

A Systematic Review of Features Identification and Extraction for Behavioural Biometric Authentication in Touchscreen Mobile Devices

Sami Abduljalil Abdulhak*, Ala Abdulhakim Alariki*

**Assistant Professor, Faculty of Information Technology and Computer Science, American university of Afghanistan, Darul Aman Road, Kabul, Afghanistan.
snaji@auaf.edu.af, aabdulaziz@auaf.edu.af*

Abstract

Today, mobile devices are being widely used in personal and professional life. By increasing the popularity of touchscreen platform as an input method in mobiles phones, touch gesture behaviour is becoming more significantly important in interaction with the phone. Due to increasing demand for safer access in touchscreen mobile phones, old strategies like pins, tokens, or passwords have failed to stay abreast of the challenges. By utilizing touch gesture behaviour biometric techniques, the authentication mechanism will improve and would make it more difficult for a shoulder surfer to replay the password, even if he observes the entire gesture. The purpose of this research is to conduct a systematic literature review SLR for the current state-of-the-art in the field of touch features gesture. The results of this research identified thirteen touch features followed by the previous studies (PSs) to authenticate users. However, based on the schemes followed by the previous studies (PSs) there was not any scheme that extract and use all touch features for mobile user authentication. There are number of areas of future work that could be carried out to advance upon this research and within the area of authentication on mobile devices. Each of the pervious study (PS) extracted only one or more features. The maximum number of features used in S14 year 2014 and S15 year 2015 were seven features. Extracting thirteen touch features and use them for the authentication will be one contribution in future work.

Keywords: Biometrics, smartphone authentication, touch gesture authentication, mobile security and android authentication.

1.0 INTRODUCTION

Mobile phones and to be specific the smartphone have largely permeated in almost all our daily lives. Currently they are part and particle of our daily lives be it at work, in schools, generally in all spheres of our lives today. This has been largely due to the wide range of services the smartphone provides such as keeping track of appointments, meetings, providing multimedia storage, access to social media and email, among others making it a very fundamental device in human life today. According to Seo et al. [1], there were 326.5 million smartphone users in 2010 globally. This was an increase of roughly 15 times in comparison to the number of users in 2005; they forecast by 2012, the number of users would reach 766.1 million. Most mobile phone services are provided via the internet making it ubiquitous, with a potential of unauthorized users

getting unlimited access to the device. This may lead to data that is private and sensitive to the owner be stolen or abused [2].

When a mobile phone in particular a smartphone is stolen, a lot of private and sensitive data can be compromised and be exploited for malicious activities, as the users of such phones usually are concerned about their sensitive data stored in the phone than the phone itself [3]. In essence, when a smartphone is lost, the consequences that come with it are dire; they include privacy intrusion, user impersonation, and sometimes severe financial loss. As a first defence step, user authentication is essential to protect a system. Currently, user authentication systems for mobile phones are mainly based on three techniques: passwords, physiological biometrics and behavioural biometrics [4]. Password authentication has well-known drawbacks, for instance, passwords can often easily be guessed and stolen through

“shoulder surfing” [5]. Moreover, password authentication method brings insufficient security level because writing them down, using simple passwords, or reusing passwords make them easy to break. In this way, it is important to make and grow uniquely adjusted systems, which are intended to be usable under these limitations.

Previous studies [6-10] have reported that biometric based person recognition is a good alternative to overcome the difficulties of password authentication. Biometric authentication is an authentication mechanism that uses human behavioural or physiological characteristics that are measurable, to define and represent the identity of a user.

Human physiological biometrics are the physical human body characteristics that uniquely identify a person, these include fingerprints, retina and human face [11]. Such biometrics are known to offer a consistent performance, however, they are also known to have a common disadvantage of being non-standardized and costly [12]. In addition, physical biometrics are difficult and intrusive for collectability, low degree of user acceptability [8]. As reported in Banerjee and Woodard [13], the use of biometrics such as face, fingerprints and signature requires additional tools to acquire the biometric which leads to an increase in costs. In contrast, behavioural

biometrics authentication relies upon a person's actions or habits to uniquely identify that person. Behavioural biometrics authentication may include signature recognition, mouse dynamics, touch gesture and keystroke dynamics. Behavioural biometrics can be an alternative to physical biometrics, therefore address some of the earlier pitfalls of physical biometrics. In addition, behavioural biometrics are easily implementable since they can be implemented at the software level [14]. These biometrics can be unobtrusive and easily collected, without the user's knowledge [11]. In addition, collection of data about the behavioural biometrics does not often require any special hardware and therefore it is cost effective [15]. Traditional biometric methods include fingerprints, face or voice recognition have been used in mobile devices for user authentication. However, face or voice recognition have an issue not very well suited in every situation. The authentication method must be able to cope with very different environments for example relatively dark or noisy. In addition, Fingerprints rely on specific scanners, which are not available on every smartphone today. Furthermore, embedding fingerprint sensors into touchscreens behind gorilla glass is challenging, and has not been demonstrated [16]. Another traditional biometric method is keystroke authentication that used traditional keyboards [17]. This method could only provide temporal information, such as time interval between keystroke and time interval of a key being pressed [18]. With the increased popularity of touchscreen mobile phones, touch gesture behaviour is increasingly becoming important in comparison to its counterpart the keystroke behaviour, since almost all smartphones use the touchscreen as the main input method [5, 19]. A gesture based authentication system would make it more difficult for a shoulder surfer to replay the password, even if he observes the entire gesture. Subtleties like force, speed, flexibility, pressure, and individual anatomical differences would prevent the casual observer of the password [20].

This research focuses on a biometric authentication method, namely touch gesture recognition. Most of the latest mobile phones have embedded sensors which can be used for touch gesture mobile biometric authentication [21]. Touch gestures, as a kind of behavioral biometric, are the way that users swipe their fingers on the screen of their mobile devices to authenticate them while they perform basic operations on the phone. In these methods, a behavioral feature is extracted from the recorded data and a discriminative classifier is trained on these extracted features for authentication. While the user performs the gesture, it leverages the touchscreen sensor to extract touch users finger features (size, pressure, timing and distance). When combined, the information from touch sensors provides a detailed view into how the individual user performs the gesture, and as it shows in this research, it can be used as a finger touch sensor to authenticate the user. Attackers willing to bypass this authentication mechanism, face a much harder task, as they have to reproduce the timing, placement, size, and pressure of each finger touch simultaneously.

This work is provided systematic literature review of touch features used by the previous studies. Therefore, the systematic literature review reported in this research is more narrowly focused, the previous study does not provide a detailed overview and discussion of identifying touch features. In addition, the previous work study did not follow a systematic approach and is more a literature survey than a systematic literature review (SLR).

This systematic literature review (SLR) summarizes the current state-of-the-art in the field of touch features gesture authentication and organized as follows: Related work in touch gesture features based on systematic literature review is explained in Section 2. Feature extraction algorithms of behavioural biometric touch gesture are described in Section 3. In Section 4, the finding of systematic literature review are listed. The concluding remarks and future works are presented in Section 5.

2.0 Related Work In Touch Gesture Features Based On Systematic Literature Review.

This SLR summarizes the current state-of-the-art in the field of touch features gesture authentication. Based on the [50] guidelines, this SLR was performed in three main phases: planning, conducting, and reporting the review. The first stage includes the recognition of the need for a systematic review and the development of the review protocol. Based on the previous studies determined by the study selection process, this SLR seeks to This SLR seeks to identify possible touch features that have been empirically evaluated and applied to authenticate the users based on their touch. To achieve this goal, we searched the literature for the corresponding PSs. To obtain a comprehensive list of previous studies (PSs), we performed an automatic search in the most popular and relevant digital libraries. Selecting all these libraries together can lead to overlapping results, which requires the identification and removal of redundant results; however, this selection of libraries increases confidence in the completeness of the review. To increase the comprehensiveness of the review, our search considered all years (2012, 2013, 2014, 2015 and 2016).

The resulting general search string is as follows: (touch features OR touch gesture oriented OR mobile authentication OR finger pressure in android OR finger size in android OR touch gesture duration methods OR touch gesture speed OR ouch gesture distance OR ouch gesture acceleration OR touch minor in android OR touch major in android) AND (touch gesture classification estimate* OR predict* OR determine* OR identify*). We followed the conventional practice of performing the automatic search within the titles and abstracts of the articles included in the digital libraries. To ensure that duplicates were ignored, we collected the search results in an Excel spreadsheet. For each article, we recorded the authors, year of publication of the article, extracted features and classification algorithms as shows in Table 1.

Table 1: Mapping between the feature references of the PSs

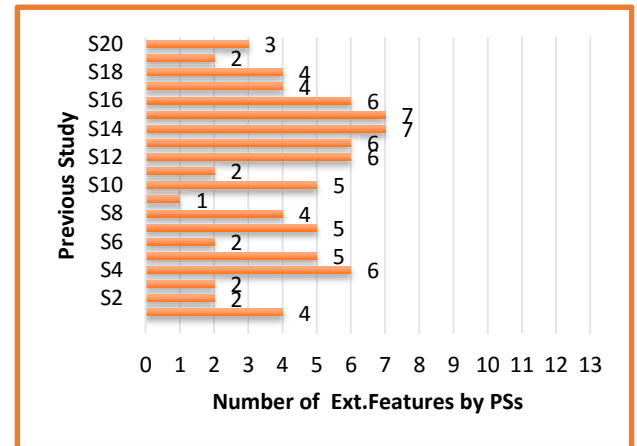
Study	Author	Features												
		Position	Touch minor up	Touch minor down	Time	Finger pressure up	Finger pressure down	Acceleration	Distance	Finger size up	Finger size down	Speed	Touch major up	Touch major down
S1	(Meng and wong, 2014)	1	0	0	1	1	1	0	0	0	0	0	0	0
S2	(Burgbacher et al., 2014)	1	0	0	1	0	0	0	0	0	0	0	0	0
S3	(Veniamin Ginodman et al., 2014)	0	0	0	1	0	0	0	0	0	0	1	0	0
S4	(Xu et al., 2014)	1	0	0	1	1	1	0	0	1	1	0	0	0
S5	(Li et al., 2013)	1	0	0	1	1	1	0	1	0	0	0	0	0
S6	(Meng et al., 2013)	0	0	0	1	0	0	0	0	0	0	1	0	0
S7	(Wolff, 2013)	1	0	0	0	1	1	0	0	1	1	0	0	0
S8	(Kolly et al., 2012)	1	0	0	1	1	1	0	0	0	0	0	0	0
S9	(Sitova et al., 2015)	0	0	0	1	0	0	0	0	0	0	0	0	0
S10	(Trojahn and Ortmeier, 2013)	0	0	0	1	1	1	0	0	1	1	0	0	0
S11	(Angulo and Wästlund, 2012)	0	0	0	1	0	0	0	0	0	0	1	0	0
S12	(De Luca et al., 2012)	1	0	0	1	1	1	0	0	1	1	0	0	0
S13	(Zheng et al., 2014)	0	0	0	1	1	1	1	0	1	1	0	0	0
S14	(Min, 2014)	1	1	1	1	0	0	1	0	0	0	0	1	1
S15	(Murmura et al., 2015)	1	1	1	0	1	1	0	0	0	0	0	1	1
S16	(Shih et al., 2015)	1	0	0	1	1	1	0	0	1	1	0	0	0
S17	(Buduru and Yau, 2015)	0	0	0	1	1	1	0	0	0	0	1	0	0
S18	(Wang et al., 2015)	0	0	0	1	1	0	0	1	1	0	0	0	0
S19	(Feng et al., 2014)	0	0	0	0	0	0	1	0	0	0	1	0	0
S20	(Qiao et al., 2015)	0	0	0	0	1	1	0	1	0	0	0	0	0
		1 represent extracted feature												
		0 represent not Extracted Feature												

Researchers have performed various study related to touch gesture features. In [24], propose a novel authentication scheme for smartphones and other touchscreen-based devices that extract touch features from the fingertip movement on touchscreens and a challenge and response authentication approach. In their proposed system, the extracted features are the location of the fingertip, and a timestamp t for each location. In [30], investigated how the adaptive mechanism affects user authentication schemes based on behavioural biometrics on mobile phones. In their study they initially developed user authentication scheme based on behavioural biometrics and experimented on two features related to gestures namely; speed and time.

In [24], suggested a touch-based authentication framework to authenticate user. The authentication proceeds in a passive way while the user performs her normal touch operations. They collected four types of touch features which are positions, time, size, pressure, and saves their touch data sequences for further analysis. In [22], proposed gestured biometric based system that could authenticate users using finger movements. In their study, the data collected was on four touch features, namely position, pressure, distance, time; this data was saved for further analysis. Another user authentication scheme was proposed by [30] that used behavioural features related to touch dynamics to accurately authenticate users. This involved the collection of detailed feature information on touch gestures like touch direction and touch duration.

3.0 Feature Extraction Algorithms

The findings of the systematic literature review (SLR) are reported in this section. This section presents the answer to the research questions and will come up with a summary of the PSs and compare it with the proposed extracted touch features in this research.

**Figure 2:** Number of extracted features by previous studies.

The total amount of extracted touch features by previous studies are thirteen features namely: position, finger pressure up, finger pressure down, finger size up, finger size down, time interval between key press and key release, distance, speed, acceleration, touch major up, touch major down, touch minor up and touch minor down. Figure 2 shows each pervious study extracted different number of features.

The details of the extracted features by previous studies are provided in Table 1 and number of extracted features is shown in Figure 2. In S1 four extracted touch features are used in their study namely: position, time, finger pressure up and finger pressure down. In S2 two extracted touch features are used in their study namely: position and time. In S3 two extracted touch features are used in their study namely: time and speed. In S4 six extracted touch features are used in their study namely: position, time, finger pressure up, finger pressure down, finger size up and finger size down. In S5 five extracted touch features are used in their study namely: position, time, finger pressure up, finger pressure down and distance.

In addition, S6 two extracted touch features are used in their study namely: time and speed. In S7 five extracted touch features are used in their study namely: position, finger pressure up, finger pressure down, finger size up and finger size down. In S8 four extracted touch features are used in their study namely: position, time, finger pressure up and finger pressure down. In S9 only time extracted touch feature is used in their study. In S10 five extracted touch features are used in their study namely: time, finger pressure up, finger pressure down, finger size up and finger size down.

Furthermore, in S11 two extracted touch features are used in their study namely: time and speed. In S12 six extracted touch features are used in their study namely: position, time, finger pressure up, finger pressure down, finger size up and finger size down. In S13 six extracted touch features are used in their study namely: time, finger pressure up, finger pressure down, acceleration,

finger size up and finger size down. In S14 seven extracted touch features are used in their study namely: position, touch minor up, touch minor down, time, acceleration, touch major up and touch major down. In S15 seven extracted touch features are used in their study namely: position, touch minor up, touch minor down, finger pressure up, finger pressure down, touch major up and touch major down.

Moreover, in S16 six extracted touch features are used in their study namely: position, time, finger pressure up, finger pressure down, finger size up and finger size down. In S17 four extracted touch features are used in their study namely: time, finger pressure up, finger pressure down and speed. In S18 four extracted touch features are used in their study namely: finger pressure up, finger pressure down, finger size up, finger size down. In S19 two extracted touch features are used in their study namely: acceleration and speed. In S20 three extracted touch features are used in their study namely: finger pressure up, finger pressure down and distance.

Based on the proposed schemes followed by the previous studies (PSs) in Table 1 they extracted the features using android touch screen mobile phone. The answer for this question is to show how the previous studies (PSs) extracted the features. The flowing section describes the way of extracting the features:

4.0 Systematic Literature Review Discussion

In this systematic literature review (SLR) we have identified thirteen touch features followed by the previous studies (PSs) to authenticate users. Table 2 shows the features extraction comparison between previous studies (PSs) and the propose scheme. Based on the comparison we can see the propose scheme will follow the same way of extracting features used by previous studies (PSs). The difference between propose scheme and previous studies focus in five contribution as shown in Table 2 below:

Table 2: Propos Scheme Feature Extraction.

Feature		Contribution
1	All Features	Each of the pervious study (PS) extracted only one or more features. The maximum number of features used in S14 year 2014 and S15 year 2015 were seven features. The propose scheme will extract thirteen touch features.
2	Distance	The pervious study only determined the distance for the first touch position and get the coordinates. The propose scheme will calculate historical point within action move during touch to get the distance accurately.
3	Speed	The pervious study used wrong calculation for distance which will affect the speed calculation. The propose scheme will calculate historical point within action move during touch to get the speed accurately.

4	Acceleration	The pervious study used wrong calculation for distance which will affect the acceleration calculation. The propose scheme will calculate historical point within action move during touch to get the acceleration accurately.
5	Position	The pervious study used one position to determine the distance, speed and acceleration. The propose scheme will extract and trace all historical point within action move and get the calculation of distance, speed and acceleration accurately.

5.0 CONCLUSION AND FUTURE WORKS

This research focuses on a biometric authentication method, namely touch gesture recognition. Most of the latest mobile phones have embedded sensors which can be used for touch gesture mobile biometric authentication. This work is provided systematic literature review of touch features used by the previous studied. Researchers have performed various study related to touch gesture features. The findings of the systematic literature review (SLR) are identified thirteen touch features followed by the previous studies (PSs) to authenticate users. However, based on the schemes followed by the previous studies (PSs) there was not any scheme that extract and use all touch features for mobile user authentication. There are number of areas of future work that could be carried out to advance upon this research and within the area of authentication on mobile devices. Each of the pervious study (PS) extracted only one or more features. The maximum number of features used in S14 year 2014 and S15 year 2015 were seven features. Extracting thirteen touch features and use them for the authentication will be one contribution in future work. The pervious study only determined the distance for the first touch position and get the coordinates. Another future work can be done by calculating historical point within action move during touch to get the distance accurately

6.0 ACKNOWLEDGEMENTS

The authors would like to thank American university of Afghanistan for their educational and financial support. This work is conducted at Information Technology and Computer Science department (ITCS) and funded by American university of Afghanistan.

REFERENCES

- [1] H. Seo, E. Kim, and H. K. Kim, "A Novel Biometric Identification Based on a User's Input Pattern Analysis for Intelligent Mobile Devices," 2012.

- [2] D. Guse and B. Müller, "Gesture-based user authentication for mobile devices," *Informatiktag (computer science days)*, 2011.
- [3] M. Kuhn and K. Johnson, *Applied predictive modeling*: Springer, 2013.
- [4] H. Crawford, "Keystroke dynamics: Characteristics and opportunities," in *Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on*, 2010.
- [5] Y. Meng, D. S. Wong, and R. Schlegel, "Touch Gestures Based Biometric Authentication Scheme for Touchscreen Mobile Phones," in *Information Security and Cryptology*, 2013.
- [6] E. Sesa-Nogueras and M. Faundez-Zanuy, "Biometric recognition using online uppercase handwritten text," *Pattern Recognition*, vol. 45, no. 1, pp. 128-144, 2012.
- [7] R. Giot, M. El-Abed, B. Hemery, and C. Rosenberger, "Unconstrained keystroke dynamics authentication with shared secret," *Computers & Security*, vol. 30, no. 6, pp. 427-445, 2011.
- [8] A. K. Jain and A. Kumar, "Biometrics of next generation: An overview," ed: Springer Berlin, Germany, 2010.
- [9] D. Shanmugapriya and G. Padmavathi, "An Efficient Feature Selection Technique for User Authentication using Keystroke Dynamics," *IJCSNS International Journal of Computer Science and Network Security*, vol. 11, no. 10, pp. 191-195, 2011.
- [10] M. Karnan, M. Akila, and N. Krishnaraj, "Biometric personal authentication using keystroke dynamics: A review," *Applied Soft Computing*, vol. 11, no. 2, pp. 1565-1573, 2011.
- [11] P. Bours, "Continuous keystroke dynamics: A different perspective towards biometric evaluation," *Information Security Technical Report*, 2012.
- [12] B. Ngugi, M. Tremaine, and P. Tarasewich, "Biometric keypads: Improving accuracy through optimal PIN selection," *Decision Support Systems*, vol. 50, no. 4, pp. 769-776, 2011.
- [13] S. P. Banerjee and D. L. Woodard, "Biometric Authentication and Identification using Keystroke Dynamics: A Survey," *Journal of Pattern Recognition Research*, vol. 7, pp. 1161-1169, 2012.
- [14] R. V. Yampolskiy and V. Govindaraju, "Taxonomy of behavioural biometrics," *Behavioral Biometrics for Human Identification*, pp. 1-43, 2010.
- [15] D. Jamil and M. N. A. Khan, "Keystroke Pattern Recognition Preventing Online Fraud," *International Journal of Engineering Science*, vol. 3, 2011.
- [16] H. Wang, D. Lymberopoulos, and J. Liu, "Sensor-Based User Authentication," in *Wireless Sensor Networks*, ed: Springer, pp. 168-185, 2015.
- [17] N. L. Clarke and S. M. Furnell, "Authenticating mobile phone users using keystroke analysis," *International Journal of Information Security*, vol. 6, no. 1, pp. 1-14, 2007.
- [18] M. Trojahn and F. Ortmeier, "Toward mobile authentication with keystroke dynamics on mobile phones and tablets," in *Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on*, 2013.
- [19] J. Guerra-Casanova, C. Sánchez-Ávila, G. Bailador, and A. de Santos Sierra, "Authentication in mobile devices through hand gesture recognition," *International Journal of Information Security*, vol. 11, no. 2, pp. 65-83, 2012.
- [20] Y. Niu and H. Chen, "Gesture authentication with touch input for mobile devices," *Security and Privacy in Mobile Information and Communication Systems*, pp. 13-24, 2012.
- [21] H. Zhang, V. M. Patel, M. Fathy, and R. Chellappa, "Touch Gesture-Based Active User Authentication Using Dictionaries," in *Applications of Computer Vision (WACV), 2015 IEEE Winter Conference on*, 2015.
- [22] L. Li, X. Zhao, and G. Xue, "Unobservable Reauthentication for Smartphones," in *NDSS*, 2013.
- [23] S. M. Kolly, R. Wattenhofer, and S. Welten, "A personal touch: recognizing users based on touch screen behavior," in *Proceedings of the Third International Workshop on Sensing Applications on Mobile Phones*, 2012.
- [24] U. Burgbacher, M. Pratorius, and K. Hinrichs, "A behavioral biometric challenge and response approach to user authentication on smartphones," in *Systems, Man and Cybernetics (SMC), 2014 IEEE International Conference on*, 2014.
- [25] A. Hematian, S. Chuprat, A. A. Manaf, S. Yazdani, and N. Parsazadeh, "Real-time FPGA-based human iris recognition embedded system: Zero-delay human iris feature extraction," in *Advances in Intelligent Systems and Computing* vol. 209 AISC, ed, 2013, pp. 195-204.
- [26] M. Wolff, "Behavioral Biometric Identification on Mobile Devices," in *Foundations of Augmented Cognition*, ed: Springer, pp. 783-791, 2013.
- [27] J. Angulo and E. Wästlund, "Exploring touch-screen biometrics for user identification on smart phones," in *Privacy and Identity Management for Life*, ed: Springer, pp. 130-143, 2012.
- [28] Z. Sitova, J. Sedenka, Q. Yang, G. Peng, G. Zhou, P. Gasti, et al., "HMOG: A New Biometric Modality for Continuous Authentication of Smartphone Users," *arXiv preprint arXiv:1501.01199*, 2015.
- [29] H. Xu, Y. Zhou, and M. R. Lyu, "Towards Continuous and Passive Authentication via Touch Biometrics: An Experimental Study on

- Smartphones," in *Symposium On Usable Privacy and Security, SOUPS*, 2014.
- [30] M. N. O. Veniamin Ginodman, Mr Ram Herkanaidu, Mr, W. Meng, D. S. Wong, and L.-F. Kwok, "The effect of adaptive mechanism on behavioural biometric based mobile phone authentication," *Information Management & Computer Security*, vol. 22, no. 2, pp. 155-166, 2014.
- [31] A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann, "Touch me once and i know it's you!: implicit authentication based on touch screen patterns," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2012.
- [32] H. Ali and M. Salami, "Keystroke pressure based typing biometrics authentication system by combining ANN and ANFIS-based classifiers," in *Signal Processing & Its Applications, 2009. CSPA 2009. 5th International Colloquium on*, 2009.
- [33] H. Liu and L. Yu, "Toward integrating feature selection algorithms for classification and clustering," *Knowledge and Data Engineering, IEEE Transactions on*, vol. 17, no. 4, pp. 491-502, 2005.
- [34] M. Shahzad, A. X. Liu, and A. Samuel, "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*, 2013.
- [35] N. Sae-Bae, K. Ahmed, K. Isbister, and N. Memon, "Biometric-rich gestures: a novel approach to authentication on multi-touch devices," in *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems*, 2012.
- [36] V. Shanmugapriya and G. Padmavathi, "Keystroke Dynamics Authentication Using Neural Network Approaches," in *Information and Communication Technologies*, 2010.
- [37] L. Al Shalabi and Z. Shaaban, "Normalization as a preprocessing engine for data mining and the approach of preference matrix," in *Dependability of Computer Systems, 2006. DepCosRELCOMEX'06. International Conference on*, 2006.
- [38] S. Kotsiantis, D. Kanellopoulos, and P. Pintelas, "Data preprocessing for supervised learning," *International Journal of Computer Science*, vol. 1, no. 2, pp. 111-117, 2006.
- [39] C. J. Tasia, T. Y. Chang, P. C. Cheng, and J. H. Lin, "Two novel biometric features in keystroke dynamics authentication systems for touch screen devices," *Security and Communication Networks*, vol. 7, no. 4, pp. 750-758, 2014.
- [40] E. Ogasawara, L. C. Martinez, D. De Oliveira, G. Zimbrão, G. L. Pappa, and M. Mattoso, "Adaptive normalization: A novel data normalization approach for non-stationary time series," in *Neural Networks (IJCNN), The 2010 International Joint Conference on*, 2010.
- [41] V. Kumar and S. Minz, "Feature Selection," *SmartCR*, vol. 4, no. 3, pp. 211-229, 2014.
- [42] Y. Saeys, I. Inza, and P. Larrañaga, "A review of feature selection techniques in bioinformatics," *bioinformatics*, vol. 23, no. 19, pp. 2507-2517, 2007.
- [43] M. R. Hossain, A. M. T. Oo, and A. S. Ali, "The combined effect of applying feature selection and parameter optimization on machine learning techniques for solar Power prediction," *American Journal of Energy Research*, vol. 1, no. 1, pp. 716, 2013.
- [44] Komatineni, S and MacLean, D. (2012). Pro Android 4 (Vol. 1). New York: Apress.
- [45] Kitchenham, B. and Charters, S (2007). Guidelines for Performing Systematic Literature Reviews in Software Engineering, Keele University and University of Durham, UK, EBSE Technical Report, Version 2.3.



Dr. Sami Naji is an assistant professor at the department of Information Technology and Computer Science at the American University of Afghanistan. He obtained his PhD from the University of Verona in computer science with dissertation title: Automatic training dataset creation for object recognition, Verona, Italy. Sami obtained his master degree from Dongseo University, Busan, South Korea in computer science and obtained his B.Sc from Multimedia University in Malaysia. His main research interest focuses on machine learning, biometric, bioinformatics, natural language processing, deep learning, etc.



Dr. Ala Abdulhakim Abdulaziz is currently an assistant professor at the department of Information Technology and Computer Science at the American University of Afghanistan. He received his PhD and MITS in computer science from the university of technology malaysia, Kuala Lumpur, Malaysia. He obtained his B.Sc in computer science from Multimedia University. His research interests include a variety of topics in the areas of Machine learning, Artificial intelligence, Biometrics Technology, etc.