Research Proposal
for
AI Researcher
at
Research Institutes of Sweden
on the topic
Behavioural multi-biometrics based mobile user recognition

Himanka Kalita
himanka.kalita.official@gmail.com
Skype ID: himanka.kalita.official
Rome, Lazio, Italy

ABSTRACT

This research proposal explores the possibility for a multi-biometric recognition model of mobile users. Insights into current research scenario in the context of mobile behavioural biometrics has been presented. A data collection application with future updates, which is devised in android platform, is also explained for possible behavioural data acquisition of mobile users and creation of behavioural templates containing raw data. Some future open research areas on the topic of mobile behavioural biometrics, public databases, and deep learning have been discussed with the possibility of finding solutions of these issues with a proposed model. Issues found during my existing research has also been discussed, and solutions to which could be found in the possible future research.

KEYWORDS

behavioral biometrics, mobile devices, biometric databases, machine learning, deep learning, android applications, multi-biometrics

1 INTRODUCTION

The safety of users of handheld devices is an area of research which is growing exponentially as such device related technology has been improving in the past years. The growth of this particular technology has encouraged almost half of the world population in using smartphone by the end of 2021[1]. Complex and sensitive tasks are now being performed relatively easily in mobile devices such as bank transactions, etc. To summarize the mobile device needs to be secure as it now contains intricate and personalised user information. This has also led to numerous security threats by human as well as non-human entity. A report suggested that 5.8% of all handheld devices in cellphone networks are used in malicious bot attacks[2].

Unlike knowledge or ownership based authentication of a person such as a password, PIN, token, etc. biometric recognition is based on what a person is physically or behaviourally [11]. Biometrics provides a solution through which recognition of users [11, 22] of mobiles devices could be achieved in both pre-, post-login scenarios. Most of the mobile devices nowadays provides physical biometric trait verification methods achieved through fingerprint, face, etc. [2, 27] integrated with the device. Behavioural biometrics in mobile devices is however a new exploration and still evolving domain of research. It exploits the behavioural traits such as touch dynamics, swipe gestures, graphical passwords, gait, signature, voice, wearable, etc. Using multi-biometrics [22] recognition models of these mobile users could further improve the security related to mobile devices. This proposal explores the possibility such a system along with a mobile multi-biometric database which will help us quantify more information about user behaviour while interacting with mobile devices.

This research proposal is explained in six sections. Section 2 discusses the state-of-the-art researches that have been performed in the field of mobile behavioural biometrics concentrating on the different traits. Section 3 explores the possible research scopes for the topic along-with wearable biometrics and research into public databases. Section 4 explains my proposed research model which I would like to explore in future. Section 5 discusses some current issues which I encountered during my research at Roma Tre University and possible solutions to it. Finally I conclude in Section 6.

2 MOBILE BEHAVIOURAL BIOMETRICS WITH APPLICATION OF HCI

A summary of the state-of-the-art mobile behavioural models is shown in Table 1. A wider survey of biometric modalities is presented in [2, 11]. They provide more insights into the theory and state-of-the-art related to physiological and behavioural biometrics respectively.

The researchers in [6] worked on 10 character keystroke password. Their work is one of the first experimental researches to be performed in the field of mobile based multi-biometric user recognition using a Gaussian distribution classifier. Free text typing

[1] https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/
[2] https://www.imperva.com/resources/resource-library/reports/mobile-bots-the-next-evolution-of-bad-bots/

Table 1: Selected state-of-the-art based on experimental complexity and applications possible from the research.

Paper	Subjects	Modality	Data	Classifier	Performance		Database Availability
					EER	IR	
Bushek et al., 2018 [5]	30	Keystroke and Touch	Free Text	Gaussian	14.26%	-	Public
Santopietro et al., 2020 [23]	190	Swipe	Touch dynamics	SVM, GMM	0.11%	-	Public
Tolosana et al., 2020 [30]	217	Graphical password	Touch dynamics	TA-RNN	2.38%	-	Public
Li et al., 2020 [14]	100	Gait	Acc and Gys	SVM, CNN	5.14%	90.04%	Private
Tolosana et al., 2020 [31]	65	Signature	Touch dynamics	Complex DTW	5.6%	-	Public

Abbreviations: Acc, Accelerometer; Gys, Gyroscope

behaviour of users in the wild, was studied by [5] using Gaussian distribution. The authors developed a custom keyboard based on Google's AOSP[3] Keyboard. They [5] listed 15 different applications based on the keystrokes, speed, postures, auto-correction, and word suggestions the users made on those applications.

Mondal et al. [16] performed two specific task for their experiments which were reading while swiping vertically and surfing images while swiping horizontally. They collected action type, device orientation while using, x-coodinate. y-coordinate, pressure, finger area, and time stamp. They used artificial neural network (ANN) and counter propagation artificial neural network (CPANN) over three verfication experiments. [23] analyses the quality factor in swipe dynamics biometrics. A quality metric was used for measurement of swipe samples. Evaluation of three datasets [3, 8, 25] have been performed. They separated the datasets based on swiping such as up, down, right, left and performed two experiments based on sample quality protocol and user quality protocol. SVM and GMM based clustering were performed.

The researchers is [18] presented the idea of haptic graphical passwords using the methods of human-haptic-computer-interaction. They studied strict conditions during password data collection and modification of verification algorithm to increase recognition performance of the system. They used ANN and Nearest Neighbour (NN) algorithm based models for recognition. [30] presented a database containing handwritten characters which could be considered as a version of graphical passwords. The recognition process was performed using time-aligned recurrent neural network (TA-RNN), a variant of the traditional RNN.

SmartCAMPP [10] and ScaNET [14] provides similar research in the field of continuous user recognition based on accelerometer and gyroscope based gait recognition of mobile users. The researchers [10] used SVM based on Radial Biased Filter (RBF) to extract the features and machine learning classification models based on SVM, RF, and LR to recognize users. The researchers in [14] collected gait information, while the users performed specific tasks such as reading, typing, and navigation on maps searching for destination. During training, one-class SVM was used to train a two streamed CNN which is later used for classification of training data and user recognition during validation and testing phase.

The research in [31] investigates two different on-line signature databases with subject size of 400 and 65 respectively. The researchers analysed and compared both databases for efficient user recognition using Euclidean distance, DTW algorithm.

[3]https://android.googlesource.com/platform/packages/inputmethods/LatinIME/

3 OPEN RESEARCH AREAS

3.1 Multi-modality of behavioural biometrics for mobile users

Considering the field of mobile behavioural biometrics which is quite new, a lot is still unexplored. Much research has been published on the individual mobile behavioural traits and some on multi-biometrics based, such as combinations of temporal and spatial features [10, 14, 26]. Discriminating features which could recognize mobile users with high robustness needs to be found. One such characteristic is the touch of human finger on the screen, where touch signifies many sub-features such as location, area, pressure, drag, etc. in comparison to features such as typing rhythm, which is easily affected by noise [5, 6]. This characteristic touch which could be acquired from numerous behavioural data and combining them using multi-biometrics might provide more information about human behaviour. Exploration in identification scenario of user through mobile behavioural data based on individual traits, let alone the multi-biometrics is also quite less.

Continuous recognition systems should be adaptable as user behaviour while using mobile devices change. This may depend on facts such as the interaction medium which is the software of mobile devices gets new updates which leads to change in behaviour. One simple example supporting the fact is, when we used to type in hardware keypad based mobile devices and suddenly android soft keyboards were introduced. Study of multi-biometric systems might provide solutions in making future continuous recognition systems more reliable.

Machine and deep learning models need large datasets and computation power. Metrics should be measured for the researches which aim to provide results for mobile based solutions [26]. Low computation requirement based deep learning models for predicting mobile user behaviour should also be focused upon. These models could be used in predicting the change in user behaviour over time and regardless of new data from exiting user could provide accurate recognition [24].

Wearable biometrics is another future area of research which could provide secure means of mobile user recognition. Research has been made into predicting user health using wearable biometric data [27]. A multi-biometric system implementing wearable behavioural data with traditional behavioural data such as from

Table 2: Selected state-of-the-art public databases.

Paper	Subjects	Modality
Frank et al., 2012 [8]	41	Swp
Serwadda et al., 2013 [25]	190	Swp
Diaz et al., 2013 [15]	100	GP & Sig
Tolosana et al., 2017 [28]	65	Sig
Belman et al., 2020 [4]	117	Touch, Swp, & Gait
Acien et al., 2021 [1]	600	Multiple

Abbreviations: Swp, Swipe; GP, Graphical password; Sig, Signature

Bluetooth's, should be researched on. While user privacy is becoming top priority in industrial applications, both these non-invasive biometric traits modelled together could solve security challenges that are emerging. While traditional mobile behavioural biometrics is considered non-invasive, percentage of users of wearable bio-devices consider them a violation of privacy which could be solved by creating social awareness, controlled social experiments, surveys, etc.

3.2 Public databases and possible improvements

As it can be observed from all the public databases listed in Table 1, 2, most researches have been conducted on one behavioural trait data or in some cases at-most two. We need to create more databases with collection of data for the research of a secured multi-biometric system. Rate of these data acquisition sessions should also be increased to counter with issues such as ageing and underfitting which is common in mobile behavioural biometric model training and testing, leading to inaccurate predictions.

Research should also be conducted into the length of data acquisition sessions in such a way, that we may understand when a predictive model could successfully recognize a user irrespective of time and new data being used for re-training [27].

Context-based data collection will also provide more insights in user behaviour. Behavioural data of person typing in a soft keyboard while sitting and while lying in bed, should provide us results which will help us better understand human behaviour leading to more accurate recognition results [5, 6].

Research should also focus on the emotional state of a subject while behavioural data acquisition is on-going. Situations where a person is normal or in panic could be a context of behavioural data collection. Two such promising recent databases [1, 4] solved most of these aforementioned issues. Although these new databases are promising, we need more of such databases to mould better behavioural biometric based recognition models.

4 PROPOSED BEHAVIOURAL MULTI-BIOMETRIC MOBILE USER RECOGNITION

My proposed research plan based on the open research areas explained in previous section 3 are explained in the following four subsections 4.1, 4.2, 4.3, and 4.4.

4.1 Data collection using ARPKEYG

Application for **R**esgistration and **P**rocessing of **K**eystrokes and **G**estures or **ARPKEYG** is the behavioural biometric data collecting android application developed for the sole purpose of mobile based behavioural biometrics template generation. The application is a combination of two softwares:

- The **ARPKEYG** application with the GUI for interacting with the users (during swipe and graphical password data collection) and generating the templates using background database service.
- The **ARPKEYG** keyboard input method service for acquiring the sensor signals, through keystrokes or touch generated on the keyboard from the users and passing (using IPC) them to the background database service for template creation.

The application uses Google's Firebase for the storage and authentication of the user's registration data and login data respectively. After the registration and login of the mobile user is successful, the user is redirected towards the template selection options menu. Keystroke and touch dynamics based templates will be created using the **ARPKEYG** keyboard input method registering not only keystrokes but different sensor's data, e.g. the x, y, z axis values of accelerometer, gyroscope, and, magnetometer at both key pressed and released, screen pressure, touch coordinate during touch event etc.

During the data collection process, the user will iteratively chose all the template options and provide the behavioural data which will be used to generate the templates by the application. All these templates will be stored in the local database of **ARPKEYG** in the mobile device, which will be extracted for processing. The different template options and the complete data collection procedure is graphically shown in the Fig. 1.

The first task of my research at RI.SE will be to start the data collection procedure with necessary modifications being made to **ARPKEYG** as explained in Subsection 4.2. The application is ready for data collection of the following traits, keystrokes and touch dynamics (7 template options), swipe gestures (1 template option), graphical passwords (1 template option), gait recognition (recorded in all templates mention above). In total 40 raw features are generated for the templates from which using, data preprocessing, higher-order statistical, and deep learning methods, more complex features could be extracted for mobile user recognition.

4.2 Future updates to ARPKEYG for Signature data collection

Current scope of the android data collection application is with the traits of keystroke and touch dynamics, swipes, and graphical passwords. Integration of signature biometric data collection module could add a significant edge to the previous version of the application. As my aim will be to create a multi-biometrics mobile user recognition model, the addition of signature trait of the mobile users should improve the performance metrics of the model significantly. Another future prospect could be the addition of voice trait considering its applications in HCI.

Signature in mobile scenario could be registered using the stylus and using the index finger of the hand. A study [29] suggests when compared two databases of stylus and finger using deep learning

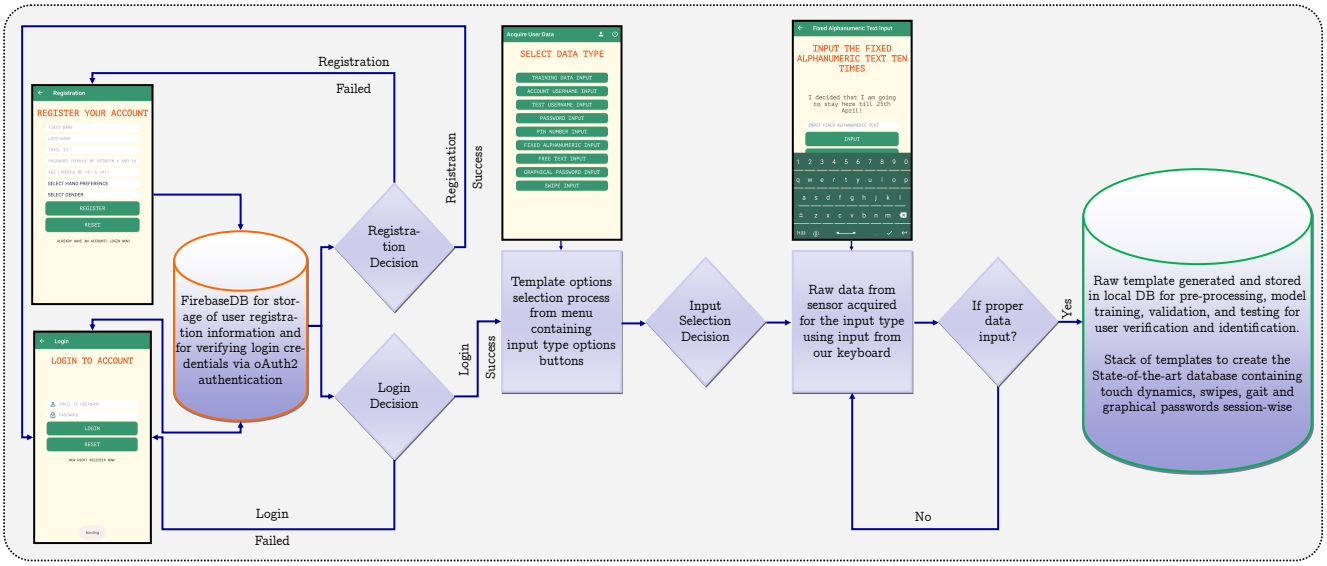

Figure 1: ARPKEYG Data collection process

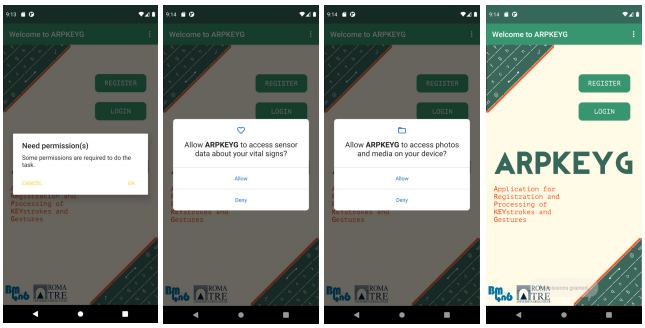

Figure 2: Screenshots of ARPKEYG requiring permissions for capturing sensor information and starting the background binding services for data transfer from activity to database service. Private GitHub repository.

models, the stylus database performance was better. Based on these results we can proceed for the data collection of mobile signatures using stylus. Moreover the collection of signature data with the finger will be comparable to the swipe and graphical password data as swiping with finger is the basic phenomenon which is being used, while registering a swipe, a graphical password and a finger signature.

4.3 Machine and deep learning implementations

Selection of proper machine learning and deep learning models is important in aspect of mobile user verification and identification. Statistical methods and fundamental machine learning algorithms are common in analysis of behavioural biometric data [19]. In recent times many deep learning models like CNN, RNN, BPNN are also well tested for verification and identification of mobile users. Common techniques such as fusion of features generated by deep learning [13] models are analysed frequently too [14].

Possible implementations of machine and deep learning models could be done using score or decision fusion techniques. Different deep learning models or streams [14] could be employed to generate the scores and decision of different features which, later could be combined using ensembling techniques for a better verification and identification rate.

I would also like to focus on the research of transfer learning [7, 17, 32] and generative adversarial networks [9, 20] based models for mobile user recognition as these models are quite unexplored for the research of mobile multi-biometrics. Some insights into causal representation learning is provided in [24], which could also be put into research for mobile user recognition as causal relations could help understand observations using reasoning beyond the already observed data.

4.4 Behavioural multi-biometric mobile user recognition

The aim to collect multiple behavioural biometric traits is to create a multi-biometric mobile user recognition model. Individual behavioural traits used for recognition of mobile users often produce weak performance results. However combining these individual traits' data using fusion (feature-, score-, decision-, and rank-level) techniques could improve the metrics drastically. A generalised model flowchart is shown in Fig. 3.

The iterative flowchart shows the process if we select multiple traits, one trait per iteration. The first trait process however could not employ the score and decision fusion algorithms as during the first iteration we will only have scores and decision from a single trait. From the process of selection of the second trait template onwards we will be able to perform fusion on the level of scores and

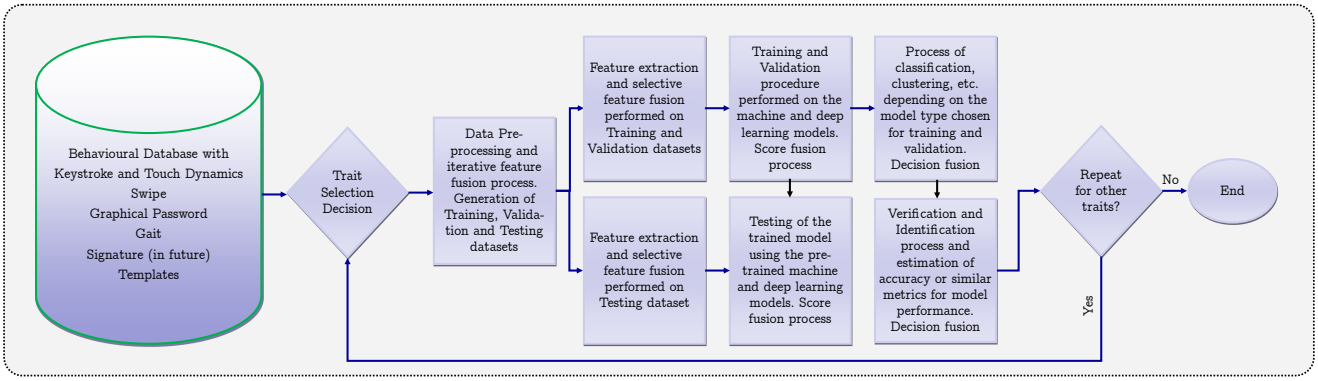

Figure 3: Generalised mobile user recognition architectural flowchart for cross validation strategy

decision (ensembling) to produce a state-of-the-art multi biometric model for mobile user recognition. I am aiming for both open-set, closed-set approach for verification and identification.

5 DISCUSSION

The process of data collection is a complex procedure. For proper empirical results we need high quality data depending on the type of input mechanism (both hardware and software), demography chosen, multiple session of the data from the same users for less data deviation, user attention during data collection, etc. Demography is a major factor which should be taken into account during data collection. A user using an English keyboard to write Greeklish [12] or Hinglish [21] for the past decade should not be asked to write English free text during data collection. The data would be collected but could produce faulty behavioural analysis.

Similar could be said for the European demography which is vast considering the languages spoken in different countries. A large multi-cultural database should be targeted with at-least 100 users from few cultures from 3 or more sessions of data with ample gap between sessions to count for the ageing effect. With age of users, their behavioural data variability or deviation rises. A smart method to tackle ageing could be to update the template after successful verification (1:1) of users, with the new data.

Although **ARPKEYG** as explained in Section 4.1, is developed to collect the data in English, it could be modified for other language inputs for a more wider reach. User attention during data collection processes also tend to falter if the process is long (generally >30 minutes). Although this is my personal experience in the lab at Roma Tre University and I do not have data to support the fact that this could lead to faulty behavioural analysis. One possible solution that could be employed is to use an interactive GUI and HCI methodologies to keep the user attentive. For getting more insights into human behaviour, users should be allowed to provide their data in supervised and unsupervised or a more relaxed environment.

6 CONCLUSION

A behavioural multi-biometrics based mobile user recognition model is presented in this proposal. Details about the research aspects still unexplored, venturing which, could provide us more understanding of human behaviour from mobile devices could be achieved. An application of multi-modality behavioural data collection is explained along with possible deep learning implementations for user recognition model is also presented. Although all possible future research directions are not possible to discuss in this proposal, some open research areas have been shown and justifying these future research areas should be done meticulously with proven empirical data. Overall, considering the existing state-of-the-art, it is quite possible to implement such a behavioural multi-biometric model for mobile user recognition.

REFERENCES

[1] Alejandro Acien, Aythami Morales, Julian Fierrez, Ruben Vera-Rodriguez, and Oscar Delgado-Mohatar. 2021. BeCAPTCHA: Behavioral bot detection using touchscreen and mobile sensors benchmarked on HuMIdb. *Engineering Applications of Artificial Intelligence* 98 (2021), 104058.

[2] A. Alzubaidi and J. Kalita. 2016. Authentication of Smartphone Users Using Behavioral Biometrics. *IEEE Communications Surveys Tutorials* 18, 3 (thirdquarter 2016), 1998–2026. https://doi.org/10.1109/COMST.2016.2537748

[3] Margit Antal, Zsolt Bokor, and László Zsolt Szabó. 2015. Information revealed from scrolling interactions on mobile devices. *Pattern Recognition Letters* 56 (2015), 7–13.

[4] Amith K. Belman and Vir V. Phoha. 2020. Discriminative Power of Typing Features on Desktops, Tablets, and Phones for User Identification. *ACM Trans. Priv. Secur.* 23, 1, Article 4 (Feb. 2020), 36 pages. https://doi.org/10.1145/3377404

[5] Daniel Buschek, Benjamin Bisinger, and Florian Alt. 2018. ResearchIME: A Mobile Keyboard Application for Studying Free Typing Behaviour in the Wild. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. ACM, New York, NY, USA, Article 255, 14 pages. https://doi.org/10.1145/3173574.3173829

[6] Daniel Buschek, Alexander De Luca, and Florian Alt. 2015. Improving Accuracy, Applicability and Usability of Keystroke Biometrics on Mobile Touchscreen Devices. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. ACM, New York, NY, USA, 1393–1402. https://doi.org/10.1145/2702123.2702252

[7] Zhangjie Cao, Mingsheng Long, Jianmin Wang, and Michael I Jordan. 2018. Partial transfer learning with selective adversarial networks. In *Proceedings of the IEEE conference on computer vision and pattern recognition*. 2724–2732.

[8] Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song. 2012. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE transactions on information forensics and security* 8, 1 (2012), 136–148.

[9] Nan Gao, Hao Xue, Wei Shao, Sichen Zhao, Kyle Kai Qin, Arian Prabowo, Mohammad Saiedur Rahaman, and Flora D Salim. 2020. Generative adversarial networks for spatio-temporal data: A survey. *arXiv preprint arXiv:2008.08903* (2020).

[10] Luis Hernández-Álvarez, José María De Fuentes, Lorena González-Manzano, and Luis Hernández Encinas. 2021. SmartCAMPP-Smartphone-based Continuous

Authentication leveraging Motion sensors with Privacy Preservation. *Pattern Recognition Letters* (2021).
[11] A.K. Jain, A. Ross, and K. Nandakumar. 2011. *Introduction to Biometrics*. Springer.
[12] Dimitris Koutsogiannis and Bessie Mitsikopoulou. 2017. Greeklish and Greekness: Trends and Discourses of "Glocalness". *Journal of Computer-Mediated Communication* 9, 1 (07 2017). https://doi.org/10.1111/j.1083-6101.2003.tb00358.x JCMC918.
[13] Yann LeCun, Yoshua Bengio, and Geoffrey Hinton. 2015. Deep learning. *nature* 521, 7553 (2015), 436–444.
[14] Yantao Li, Hailong Hu, Zhangqian Zhu, and Gang Zhou. 2020. SCANet: sensor-based continuous authentication with two-stream convolutional neural networks. *ACM Transactions on Sensor Networks (TOSN)* 16, 3 (2020), 1–27.
[15] Marcos Martinez-Diaz, Julian Fierrez, and Javier Galbally. 2013. The DooDB graphical password database: Data analysis and benchmark results. *IEEE Access* 1 (2013), 596–605.
[16] Soumik Mondal and Patrick Bours. 2015. Swipe gesture based continuous authentication for mobile devices. In *2015 International Conference on Biometrics (ICB)*. IEEE, 458–465.
[17] Shuteng Niu, Yongxin Liu, Jian Wang, and Houbing Song. 2020. A decade survey of transfer learning (2010–2020). *IEEE Transactions on Artificial Intelligence* 1, 2 (2020), 151–166.
[18] Mauricio Orozco, Behzad Malek, Mohamad Eid, and Abdulmotaleb El Saddik. 2006. Haptic-based sensible graphical password. In *Proceedings of Virtual Concept*, Vol. 56. Citeseer, 1–4.
[19] Salil P. Banerjee and Damon L. Woodard. 2012. Biometric Authentication and Identification Using Keystroke Dynamics: A Survey. *Journal of Pattern Recognition Research* 7 (01 2012), 116–139. https://doi.org/10.13176/11.427
[20] Zhaoqing Pan, Weijie Yu, Xiaokai Yi, Asifullah Khan, Feng Yuan, and Yuhui Zheng. 2019. Recent progress on generative adversarial networks (GANs): A survey. *IEEE Access* 7 (2019), 36322–36333.
[21] Rana D. Parshad, Suman Bhowmick, Vineeta Chand, Nitu Kumari, and Neha Sinha. 2016. What is India speaking? Exploring the "Hinglish" invasion. *Physica A: Statistical Mechanics and its Applications* 449 (2016), 375–389. https://doi.org/10.1016/j.physa.2016.01.015
[22] A. Ross and A. K. Jain. 2004. Multimodal biometrics: An overview. In *2004 12th European Signal Processing Conference*. 1221–1224.
[23] Marco Santopietro, Ruben Vera-Rodriguez, Richard Guest, Aythami Morales, and Alejandro Acien. 2020. Assessing the Quality of Swipe Interactions for Mobile Biometric Systems. In *2020 IEEE International Joint Conference on Biometrics (IJCB)*. IEEE, 1–8.
[24] Bernhard Schölkopf, Francesco Locatello, Stefan Bauer, Nan Rosemary Ke, Nal Kalchbrenner, Anirudh Goyal, and Yoshua Bengio. 2021. Toward Causal Representation Learning. *Proc. IEEE* 109, 5 (2021), 612–634. https://doi.org/10.1109/JPROC.2021.3058954
[25] Abdul Serwadda, Vir V Phoha, and Zibo Wang. 2013. Which verifiers work?: A benchmark evaluation of touch-based authentication algorithms. In *2013 IEEE sixth international conference on biometrics: theory, applications and systems (BTAS)*. IEEE, 1–8.
[26] Ioannis Stylios, Spyros Kokolakis, Olga Thanou, and Sotirios Chatzis. 2021. Behavioral biometrics & continuous user authentication on mobile devices: A survey. *Information Fusion* 66 (2021), 76–99.
[27] Aditya Sundararajan, Arif I. Sarwat, and Alexander Pons. 2019. A Survey on Modality Characteristics, Performance Evaluation Metrics, and Security for Traditional and Wearable Biometric Systems. *Comput. Surveys* 52, 2 (2019), 39:1–39:36.
[28] Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez, Aythami Morales, and Javier Ortega-Garcia. 2017. Benchmarking desktop and mobile handwriting across COTS devices: The e-BioSign biometric database. *PloS one* 12, 5 (2017), e0176792.
[29] Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez, and Javier Ortega-Garcia. 2018. Exploring recurrent neural networks for on-line handwritten signature biometrics. *Ieee Access* 6 (2018), 5128–5138.
[30] Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez, and Javier Ortega-Garcia. 2020. BioTouchPass2: Touchscreen password biometrics using time-aligned recurrent neural networks. *IEEE Transactions on Information Forensics and Security* 15 (2020), 2616–2628.
[31] Ruben Tolosana, Ruben Vera-Rodriguez, Richard Guest, Julian Fierrez, and Javier Ortega-Garcia. 2020. Exploiting complexity in pen-and touch-based signature biometrics. *International Journal on Document Analysis and Recognition (IJDAR)* 23, 2 (2020), 129–141.
[32] Fuzhen Zhuang, Zhiyuan Qi, Keyu Duan, Dongbo Xi, Yongchun Zhu, Hengshu Zhu, Hui Xiong, and Qing He. 2020. A comprehensive survey on transfer learning. *Proc. IEEE* 109, 1 (2020), 43–76.