-1

dynamics: Approaches, security and challenges," in *International Journal of Computer Science and Information Security*, vol. 5, no. 1, 2009.

[28] S. Banerjee and D. Woodard, "Biometric authentication and identification using keystroke dynamics: A survey," in *Journal of Pattern Recognition Research*, vol. 7, 2012, pp. 116–139.

[29] R. Joyce and G. Gupta, "Identity authentication based on keystroke latencies," in *Commun. ACM*, vol. 33. New York, NY, USA: ACM, 1990, pp. 168–176.

[30] T. Ord and S. Furnell, "User authentication for keypad-based devices using keystroke analysis," in *Proc. 2nd Int'l Network Conf. (INC 2000)*, 2000, pp. 263–272.

[31] N. L. Clarke and S. M. Furnell, "Authenticating mobile phone users using keystroke analysis," in *Int. J. Inf. Secur*, vol. 6. Berlin, Heidelberg: Springer-Verlag, 2006, pp. 1–14.

[32] H. Saevanee and P. Bhattarakosol, "Authenticating user using keystroke dynamics and finger pressure," in *Consumer Communications and Networking Conference, 2009. 6th IEEE*, 2009, pp. 1–2.

[33] M. Trojahn and F. Ortmeier, "Biometric authentication through a virtual keyboard for smartphones," in *International Journal of Computer Science & Information Technology (IJCSIT)*, 2012.

[34] A. Ross and A. K. Jain, "Information fusion in biometrics," in *Pattern Recognition Letters*, vol. 24, 2003, pp. 2115–2125.

[35] E. Lau, X. Liu, C. Xiao, and X. Yu, "Enhanced user authentication through keystroke biometrics," in *Computer and Network Security*, 2004.

[36] A. Peacock, X. Ke, and M. Wilkerson, "Typing patterns: A key to user identification," in *IEEE Security and Privacy*, vol. 2, no. 5, 2004, pp. 40–47.

[37] D. N. Glaser, B. C. Tatum, D. M. Nebeker, R. C. Sorenson, and J. R. Aiello, "Workload and social support: Effects on performance and stress," in *Human Performance*, vol. 12, no. 2, 1999, pp. 155–176.

[38] Z. Syed, S. Banerjee, Qi Cheng, and B. Cukic, "Effects of user habituation in keystroke dynamics on password security policy," in *High-Assurance Systems Engineering (HASE), 2011 IEEE 13th International Symposium on*, 2011, pp. 352–359.

[39] H. Khurana, M. Hadley, Ning Lu, and D. Frincke, "Smart-grid security issues," in *Security & Privacy, IEEE*, vol. 8, no. 1, 2010, pp. 81–85.

[40] A. Metke and R. Ekl, "Security technology for smart grid networks," in *IEEE Transactions on Smart Grid*, vol. 1, no. 1, 2010, pp. 99–107.

[41] S.-s. Hwang, S. Cho, and S. Park, "Keystroke dynamics-based authentication for mobile devices," in *Computers & Security*, vol. 28, no. 1–2, 2009, pp. 85–93.

 ISBN: 978-1-61208-313-1