2017 Second International Conference on Recent Trends and Challenges in Computational Models

A secure gesture based authentication scheme to unlock the smartphones

S.Milton Ganesh
Assistant Professor,
Deptment of Computer Science and Engineering
University College of Engineering Tindivanam
Melpakkam, Tamilnadu, India - 604 001
e-mail: softengineermilton@gmail.com

P.Vijayakumar
Dean i/c
University College of Engineering Tindivanam
Melpakkam, Tindivanam, India - 604001
e-mail: vijibond2000@gmail.com

L.Jegatha Deborah
Assistant Professor and Head i/c,
Deptment of Computer Science and Engineering
University College of Engineering Tindivanam
Melpakkam, Tamilnadu, India - 604 001
e-mail: blessedjeny@gmail.com

***Abstract*—In the recent times, the smart phones have become versatile that they are used for sensitive applications such as m-banking, m-commerce, m-governance, m-health, digital marketing, SMS and have become a vital gadget to share posts in social networking applications such as Facebook, Twitter, WhatsApp and others. It is also used for online gaming, surfing, chatting and also used for storing the personal information like photos, videos, documents and other important files. In this scenario, it is no surprise that the basic demand for utilizing a smart phone is secure authentication. Though a number of authentication schemes have been proposed in the literature through PIN numbers, passwords and patterns, they are susceptible for shoulder surfing or smudging attacks. Thus, combing gestures with such authentication schemes prove to be more successful in the present times and hence a new kind of pattern has been proposed with essential gestures such as finger pressure and inclination of the phone while it is being unlocked. This work is different from the previous works in two dimensions. First, the proposed pattern is secure against both shoulder surfing and smudging attacks. Second, the computational complexity of authentication scheme has been reduced. Through extensive experiments it can be proved that this work outperforms many works in the recent literature and hence it would be an ideal candidate for the secure authentication of smart phones.**

Keywords- Smartphone, authentication, gesture, fuzzy, security, biometric

I. INTRODUCTION

A smart phone is more than used as a mobile phone today and it has a technologically updated operating system like Android, iOS, and Windows Mobile [15]. In the present market, smart phones are available cheap in the market with at least 2GB RAM powered by a dual core processor technology. Hence, a smart phone is capable of running applications specially designed for them. The applications which run on smart phones are called as apps and each business reaches out to its customers through dedicated apps and governments try to interact with the citizens through apps designed for necessary purposes. Digital marketing strategies change the way marketing and advertisements are done and hence it has added a new dimension in which the products are brought to the notice of the customer through mobile phones. Even banks prefer their customers to do transactions through mobile banking and this case is true with each and every sector of our life. In line with this scenario, at present, smart phones have become a part and parcel of human life. In future, with the widespread explosion of cloud computing and Internet of Things, the impact of smart phones in our life would be an indispensable one and hence authentication for smart phones is mandatory to protect the sensitive and valuable information stored in them [17-18].

With the advent of touch screens and the prevalence of mobile phones in today's digital life, the information stored in the gadgets becomes crucial and hence a number of authentication procedures have been invented especially for touch screen mobile phones. One of the earliest approaches to protect the touch screens was through PIN numbers. A user who enters the correct PIN number is authenticated. Followed by this, password based authentication mechanisms were invented in which a user enters a password composed of alphanumerical characters and proved to be more secure approach than the former mechanism. A third procedure using patterns was introduced in smart phones which became the default authentication scheme for millions of users of the smart phones. Patterns are special diagrams in which a user who attempts to authenticate a smart phone shall connect the dots which refer to the secret numbers. If the dots are connected in sequence, the gadget is unlocked.

Each of the schemes is being used by different sections of the society who use smart phones. Among them, patterns have become widespread. Two major attacks which challenge the above mentioned three authentication schemes

978-1-5090-4799-4/17 $31.00 © 2017 IEEE
DOI 10.1109/ICRTCCM.2017.31

are shoulder surfing attack and smudging attack. In shoulder surfing attack, the attacker who wants to masquerade, gets a visible observation on the way a pattern is drawn, PIN or password is entered. Hence, in this way, an intruder can easily unlock the phone if the phone is not properly protected during the intruder's authentication attempts. In smudging attacks, the oil residues left on the screen of a smart phone is traceable under proper lighting scenarios. In such attacks, a user who unlocks a phone leaves oil residues on the screen of smart phones. If the phone is lost or stolen, then the attacker can use proper lighting conditions in an attempt to unlock the phone by seeing the smudges left on the screen by the authenticated user. An accuracy of 68% was achieved when a team of investigators from the University of Pennsylvania [16] attempted to unlock the phone using smudging attacks.

But gesture based authentication schemes have evolved in the recent times to resist the authentication procedures from the shoulder surfing and smudging attacks. They are based on how does a user input the pin number, password or draws a pattern. Previous works concentrated only on what the users give as input to the authentication scheme. But, the gestures are referred to as biometric features and they are combined with PIN/Password/Pattern based approach for unlocking the smart phones. Since the gestures exhibit the biometric features of a person which are unique to each and every human, an attempt to unlock the phone by an attacker becomes impossible. Previously, gestures were embedded with PIN numbers and Password procedures. In the recent past literature, a number of gesture based authentication schemes have been introduced which proved to be highly resistive to the aforementioned attacks. Some of the major drawbacks of these approaches is that the computational complexity involved in the scheme, high false positive rate and the requirement to embed special sensors for the purpose of authentication. Hence, a scheme which involves low computational complexity, provides an enhanced true positive rate, more accurate in authenticating the user without the need for special sensors is the need of the hour.

The rest of the proposed work has been organized as follows. A detailed literature survey of the recent works on gesture based authentication schemes is given in section 2. Section 3 gives a basic overview of the proposed system and section 4 describes the proposed model of providing authentication using gestures. Section 5 concludes the proposed work and gives future research directions.

II. LITERATURE SURVEY

Numerous research works on gesture based authentication have been proposed by researchers and the major mobile phone vendors in an attempt to give better authentication procedures to the smart phones. In the earlier days, biometric features used for the authentication include fingerprints [26-30], face [31-35], voice [36-38], ear [39-40], iris and others. Gestures which have been widely used for the authentication of touch screens include keystroke based authentication [19-20], gait based authentication [21-22], pattern based authentication [23-24], touch based authentication [26] and the latest research in this line of invention is hand waving gesture based authentication.

H. Saevanee and P. Bhattarakosol [2] had proposed a work on keystroke dynamics and finger pressure in 2009 which detected the finger pressure, the key hold time and key time between the two key presses to provide a quick authentication scheme. They have proved that using the finger pressure alone, the accuracy obtained was 99%. Another work on keystroke based authentication was proposed by Ting-Yi Chang and others [1] in 2012 in which a new password based on graphical features was proposed which increased the number of passwords a user can use to authenticate the phone. The gesture used for authentication is the pressure exerted by a user while entering the password and this method reduced the EER (Equal Error Rate) to 6.9% from 12.2% which was better than the previous works. A work done by Cristiano Giuffrida et al [3] in 2014 combined the gesture features from the accelerometer sensor and gyroscope sensor. From the accelerometer sensors, the features such as movement of the phone in three axes were observed and from the gyroscope sensor, the features such as inclination of the device in the three axes were observed. Thus, by combing all these features, they were able to provide an ERR of 0.08% using the K-Nearest Neighbor (K-NN) classifier.

Authenticating a user based on the way a user walks is another approach in which video cameras were used for authentication in the olden times and the sensors were attached to the body of a user for the same purpose in the recent times. A work done by R.Ferrero et al. [4] in 2015 embedded gait sensor in the hip of a user and when measured, an EER of 7% and 33% was achieved as minimum and maximum. Another work by Watanabe.Y et al. [6] in 2014 considered both the linear and rational movements of the user during his authentication procedure. For this purpose, sensors used were gyroscope and electromagnetic compass and the features obtained were combined for authenticating the user. A work by C.Nicket et al. [5] used extensive evaluation using 48 different persons and the testing was conducted for nearly two days in which the training was provided on both flat and non linear pathways which improved the authentication applicability to a real world scenario.

A more convenient way preferred by the users of this modern world is to authenticate the smart phone using convenient patterns. A pattern consists of an arrangement of dots which need to be connected in the correct order for correct authentication and relatively only a few works have been proposed in this direction. Orcan Alpar [7] had proposed a pattern consisting of numbers for the authentication, and classified the inputs using Artificial Neural Networks, Neuro-Fuzzy systems and histogram based approach. Julio Angulo et al. [8] proposed another work in which people from different age groups were tested for authentication in which the time duration of the finger inside the dots and the time duration of the finger between

the dots were considered. Random forest classifier was used for the classification and it proved to be successful than the previous algorithms. A work proposed by A.J.Aviv [9] studied the smudge attacks done on patterns using different lighting conditions and their impacts. It was found that, if a smudge attack was posed based on different lighting angles, then it is possible to unlock a smart phone using only a few attempts.

Ankita Jain et al. [10] proposed an authentication scheme based on touch dynamics to unlock the smart phones. The biometric features from orientation sensor, accelerometer sensor and the touch sensor were used for the authentication. Different authentication samples such as from right to left and vice versa, zoom in, zoom out, tapping the touch screen and the finger touch area were considered and this method provided an EER of 0.31%. Y.Meng et al. [11] done an extensive analysis in which 20 persons were used for the training purpose and the classification was done based on 120 sessions. Though this method incurred more computational complexity, it is one of the significant works in touch dynamics as it employed both single touch and multi touch behaviors of users.

One of the recent authentication schemes based on gestures is the authentication of smart phones using hand waving biometrics. This method does not employ any keystrokes, gait patterns or pattern locks. Rather, a user is expected to expose his unique biometrics through a simple hand wave of a phone which reduces the overall time for the authentication scheme and shows more convenience. Lei Yang et al. [12] had proved that a user can authenticate a phone by waving for just 1 to 2 seconds continuously. Support Vector Machine was used for classification of the inputs from the accelerometers which observed the inputs from the movement of the smart phone in x,y and z axes. Another proposal by S.Karita et al. [13] used clustering approach in which the collected features such as the rotation of the wrist, movement of the phone from left to right and from right to left were saved in a server and during authentication, the features observed were compared with the ones from the server. A recent work by J. Guerra-Casanova et al. [14] considered the accelerometer movements of the phone in three axes for the user authentication in which 100 users were tested and each user was asked to give 8 samples for the training purpose. Though additional sensors are not needed in this approach, the computational complexity needs to be improved further.

Thus, though a number of works have been put forward in the past literature, none of them provides convenient gestures with less computational complexity and more accuracy for authenticating a smart phone. Thus the objectives of the proposed work are as follows.

(1) To authenticate a valid user with low computational complexity to support the energy constrained smart phones.
(2) To increase the true positive rate of the approach such that the number of valid authentication attempts are increased.
(3) To enhance the accuracy of the authentication scheme using an intelligent decision making system like Fuzzy Inference System.

To provide authentication based on the sensors which are prevalent in most of the smart phones making this scheme applicable to all the touch screen phones.

III. OVERVIEW OF THE PROPOSED SYSTEM

The proposed work consists of three new components.

A. Pattern

A new kind of pattern in the shape of a circle as in Fig. 1 is proposed in this work in which the numbers from 0 to 9 are displayed. A user is required to remember the password and draw the correct pattern by connecting the numbers present in the pattern. A salient feature of this pattern is that the numbers in the pattern change their locations during each attempt to unlock the phone. This means that a person who has seen a particular number, for example '2' at a particular location in the circle, will not find it at the same location during the second attempt to unlock the smart phone.

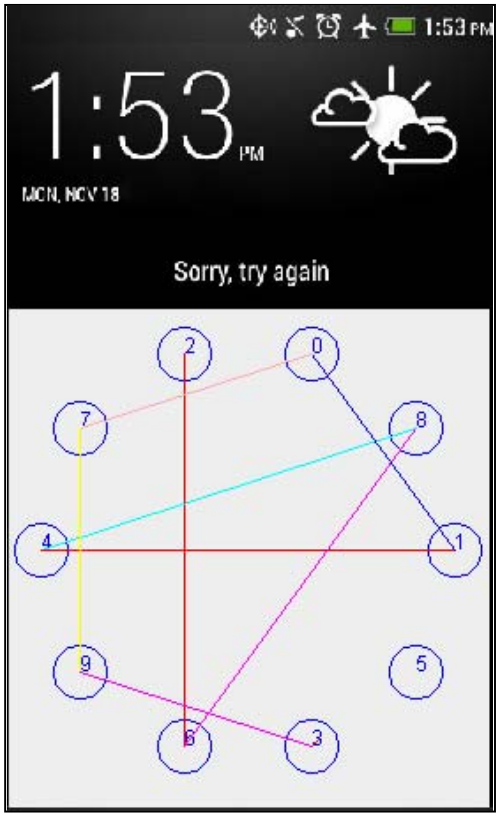

Fig. 1. A new pattern used in the proposed approach

B. Biometric Features

The biometric features selected for authentication include finger pressure and the inclination of the phone with respect to x, y and z axes. Each person in this world exerts a different pressure pattern on the touch screens during authentication. This unique feature is considered for authentication. Moreover, each user holds the smart phone at a particular angle during the usage of a phone and hence during the authentication process as well. Thus, the combination of features such as finger pressure and the inclination of phone will be a better biometric signature to uniquely identify the genuineness of a valid user. This biometric authentication process would add another layer of security to the normal patters being used for authentication.

C. Fuzzy Inference System

It was introduced by Lotfi L. Zadeh in 1964. A fuzzy inference system as illustrated in Fig. 2 is based on if-then rules is used in this proposed work. The mechanism of the fuzzy intelligent decision making system is that, the given input values are converted into fuzzy values. As the fuzzy expert sytems are interdisciplinary in nature, the fuzzy if-then rules are applied on the input dataset. The corresponding fuzzy output is then converted into the crisp output. If the output of the fuzzy expert system crosses the threshold value of 85%, then the user who tries to authenticate the smart phone is authenticated. Otherwise, the user is an invalid user.

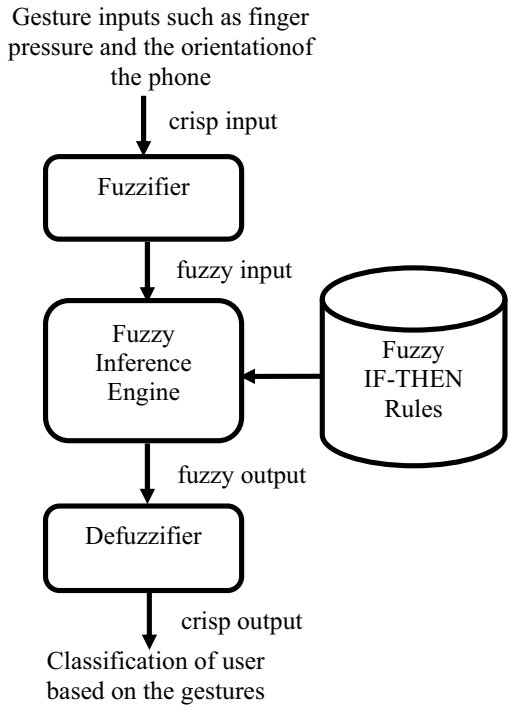

Fig.2. User classification by fuzzy inference system

A new kind of pattern based on circular shape in which numbers from 0 to 9 are displayed. A user is required to remember the password and draw the correct pattern by connecting the numbers present in the pattern. Since the position of numbers change, it is difficult for an attacker to unlock it using smudging attacks. A person who identified a particular number at a particular place in the circle will not find it at the same place during the successive attempt to unlock the smart phone.

IV. PROPOSED WORK

The proposed work consists of two stages. In the first stage, the fuzzy inference system is trained using the relevant number of training samples. During each training sample collection, the necessary gesture parameters for the finger pressure and the phone inclination are collected and stored in the database. The training samples are collected till the average of training samples becomes greater than or equal to 95% of the true positive rates.

A. Training the Classifier

The smart phones of today are equipped with sensors to detect the motion of the fingers drawing patterns in the touch screen. The proposed work consists of smart phones which have an embedded sensor for sensing the finger pressure exerted while a user draws a pattern and the orientation sensor such as gyroscope from which the inclination of the phone with x, y and z axes are received. For each drawn pattern, the finger pressure exerted by the finger of the valid user is noted down in the database and an average threshold value based on the above two parameters are calculated until the true positive rate is maintained at 95% during training.

B. Authentication using gestures

The actual authentication procedure consists of two layers of security. The first layer of defense is verifying whether the drawn pattern connects the actual PIN numbers. For example, a user may store a password along with the gestures in the smart phone during training. Suppose, the user has used the PIN number 13476 as the numbers to be connected for authentication. Thus during authentication, this PIN number along with the necessary biometric features are stored in the database

1) Drawing the right pattern: During the user authentication process, the user who wants to unlock the phone has to first draw the correct pattern containing the PIN numbers registered during the training phase. Since the user has used the PIN number 13476 during the training phase, the same numbers need to be connected during the first phase of authentication process. If it is wrong, then the authentication resists the user by saying that the PIN number is incorrect. The highlight of this approach is that the position of the numbers in the pattern constant change during each authentication attempt by a user.

2) Authentication using biometric getrures: While a user inputs the correct pattern by connecting the dots, the system collects the relevant biometric features related to the

finger pressure and orientation. At present, the system makes intelligent decisions using the Fuzzy Inference Engine.

To make accurate decisions and reflect the human perspective, the fuzzy sets for the finger pressure gesture need to be well defined. In this regard, Table I lists the fuzzy sets for the gestures pertaining to the finger pressure and the orientation of the smart phone while a user unlocks a smart phone.

TABLE I. FUZZY SETS FOR THE GESTURES

Gesture parameter	Input metrices	Linguistic value	Degree of membership
Finger Pressure	Top to bottom	Low, medium, high	{0, 0.5, 1}
	Bottom to top	Low, medium, high	{0, 0.5, 1}
	Left to right	Low, medium, high	{0, 0.5, 1}
	Right to left	Low, medium, high	{0, 0.5, 1}
Orientation	x –axis	Very low, low, medium, high, very high	{0, 0.25, 0.5, 0.75, 1}
	y-axis	Very low, low, medium, high, very high	{0, 0.25, 0.5, 0.75, 1}
	z-axis	Very low, low, medium, high, very high	{0, 0.25, 0.5, 0.75, 1}
Authentication accuracy	Input from finger pressure and orientation	Low, medium, high	{0, 0.5, 1}

The main component of the fuzzy inference system is the fuzzy rule base which form the basis for the expert decisions. The rule base of the proposed fuzzy inference system is mentioned in Table II as follows:

TABLE II. FUZZY RULES

S.No.	Fuzzy rule
1.	If finger pressure is low, x-axis is low, y-axis low and z-axis is low, then authentication accuracy is low
2.	If finger pressure is low, x-axis is high, y-axis high and z-axis is low, then authentication accuracy is medium
3.	If finger pressure is low, x-axis is high, y-axis high and z-axis is high, then authentication accuracy is medium
4.	If finger pressure is high, x-axis is low, y-axis low and z-axis is low, then authentication accuracy is medium
5.	If finger pressure is high, x-axis is medium, y-axis very low and z-axis is very low, then authentication accuracy is low
6.	If finger pressure is high, x-axis is very low, y-axis very low and z-axis is high, then authentication accuracy is medium
7.	If finger pressure is low, x-axis is very high, y-axis very high and z-axis is very high, then authentication accuracy is medium
8.	If finger pressure is high, x-axis is medium, y-axis low and z-axis is high, then authentication accuracy is high
9.	If finger pressure is low, x-axis is high, y-axis very high and z-axis is very high, then authentication accuracy is medium
10.	If finger pressure is high, x-axis is very high, y-axis very high and z-axis is medium, then authentication accuracy is high
11.	If finger pressure is high, x-axis is very high, y-axis very high and z-axis is very high, then authentication accuracy is high
12.	If finger pressure is medium, x-axis is very high, y-axis very high and z-axis is very high, then authentication accuracy is high

When the system confirms that a user has successfully passed the first stage of authentication by drawing the correct pattern, then the biometric features of the user are collected. At this stage, the input values are vague and hence are crisp values. The fuzzy inference system can process the data only if the data is mentioned in terms of fuzzy sets. Thus, the fuzzifier component converts the input data collected using the sensors into the corresponding fuzzy input. The fuzzy input is a representation of the input data in terms of fuzzy membership functions. Now, the fuzzy inference system makes intelligent decisions based on the aforementioned rule base and predicts the output. The output value is a fuzzy membership function again and hence it is converted into the crisp output using the relevant defuzzifier. The crisp output is then compared with the threshold value as to whether the output value is greater than or equal to the threshold value. If it holds true, then the user is authenticated and else, the user is informed about the invalid login attempt and the login failure notice. The user tries to authenticate the system again.

V. CONCLUSIONS

A gesture based authentication scheme has been proposed in this work to securely unlock the smart phones with touch screens. This authentication approach is based on the fuzzy inference system which makes decisions based on the finger pressure of the user and the inclination of the phone with respect to the three axes. The system is trained using relevant datasets containing the necessary features from the authorized user. During an actual authentication attempt, the fuzzy system makes intelligent decisions with the input parameters against a threshold value to securely unlock the phones. Because of the proven ability of the inference system, the equal error rate, true positive rate are increased and hence the false positive rate is reduced. Future works include authentication procedure being enhanced to support alphanumerical characters in the pattern and more biometric features with further reduction in the computational complexity.

REFERENCES

[1] Ting-Yi Changa, Cheng-Jung Tsai and Jyun-Hao Lin, “A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices”, in the Journal of Systems and Software 85, pp 1157– 1165, IEEE, 2012.

[2] H. Saevanee and P. Bhattarakosol, “Authenticating user using keystroke dynamics and finger pressure”, in Consumer Communications and Networking Conference, IEEE Xplore, 2009.

[3] Cristiano Giuffrida, KamilMajdanik, Mauro Conti, and Herbert Bos, “I Sensed It Was You: Authenticating Mobile Users with Sensor-Enhanced Keystroke Dynamics”, in the proceedings of 11th International Conference, DIMVA 2014, Egham, UK, July 10-11, pp 92-111, Springer,2014

[4] Ferrero, R, Dipt. diAutom. e Inf., Politec. di Torino, Turin, Italy, Gandino, F, Montrucchio, B, Rebaudengo, M.,"On gait

recognition with smartphone accelerometer",in the 4th Mediterranean Conference onEmbedded Computing (MECO),Budva,June 14-18,pp 368-373,IEEE,2015.

[5] Claudia Nickel, Christoph Busch, "Classifying Accelerometer Data via Hidden Markov Models to Authenticate People by the Way They Walk",in Aerospace and Electronic Systems Magazine,Volume:28,pp 29-35,IEEE,2013.

[6] Watanabe. Y, "Influence of Holding Smart Phone for Acceleration-Based Gait Authentication", in Fifth International Conference on Emerging Security Technologies (EST), Alcala de Henares, pp 30-33, IEEE, 2014 .

[7] OrcanAlpar , "Intelligent biometric pattern password authentication systemsfor touchscreens," in the journal of Expert Systems with Applications, pp 6286–6294, Elsevier, 2015.

[8] Julio Angulo, Erik Wästlund, "Exploring Touch-Screen Biometrics for User Identification on Smart Phones", in the journal Privacy and Identity Management for Life, pp 130-143, Springer, 2012.

[9] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," in Proc. 4th USENIX Conf. on Offensive technologies, pp. 1–10, 2010.

[10] Ankita Jain and VivekKanhangad,"Exploring orientation and accelerometer sensor data for personal authentication in smartphones using touchscreen gestures", to appear in the journal of Pattern Recognition Letters, Elsevier, 2015.

[11] YuxinMeng, Duncan S. Wong, Roman Schlegel, and Lam-for Kwok,"Touch Gestures Based Biometric Authentication Scheme for Touchscreen Mobile Phones", in the8th International Conference(Inscrypt 2012), Beijing, China, November 28-30,pp 331-350, Springer-Verlag, 2013.

[12] Lei Yang,YiGuo,XuanDing,Jinsong Han ,"OpenSesame: Unlocking Smart Phone through Handwaving Biometrics", in Transactions On Mobile Computing, pp 1044 – 1055, IEEE, 2015.

[13] Shigeki Karitat, KumiNakamurat, Kazuhiro Konott, Yoshimichitottt, Noboru Babaguchit, "OWNER Authentication For Mob Ile Devices Using Motion Gestures Based On Multi-Owner Template UPDATE", in the International Conference on Multimedia & Expo Workshops (ICMEW), June 29 2015-July 3, pp 1-6, IEEE,2015.

[14] J. Guerra-Casanova , C. Sánchez-Ávila, G. Bailador , A. de Santos Sierra,"Authentication in mobile devices through hand gesture recognition", in International Journal of Information Security, volume 11, pp 65-83, Springer,2012.

[15] https://en.wikipedia.org/wiki/Smartphone

[16] https://en.wikipedia.org/wiki/Smudge_attack

[17] "2002 NTA Monitor password survey," http://www.outlaw.com/page-3193, Last visit: 04.09.2006.

[18] Baum, L. E., and Petrie, T. Statistical inference for probabilistic functions of finite state markov chains. The Annals of Mathematical Statistics, Vol. 37, 6 (1966), 1554–1563.

[19] Matthias Trojahn, Frank Ortmeier, "Toward mobile authentication with keystroke dynamics on mobile phones and tablets," in the 27th International Conference on Advanced Information Networking and Applications Workshops, pp 697 - 702, IEEE, 2014.

[20] PapamartzivanosandEmmanouilPavlidakis,"Introducing touchstroke: keystroke-based authentication system for smartphones," in Security Comm. Networks, John Wiley and Sons Pvt. Ltd, 2014.

[21] Thang Hoang, DeokjaiChoi,Thuc Nguyen ,"Gait authentication on mobile phone using biometriccryptosystem and fuzzy commitment scheme", in Internal Journal of Information Security, pp 1-12, Springer, 2015.

[22] Mohammad Derawi , Patrick Bours,"Gait and activity recognition using commercial phones", in the Journal of Computers and Security, Volume 39, pp 137-144, Elsevier, 2013.

[23] Alexander De Luca, Alina Hang, FrederikBrudy, Christian Lindner, Heinrich Hussmann, "Touch me once and I know it's you! Implicit Authentication based on Touch Screen Patterns", in 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA), Fukuoka , 704 - 707, Mar 26-29, IEEE, 2012.

[24] Emanuel von Zezschwitz, Anton Koslow, Alexander De Luca, Heinrich Hussmann,"Making graphic-based authentication secure against smudge attacks", in Proceedings of the international conference on Intelligent user interfaces(IUI '13),March 19–22, Santa Monica, CA, USA, ACM, 2013.

[25] Napa Sae-Bae, Kowsar Ahmed, Katherine Isbister and NasirMemon," Biometric-Rich Gestures: A Novel Approach to Authentication on Multi-touch Devices", in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12), New York, NY, USA,pp 977-986,ACM,2012.

[26] J. H. Wegstein, An Automated Fingerprint Identification System, National Bureau of Standards Special Publication 500-89,republished by National Technical Information Service, U.S. Dept. Commerce, Springfield, VA, 1982.

[27] M. Kawagoe and A. Tojo, "Fingerprint pattern classification," Pattern Recognit., vol. 17, no. 3, pp. 295–303, 1984.

[28] Federal Bureau of Investigation, "The Science of Fingerprints: Classification and Uses", Washington, D.C.: GPO, 1984.

[29] A. Dvorak, N. Merrick, W. Dealey, and G. Ford,"TypewritingBehavior", American Book Company, NewYork, USA, 1936.

[30] F. Galton. Finger Prints. Mcmillan, London, 1892.

[31] M.E.Fathy, V.M.Patel, R.Chellappa, "Face-based Active Authentication on mobile devices", in the International Conference on Acoustics, Speech and Signal Processing (ICASSP), South Brisbane, QLD, pp 1687-1691, IEEE, 2015.

[32] M.A. Turk and A.P. Pentland, "Face Recognition Using Eigenfaces," Proc. IEEE Conf. Computer Vision and Pat ern Recognition (CVPR 91), 1991, pp. 586–591.

[33] A. Nefian, M. Hayes, "An Embedded HMM-based Approach for Face Detection and Recognition", IEEE International Conference on Acoustic Speech and Signal Processing, vol. 6, 1999.

[34] P. J. Phillips, A. Martin, C. L. Wilson, and M. Przybocki, "An introduction evaluating biometric systems," Computer, vol. 33, no. 2, pp. 56–63, 2000.

[35] A. Nefian, M. Hayes, "An Embedded HMM-based Approach for Face Detection and Recognition", Proc. IEEE Int. Conf. On Acoustics, Speech and Signal Processing, vol. 6, 1999.

[36] L. Rabiner, "A tutorial on hidden Markov models and selected applications in speech recognition", Proc. IEEE.Vol. 77(2), 257-286, 1989.

[37] D. O'Shaughnessy, "Speech Communication - Human and Machine", Addison-Wesley, New York, 1987.

[38] P. Jourlin, J. Luettin, D. Genoud, H. Wassner, "Acoustic-labial speaker authentication", Pattern Recognition Letter. 18. 853-858, 1997.

[39] Li Yuan, Zhichun Mu, Zhengguang Xu, "Using Ear Biometrics for Personal Recognition", in the proceedings of the International Wokshop on Biometric Recognition Systems (IWBRS) 2005, Beijing, China, Oct 22-23, Springer, 2005.

[40] AfredIannarelli: Ear Identification. Forensic Identification Series.ParamountPublishingCompany, Fremont, California (1989).