Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, No. 5, May : 2023

THE SIGNIFICANCE OF CONTINUOUS USER AUTHENTICATION ON MOBILE GADGETS: A REVIEW

Mrs. Atmaprabha, Assistant Professor, Department of Information Technology, Lalit Narayan Mishra College of Business Management , Muzaffarpur, Bihar - atmaprabha.ani@gmail.com

Abstract- In recent years, mobile devices have offered us a great deal of convenience by enabling users to experience a variety of apps like online shopping, Internet banking, navigation, and mobile media anytime, anywhere. While customers benefit from the "Go Mobile" trend's flexibility and convenience, their sensitive private information (such as their name and credit card number) on the mobile devices may be compromised. By unlocking the mobile devices, a foe could gain access to the delicate private information kept within. Additionally, all of the user's mobile services and applications are susceptible to security risks. The adversary could, for instance, use the user's mobile device to carry out prohibited activities (such as making online transactions and installing malware). In order to identify these authentication methods' weaknesses, we also evaluate the current attacks against them. The study makes the case that multi-factor authentication which establishes the user's identification by integrating, as opposed to merely combining, multiple authentication metrics will become increasingly popular for use with mobile devices. When a user inputs knowledge-based secrets, such as a PIN, for instance, the user's behaviour biometrics, such as keystroke dynamics, may be extracted concurrently. This can provide enhanced authentication while saving the user the trouble of conducting multiple inputs for various authentication metrics.

Keywords— *Significance, Continuous, User Authentication, Mobile Gadgets,* PIN, *Online Shopping, Internet Banking, Navigation, And Mobile Media.*

INTRODUCTION

There has been a huge increase in the use of mobile devices like smartphones and tablets as a result of recent breakthroughs in sensing and communication technology. Users must continuously worry about security and privacy as the use of mobile devices grows because the loss of a mobile device could expose personal data. Continuous authentication systems, also known as active authentication systems, have been proposed as a solution to this issue, in which users are continuously tracked after gaining initial access to a mobile device. We give an overview of various continuous authentication techniques on mobile devices in this post. We address the benefits and shortcomings of the present strategies and point out intriguing directions for further study in this quickly developing subject. On explicit authentication mechanisms like a password, personal identification number (PIN), or a secret pattern, conventional techniques for authenticating users on mobile devices are based. According to studies, people frequently use the passwords "12345," "abc1234," or even "password" to safeguard their data. Because of this, hackers may quickly access several accounts by simply attempting the most widely used passwords. Additionally, users have a tendency to utilise the same secret pattern repeatedly on mobile devices when secret patterns are used for first access. They consequently create greasy traces or smudges on the phone's screen. It has been demonstrated that one may quickly determine the location using high quality photographs and proper lighting. the gadget therefore, if a password is hacked or if the user does not maintain appropriate vigilance after initial authentication, unauthorised individuals may improperly get access to the user's personal information.The biometrics and security research communities have created methods for continuous authentication on mobile devices to address these problems. These methods fundamentally leverage physiological and behavioural biometrics, continuously monitoring user identity utilising built-in sensors and peripherals such the gyroscope, touch screen, accelerometer, orientation sensor, and pressure sensor. For instance, physiological biometrics, like those of the face, can be recorded using a mobile device's front-facing camera and used to continually authenticate a user of that device. The ease of using

mobile devices, such smartphones and smartwatches, has significantly fueled the expansion of the mobile business in recent years. According to recent mobile marketing figures, there will be 4.78 billion mobile phone users worldwide in 2020. Despite the great convenience that mobile device users experience, there are significant security concerns raised by the widespread use of mobile devices and mobile applications due to the fact that they have full access to the sensitive data of users (such as demographics, locations, photos, and contact lists). In order to confirm users' identities before enabling them to execute further actions, the majority of mobile devices and mobile applications often use user authentication protocols. Despite the fact that there are already surveys on user authentications, a fresh and thorough study of user authentication on mobile devices is still in great demand for the following reasons. First of all, the surveys on knowledge-based authentication and graphic-based authentication and all older than ten years, whereas the current surveys reviewing user authentication on mobile devices through only concentrate on one type of mobile authentication, such as the biometric-based authentication category, behavioural biometric authentication, or touch/keystroke dynamics authentication. Second, many novel mobile sensing technologies-based authentication techniques, particularly those that rely on behavioural biometrics and multi-factor authentication, have not been well examined. One recent survey looked at both conventional (such as PIN/password, pattern) and biometric (such as fingerprint, voice, and iris) approaches for Android smartphones. The developing mobile authentication techniques that make use of behavioural biometrics or multiple authentication metrics were not included by this survey, which only examined a limited subset of the authentication mechanisms. Third, since adversaries have created new attacks this year that target these authentication systems, it is necessary to reevaluate the authentication techniques covered by the present surveys. Therefore, a full analysis and methodical comparison of all these key mobile authentication categories is required.

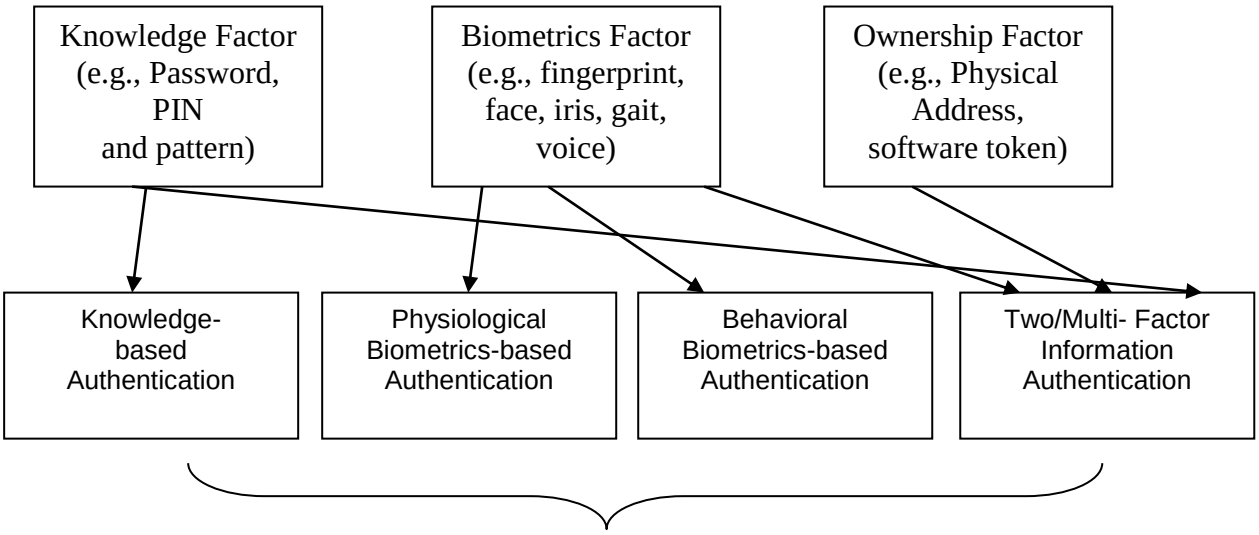

Figure 1. The four authentication categories and the general authentication model

(i) Knowledge-based Authentication- Knowledge-based since authentication is a holdover from traditional user authentication and has amassed a sizable user base over a long history, it is the most widely used technique for user verification on mobile devices. In order to authenticate users, it uses knowledge (such as a string of numbers or letters) that is only known by the user and the system. The knowledge-based secret may be visual or text-based, such as a lock pattern or secret click locations on images. Text-based examples of knowledge-based secrets include digit PINs and alphanumeric passwords. To authenticate their identity throughout the authentication process, a user might easily enter such secrets through the touch screen of a mobile device.

(ii) Physiological Biometrics-based Authentication- In addition to knowledge-based authentication, physiological biometrics-based authentication has been implemented on numerous mobile devices. Because it uses the distinct human biometric characteristics (like fingerprints, iris patterns, hand geometry, and face contour) that are inherent in users' body parts for authentication, physiological biometrics-based authentication is more convenient (i.e., there is no need to memorise secret codes) and more secure (i.e., harder to be stolen) than knowledge-based authentication. However, mobile devices typically need to use specialised sensors, such as the capacitive fingerprint scanner and depth camera on iPhones and the iris reader on Samsung smartphones, to acquire the biometric characteristics from users' body parts.

(iii) Behavioral Biometrics-based Authentication- These years, behavioural biometrics-based authentication has received a lot of attention. For authentication, it makes use of the behavioural biometrics that record each user's particular behavioural traits or routines. For instance, the user's finger motions when tapping or swiping on the touch screen display a special behavioural pattern that can be utilised for authentication. Similar to how talking and walking produce distinctive voice and gait patterns, users can be distinguished by these characteristics. Users tend to choose behavioural biometrics-based authentication over physiological biometrics-based authentication. This is due to the fact that behavioural biometrics are less private information than the constant physical features.

(iv) Two/multi-factor Authentication- Two/multi-factor To provide more secure authentication than utilising a single factor, authentication typically combines two or more authentication metrics. To pass the authentication, the authentication system can, for instance, request that the user submit several biometrics, such as their voice, face ID, and fingerprints. Additionally, the system can ask the user to enter each biometric piece of data and secret knowledge individually during the verification stage. While it takes an adversary more work to compromise multiple authentication metrics, using many inputs to confirm one's identity is less convenient than using a single factor.

LITERATURE REVIEW

the timeline of publications concerning various aspects of Continuous Authentication on Mobile Devices is presented in the following tables, grouped according to the behavioral modalities.

Benabdelkader et al. presented a parametric approach for human identification from low-resolution video using height and stride parameters of walking gait. They showed that a person is correctly identified with 49% probability when using height and stride parameters. Their method worked with low-resolution
images of people, and was resilient to changes in lighting, clothing, and tracking errors.

Mantyjarvi et al. showed that users can be identified with a novel method of gait recognition. They tested their subjects who walked with fast, normal and slow walking speeds in enrolment and test sessions on separate days wearing the accelerometer device on their belt, at back. They used three approaches,
correlation, frequency domain and data distribution statistics. Best equal error rate (EER=7%) was achieved with signal correlation method, while frequency domain method and two variations of data distribution statistics method produced EER of 10%, 18% and 19%, respectively.

Gafurov et al. introduced an approach where gait patterns are extracted from a physical device attached to the lower leg of the participants. Using the output of the device they obtained accelerations in three directions: vertical, forward-backward, and sideways motion of the lower leg. Following, they used a
combination of these accelerations for authentication. By applying two different methods, histogram similarity and cycle length, they achieved equal error rates (EER) of 5% and 9%, respectively.

Derawi et al. collected data with a commercially available mobile device containing low-grade embedded accelerometers. The mobile device was placed at the hip on each volunteer to collect gait data. Preprocessing, cycle detection and recognition- analysis were applied to the acceleration signal.

The performance of the system was evaluated with 51 volunteers and yielded in an equal error rate (EER) of 20%.

Kwapisz et al. published a system to identify and authenticate users based on accelerometer data. They used a dataset of 36 users, labeled according to activities such as walking, jogging, and climbing stairs. These labels were used as context and the authors presented analysis with and without these labels. For feature extraction, they divided the 3 axes readings of the accelerometer into windows of 10-seconds, and for each window they extracted features such as mean, standard deviation, resultant, and binned distribution. For identification, the authors performed a 36-class classification, whereas for the task of authentication, the authors reduced the problem to a 2-class problem. They achieved a classification accuracy of 72.2% for 10-second windows. While they concluded based on their results that it is not critical to know what activity the user is performing, their dataset was generated by users repeating a limited set of predefined activities.

Feng et al. exploited mobile motion data as a novel biometric modality and their experimental results showed that user movements (e.g., walking) have a high impact on the verification performance.

Saevanee et al. investigated the potential use of three behavioral biometrics as a part of the authentication system of mobile devices. Those behavioral biometrics were the hold-time, the inter-key behavior, and the finger pressure. The results showed that using only the finger pressure can indicate users with accuracy rate as 99% which is the same as using the combination of the hold-time and the finger pressure.

Li et al.proposed a novel biometric-based system to achieve continuous and unobservable re-authentication for smartphones. Their system uses a classifier to learn the owner's finger movement patterns and checks the current user's finger movement patterns against the owner's. The system continuously re- authenticates the current user without interrupting user- smartphone interactions. Experiments showed that their system is efficient on smartphones while they also achieved high accuracy. The accuracy of the sliding up gesture was 95.78%, of the sliding down 95.30%, of the sliding left 93.06%, of the sliding right 92.56%, of the up & tap 93.02%, of the down & tap 89.25%, of the left & tap 88.28%, and of the right & tap 89.66%.

Zhao et al. proposed a novel Graphic Touch Gesture Feature (GTGF) to extract the identity traits from the touch traces. The traces' movement and pressure dynamics were represented by intensity values and shapes of the GTGF. To evaluate its usability on the authentication problem, they collected touch gesture datasets which included three sets of commonly used touch gestures (flick up/down, flick right/left, zoom in/out). They achieved an Equal Error Rate of 2.62% combining six gestures together, which demonstrated the effectiveness of their methods.

BACKGROUND OF USER AUTHENTICATION ON MOBILE GADGETS /DEVICES

(i) Mobile Sensing Technologies for Convenient User Authentication- Different from the traditional user authentication on computers, the mobile user authentication mainly leverages the various embedded sensors in the mobile devices to capture the unique identity information for verifying the users. The touch screen is the most frequently used sensor on mobile devices for getting the user input for authentication. It has been widely used for the knowledge-based authentication methods. For example, the mobile devices usually provide the users with the option to enter PINs, passwords or lock patterns on the touch screen for user verification. The camera is usually used to capture human faces or iris patterns for physiological biometrics-based authentication. Similarly, the fingerprint scanner is deployed in some

mobile devices to read the user's fingerprint for convenient physiological biometrics-based authentication. Recently, the motion sensors (e.g., accelerometer and gyroscope) and wireless communication interfaces (e.g., WiFi and Bluetooth) are shown to be capable of capturing users' unique behavioral patterns, which facilitate the behavioral biometrics-based authentication. Besides, the microphone in mobile devices can capture the acoustic sound at a high sampling rate (e.g., 8kHz, 44.1kHz), which provides rich information of the human voices to enable the authentication based on voice. Overall, the various sensing technologies available in mobile devices provide great flexibility and convenience for the user to verify him/herself.

(ii) Design Criteria of User Authentication on Mobile Devices- Designing a user authentication approach on mobile devices needs to consider both the security strength and the usability. As the adversary attempts to access the system by either stealing or forging the legitimate user's identity information, it is essential to develop the authentication methods that are robust against the various attacks. The security strength describes how well the authentication methods can protect the system from the attacks and prevent the unauthorized users, either intentionally or accidentally. The usability indicates how convenient that an authentication method is to users, which also suggests whether the method is practical for real use cases or not. To evaluate the usability, we consider following aspects: 1) the compatibility of the authentication method in different model of mobile devices; 2) the cost in terms of limited resources of mobile devices (i.e., computing power and battery); 3) the user-friendliness; 4) the robustness to dynamic environmental interference (e.g., ambient light and acoustic noises). Usually, there are trade-offs between usability and security strength in user authentication. For example, using long and random alphanumerical contents for passwords can achieve the strong security strength but the passwords would be very hard to memorize, which is inconvenient for users, especially for elderly users. In this paper, we review the existing studies from both of these aspects and aim to provide a comprehensive picture of user authentication on mobile devices by analyzing the trade-offs.

(iii) Attack Models- The main goal of an attacker is to gain access to users' private information or conduct non-permitted actions by taking control of mobile devices, which are protected by authentication systems. To achieve this goal, the attacker needs to either pass the authentication system using the user's identity information or refer to other techniques to bypass the authentication process (e.g., hacking the database in the remote server or intercepting data transmission). In this paper, we assume the attacker cannot bypass the authentication process in any way and focus on reviewing the various authentication methods and corresponding adversarial techniques that are threats to them. We summarize the major methods an adversary could leverage to obtain a user's identity-related information and pass the authentication: Brutal-force and Guessing Attacks. Basically, brutal-force attacks are to try a large number of identity-related information for the required authentication metrics (e.g., passwords, finger-prints, and mobile device physical addresses) for passing the authentication. Such exhaustive methods are usually costly in the form of computing power and time. Guessing attacks are a type of opportunistic attacks. For example, the attacker could randomly pick up a password or rely on a dictionary to try a bunch of passwords. Such attacks usually show low success rates, because the adversary knows nothing about the user's identity related information.

Study	Number of Users	Classifiers	Feature Dimension	Performance
Frank et al.	**41**	**SVM, KNN**	**27**	**EER: 0.00–4.00**

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, No. 5, May : 2023

Zhang et al.	**50**	**Sparsity-based classifiers**	**27**	**EER: 0.77**
Li et al.	**75**	**SVM**	**10**	**EER: ~ 3.0**
Feng et al.	**40**	**Random forest, J48 tree, Bayes' net**	**53**	**FAR: ~ 7.50, FRR: ~8.00**
Serwadda et al.	**138**	**Ten different classifiers**	**28**	**EER: 10.50**
Zhao et al.	**78**	**L1 distance**	**100*150 images**	**EER: 6.3315.40**

Table 1- Key Touch dynamic based continuous authentication

SIGNIFICANCE OF CONTINUOUS AUTHENTICATION APPROACHES

the fundamental idea behind a biometrics-based continuous authentication system for mobile devices. The sensors and accessories in a mobile device can measure biometric modalities like voice, face, motion, and keystrokes. The biometric system will then decide whether or not a legitimate user possesses these biometric qualities. The biometric system will keep processing the fresh incoming data if the features indeed match a real user. The user will be prompted to confirm their identity using the traditional explicit authentication techniques based on PIN, face, or secret pattern if the biometric system returns a negative result. The mobile device will only remain functional if the user can verify their identity; else, it will be locked.

(i) Touch dynamics- Touch dynamics is one of the most commonly used continuous authentication methods for mobile devices. In touch dynamics, touch screen input is used as a data source. In particular, screen touch gestures the way users swipe their fingers on the touch screen of their mobile devices are used as a behavioral bio-metric to continuously authenticate users while they perform basic smartphone operations. In these methods, a behavioral feature vector is extracted from the recorded screen touch data, and a discriminative classifier is trained on these extracted features for authentication. Figure 4 shows some swipes performed by eight different users while reading text on an Android device . It is interesting to see that even for the same task, touch data of different users show significant differences.

(ii) Face recognition- A face recognition-based continuous authentication system is another popular choice for continuously tracking a user's identification on a mobile device. There are three main phases to a general facial recognition system. In the first, faces are found in photos or videos taken by the front-facing cameras of smartphones. Then, from the discovered faces, holistic or local features are retrieved. Finally, a classifier is provided with these features for authentication. In the literature, numerous approaches for detecting and identifying faces on mobile devices have been put forth (table 1). Here, we'll quickly go through a few of these techniques.

(iii) Gait dynamics- it identify users based on how they walk. The data needed for gait-based authentication are often measured by the built-in accelerometer and gyroscope sensors. Once the raw data are measured, discriminative features are extracted, which are then fed into a classifier to distinguish users. In recent years, several methods have been developed for gait-based recognition on mobile devices. These methods differ essentially in the types of features extracted from the raw data for classification or the types of classification methods used for authentication. For instance, methods based on correlation, frequency domain analysis, and data distribution statics are used in, while methods based on dynamic time warping are used in. Rather than using the gait cycles for extracting features, proposes an application of hidden Markov models (HMMs) for gait recognition. In particular, a sensor orientation invariant gait representation called gait dynamic images (GDIs) was proposed in [39]. Given a 3-D time series captured by a three-axis accelerometer, its GDI is calculated by the cosine similarity of the motion measurement at time t with the time-lagged signal of lag l.

(iv) Behavior-based profiling - Based on the applications and services a user uses, behaviour profiling techniques validate that person's identification. Beginning in the late 1990s, research into mobile behaviour profiling concentrated primarily on creating intrusion detection systems (IDSs) to track user migration and calling patterns in order to identify telephony service fraud. In these systems, user profiles are generated by keeping track of users' actions over time and comparing them to the users' actual activity profiles (table 2). A potential incursion is identified if a sizable divergence is seen.

Study	Behavior	Data Set (Users	Classifier	Performance (%)
Li et al.	**Application usage**	**MIT Reality**	**Neural net**	**EER: 13.5**
Li et al.	**Text message**	**MIT Reality**	**Neural net**	**EER: 75**
Li et al.	**Calls**	**MIT Reality**	**Neural net**	**EER: 87**
Li et al.	**Historical usage data**	**MIT Reality**	**Neural net**	**EER: 13.0**
Neal et al.	**Application usage, Bluetooth, and Wi-Fi**	**UND data set (200)**	**Nearest neighbor**	**RR: 80-93**

Table 2- Key behavior profiling based continuous authentication methods for mobile devices

CONCLUSION

In order to safeguard users' sensitive data, user authentication on mobile devices is a crucial technology. It prohibits unauthorised access to a mobile device or mobile application. This study provides a thorough analysis of user authentication methods on mobile devices. We categorise the user authentication techniques on mobile devices into four groups based on the fundamental authentication metrics (knowledge, biometrics, and ownership) used in the current authentication approaches to establish a user's identity. These categories are knowledge-based, physiological biometrics-based, behavioural biometrics-based, and two/multi-factor based authentication. To provide a thorough understanding of the development history and cutting-edge mobile user authentication technologies, including the involved sensing technologies, the various strategies to apply a single or multiple authentication metrics, and their security strength and usability, we review and discuss a wide range of work in each category. The knowledge-based authentication (i.e., text-based or graphics-based) inherits a sizable user base from a long history and has a relatively greater usability, as we have seen. Although widely used, authentication based on user knowledge is susceptible to several attack techniques (such as side-channel assaults and shoulder-surfing), which can be used to obtain or extract user knowledge-based secrets. We anticipate that the development of novel authentication strategies built on the integration of several authentication metrics (such as knowledge, biometrics, and ownership) will be the future trend of research on user authentication on mobile devices. Additionally, the widely accessible sensors on mobile devices should be able to be used to acquire the multi-dimensional identity information. Future research paths could also considerably strengthen the security and usability of user authentication on mobile devices by limiting the leakage or reuse of sensor data.

REFERENCES

[1] “Number of mobile phone users worldwide from 2015 to 2020 (in billions),”
[2] X. Suo, Y. Zhu, and G. S. Owen, “Graphical passwords: A survey,” in Proceedings of the 21st Annual Computer Security Applications Conference. IEEE, 2005.
[3] F. Towhidi and M. Masrom, “A survey on recognition based graphical user authentication algorithms,” arXiv preprint arXiv:0912.0942, 2009.
[4] R. Spolaor, Q. Li, M. Monaro, M. Conti, L. Gamberini, and G. Sartori, “Biometric authentication methods on smartphones: A survey.” PsychNology Journal, vol. 14, no. 2, 2016.

[5] A. Mahfouz, T. M. Mahmoud, and A. S. Eldin, "A survey on behavioral biometric authentication on smartphones," Journal of Information Security and Applications, vol. 37, pp. 28–37, 2017.
[6] P. S. Teh, N. Zhang, A. B. J. Teoh, and K. Chen, "A survey on touch dynamics authentication in mobile devices," Computers & Security, vol. 59, pp. 210–235, 2016.
[7] R. Saifan, A. Salem, D. Zaidan, and A. Swidan, "A survey of behavioral authentication using keystroke dynamics: Touch screens and mobile devices," Journal of Social Sciences (COES&RJ-JSS),
vol. 5, pp. 29–41, 2016.
[8] D. Kunda and M. Chishimba, "A survey of android mobile phone authentication schemes," Mobile Networks and Applications, pp. 1–9, 2018.
[9] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," Proceedings of the IEEE, vol. 91, no. 12, pp. 2021– 2040, 2003.
[10] S. Uellenbeck, M. Dürmuth, C. Wolf, and T. Holz, "Quantifying the security of graphical passwords: the case of android unlock patterns," in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM, 2013, pp. 161–172.
[11] H. Zhang, V. M. Patel, M. E. Fathy, and R. Chellappa, "Touch gesture-based active user authentication using dictionaries," in Proc. IEEE Winter Conf. Applicat. Comput. Vision, 2015, pp. 207–214.
[12] T. Feng, Z. Liu, K. A. Kwon, W. Shi, B. Carbunar, Y. Jiang, and N. Nguyen, "Continuous mobile authentication using touchscreen gestures," in Proc. IEEE Conf. Technol. Homeland Security, Nov. 2012, pp. 451–456.
[13] M. Sherman, G. Clark, Y. Yang, S. Sugrim, A. Modig, J. Lindqvist, A. Oulasvir-ta, and T. Roos, "User-generated free-form gestures for authentication: Security and memorability," in Proc. 12th Annu. Int. Conf. Mobile Syst., Applicat., and Services, 2014, pp. 176–189
[14] X. Zhao, T. Feng, and W. Shi, "Continuous mobile authentication using a novel graphic touch gesture feature," in Proc. IEEE Int. Conf. Biometrics: Theory, Appli-cat. and Syst ., Sept. 2013, pp. 1–6.
[15] X. Zhao, T. Feng, W. Shi, and I. Kakadiaris, "Mobile user authentication using statistical touch dynamics images,"
IEEE Trans. Inform. Forensics and Security, vol. 9, no. 11, pp. 1780–1789, 2014.
[16] A. Hadid, J. Heikkila, O. Silven, and M. Pietikainen, "Face and eye detection for person authentication in mobile phones," in Proc. ACM/IEEE Int. Conf. Distrib-uted Smart Cameras, Sept. 2007, pp. 101–108.
[17] P. A. Viola and M. J. Jones, "Robust real-time face detection," Int. J. Comput, Vision, vol. 57, no. 2, pp. 137–154, 2004. [18] T. Ojala, M. Pietikainen, and T. Maenpaa, "Multiresolution gray-scale and rota-tion invariant texture classification with local binary patterns," IEEE Trans. Pattern Anal. and Mach. Intell., vol. 24, no. 7, pp. 971–987, 2002.
[19] S. Sarkar, V. M. Patel, and R. Chellappa, "Deep feature-based face detection on mobile devices," in Proc. IEEE Int. Conf. Identity, Security and Behavior Anal., 2016.
[20] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," in Advances in Neural Inform. Processing Syst ., 2012, pp. 1097–1105.