Biometric Swiping on Touchscreens

Orcan Alpar and Ondrej Krejcar(✉)

Faculty of Informatics and Management, Center for Basic and Applied Research,
University of Hradec Kralove, Rokitanskeho 62 500 03, Hradec Kralove, Czech Republic
orcanalpar@hotmail.com, ondrej@krejcar.org

Abstract. Touchscreen devices have become very popular in the last decade and eased our modern life. It is now possible to automatically log in to any web page connected to our touchscreen phones, such as social networks, e-commerce sites and even mobile banking. Given these facts, the emerging touchscreen technology brings out a potential security issue: weakness of authentication protocols. Therefore, we put forward a biometric enhancement on "swiping" authentication, which is one of the options to log in a touchscreen phone however with the lowest security. We created a ghost password by extracting the features of coordinates and swipe durations to use them as the inputs of the Levenberg-Marquardt based neural network and adaptive neuro-fuzzy classifiers which both discriminate real attempts from fraud attacks after training.

Keywords: Touchscreen · Biometric · Authentication · Swiping · Security

1 Introduction

Biometrics is the general term for human traits which are so unique that makes them really hard to mimic. The biometric authentication systems are developed for extracting physical, biological or behavioral characteristics to identify or discriminate the users when necessary. Among the several types of biometric systems, keystroke recognition has an unusual enhancement since the features could be designed intentionally and changed on request. Considering other well-known biometric systems, such as iris, gait, fingerprint, finger veins, hand geometry, the traits are biological or physical that cannot be changed, but in keystroke systems, the password design can be natural or a ghost password can be designed.

Keystroke recognition is basically based on the uniqueness of entering an alphanumeric password. The infrastructure of keystroke authentication systems is more or less similar; collecting inter-key durations as the main feature. Moreover, keystroke techniques are extended subsequent to emerging technologies of touchscreens and now it is comprising a basis for touchscreen authentication and related. However the kernel stays same, no matter the input device is a keyboard or a touchscreen. In addition to alphanumeric passwords, the touchscreens have various authentication methods such as pattern passwords and swiping.

Despite the security issues, swiping is the easiest method to authenticate to a touchscreen. In this process, the users only need to do a fingertip gesture on the screen

K. Saeed and W. Homenda (Eds.): CISIM 2015, LNCS 9339, pp. 193–203, 2015.
DOI: 10.1007/978-3-319-24369-6_16

and simply drawing a line while touching is enough to authenticate. In spite of the given ease of use, this procedure however has a security drawback since most new generation mobile phones and tablets remember passwords of very crucial websites, like e-banking, e-commerce or all kind of social networks. Therefore, what we briefly propose in this research is to strength the swiping authentication systems using biometrical features.

There are three major subsystems introduced in this paper, namely; Feature Extraction, Training and Classifying which could be seen in Figure 1 below,

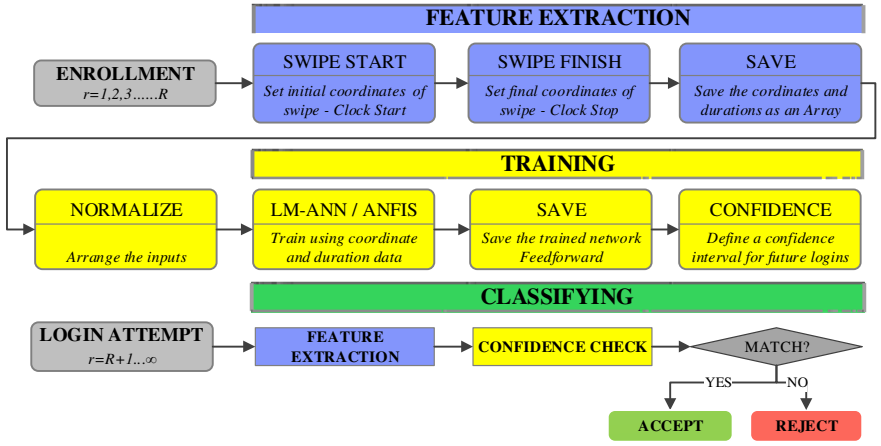

Fig. 1. Workflow of Enhanced Swiping Authentication System

Initially, an interface is written to emulate the screen dimensions of Samsung I8262 Galaxy Core Duos smartphone, which is 800x480 pixel-square. As the swiping starts in enrollment step, the feature extraction subsystem marks the initial coordinates. The subsystem also records the touch duration until the swipe is over and points the final coordinates. Using these five inputs, Swipe Start x, Swipe Start y, Swipe Finish x, Swipe Finish y and the time data, the neural networks based classifiers, Levenberg-Marquardt based artificial neural (LM-ANN) and adaptive neuro-fuzzy (ANFIS), are trained.

Although numerous articles have been published in the last decade regarding keystroke recognition like [1] [2] [5] [7] [8] [9] [11] [12] [13] [14] [15] [16] [17] [20] [21], there are several papers in the literature that are relevant of our research.

Very briefly; Sae-bae et.al. [4] introduced a gesture-based authentication method using five-finger touch gestures. They collected the biometric data from the movement characteristics of the palm and created a classifier to recognize unique biometric gesture features and to check the future logins. They achieved an equal error rate (EER) of 5% – 10%. Chang et al. [3] utilized the pressure feature for a graphical authentication system for touchscreens with an EER of 6.9% – 14.6%.

Furthermore, Angulo and Wästlund [6] dealt with lock pattern dynamics and developed an application for the Android mobile platform to collect data. As a result of

the experiments they made, an EER of 10.39% was revealed. Maiorana et al. [10] proposed a method of keystroke recognition to enhance keypad authentication for mobile devices and reached 13.59% – 24.15% EER. Tasia et. al [22] also proposed a twelve key virtual keypad as an interface for users to enter their biometric pins. The result is encouraging that they achieved a constant 8.4% EER. Kang and Cho [23] presented three different interfaces for touchscreens to collect biometric data and their experiment resulted in 5.64% – 16.62% EER.

Moreover; Kambourakis et al. [24] implemented a biometric keystroke system for touchscreens using for traits: speed, distance, hold-time and inter-time and achieved an EER of 13.6% – 26%. Sae-bae et. al. [18] dealt with multi touch gestures, especially hand and finger muscle behavior. They pointed the initial points of the five fingers, traced the movement as the fingers move, calculated the distances to propose a gesture based user authentication system and reached 5.14% – 27.73% EER. Finally, Zhao et al [19] determined gesture types for single and multiple touches and introduced the "Graphical Touch Gesture Feature" with an EER of 4.1% – 10.5%.

Comparing with these enhancements, what we put forward is two types of intelligent classifiers to strengthen the swiping process on touchscreens.

2 Feature Extraction

Since the major concern of this research is enhancing the existing and built-in authentication algorithm in touchscreens, the swiping process is considered not as a gesture as in previous works, but as a simple and basic motion. Therefore and initially, an invisible interface is created to collect coordinate and duration data. The ghost password beneath the swipes is 5-bit array which can be represented by

$$P = \left[x_i, y_i, x_f, y_f, t\right] \tag{1}$$

where *x* represents the horizontal axis, y represents the vertical axis, *i* is initial,*f* is final point and t is the duration and $x_i\ y_i\ x_f\ y_f \in \mathbb{Z}^+, \forall x_i, x_f \in [0\ 480]\ \forall y_i, y_f \in [0\ 800]$.

3 Training Algorithms

As the classifier system, we firstly selected artificial neural network (ANN) which is a learning system that simulates the neurological processing ability of the human brain and can be used in correlating the nonlinearity between inputs and outputs. The ANNs are usually trained by the backpropagation algorithms however we used the Levenberg-Marquardt [25] [26] algorithm, which is actually a nonlinear optimization protocol since it has lower dissolution time.

Like the quasi-newton models, the LM algorithm is designed to find x_{k+1} from x_k using the Hessian and gradient matrices however in LM, the Hessian matrix is approximated by Jacobian matrix. On the other hand, we're dealing with the optimization of the weights therefore the equation is written for the weights, namely,

$$w_{n+1} = w_n - [J_n^T J_n + \mu_n I]^{-1} J_n e_n \tag{2}$$

where e is the vector form of errors for n[th] iteration, μ is initial leaning rate, $J_n e_n$ is the gradient, $J_n^T J_n$ is the approximation of Hessian and J_n is the Jacobian matrix:

$$J = \begin{bmatrix} \frac{\partial e_{1,1}}{\partial w_1} & \frac{\partial e_{1,1}}{\partial w_2} & \cdots & \frac{\partial e_{1,1}}{\partial w_N} \\ \frac{\partial e_{1,2}}{\partial w_1} & \frac{\partial e_{1,2}}{\partial w_2} & \cdots & \frac{\partial e_{1,2}}{\partial w_N} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{\partial e_{P,M}}{\partial w_1} & \frac{\partial e_{P,M}}{\partial w_2} & \cdots & \frac{\partial e_{P,M}}{\partial w_N} \end{bmatrix} \tag{3}$$

When the initial leaning rate μ is zero, this gives the Newton method with approximated Hessian. The main difference in LM is the general procedure of forcing the Hessian to be positive definite by $J_n^T J_n + \mu_n I$ such that; in each iteration, μ_n is adjusted to make the Hessian positive if it is not.

The errors are computed by sum of squares namely;

$$E(w) = \frac{1}{2} \sum_{p=1}^{P} \sum_{m=1}^{M} e^2{}_{p,m} \tag{4}$$

where p is the index of inputs for P inputs, m is the index of outputs for M outputs and $e_{p,m} = \dot{o}_{p,m} - o_{p,m}$ where $\dot{o}_{p,m}$ is expected and $o_{p,m}$ is the actual output.

As the initiation of the experiment, 10 real attempts are saved to train the network. Although the right thumb movement is simulated which should reveal a trace like a nonlinear curve, since only the initial and final coordinates of the swipes are extracted, the swipes therefore look like straight lines as in Figure 2.

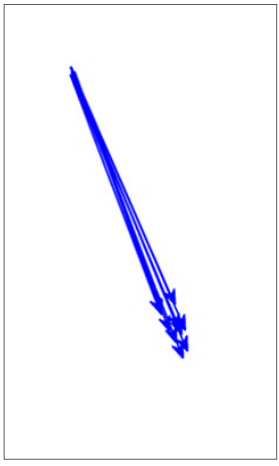

Fig. 2. Training set consisting of 10 swipes.

The data includes the coordinates in pixel numbers such as $\forall x_i\ y_i\ x_f\ y_f \in \mathbb{Z}^+$ where $\forall x_i, x_f \in [0\ 480]\ \forall y_i, y_f \in [0\ 800]$ however these values are normalized to; $\forall \dot{x}_i\ \dot{y}_i\ \dot{x}_f\ \dot{y}_f \in \mathbb{R}^+$ where $\forall \dot{x}_i, \dot{x_f}, \dot{y}_i, \dot{y}_f \in [0\ 1]$ namely;

$$\dot{P} = \left[\ \dot{x}_i = x_i/480,\ \dot{y}_i = y_i/800,\ \dot{x}_f = x_f/480,\ \dot{y}_f = y_f/800,\ t\right] \tag{5}$$

We trained the network with 10 input arrays and for initial learning rate $\mu_0 = 0.5$ by iterating the network, involving standard sigmoid perceptron and 5 nodes in one hidden layer, for 200 epochs and optimized the weights using LM. The input matrix is also used as the checking data to determine the confidence interval by feedforwarding the network and the following values are achieved in Figure 3.

Given the maximum and minimum levels of the Figure 3, the confidence interval is determined as $o_{max} = 1.0008$ and $o_{min} = 0.9995$ however we extended the interval by doubling the range as $\dot{o}_{max} = 1.0016$ and $\dot{o}_{min} = 0.9990$ and therefore if the results of feedforward process of succeeding attempts result in outside of this region, they will be rejected.

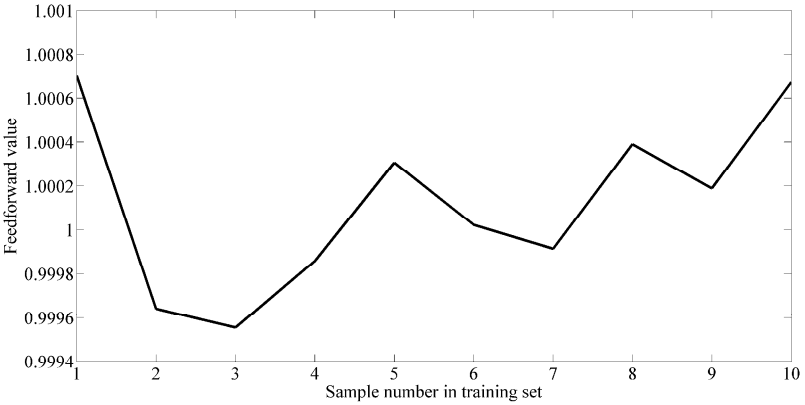

Fig. 3. Feedforward values of the input matrix as the confidence region

These values also represent the correspondence between the individual value and the whole training set.

In addition, we developed an ANFIS structure to utilize as the second classifier with generating a Sugeno style fuzzy inference system (FIS) with gird partitioning for 30 epochs. The membership function styles are selected as Gaussian, with three members each. However, ANFIS itself is not capable of differentiating the attempts, since, as a curve fitting algorithm, it is not designed for biometric classification. Therefore an imaginary fraud training set is computed and concatenated to (1) namely;

$$P = \left[x_i, y_i, x_f, y_f, t\right] \rightarrow 1 \tag{5}$$

$$P' = \left[480 - x_i, 800 - y_i, 480 - x_f, 800 - y_f, 2 - t\right] \rightarrow 0 \tag{6}$$

so we achieve;

$$P_{new} = [P\,;P'] \tag{7}$$

Using P_{new} as the main training set consisting of 20 trials, the ANFIS is trained and the training set is tested to validate the success of training by plotting the FIS output vs training data in Figure 4. The generated Sugeno-FIS has 5 inputs and Gaussian membership functions which are shown in Figure 5.

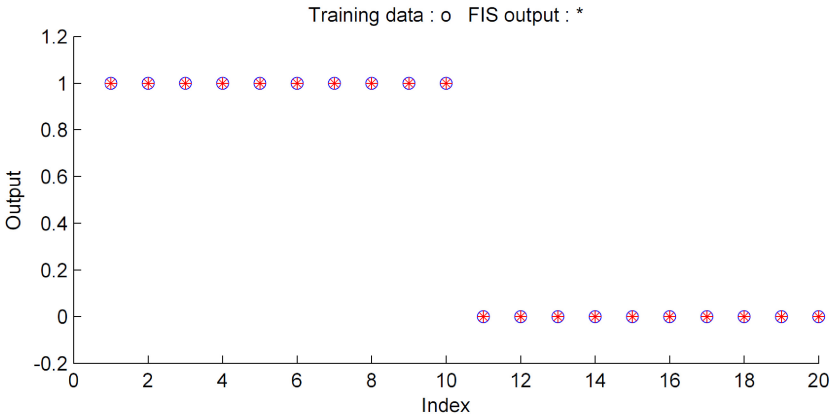

Fig. 4. ANFIS testing.

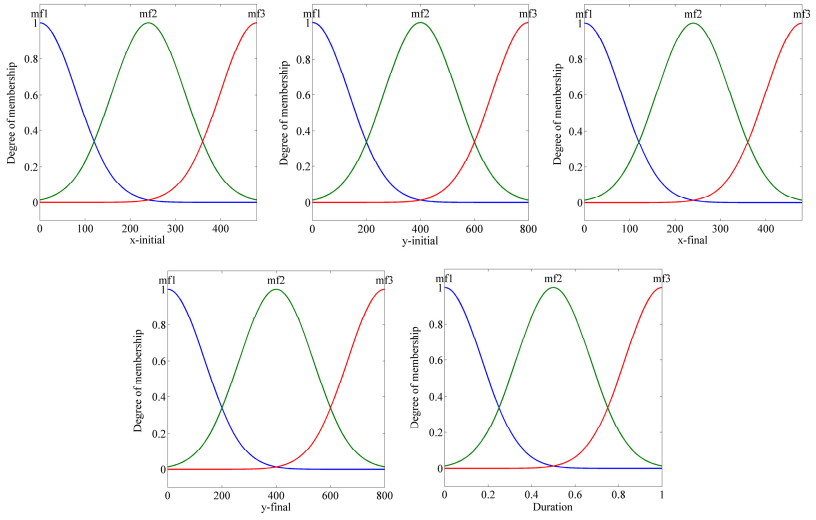

Fig. 5. FIS Membership functions

Although the expected result to validate the attempt is 1, we again defined a confidence interval between $o_{max} = 1.02$ and $o_{min} = 0.98$. Given the results of training session, both systems are perfectly adjusted to discriminate real attempts from fraud attacks.

4 Experimental Results

In the testing phase, 100 fraud and 100 real attempts are collected to check the performance of the systems. 100 fraud attacks are completely unbiased and totally random, however real attempts are made by the owner himself, therefore the paths and durations are more or less similar with the training set, which could be seen in Figure 6.

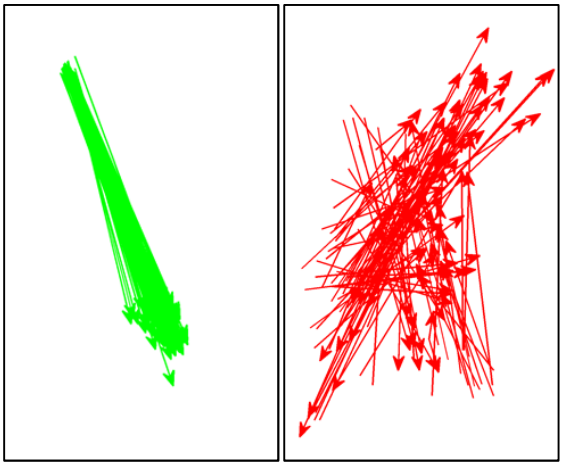

Fig. 6. Real Attempts (on the left) vs Fraud Attacks (on the right)

Initially, the LM-ANN results are analyzed to find false reject rate (FRR), false accept rate (FAR) and EER. According to the classification of LM-ANN, the FRR=8% which is higher than expected, in contrast FAR=1% which means that only 1% percent of the fraud attacks are granted. Equal error rate, which corresponds the intersection points of FRR and FAR, is linearly interpolated as EER=2.2%.

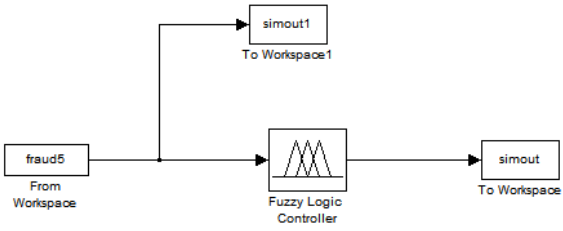

Fig. 7. Simulink Design for ANFIS

By the help of Simulink, the fraud and real attempts were easily calculated by the FIS that the ANFIS generated.

The results of ANFIS are a little reverse that FRR=0%, FAR=10% and EER is estimated as 5.4%. The consolidated EER points of output curves for both classifiers are shown in Figure 8.

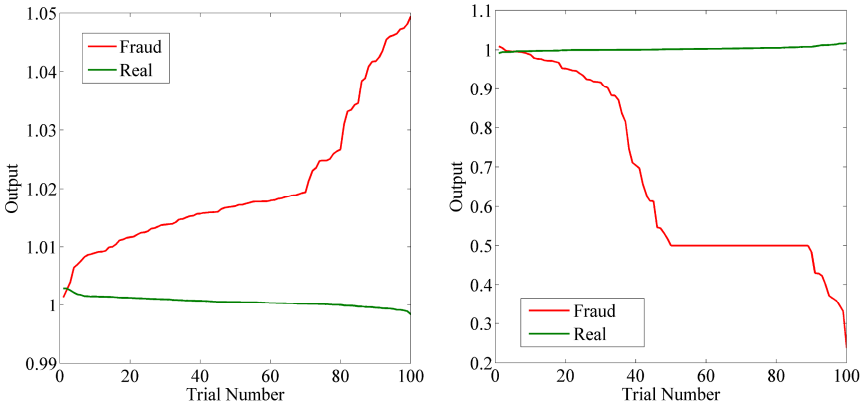

Fig. 8. Output Curves and EER points (LM-ANN on the left, ANFIS on the right)

Beside of these methods, two curves are mandatory to evaluate the performance of biometric authentication systems. Receiver Operating Characteristic (ROC) curve is a general tool to summarize the results using 1-FRR and FAR percentages while, Detection Error Trade-off (DET) curve is a useful tool to plot the error rates on both axes by FAR% and FRR% with a special scale-free diagram as in Figure 9.

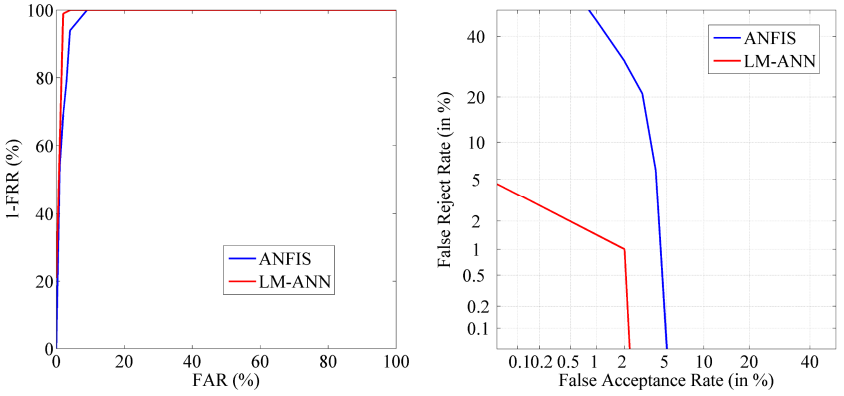

Fig. 9. ROC Curves on the left, DET curves on the right

The ROC curves also provide an insight for sensitivity since they are calculated by altering the $\dot{o}_{max}$ and $\dot{o}_{min}$ values to check the system performance within various intervals. However for each new interval the calculated FAR and FRR rates could be the same and we selected the points that will start from (0,0),end in (100,100) and reveal a continuous line. The infrastructure beneath the ROC concept is briefly the unconditional existence very narrow and very large intervals to make the FAR and FRR both 0 and 100.

According to the ROC curves, the performance of the LM-ANN is slightly better than ANFIS since it is increasing more sharply and ANFIS is closer to the x=y axis. Moreover, the DET curves prove the same argument: in ANFIS to reduce FAR by 3% we need to sacrifice 30% FRR, however in LM-ANN only 5% FRR will be sacrificed for %2 reduction of FAR.

5 Conclusions and Discussions

As a brief summary, we introduced two types of artificial intelligence based classifier to strengthen the swiping authentication. According to the results, both seems useful on enhancing swiping process by biometric features since the equal error rates are promising though LM-ANN had slightly better EER. ROC and DET curves are encouraging for both classifiers yet LM-ANN is again superior.

Regarding LM-ANN, the network is trained by 200 epochs however the number of iterations could be extended or reduced based on the desired narrowness level. If extended, the resulting interval would be so narrow that the FAR will be higher however if reduced FRR will increase. In contrast we trained ANFIS by 30 epochs which seems enough to fit the training data and FIS outputs. However the main disadvantage of ANFIS is necessity of an imaginary set to generate the FIS.

As future research, whole trace could be extracted instead of initial and final coordinates. If LM-ANN is desired to be the major training algorithm then it is possible to create a skip-layer network to give importance to the duration data. Although our network is fully connected, it is plausible to erase some connections to achieve more precise results however it is not recommended for this project since the coordinate data we're using is in order. Additionally the kernel seems suitable for nearest neighbor algorithms if the features will be the coordinates. On the other hand, the points could be turned into angles to reduce the number of inputs however the starting point of swiping will be lost this time.

Acknowledgment. This work and the contribution were supported by project "SP/2014/05 - Smart Solutions for Ubiquitous Computing Environments" from University of Hradec Kralove.

References

1. Zheng, N., Bai, K., Huang, H., Wang, H.: You are how you touch: User verification on smartphones via tapping behaviors. Technical Report, College of William and Mary (2012)
2. Kwapisz, J., Weiss, G., Moore, S.: Cell phone-based biometric identification. In: Proceedings IEEE Int. Conf. on Biometrics: Theory Applications and Systems (2010)
3. Chang, T.Y., Tsai, C.J., Lin, J.H.: A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices. Journal of Systems and Software **85**(5), 1157–1165 (2012)
4. Sae-Bae, N., Ahmed, K., Isbister, K., Memon, N.: Biometric-rich gestures: a novel approach to authentication on multi-touch devices. In: CHI 2012 Proceedings of the 2012 ACM Annual Conference on Human Factors in Computing Systems, New York (2012)
5. De Luca, A., Hang, A., Brudy, F., Lindner, C., Hussmann, H.: Touch me once and i know it's you!: implicit authentication based on touch screen patterns. In: CHI 2012 Proceedings of the 2012 ACM Annual Conference on Human Factors in Computing Systems, New York (2012)
6. Angulo, J., Wästlund, E.: Exploring touch-screen biometrics for user identification on smart phones. In: Camenisch, J., Crispo, B., Fischer-Hübner, S., Leenes, R., Russello, G. (eds.) Privacy and Identity Management for Life. IFIP AICT, vol. 375, pp. 130–143. Springer, Heidelberg (2012)
7. Shahzad, M., Liu, A.X., Samuel, A.: Secure unlocking of mobile touch screen devices by simple gestures: you can see it but you can not do it. In: Proceedings of the 19th Annual International Conference on Mobile Computing & Networking. ACM (2013)
8. Schaub, F., Deyhle, R., Weber, M.: Password entry usability and shoulder surfing susceptibility on different smartphone platforms. In: Proceedings of Mobile & Ubiquitous Multimedia (2012)
9. Shahzad, M., Zahid, S., Farooq, M.: A hybrid GA-PSO fuzzy system for user identification on smart phones. In: ACM, Proceedings of the 11th Annual Conference on Genetic and Evolutionary Computation, pp. 1617–1624 (2009)
10. Maiorana, E., Campisi, P., González-Carballo, N., Neri, A.: Keystroke dynamics authentication for mobile phones. In: Proceedings of the 2011 ACM Symposium on Applied Computing, pp. 21–26. ACM (2011)
11. Rao, M.K., Aparna, P., Akash, G.A., Mounica, K.: A Graphical Password Authentication System for Touch Screen Based Devices. International Journal of Applied Engineering Research **9**(18), 4917–4924 (2014)
12. Jeanjaitrong, N., Bhattarakosol, P.: Feasibility study on authentication based keystroke dynamic over touch-screen devices. In: 2013 13th International Symposium on Communications and Information Technologies (ISCIT), pp. 238–242. IEEE (2013)
13. Do, S., Hoang, T., Luong, C., Choi, S., Lee, D., Bang, K., Choi, D.: Using Keystroke Dynamics for Implicit Authentication on Smartphone. 멀티미디어학회논문지 **17**(8), 968–976 (2014)
14. Trojahn, M., Arndt, F., Ortmeier, F.: Authentication with time features for keystroke dynamics on touchscreens. In: De Decker, B., Dittmann, J., Kraetzer, C., Vielhauer, C. (eds.) CMS 2013. LNCS, vol. 8099, pp. 197–199. Springer, Heidelberg (2013)
15. Rogowski, M., Saeed, K., Rybnik, M., Tabedzki, M., Adamski, M.: User authentication for mobile devices. In: Saeed, K., Chaki, R., Cortesi, A., Wierzchoń, S. (eds.) CISIM 2013. LNCS, vol. 8104, pp. 47–58. Springer, Heidelberg (2013)

16. Bours, P., Masoudian, E.: Applying keystroke dynamics on one-time pin codes. In: 2014 International Workshop on Biometrics and Forensics (IWBF), pp. 1–6. IEEE (2014)
17. Frank, M., Biedert, R., Ma, E., Martinovic, I., Song, D.: Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE Transactions on Information Forensics and Security **8**(1), 136–148 (2013)
18. Sae-Bae, N., Memon, N., Isbister, K., Ahmed, K.: Multitouch Gesture-Based Authentication. IEEE Transactions on Information Forensics and Security **9**(4), 568–582 (2014)
19. Zhao, X., Feng, T., Shi, W., Kakadiaris, I.: Mobile User Authentication Using Statistical Touch Dynamics Images. IEEE Transactions on Information Forensics and Security **9**(11), 1780–1789 (2014)
20. Alpar, O.: Keystroke recognition in user authentication using ANN based RGB histogram technique. Engineering Applications of Artificial Intelligence **32**, 213–217 (2014)
21. Campisi, P., Maiorana, E., Bosco, M.L., Neri, A.: User Authentication Using Keystroke Dynamics for Cellular Phones. IET Signal Processing - Special Issue on Biometric Recognition **3**(4), 333–341 (2009)
22. Tasia, C.J., Chang, T.Y., Cheng, P.C., Lin, J.H.: Two novel biometric features in keystroke dynamics authentication systems for touch screen devices. Security and Communication Networks **7**(4), 750–758 (2014)
23. Kang, P., Cho, S.: Keystroke dynamics-based user authentication using long and free text strings from various input devices. Information Sciences (2014). http://dx.doi.org/10.1016/j.ins.2014.08.070
24. Kambourakis, G., Damopoulos, D., Papamartzivanos, D., Pavlidakis, E.: Introducing touchstroke: keystroke-based authentication system for smartphones. Security and Communication Networks (2014). doi:10.1002/sec.1061
25. Levenberg, K.: A method for the solution of certain problems in least squares. Quarterly of Applied Mathematics **2**, 164–168 (1944)
26. Marquardt, D.W.: An algorithm for least-squares estimation of nonlinear parameters. Journal of the Society for Industrial & Applied Mathematics **11**(2), 431–441 (1963)