International Journal of Engineering & Technology, 7 (4.19) (2018) 425-429

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Evolution of User Authentication Methods in Mobile Phones: A Security Perspective

Deborah Ooi Yee Hui[1], Kok Kian Yuen[1], Bibi Asha Farina Binti Shikh Mohd Zahor[1], Kelvin Lim Ching Wei[1], Zarul Fitri Zaaba[1*], Renas Rajab Asaad[2]

[1]School of Computer Sciences Universiti Sains Malaysia, 11800 Minden, Pulau Pinang.
[2]College of Computer Science and Information Technology, Department of Computer Science, Nawroz University
**Corresponding Author Email: zarulfitri@usm.my*

Abstract

There are many ways of performing user authentication in mobile phones. Back then, a specific button is assigned as a security lock button such as the asterisk yet major concerns on security issues over personal data stored in mobile phones have been raised. Password-based authentication took over the trend with pattern and PIN unlock being commonly used by users of mobile phones. However, these methods are still prone to fraud as unethical users tend to break the passcode using shoulder surfing or hacking. To further strengthen the security in mobile phones, biometric authentication approaches are proposed. In this paper, four biometric-based authentication methods are being compared through a several aspects. As a result, the most significant biometric-based authentication approach is presented.

Keywords: *User authentication; fingerprint recognition; iris recognition; voiceprint recognition; face recognition; security*

1. Introduction

The rise in the usage of Mobile Phones nowadays is undeniable. According to the Global Report, almost two-thirds of the world's population now has a mobile phone [1]. However, more than 52% of the 1500 Google Customer Survey respondents stated that the respondent would rather leave their phones unlocked [2]. This is extremely dangerous as smartphone theft has increased from 8% to 42% over a period of 10 years in New York City [3]. If such forms of user perception persist, a phone which is stolen and password-free may allow the thief to access the owner's personal identity and eventually result in not only the phone being stolen, but the owner's identity will also be misused.

Therefore, various authentication techniques have been introduced to protect the personal data which are stored in the phone. Out of the many approaches, the methods are grouped into three main classifications, namely knowledge-based authentication, ownership-based authentication, and biometric-based authentication. Knowledge-based authentication are enforced with a passcode, either in the form of a set of numbers or pattern. In such a situation, users are required to remember and recall a password which is set by the user. However, it is learnt in a survey conducted by [4] that knowledge-based unlocking methods have been deemed annoying by 46.8% of the 320 respondents. This is because extra time and effort are required to recall the passcode.

Ownership-based authentication may be another option. In such an approach, personal identities are stored in a physical object such as smartcards or electronic tokens. Even though the user is no longer required to remember the passcode, the user has to carry an extra object along.

Such physical objects may be bulky and can be easily lost, hence this method of unlocking is not exactly suitable for the purpose of authenticating mobile phones. Furthermore, RFID tags or NFC tags can be stolen and could potentially grant an unauthorised user access to the valuable data inside the mobile phone [5]. Since there is a drawback for each knowledge-based and ownership-based authentication, the third approach which is biometric-based is proposed to be more secure and user-friendly than the other two authentication methods.

The main objective of this paper is to analyse the reliability and effectiveness of each biometric-based authentication method for being used in the authentication of mobile phones in the current trend. Based on the results of the investigation, this study will determine which biometric authentication method is the best.

The rest of the paper is organized as follows. Section 2 critically reviews the challenges and problem faced by each biometric-based authentication method as identified by authors of related works. Section 3 provides in depth comparison and contrast between the different biometric approaches and the best biometric approach is identified in Section 4.

2. Background of Problem

According to [6], biometric is defined as a way of portraying unique recognition to the personal identity by means of measuring and analysing the biological and behavioural characteristics. It is also stated that the advantage of using biometric-based identification over the other two approaches would be the ease of mobile phone users in recalling the passwords or carrying the access device, owing to the fact that each individual has a biometric trait which is unique to that individual [4].

In general, there are many ways to differentiate one person from the other. Be it in walking pattern, method of gripping the phone or their own fingerprint, each person has traits and characteristics of their own which no one else in the world will be able to exactly duplicate. The available biometric traits are split into two categories, namely biological characteristics and behavioural characteristics [7].

Some common examples of biological characteristics are face, iris and fingerprint. Unlike biological characteristics, behavioural characteristics are less straightforward. Some examples are grip gesture, penmanship and gait-recognition. From a logical perspective, behavioural characteristics are more error-prone as compared to biological characteristics.

In light of the above problems, it can be seen that each biometric-based identification method has its own drawbacks and disadvantages. Therefore, the mobile phone industry faces the challenge of deciding which mobile phone authentication methods is the best.

3. Analysis and Findings

According to [10], biometric characteristics are defined as any human physiological or behavioural characteristic that is universal, distinctive, permanent and can be measured quantitatively. However, performance and acceptability issues should also be taken into consideration. Nowadays, the top biometric authentication methods for mobile phones are face, iris, voice and fingerprint. Therefore, more investigation was carried out in terms of the algorithm used, adaptability, degree of accuracy and vulnerability to fraud. These topics will be discussed in the following subsections.

This is because biological characteristics will not change over time whereas behavioural characteristics have a tendency to evolve and change over time. For example, the methods of gripping the phone can vary according to the emotional states of the person whereas traits such as fingerprints or iris will not change over time. Nonetheless, each method has its own disadvantages. Based on previous works, researchers have identified a few problems in each biometric-based authentication method. Table 1 provides a brief summary of the biometric identification methods and their respective problems.

Table 1: Summary of Problems Faced In Each Biometric Identifier

Biometric Identifier	Overview
Face	• Illumination inconsistencies, background environment changes and different viewpoints may cause difficulty in recognising the user's face [9]. • Features extracted from biometric characteristics of different individuals can be quite similar due to genetic factors [10]. • Variations in pose, expressions, facial hair, wearing of spectacles causes "intra-class variation" where the data acquired during verification is not identical to the data during enrolment [10].
Iris	• The identification process may face performance degradation due to illumination, user's gazing point and low central processing unit in a mobile phone [11]. • Eyelashes and eyelids can distract focus on the upper and lower eyelids. The user also cannot be wearing contact lenses or spectacles as it causes the overshadowing of eye image [12]. • Iris varies throughout an individual life, thus it will be not be the same for phase of adulthood and adolescence of the user. Changes of the structures happen due to aging. Iris contains complex pattern as it has a lot of distinctive features of the eye, such as: furrows, ridges, rings, corona, freckles and arching ligaments [13].
Voice	• It is unreliable when it faces age deterioration as the user's voice may change due to aging [14]. • Human voices may change over time due the behavioural characteristic of each individual such as age, health and emotion [13]. • Different types of handsets and the varying quality of telephone connection may cause the identification process to be complicated [15].
Fingerprint	• Fraud may happen easily as criminals may cover the fingers with fake fingerprints or mutilate their fingers to avoid fraud identification by automated systems or even human experts [16]. • A lot of computation resources are required [13].

3.1. Algorithm Used

In any biometric authentication method that utilizes image detection algorithm such as face and iris, the processes are somewhat similar. Both authentication methods follow a three-step procedure, which is:

- capturing and detecting the presence of face or iris,
- defining the location of the face or iris and performing image optimization (to reduce noise) and comparing the image obtained with the template stored in the database [17].

In order to accurately detect a face, the shape and location of facial attributes such as the lips, chin, eyes, eyebrows, nose and the space between them play a crucial role. A well-known face detection algorithm is the Viola and Jones face detection algorithm which combines AdaBoost learning algorithms which selects the most prominent features first and Haar-like features which extract facial features at different scales very quickly [18].

By combining these two approaches, the result is a fast and accurate acquisition of facial features that can then be compared with the template stored in the database.

However, for iris recognition, the challenge is to isolate the iris from other parts of the eye, such as the eyelids. While the Daugman system which focuses on iris recognition simply ignores the upper and lower parts of the image altogether, the system proposed by [19], edge detection algorithm is used followed by circle Hough transform in order to accurately detect the boundaries of the eyelids. In both systems, the derived information of the image intensity is fine-tuned by the expected configuration of model components. However, these algorithms are not specifically designed for mobile phones. For mobile phones, [20] proposes the use of an Adaptive Gabor Filter. This Gabor Filter is used when extracting iris feature code. Since most mobile phone users tend to use their mobile phones in outdoor situations and in sunlight, the algorithm has to take the amount of blurring and sunlight into consideration as well. This algorithm utilises infrared technology to measure the amount of sunlight involved, as well as the iris focusing mask proposed by [20] to check whether the image is blurred or not. Then the results are used for selecting the kernel size, frequency and amplitude of the Gabor filter. The system then proceeds with Daugman algorithm to extract iris code and Hamming Distance to measure the differences between the two iris codes [20].

The unique characteristics of fingerprints are their complex patterns of ridges and valleys that are different for every individual and thereby provide an optimal biometric verification method. The upper skin layer segments of the finger are called ridges and the lower segments are called valleys. The ridges form so called minutia points. Minutia-based matching and pattern-based matching are the two main algorithm families commonly used in fingerprint recognition. Specific details within the fingerprint ridges are compared in minutia matching whereas in pattern matching, the overall characteristics of fingerprints are compared. This is done by obtaining the image center of the fingerprint and then cropping the image around this graphical center. The cropped image is then compressed and stored for a subsequent match. Minutia based matching is one of the most well-known and well-researched fingerprint verification methods while pattern based matching works well with all fingerprint sensor types [17].

3.2. Adaptability

Even though these algorithms are commonly implemented in their various biometric verification fields, it cannot be denied that these complex algorithms also take up a significant amount of computing power, memory and time. As such, concerns arise as to the adaptability of these biometric verification systems in our humble everyday mobile phones. This adaptability can be categorised into three categories, namely: speed, memory space and the input devices used to implement these authentication methods. The results are shown in Table 2.

Table 2: Comparison of Various Criteria of Adaptability in Mobile Phone Authentication

Authentication Method	Face	Iris	Voice	Fingerprint
Processing Time	90 μs [23]	< 1 μs [23]	1.47 s [24]	10 ms [23]
Minimum Memory Usage	480 KB RAM [8] 31 MB ROM [9]	2 KB ROM per picture [25] 512 MB [26]	128 MB of RAM [8]	2 MB of RAM [27]
Input Device	Camera [28]	Camera [20]	Microphone [28]	Capacative Sensors [29]
Processing Power	High [30]	High [20]	High	High

As seen in Table 2, all the biometric authentication methods require high processing power. However, the iris recognition system has the fastest processing time but require the most amount of memory. Voice recognition system, on the other hand has the longest processing time and the second largest memory usage. Face authentication system requires less processing time and less RAM memory than fingerprint authentication. All the biometric authentication methods in mobile phones require some sort of input device, such as camera, microphone and sensors. This could significantly affect the cost of the mobile phone as some input devices such as camera are already built into the mobile phone, while fingerprint sensors require some extra cost.

3.3. Degree of Accuracy

After thoroughly analysing all the algorithms used to implement these biometric authentication methods, the question remains: “How accurate is it?” To answer that question, the biometric authentication methods will be analysed from the four main measures of biometric accuracy, namely TAR, FAR, TRR and FRR. The definitions are as seen in [31, Table 3].

As we can see from Table 4 in the following page, iris biometric authentication method has the lowest degree of FRR and FAR while face authentication method has the highest degree of FRR. However, face authentication method has the lowest degree of FAR with only 1%. Face authentication methods could be deemed annoying as the same individual could be rejected from accessing his / her own mobile phone multiple times due to inconsistencies in lighting and background.

However, it would not easily verify another individual as the rightful phone owner. In the voice biometric authentication methods, the false reject rate is equal to that of face authentication method, if not slightly better. This is due to multi-lingualism and the fact that it does not depend on any written form of text.

Table 3: Summary of Definitions of Biometric Accuracy Standard

Measure of Biometric Accuracy	Description
True Acceptance Rate (TAR) / True Match Rate (TMR)	The degree that the biometric system is able to correctly match the biometric information from the same person. Developers of biometric systems attempt to maximise this measure.
False Acceptance Rate (FAR) / False Match Rate (FMR)	The degree of frequency where biometric information from two different people are falsely reported to be from the same person. Developers attempt to minimise this measure.
True Rejection Rate / True Non-Match Rate (TNMR)	The frequency of cases when biometric information from one person is correctly not matched to any records in a database because, in fact, that person is not in the database. Developers attempt to maximize this measure.
False Rejection Rate (FRR) / False Non-Match Rate (FNMR)	The frequency of cases when two biometric measurements from the same person is falsely reported to be from two different people. Developers attempt to minimize this measure.

Table 4: FAR and FRR of the Various Methods under Certain Test Conditions

Biometric Authentication Method	Test Parameters	False Rejection Rate (FRR)	False Acceptance Rate (FAR)
Fingerprint	Exaggerated skin distortion, rotation [7]	2%	2%
Face	Varied lighting, outdoor/indoor [9]	10%	1%
Voice	Text independent, multilingual [10]	5 – 10%	2 – 5%
Iris	Varied lighting, outdoor in sunlight [11]	0.00003 %	0.003%

Voice authentication method also has the highest possible False Accept Rate of 5%, which means that it is relatively easier for an unauthorised person to gain access to the mobile phone. Fingerprint biometric authentication method has an equal FAR and FRR of 2% respectively. Since 2% is quite a low percentage, it could be said that fingerprint is quite a good and secure method of locking mobile phones as the rightful owner of the mobile phone can be verified accurately with minimal errors and other unauthorised individuals will not be able to unlock the mobile phone.

3.4. Vulnerability to Fraud

According to [32], spoofing is the act of intentionally outwitting a biometric system by presenting fake evidence in order to gain authentication. This can take the form of an artificial finger, a mask over a face, or a contact lens on an eye. Such an attack is quite easily forged in facial recognition systems, because photographs or videos of a valid user can be easily captured from a distance or obtained through online social networks. Access can be gained by simply showing the printed photos of the authorised user or replaying their recorded videos to the sensor [33]. Besides the use of gelatine-made fake fingers, spoofing in fingerprint authentication could be as sinister as dismembering a finger or by simply placing a latent print on a sensor and activating the sensor by breathing on it [32]. Since mobile phone fingerprint sensors are mostly capacitive sensors, these latent prints could be activated by touching the print with a capacitive stylus or any conductive material held with the human hand.

In terms of the text-independent voice authentication method, where the user's voice is used as a medium of identification instead of text, this method has more protection against fraud compared to a text-dependent system [17]. The user's voice cannot be imitated easily because according to [34], no two people in this world may own the same voice. This is significant because each human have different voice frequencies in terms of pitch, tone and rate. However [35] points out that unethical users may commit fraud by simply recording the voice of an authorised user to gain authentication. This increases the possibility of shoulder surfing attacks even on text-independent authentication systems.

The biometric authentication method that is most fraud-resistant is iris authentication method. If the users sets the system up correctly (without wearing spectacles or contact lens at the point of sign up), it is almost impossible to gain unauthorised access into an iris biometric authentication system as the accuracy of iris recognition has achieved 99% [35].

4. Discussion

Having thoroughly analysed the four biometric authentication methods and their adaptability to mobile phones, degree of accuracy and vulnerability to fraud, these four biometric methods will be compared with each other to determine which biometric authentication method is the best. Based purely off the degree of accuracy, Iris Recognition System is definitely the most accurate with only 0.00003% FRR and 0.003% FAR. However, as with everything else, there is a trade-off. Although the Iris Recognition System is the fastest and also the most fraud-resistant, it also requires the largest amount of RAM memory to process the complex algorithms within that very short and limited timespan. Face authentication methods, on the other hand, use the least amount of RAM memory to process the data, but it could also be deemed as one of the most annoying biometric authentication methods for mobile phones as it has a FRR of as much as 10%. This means that 1 out of 10 users unlock attempts would result in failure, even if the individual is in fact an authorised user. The same goes for voice authentication method, which also has a FRR of 10%.

However, face authentication method fares slightly better than the voice authentication method as the face authentication method is much faster and has a lower FAR than voice authentication method. With this, the voice recognition algorithm could be considered as the most annoying and also the most unreliable method of phone unlocking. Practically speaking, it would also be impractical to for a user to unlock his or her phone by repeating a set of phrases every time, especially when situations do not condone it, such as when people are asleep, or when the user is in a meeting.

The fingerprint authentication method sits comfortably in between iris authentication method and face authentication method, with an FAR and FRR of 2% each. It is generally quite average in terms of speed and memory, with a processing speed that is slower than face but faster than voice and a RAM memory usage that is greater than face but less than voice. In that sense, it can be considered as being worse than face in terms of processing time and memory but if accuracy were to be taken into consideration, the fingerprint authentication method would fare better than face. Since the possibilities of frauds are endless, accuracy is definitely of the most importance. If an authentication method has very high accuracy such as iris, there would be less chances of any kind of fraud being able to take place.

5. Conclusion

With that being said, iris recognition would be the most suitable biometric authentication method for mobile phones, followed by fingerprint authentication method, and then face authentication method. Until further progress is made to increase the accuracy rate of voice authentication as well as reduce the processing time and RAM memory usage, this authentication method will remain the least suitable authentication method to be implemented in mobile phones.

Acknowledgement

"This research is fully supported by University Research Grant from Sultan Idris Education University under the grant number of 2018-0134-109-01."

References

[1] Kemp, S., 'Digital in 2017: Global Overview.' We Are Social, 2017,https://wearesocial.com/special-reports/digital-in-2017-global-overview. Accessed 9 October 2017.

[2] Bursztein, E., 'Survey: Most People Don't Lock Their Android Phones – But Should.' Elie, 2014, https://www.elie.net/blog/survey-most-people-dont-lock-their-android-phones-but-should. Accessed 10 October 2017.

[3] Baldwin, R., 'Don't Be Silly. Lock Down and Encrypt Your Smartphone.' Wired, 2013, http://www.wired.com/2013/10/keep-your-smartphone-locked. Accessed 10 October 2017.

[4] Harbach, M., De Luca, A. & Egelman, S., "The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens," in CHI '16 Proceedings of the 34th Annual ACM Conference on Human Factors in Computing System, San Jose, CA, 2016, pp. 4806-4817.

[5] Schlöglhofer, R. & Sametinger, J., "Secure and Usable Authentication on Mobile Devices," in The 10th International Conference on Advanced Computing & Multimedia, Bali, 2012, pp. 257-262.

[6] "Biometrics." Def. 2. Merriam-Webster Online. Meriam-Webster, 2017. Web. Accessed 10 October 2017.

[7] Mohammed, S. K. & Fajri, K., "A Review of Fingerprint Preprocessing Using A Mobile Phone," in Proceedings of the 2012 International Conference on Wavelet Analysis and Pattern Recognition, Xian, China, 2012, pp. 152-157.

[8] Ijiri, Y., Sakuragi, M. & Shihong, L., "Security Management for Mobile Devices by Face Recognition," in The 7th International Conference on Mobile Data Management, Nara, Japan, 2006.

[9] Hadid, A., Heikkild, J. Y., Silven, O. & Pietikdinen, M., "Face and Eye Detection For Person Authentication In Mobile Phones," in First ACM/IEEE International Conference on Distributed Smart Cameras, Vienna, Austria, 2007.

[10] Jain, A., "Biometric Recognition: How Do I Know Who You Are?," in Proceedings of the IEEE 12th Signal Processing and Communications Applications Conference 2004, Kusadasi, Turkey, 2004.

[11] Kim, Dongik, Jung, Yujin, Toh, Kar-Ann, Son, Byungjun & Kim, Jaihie., "An Empirical Study on Iris Recognition in a Mobile Phone," in Expert Systems with Applications, Tarrytown, New York, 2016, pp. 328-339.

[12] S., C. S., & Shinde, G. N., "Iris Biometrics Recognition Application in Security Management," in 2008 Congress on Image and Signal Processing, Sanya, China 2008.

[13] Delac, K. & Grgic, M., "A Survey on Biometric Methods," in 46th International Symposium Electronics in Marine, Zadar, Croatia, 2004, pp. 184-193.

[14] Bhattacharyya, D., Ranjan, R., Alisherov, F. & Minkyu, C., "Biometric Authentication: A Review," in International Journal of u- and e- Service, Science and Technology, Vol. 2(3), Australia, 2009, pp. 13-28.

[15] Philips, P. J., Martin, A., Wilson, C. L. & Przybocki, M., "An Introduction to Evaluating Biometric Systems," in Computer, Vol. 33(2), Los Alamitos, California, 2000, pp. 56-63.

[16] Anil, K. J., Jianjiang, F. & Karthik, N., "Fingerprint Matching," in Computer, Vol. 43(2), Los Alamitos, California, 2010, pp. 36-44.

[17] Anil K. J., Ross, A. & Prabhakar, S., “An Introduction to Biometric Recognition,” in IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14 (1), 2004, pp. 4-20.

[18] Viola, P. & Jones, M., “Rapid Object Detection Using A Boosted Cascade of Simple Features,” in Proceedings of the 2001 IEEE Computer Science Society Conference on Computer Vision and Pattern Recognition, Kauai, Hawaii, 2001.

[19] Wildes, R. P., “Iris Recognitions: An Emerging Biometric Technology,” in Proceedings of the IEEE, Vol. 85(9), Princeton, New Jersey, 1997, pp. 1348-1363.

[20] Jeong, D. S., Park, H. A., Park, K. R. & Kim, J., “Iris Recognition in Mobile Phone Based on Adaptive Gabor Filter,” in Zhang, D. & Anil, K. J., (eds) Advances in Biometrics, ICB 2006. Lecture Notes in Computer Science, Vol. 3832, Berlin, Heidelberg: Springer, 2005.

[21] Zhang, J. & Chen, X. M., “A Research of Improved Algorithm for GMM Voiceprint Recognition Model,” in Control and Decision Conference (CCDC), Yinchuan, China, 2016, pp. 5560-5564.

[22] Shoup, A., Talkar, T., Chen, J. & Anil, K. J., An Overview and Analysis of Voice Authentication Methods, 2016. Unpublished manuscript.

[23] Anil, K. J., Sharath, P., Salil, P., Hong, L. & Arun, R., “Biometrics: A Grand Challenge,” in Proceedings of the 17th International Conference on Pattern Recognition, Cambridge, UK, 2004.

[24] Robert, G. Z. & Olsen, J., Voice Recognition Software Versus A Traditional Transcription Service For Physician Charting in the ED. Chicago, IL: University of Chicago Hospitals Section of Emergency Medicine, 2001.

[25] Matschitsch, S., Tschinder, M. & Uhl, A., “Comparison of Compression Algorithms’ Impact on Iris Recognition Accuracy,” in Lee, S. W. & Li, S. Z. (eds) Advances in Biometrics, ICB 2007. Lecture Notes in Computer Sciences, Vol. 4642. Berlin, Heidelberg: Springer, 2007.

[26] Dongik, K., Yujin, J., Kar-Ann, D., Byungjun, S., Jaihie, K., “An Empirical Study on Iris Recognition in a Mobile Phone,” in Expert Systems with Applications, Vol. 54, Tarrytown, New York, 2016, pp. 328-339.

[27] Cappelli, R., Maio, D., Maltoni, D., Wayman, J. & Anil, K. J., “Performance Evaluation of Fingerprint Verification Systems,” in IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 28(1), 2006, pp. 3-18.

[28] Clarke, N. L., Furnell, S. M. & Reynolds, P. L., “Biometric Authentication for Mobile Devices,” in 3rd Australian Information Welfare and Security Conference, Sydney, Australia, 2002, pp. 61-69.

[29] Gao, M., Hu, X., Cao, B. & Li, D., “Fingerprint Sensors in Mobile Devices,” in IEEE 9th Conference on Industrial Electronics and Applications, Hangzhou, China, 2014, pp. 1437-1440.

[30] Choi, K., Toh, K. & Byun, H., “Realtime Training on Mobile Devices for Face Recognition Applications,” in Pattern Recognition, Vol. 42(2), 2011, pp. 386-400.

[31] Andrew, S. P., ‘Fingerprint Concerns: Performance, Usability and Acceptance of Fingerprint Biometric Systems.’ 2008, https://www.andrewpatrick.ca/essays/fingerprint-concerns-performance-usability-and-acceptance-of-fingerprint-biometric-systems. Accessed 19 November 2017.

[32] Nixon, K., Aimale, V., Rowe, R., Anil, K. J., Flynn, P. & Ross, A., Spoof Detection Schemes in Handbook of Biometrics, pp. 403-423. New York, NY: Springer-Verlag, 2008.

[33] Erdogmus, N. & Marcel, S., “Spoofing Face Recognition with 3D Masks,” in IEEE Transactions on Information Forensics and Security, Vol. 9(7), 2014, pp. 1084-1097.

[34] Rabiner, L. R., “A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition,” in Proceedings of the IEEE 77.2, 2011, pp. 257-286.

[35] Shafique, U., Sher, A., Ullah, R., Hikmat, K., Zeb, A., Ullah, R., Waqar, S., Shafi, U., Bashir, F. & Shah, M. A., “Modern Authentication Technique in Smart Phones: Security and Usability Perspective,” in International Journal of Advanced Computer Sciences and Applications, Vol. 8(1), 2017, pp. 331-335.