International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: 10.31695/IJERAT.2020.3667

E-ISSN : 2454-6135

Volume.6, Issue 11
November -2020

Subject Review: Authentication Techniques for Smartphone

Ahmed Abd Ali Abdulkadhim[1], **Dena Nadir George**[2]

[1-2]Computer Science Department

Collage of education, Mustansiriyah University

Baghdad- Iraq

ABSTRACT

The rapid development of smart phone devices and users' satisfaction with them, also have storage and accounting capabilities that compete with computers. Smart phones carry a lot of personal information and important financial information, so they are vulnerable to theft or access by unauthorized persons to that information. Increased need for ways to protect that information. Smartphones have several built-in sensors that facilitate the capture of biometrics and behavioral traits This paper reviews the authentication techniques for mobile, as it covers a comprehensive survey on authentication methods and comparison between these techniques.

.

Keywords: Authentication, Biometric, Smartphone.

1. INTRODUCTION

The increase in the use of smart phones and the storage of personal and important information for the user, which creates a concern for the user about the protection of information [1]n. And misuse or theft of personal or financial information, there is a need to protect this information and prevent unauthorized access to it, authentication plays an important role to help prove identity. User authentication is a process used to verify a user’s identity [2] The authentication methods are classified into three types, including password-based, card-based, or biometrics (finger / iris scan / face).[3]

Through the user experience of the Internet, the user prefers and an interested in biometric authentication because more than 75% have experience failure in authentication by forgetting usernames and passwords or responding to questions based on knowledge. This is why the unique physiological biometric techniques (face, iris, voice and fingerprint), It is more acceptable and desirable for the user instead of using the password or the symbol [4].

In recent years, it has proposed various authentication methods due to the increasing problems of fake people. In this paper, we We do a careful analysis of the smart phone authentication technology. The remainder of this research article is organized as follows: In part 2, a literature survey of some of the schemes proposed in the last decade. In part 3 the comparative analysis of the methods discussed in part 2. Finally, conclusions are presented in part 4.

2.LITERATURE SURVEY. .

There are several technologies that are involved in studying smartphone authentication, and we will discuss some of this research in this section

In this paper, Fathy, M. E., Patel, V. M., & Chellappa, R [5],we focus on solving the problem of smart phone active authentication via automatic face recognition. Video clips recorded by the front camera are used to report the results of face authentication. Taking video clips of the user in different three surrounding conditions and to capture the kind of difference that appears during navigation and reveals the preferred and difficult characteristics that are unique to the video clips on smartphones .Four methods were used on the still image. including Eigenfaces (EF) , Fisherfaces (FF) , Large-Margin Nearest Neighbour (LMNN) and Sparse Representation-based Classification (SRC) .we dropped the first three principal components in EF and use the subsequent 150 components to define the PCA projection matrix.

In this work Raja, K. B., Raghavendra, R., Stokkenes, M., & Busch, C [6]Suggest an authentication system based on facial characteristics, iris and eye contour. Test the system on two Samsung Galaxy S5 smartphones and Samsung Galaxy Note 10 tablet.In order to test the proposed system to see the ability of safe authentication. The tests were performed on biometrics separately and other tests were conducted after the system was integrated. The results that were reached was an error rate (EER) equal to 0.68%, which is one of the experiments that indicates the strength of the proposed system

In this paper Javidnia, H., Ungureanu, A., & Corcoran, P[7], a palm-based authentication method is proposed. This method can be used on all smartphones but on condition that they have a back camera and for this it is considered reliable. A color threshold is suggested and then its results are compared. Initially the YCbCr color space is used to estimate the distribution of surface pixels in the central part of the image and then superimpose this time interval over the entire Cb and Cr channels. The other methods use HSI color spaces to detect the skin, which illustrate different ways to represent color information, the Harris Corner detection method used in the search. Based on the calculation, the focal point of the hand is applied to extract the product next, LBP and SIFT were applied to extracted ROI to find the features. In both cases the geometric transformation represents the matching features.

Laghari, A., & Memon, Z. A.[8],Proposing an authentication mechanism using the motion sensor of smart phones, authentication is done by moving. The user's phone and the movement pattern is detected on the smartphone's accelerometer Since smartphones have a built-in motion sensor, there is no need to use attached devices. All that the user can do is sign, unlike the traditional manual signature, it must be done in the air by carrying the smartphone in hand. The proposed system consists of two phases, the first of which is the user registers himself in the system, then chooses an expectation and repeats it five times In the second trip, the authentication phase, the user enters the password he had previously chosen and puts his signature and the authentication process is completed. Through the results, we notice that the FRR rate was 6.87% FAR and it was 1.46%. However, this method can be improved further by increasing the number of features from the collected data. Signature signal frequency analysis can be done to make authentication more accurate.

In this paper, Rahmawati, E., Listyasari, M., Aziz, A. S., [9] a proposal for a digital signature system that combines Between the phone sensor, fingerprint and digital signature. The data is encrypted when the user sends a file to another person and the user has to put his fingerprints in the fingerprint sensor of the smartphone, and the document will be encrypted. The recipient of the message decrypts the message by using the public key. The fingerprint is a way to retrieve the value of the user's private key from .the database To generate a pair of keys in this system we use RSA algorithm

In this paper Zhang, X., Cheng, D., Dai, Y., & Xu, X [10],propose a multi-media authentication system that combines face and voice to solve the problems of individual biometrics .the central processing unit of the phone that cannot store large amounts of data where after the destination is detected, we delete the background that is of no use. In order to improve the robustness of the authentication system, the LBP operator is improved, in order to handle and mute the transmission information of the audio stream. The endpoint detection technology is improved. Adaptive integration method is used in the verification process, was note that the results obtained are in the accuracy of the algorithm authentication up to 100% and when the training sample number is5 and the verification time is about 341ms

In this paper, Chakraborty, B[11],a new method for user authentication is proposed based on human walking activities that were It was observed that the activity-based authentication method gives better accuracy than .extracted from smartphone sensor data the activity independent authentication. The convolutional neural network-based classification was also found to compared to the classic machine learning classifiers. Data were collected from 30 users, whose ages range from 19 to 40 years Each user performed 6 activities (walking, walking, sitting, standing, and standing) using a smartphone, depending on the acceleration sensors built into the smartphone. 70 volunteer users were identified for training and 30 tests. I used a convolutional neural network for the authentication. It is observed that(CNN) takes longer, but gives better results

In this paper Dai, H., Wang, W., Liu, A. X., Ling, K., & Sun, J[12], a proposal for an ultrasound-based human speech verification system is Speak Print .The traditional speech authentication system focuses on what the user is speaking while the SpeakPrint system focuses on how a person speaks and records the voice movement and mouth movement through the ultrasound signal . SpeakPrint extracts normal audio frequency MFCC and MMSI features from the ultrasound signal. The SVM classifier was

DOI : 10.31695/IJERAT.2020.3667

trained to detect these attacks by comparing feature differences. Use Samsung S5 to test the results. 40 users tested where rebooting tests were detected with 100% accuracy

.

In this paper, Razaque, A., Myrzabekovna, K[13], a proposed authentication system based on passwords and fingerprints, which is a single-scale but takes advantage of combining biometric authentication for fingerprint with a password-driven method. The proposed system provides the highest accuracy of potential (FAR) ,(ERR) and (TAR) as compared to other methods. The proposed system has been implemented on Java and Android Studio platforms. Using real equipment and participating in 1000 volunteers, the proposed system is tested .Suggested method The results confirm 100% accuracy higher than other competitors Biometric methods

3. COMPARATIVE ANALYSIS OF SYSTEMS

Table 1 shows details between the previous systems

Ref.	FAR	FRR	N. of samples	Device type	Algorithms Or methods	Biometric
5	--------	---------	50	Samsung Galaxy S4	Fisherfaces Eigenfaces LMNN SRC	Face
6	2.02	---------	78	Samsung Galaxy S5 tablet Samsung Galaxy Note 10.1	SURF BSIF	Face, eye contour and iris
7	0.001	-------	100000	Samsung Galaxy S7	LBP SIFT	Palm-print
8	1.46	6.87	10	Samsung Galaxy S6	---------	Signature
9	--------	-------	-----	Samsung Note	AES	Signature
10	0.0	0.0	100	Samsung Note 5	MFCC GMM LBP	face and voice
11	-----------		30	Samsung Galaxy S1	CNN	Gait
12	0.013	0.417	40	Samsung Galaxy S5	MFCC SVM	VOICE
13	SBA=98.93 BPA=99.48 EBT=99.8	SBA=98.37 BPA=99.51 EBT=99.2	1000	Galaxy A	-----------	Passwords and Fingerprint

4. CONCLUSION

In this research article, we reviewed a timeline of a different ways to smart phone authentication techniques for the period (2015-2020) to define the main characteristics of the performance of biometric authentication for smartphones, and to obtain the results, .the study tends to favor biometric authentication among smartphone users. All technologies reviewed are not without flaws

REFERENCES

[1] Abuhamad, M., Abusnaina, A., Nyang, D., & Mohaisen, D. (2020). Sensor-based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Survey. *arXiv preprint arXiv:2001.08578*.

[2] Zabidi, N. S., Norowi, N. M., & Rahmat, R. W. O. (2018). A Survey of User Preferences on Biometric Authentication for Smartphones. *International Journal of Engineering & Technology*, *7*(4.15), 491-495.

[3] Shen, C., Li, Y., Chen, Y., Guan, X., & Maxion, R. A. (2017). Performance analysis of multi-motion sensor behavior for active smartphone authentication. *IEEE Transactions on Information Forensics and Security*, *13*(1), 48-62.

[4] Laghari, A., & Memon, Z. A. (2016, January). Biometric authentication technique using smartphone sensor. In *2016 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST)* (pp. 381-384). IEEE.

[5]Fathy, M. E., Patel, V. M., & Chellappa, R. (2015, April). Face-based active authentication on mobile devices. In *2015 IEEE international conference on acoustics, speech and signal processing (ICASSP)* (pp. 1687-1691). IEEE.

[6]Raja, K. B., Raghavendra, R., Stokkenes, M., & Busch, C. (2015, May). Multi-modal authentication system for smartphones using face, iris and periocular. In *2015 International Conference on Biometrics (ICB)* (pp. 143-150). IEEE.

[7] Javidnia, H., Ungureanu, A., & Corcoran, P. (2015, November). Palm-print recognition for authentication on smartphones. In *2015 IEEE International Symposium on Technology and Society (ISTAS)* (pp. 1-5). IEEE.

[8]Laghari, A., & Memon, Z. A. (2016, January). Biometric authentication technique using smartphone sensor. In *2016 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST)* (pp. 381-384). IEEE.

[9]Rahmawati, E., Listyasari, M., Aziz, A. S., Sukaridhoto, S., Damastuti, F. A., Bachtiar, M. M., & Sudarsono, A. (2017, September). Digital signature on file using biometric fingerprint with fingerprint sensor on smartphone. In *2017 International Electronics Symposium on Engineering Technology and Applications (IES-ETA)* (pp. 234-238). IEEE.

[10]Zhang, X., Cheng, D., Dai, Y., & Xu, X. (2018, December). Multimodal biometric authentication system for smartphone based on face and voice using matching level fusion. In *2018 IEEE 4th International Conference on Computer and Communications (ICCC)* (pp. 1468-1472). IEEE.

[11]Chakraborty, B. (2018, December). Gait related activity based person authentication with smartphone sensors. In 2018 12th International Conference on Sensing Technology (ICST) (pp. 208-212). IEEE.

[12]Dai, H., Wang, W., Liu, A. X., Ling, K., & Sun, J. (2019, June). Speech Based Human Authentication on Smartphones. In 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON) (pp. 1-9). IEEE.

[13]Razaque, A., Myrzabekovna, K. K., Magbatkyzy, S. Y., Almiani, M., Doszhanovna, B. A., & Alnusair, A. (2020, April). Secure Password-Driven Fingerprint Biometrics Authentication. In 2020 Seventh International Conference on Software Defined Systems (SDS) (pp. 95-99). IEEE.

.

DOI : 10.31695/IJERAT.2020.3667