The Study on Using Biometric Authentication on Mobile Device

Onsiri Silasai * and Wachana Khowfa

Department of Computer Science, Faculty of Science and Technology
Suan Dusit University, Bangkok, Thailand

* Corresponding author. Email: onsiri_sil@dusit.ac.th

ABTRACT

With the advanced of technology on mobile device, living the life through modern technology seems convenient and beneficial. Various of sensor and application installed on mobile device support and continuously change the way of people's life such as how to communicate with each other, to shop and to make transaction on financial and banking. One of the most things needed to be considered is how people protect on their own rights, data and private information among the insecure environment aside the mobile technology. Thus, security becomes seriously and complexity issues. Many techniques were developed and tested in order to ensure the reliability for user on using mobile device and its technology over decade. Biometrics which represents something existing in every human being is used to identify individual as it is unique. In this paper, the review of mobile user authentication and problems, the benefit of using physical biometric such as face, fingerprint, retina and iris also behavioral biometric for example voice, keystroke and touch dynamics are defined. The practical attacks on biometric recognition approaches available presently are stated along with the future work of biometric authentication. As a result, to improve accuracy and to enhance resistance against many types of attack on mobile device, the dynamic authentication with machine learning and deep learning techniques and applying biometric as two-factor authentication should be considered to use.

Keywords: Biometrics, Biometric Authentication, Mobile Device, Mobile Device Attack

INTRODUCTION

Security on mobile phone is important as mobile device and its application change the way of human's life. With the supporting for life and activities anywhere anytime, authentication on mobile device should be concerned as it provides reliability and trust for each user on their private data and access rights into sensitive information such as password, financial transaction and banking accounts. User authentication is typical way to verify and validate the right of user on their mobile phone using Password and Personal Identification Number (PIN). Anyway, as many services available need the secured password to gain access rights, each user has more load to remember all of their own keys. Therefore, most of active users decide to apply the easy to remember password which leads them into an insecure situation and mobile phone crimes (Fudong Li, 2013). The use of authenticated tokens and

Article history:
Received 12 March 2020; Received in revised form 20 April 2020;
Accepted 18 May 2020; Available online 2 June 2020

biometrics become considerate as other alternatives way to protect their right. Authentication using token has many drawbacks as it can be easily to lose and stolen, moreover, inconvenient as it requires extra equipment.

Recently, the researches in biometrics have extended many techniques and ways to user for keeping their right protected. Even though, the use of biometrics to validate user requires additional hardware but provides reliability, efficiency and optimized algorithms technology (Liu, Wang, Zhao, Yan, & Ding, 2016). Thus, user's access rights can be safe and protected. As the method based on something user is which is very unique, cannot copy, share and steal (Clarke & Furnell, 2007) (Kim, Chung, & Hong, 2010) (W. Meng et al., 2015). Existing research papers as follows, Yanushkevich and Nixon (Yanushkevich, 2007) mentioned on behavioral biometrics for online computer. Zirjawi et al (Zirjawi, Kurtanović, & Maalej, 2015) reported user requirements and preferences for biometric authentication on smartphones however, they focused only on iris recognition. Rajput and Sable (Rajput & Sable, 2016) made a survey on the use of iris biometrics recognition technique start from 2010 to 2015 as it has high recognition rate and performs better accuracy than others. While Padma and Srinivasan (Padma & Selvaraj, 2016) focused on using biometrics to authenticate user in the cloud computing environment. Alzubaidi and Kalita (Alzubaidi & Kalita, 2016) researched on the potential risks to occur when smartphones are lost and discussed on the concept of continuous authentication techniques using behavioral biometrics, especially keystroke dynamic and its evaluation. Recently, Benarous et al (Benarous, Kadri, & Bouridane, 2017) made a review of cyber security evolution and threats. Then introduced the solution for biometric authentication to handle with the security problems.

This paper starts with background knowledge of mobile device and its authentication involves with mobile user authentication methods, biometrics used in user authentication on mobile device, biometric authentication techniques, algorithms used in biometric authentication, type of attack on biometric authentication followed by future work for biometric authentication on mobile device will be defined and discussed. The end of this work is the conclusion.

BACKGROUND KNOWLEDGE

A. Mobile User Authentication Methods

Typical way to gain the access right into mobile system is the use of knowledge-based authentication which can be represented as something you know for example Password and PINs. The limitations of using password are as follows 1) It can be forgettable therefore user applies simply and easy to remember password or even uses the same password to every account they own. As a result, when attacker gets unauthorized access to account, they can gain access to others account of this user as well. 2) It can be stolen and copied, when user writes down their own password for self-reminded, the password can be easily taken away. 3) With the limitation of CPU and storage available on mobile devices, the number of characters used as Password/PINs approximately four to eight characters.

Therefore, another method, token-based authentication or something you have, is applied by using token hardware such as USB or smart card. However, this authentication method requires specific hardware and software (Ben-Asher et al., 2011). Though it provides user more security than keeping their password in a piece of paper. But it is inconvenient moreover the token can be lost and stolen as well.

Two categories of biometric which are physical and behavioral are used. Physical biometric relates to the physical characteristics of person. This type of biometric is considered unique to individual for example fingerprint, face, retina and iris. On the other hand, the behavioral biometric represents how people act or do things for example voice, keystroke dynamic and touch dynamic which can be represented in an individual pattern. By applying the something you are in authentication process, it is obviously that attackers encounter more difficult to generate a copy of personal biometrical characteristic (Rathgeb & Uhl, 2011) (W. Meng, Wong, Furnell, & Zhou, 2015) as well as it is easy for general user to use (Marous, 2016). Lately, biometrics-based authentication or something you are, for instance fingerprint and face, is playing an important role in mobile authentication. The comparison of each authentication methods in terms of the advantages and disadvantages as shown in Table 1.

Table 1 The comparison of authentication methods (Clarke & Furnell, 2007) (Kim, Chung, & Hong, 2010) (Liu, Wang, Zhao, Yan, & Ding, 2016) (W. Meng et al., 2015)

Authentication method	**Advantages**	**Disadvantages**
Password/PINs	• Easy to use • Inexpensive • No require specific hardware or software	• Can be forgettable • Can be stolen • Easy to copy, replicated
Token hardware	• Easy to use	• Can be stolen • Require specific hardware or software
Biometric	• Reliability • High security level • Difficult to copy, replicated • No require specific hardware or software	• Expensive/ High cost

To evaluate the used of biometric, seven criteria also available as follow: (W. Meng et al., 2015) (El-Abed & Charrier, 2012)

1. Universality: biometric is something that everybody must have.
2. Uniqueness: biometric is individual for person even in twin.
3. Permanence: biometric is long last and stay with person for the whole life.
4. Collectability: biometric is easy to collect, measure and evaluate.
5. Acceptability: biometric is widely accepted by everyone.
6. Circumvention: biometric is hard to copy and fake.

7. Performance: result of using biometric is accuracy.

B. Biometrics used to Authenticate User on Mobile Device

Presently, as many types of sensor are available in mobile device. These provide user continent support at the same time biometrics values which obtained from those sensors can be adopted in authentication user as well. In this section, two general categories of biometric as shown in Figure 1 are using in mobile authentication will be stated.

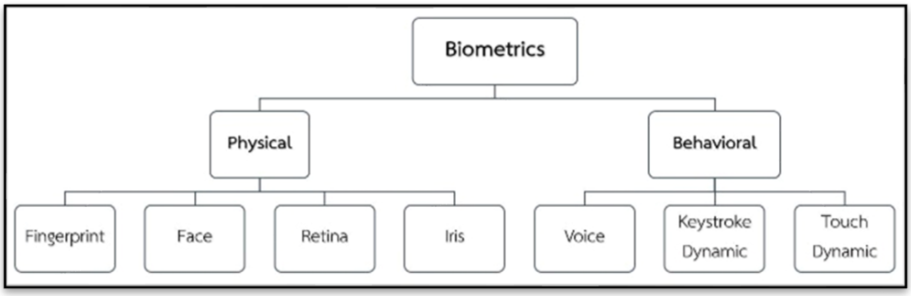

Figure 1 General category of biometrics

1. Physical biometric authentication is the used of individual personal characteristic involved with fingerprint, face, retina and iris as the unique characteristic of each person cannot duplicate or even share. As the pattern of fingerprint is unique even twins who share the same DNA still have got different fingerprint and it is not changed over time of human being's life (Yoon, 2014). Fingerprint is the most acceptable biometric this day as it is commonly used in user authentication system. Three basic patterns of fingerprint that used to recognize person are the arch, the loop, and the whorl. Face has the potential of identification person at distance of many meters as well as the reliable ability to identify the person among the crowd (Nissenbaum) but there is still a limitation as it requires high quality camera to capture people's face. Retina consists of a thin tissue of neural cells. It is located in the back of every human being's eye. Retina includes a complex structure patterns of blood vessels. Individual person's retina is unique even in twins. Retina remains stable over a lifetime of people (Seto, 2015) (Ushe, Tosa, & Friedman, 2015). Retina is the most accurate and most reliable. As well as, iris which is different by several characteristics as follow ligaments, furrows, ridges, crypts, rings, corona, freckles, and a zigzag collarette. The iris on each eye of every person is believed that it is unique and remains stable over time (Ushe, Tosa, & Friedman, 2015).

2. Behavioral biometric authentication which consists of action or manner of individual person for example voice, keystroke dynamic and touch dynamic can be applied to identify people. Voice can categorize the individual of person as the way people speak is dissimilar. Different person can create different tone even speak out the same word. Voice has more unique features than fingerprint however, the

limitation of using voice in authentication is that it is changeable due to age, sickness, tiredness and stress. Keystroke dynamic refers to the method that identifies the identity of person based on their individual manner and the rhythm of typing. Two terms of time which are 1) the duration to press a key called dwell time and 2) the time between release a key and press the next one called flight time are generally used in keystroke measurement. The rhythm while typing of each person can be used to identify as it is very personal independent (Bhatt & Santhanam, 2013). While, touch dynamic is wildly used as touchscreen technology is available in currently mobile devices. The benefit of touch dynamic over keystroke is that it provides more flexible to user in order to input such as multi-touch, scroll and tap (W. Meng et al., 2015). Similar to keystroke dynamic, touch dynamic can classify distinct of person however there is a limitation on accuracy as well.

C. Biometric Authentication Techniques on Mobile Device

Physical and behavioral biometrics can be applied in many ways of use. Common examples of these which related to people’s everyday life are the building security access systems and the computer access rights. Mobile device and technology are now moved on to apply biometrics for authenticating process as well. Table 2 below states the characteristics of each biometric authentication techniques which point out reason of using biometrics in authentication process.

Table 2 Biometrics authentication technique and characteristics (W. Meng et al., 2015)

Characteristics	Type of Biometrics						
	Finger print	**Face**	**Retina**	**Iris**	**Voice**	**Keystroke dynamics**	**Touch dynamics**
Commonly accepted	Y	Y		Y	Y		
Easy to use	Y	Y			Y		
High accuracy	Y	Y	Y	Y			
Low accuracy					Y		
Not consistence accuracy						Y	Y
Continuous authentication						Y	Y
Require specific hardware	Y	Y	Y	Y		N	N
Ability to work under poor condition	N	N	N	N	N	N	N
Expensive			Y				
Inexpensive	Y			Y			

Note: ‘Y’ stands for Yes and ‘N’ stands for No

1. Fingerprint recognition is widely accepted and used on mobile devices by means of successful technique to identify person (W. Meng et al., 2015). Many researches paid their attention on how to improve the ability to identify the fingerprint

pattern under low condition. For example, Wang et al (Wang, Bhattacharjee, Gupta, & Srinivasan, 2010) suggested the adaptive image pre-processing method. This proposed technique aimed to improve the clarity and quality of fingerprint image in order to determine the minutia extraction's accuracy and reliability in an automatic fingerprint recognition system. In 2015, Hariyanto et al. (Hariyanto, Sudiro, & Lukman, 2015) introduced a hardware based artificial neural network using minutiae matching algorithm as an embedded system environment to examine the fingerprint pattern as a vectors of minutiae spots. With this hardware, the process in matching and the used of cognistix making were faster. Jain et al (Jain et al., 2016) proposed the algorithm of image enhancement in order to improve quality fingerprint and evaluate identification accuracy for newborn baby. As a result, the possibility to recognize fingerprint of each person could be done since infant older than 4 weeks. At the same time, Feng et al (Feng, Li, & Wang, 2016) presented the user's identifying system using individual's fingerprint information and provided security to some of important information using MD5. The testing result shown that the authentication method had more available, reliable and secure.

2. Face recognition is the process of making decision whether the input image is matched to original one that kept in database. The objective of this process is to identify the individual person. There are many works on facial recognition with different algorithms over the past seven years as follow. Tan and Triggs (Tan & Triggs, 2010) proposed an efficient preprocessing method to eliminate the effects of changing in illumination. They applied the local ternary patterns (LTP) to improves the performance of the local binary pattern (LBP) based face recognition. As a result of testing with three data sets which widely used, this method had performance to work out under difficult illumination conditions. Schwartz et al (Schwartz, Guo, Choi, & Davis, 2012) used partial least squares in face identification to perform the multichannel feature weighting. Then extended this method to a tree-based discriminative structure in order to reduce the time in evaluating the samples. As a result, their identification method outperformed other techniques and could identify faces acquired across varying conditions. Furthermore, enhanced the ability of face recognition. Zafeiriou et al (Zafeiriou et al., 2013) presented the Photoface Database which was a 2-D and 3-D database used in face recognition based on photometric stereo in 2013.

3. Retina recognition is a low rate of false acceptance and false rejection technology in biometric authentication. However, the retina is small so that it is more difficult to measure and capture than other biometrics. At the same time, the process of retina recognition requires a specific hardware. Main area in retina recognition is to improve the accuracy of output which processed under various conditions for example Kakarwal and Deshmukh (Kakarwal & Deshmukh, 2010) presented an automated technique to recognize person based on individual retina then compared the performance in calculation the correlation and covariance matrix of the retinal images. While, Latha et al (Latha, Pabitha, & Thangasamy, 2010) proposed the method to initial the segmentation process of identifying blood vessel intersection points in the retina. Then generated the template which consisted of bifurcation points

in the blood vessels before matched the intersection points in different forms. In 2013 J. Fatima et al. (J. Fatima, A. M. Syed, & M. Usman Akram, 2013a) (J. Fatima, A. M. Syed, & M. U. Akram, 2013b) worked on two researches in retina recognition area. In the first work, they implemented wavelets and multilayers thresholding technique to extract the vascular pattern. This system based on vascular pattern of human retina. As a result, the proposed system performed high accuracy for retina recognition. Then in their second study, they proposed the method to improve the accuracy rate in retina vascular pattern recognition using windowing technique on skeleton vascular pattern. This technique eliminated the false feature points which appeared in vessel breakages, short vessel and spurs. Lately in 2015, Borah et al (Borah, Sarma, & Talukdar, 2015) presented a retina recognition system using Adaptive Neuro Fuzzy Inference System (ANFIS) and Principal Component Analysis (PCA). This system classified and performed the bloods vessel's feature extraction. The result stated that the recognition system was reliable and could be used to identify retina of kids as well.

4. Iris recognition is known as a very high rate of accuracy method. To perform the iris recognition, the process of verifying individual requires specific equipment and high-quality camera to capture the eyes color (Nissenbaum). Iris recognition applies the mathematical pattern recognition techniques to determine individual's eye which is unique and can be seen from distance. Kekre et al (Kekre et al., 2010) proposed an iris recognition system using Vector Quantization and Kekre's Fast Codebook Generation Algorithm (KFCG). Then compared the performance by using the Discrete Cosine Transform (DCT). The result of KFCG method returned better performance at 89.10% of accuracy than the DCT which had 66.10% of accuracy. Suciati et al (Suciati et al., 2016) developed the iris recognition using Canny Edge Detection and Hough Transform method. This method could automatically identify individual person using the eye image data. Before applied the statistical moments of Wavelet Transform to extract the feature of iris image with Support Vector Machine as a classify method. The result of this experiment returned good recognition rate with 93.5%. At the same time, L. E. Ali et al. (L. E. Ali, Luo, & Ma, 2016) introduced method of iris recognition from distantly acquired facial images using K-Nearest Neighbor (KNN), Support Vector Machine (SVM) and Kernel based Extreme Learning Machine (KELM) algorithms. The results shown that the performance of KELM to recognized iris at 98.60%.

5. Voice recognition is the process of decoding the human's voice then compares the voice to a voiceprint which stored on file. Voice recognition can be applied to use in authentication to secure user's information on mobile device as it can identify or confirm the identity of each person based on their voice as plus it is not limited under time (Kang, Lee, Park, & Park, 2014). Also, it cannot be copied. Many works on voice recognition aimed to improve the accuracy by applying different methods. Darojah and Ningrum (Darojah & Ningrum, 2016) focused on improving the performance of using Neural Network (NN) in voice recognition classification by applied Extended Kalman Filter method (EKF) as the training algorithm. The result of this work stated that the EKF provided the performance rate at 100% and could be used to improve the performance of Neural Network in voice

recognition. At the same time, Ranny (Ranny, 2016) developed method which could eliminate the outliner data by using K Nearest Neighbor (KNN) compared to Double Distance Measurement to point out the distance between individual data and the center of the KNN. The result shown that Double Distance Measurement performed better than KNN with 96.77% of accuracy while KNN had 84.85% of accuracy in voice recognition.

6. Keystroke dynamic recognition is commonly used to identify personal based on their personal typing behavior or style (Saevanee, Clarke, & Furnell, 2012). Existing works on keystroke dynamic focused on accuracy. Lee et al (Lee, Choi, & Moon, 2007) proposed the method to identify user by the typing characteristics using n-dimensional of vectors with the ellipsoidal hypothesis of space to separate a set of the time vectors before evolved by Genetic Algorithm. In this work, a filtering technique and an adaptation mechanism were applied in order to enhance the constancy and effectiveness. The result shown that there was small error rate in authentication process when using this method. Dholi and Chaudhari (Dholi & Chaudhari, 2013) introduced an approach to classify user's keystroke dynamic using K Nearest Neighbor (KNN). The keystroke was checked within the cluster to reduce the verification load. Later, Çeker and Upadhyaya (Çeker & Upadhyaya, 2015) applied the Gaussian Mixture Model (GMM) to perform the experimental using a data set which was collected from a restricted environment. As the result of this study, GMM performed the recognize keystroke dynamics recognition more correctly and ensured users with 0.08% of Equal Error Rate (EER). Moreover, it produced higher confidence level when compared to the pure Gaussian which had 1.3% of EER. Çeker and Upadhyaya they (Çeker & Upadhyaya, 2016) again extended the use of Support Vector Machine (SVM) to perform the continuous authentication with long - text data. As a result, the level of authenticate user and reject impostor were approximately 0% when set a one - class SVM for each user. In addition, with standardize of the input and set the correct kernel of scale, one - class SVM could be used as an efficiency tool to authenticate user continuously and recognized user's keystroke dynamics with high accuracy rate. M. L. Ali et al. (M. L. Ali, Thakur, Tappert, & Qiu, 2016) proposed a novel of user authentication technique using 1-substate of Hidden Markov Model. The result from this extensive experiment stated that this proposed technique achieved 80% of accuracy.

7. Touch dynamic recognition is an inconsistence accuracy approach in biometric due to the limitation of fat finger problem. Users can not be able to point on a touch screen confidently. The controlled area and target point are not visible as it is obstructed by the finger (Kolly, Wattenhofer, & Welten, 2012). Therefore, researches on touch dynamic recognition aim to improve the accuracy as follow, Sae-Bae et al (Sae-Bae, Ahmed, Isbister, & Memon, 2012) presented a multitouch gesture-based authentication method by applying a comprehensive collection of five finger touch gesture to classify the movement characteristics of user's palm and fingertips. This method achieved 90% of accuracy with single gesture and indicated that the performance would improve by using the multi-gesture. Thus, the multi-touch gesture could be promised as authentication technique. Y. Meng et al. (Y. Meng, Wong, &

Kwok, 2014) present a user authentication technique using a lightweight touch dynamic on a mobile phone's touchscreen. In addition, they applied an Adaptive Mechanism to periodically select a better classifier for preserve the accuracy while authenticate user. The result indicated that this proposed technique had 2.46% of an Average Error Rate and the Adaptive Mechanism could help to keep the authentication accuracy at stable level.

D. Algorithms Used in Biometric Authentication

The method of authentication each's biometric can be divided into two categories consider the way to identify user.

1. Static authentication represents the process of identification and authentication user via the physical features which encounter security weaknesses. Whenever the data used to authentication user is hacked or created a copy, then the attacker can gain access rights over user (Vergara, 2019).

2. Dynamic authentication is the method of learn and analyze individual pattern of user behavior to authenticate user. It is normally applied to work with behavior biometric as well. This type of authentication can provide continue monitoring and can be adjustable when user's behavior changed. For this reason, the dynamic biometric method is trustworthy way to the authentication user and provides greater security than the static method (Smejkal & Kodl, 2018). Some researches started work on behavioral biometrics for example keystroke dynamic to perform a continuous authentication as well.

Many researches worked on existing algorithms and their proposed methods in order to ensure users the acceptable, reliable and consistent of biometric authentication process both in static and dynamic as shown in Table 3.

Table 3 Algorithms used in biometric authentication

Biometric authentication technique	Method		Algorithm/Technique	Result
	Static	Dynamic		
Fingerprint recognition (Wang, Bhattacharjee, Gupta, & Srinivasan, 2010) (Hariyanto, Sudiro, & Lukman, 2015)	✓		Adaptive image Pre-Processing Approach, Artificial Neural Network	Performance when perform with poor quality of images is better and work faster
Face recognition (Tan & Triggs,	✓		Local Ternary Patterns, Partial Least Squares	improves the performance and can identify faces acquired across varying conditions

Biometric authentication technique	Method		Algorithm/Technique	Result
	Static	Dynamic		
2010) (Schwartz, Guo, Choi, & Davis, 2012)				
Retina recognition (J. Fatima, A. M. Syed, & M. U. Akram, 2013a)	✓		Wavelets and Multilayered Thresholding Technique	99.57% and 97% of recognition rate
Iris recognition (Kekre et al., 2010) (Suciati et al., 2016) (L. E. Ali, Luo, & Ma, 2016)	✓		Vector Quantization used Kekre's Fast Codebook Generation Algorithm, Support Vector Machine, K-Nearest Neighbor and Kernel based Extreme Learning Machine	89.10% to 98.60% of accuracy
Voice recognition (Darojah & Ningrum, 2016) (Ranny, 2016)	✓		Neural Network, Extended Kalman Filter method, K Nearest Neighbor, double distance measurement	96.97% to 100% of accuracy
Keystroke dynamic recognition (Çeker & Upadhyaya, 2015) (Çeker & Upadhyaya, 2016) (M. L. Ali, Thakur, Tappert, & Qiu, 2016) (Buza, 2016)	✓		Gaussian Mixture Model, Support Vector Machine and Hidden Markov Model	Close to 0% of equal error rate and 80% of accuracy
Keystroke dynamic recognition (Pisani, Lorena, & Carvalho, 2015)		✓	Enhanced Template Update and kNN, 1NN-Dynamic Time Wrapping, Nearest Neighbor Regression with Error Correction	improve the predictive performance and performed well for personal identification
Touch dynamic recognition	✓		Multi-Touch Gesture	90% of accuracy

Biometric authentication technique	Method		Algorithm/Technique	Result
	Static	Dynamic		
(Sae-Bae, Ahmed, Isbister, & Memon, 2012)				

E. Type of Attack on Biometric Authentication

Mobile device has many limitations for example 1) its structure, operation and CUP 2) its various type of sensor and its size. For these reasons, mobile device user encounters many attacks. Current type of biometric authentication attack available on mobile device and how to attack will be discussed in this section. The study on practical attack in biometric authentication has done so far. Type of attack available on biometrics both physical and behavioral are shown in Table 4.

Table 4 The Type of Attack on Biometric Authentication

Type of Attack	Biometric Authentication						
	Fingerprint	Face	Retina	Iris	Voice	Keystroke	Touch
Playback attack/ Replay attack (Wei & Stevenson, 2008) (Smith, Wiliem, & Lovell, 2015a) (Pandey & Pandey, 2015) (Smith, Wiliem, & Lovell, 2015b) (Abdal-Ghafour, Abdel-Hamid, Nasr, & Khamis, 2016)	✓	✓			✓		
Direct attack/ Attack at the sensor (Ortiz-Lopez, Galbally, Fierrez, & Ortega-Garcia, 2011)	✓	✓	✓	✓			
Mimic attack/ Presentation attack (Yu, Guo, & Stojmenovic, 2012) (Yu, Guo, & Stojmenovic, 2015)	✓	✓				✓	✓
Fake face attack/ deepfake/ Face spoofing attack (Gavrilescu, 2016)		✓					

Type of Attack	**Biometric Authentication**						
	Fingerprint	**Face**	**Retina**	**Iris**	**Voice**	**Keystroke**	**Touch**
(Nguyen, Retrain, Morain-Nicolier, & Delahaies, 2016)							

Payback or replay attack happens when attacker spies on data or information that is sent between sender and receiver. Then the attacker can intercept that information and retransmit to receiver. Wei and Stevenson (Wei & Stevenson, 2008) developed the Playback Attack Detector (PAD). The PAD could be mobilized in guarding speaker verification systems against playback attacks. The PAD used a feature set called Peakmap to detect playback attacks. Peakmap consisted of the frame and the FFT bin numbers of the top five highest spectral peaks from each of the voiced frames. The incoming voice recording was extracted and then compared to all the recordings stored in the system. When the similarity score above a threshold was maximum, the system would be declared to be a playback recording. Smith et al (Smith, Wiliem, & Lovell, 2015a) applied a Noninvasive Challenge and Response Technique to handle with replay attack over face recognition on smart device. The result indicated that this technique could classify the sequences of face reflection under the condition with high degree of confidence. The studied on fake face attack was done by Pandey and Pandey (Pandey & Pandey, 2015). They developed the model based on spectral analysis of the captured images to classify real face and face image. The Fourier and Cosine transform of the image was performed using Neural Networks to evaluate the various Image Quality Measures (IQMs). Result from the proposed method would be compared with several conventional IQMs and tested against Replay-Attack. The result shown that there was an improvement in performance. While Smith et al (Smith, Wiliem, & Lovell, 2015b) proposed a method, which could address the problem of replay attacks in face recognition. By inserting binary watermark into the captured video, it provided high contrast between the signal states. It was robust signal in a wide range of conditions and also robust to different cameras and tolerates relative movements as well. In 2016, Abdal-Ghafour et al. (Abdal-Ghafour, Abdel-Hamid, Nasr, & Khamis, 2016) presented two proposed authentication techniques to enhance technique for seed key of BAC and technique to extract minutiae features from a fingerprint's scanned. The performance of method was evaluated via MATLAB and proved that it could enhance authentication of BAC and increased the entropy of seed key with smallest delay. Then, tested the strength of this technique against the attacking by using real fingerprint recognition database system.

Direct attack also refers to an attack at the sensor which does not require any specific knowledge about the system operation. The attacker will create a fake biometric then apply to related sensor on mobile device such as fingerprint sensor. As a result, the attacker can gain the access rights because sensor is unable to recognize between fake and real biometric. Ortiz-Lopez et al. (Ortiz-Lopez, Galbally, Fierrez, & Ortega-Garcia, 2011) introduced an attacking on iris recognition by vulnerability prediction scheme. Then tested the resistance of system using real and fake iris images for 1,600 subjects. The result indicated that the ability to classify real user was at 84% correctly rate. Furthermore, this method had an advantage against spoofing attack as well.

Mimic or Presentation attack uses the artefact or artificial biometric for example fake fingerprint, fake face and fake keystroke dynamics to attack mobile device. Fingerprint is easily to make a copy using oily left on mobile screen, then the attacker uses it to bypass into mobile device. However, Yu et al. (Yu, Guo, & Stojmenovic, 2012) studied on the relation between botnet and mimic attack. Three years later, they (Yu, Guo, & Stojmenovic, 2015) stated that, in practice, it was difficult for botnet owners to collect satisfactory number of active bots. They also established a semi-Markov Model to study botnet's behavior thus they found out that it was impossible to detect mimicking attack using statistics when the number of active bots was sufficiently large. Also, it was difficult for botnet owners to satisfy the condition to carry out a mimicking attack. Therefore, the mimic attacks could be discriminated from genuine flash crowds using second order statistical metrics.

For face spoofing attack, attacker uses 2D and 3D fake face to fool the recognition system and unlock mobile device. Face spoofing attack using 2D is more popular than 3D as 2D can easily create artificial face and the limitation of generating 3D face. There are many works that try to handle with this kind of attack for instance Gavrilescu (Gavrilescu, 2016) developed a video-based face recognition called soft biometric Neural Network based system. This system could analyze the individual pattern of face on multiple frames. Results of this work shown that the system was possible to work with accuracy higher than 85%. It also shown that the proposed method was attack resistant when tested against the photo spoofing attacks. Lately, in 2017, Nguyen et al (Nguyen, Retrain, Morain-Nicolier, & Delahaies, 2016) worked on the problem of spoofing attack on facial recognition in differences condition. This method applied the statistic behavior of the distribution of noise's local variances which performed different between real and fake face images then applied SVM as classification method. The results revealed that this proposed method had high performance against spoofing attack.

F. Future work for Biometric Authentication on Mobile Device

Future and trend of biometric authentication on mobile device can be focused in term of 1) the performance to improve accuracy and 2) the security to enhance resistance against many types of attack available presently as follow.

The accuracy is considered important in biometric authentication especially on mobile device in terms of the acceptable error rate and how to determine if the mobile system can detect fake user. To evaluate the performance of biometrics in authentication, out of accuracy rate, the binary classification (0,1) is regularly used in term of true positive, true negative, false positive and false negative as shown in literature reviews above. There are many researches which aim to increase the performance of techniques using in authenticating users as follow. Rasmus and Green

(Rasmus & Green, 2012) improved the accuracy of face recognition using a filter that available in contextual information. Moreover, measured the co-occurrence, recurrence and relative physical distance to predict the identity of each person. As a result of using genealogical data as context indicated that at hit list size 1, the accuracy improved by 26% while at size 5, the accuracy improved by 21% over the use of face recognition. Elazhari and Ahmadi (Elazhari & Ahmadi, 2013) presented the effect of using 1) Interpolation schemes 2) Namely 3) Nearest-Neighbor and 4) Bilinear and bicubic to low-resolution images of human as preprocessing in face recognition. Images stored in the ORL database were tested. Result shown that Bicubic and bilinear could improve the recognition rate of low-resolution images. M et al (M et al., 2013) studied how users perform the touch sequences on large touch screen surface. The result of study revealed that the location of predecessor on a touch had a considerable impact on the location and position of the touch ellipsis. The touch accuracy of standard hardware could be increased at least 7% and created better recognition rates on the same screen.

In the area of security, Sadi et al. (Sadi, Bouchair, Zebbiche, & Laadjel, 2014) introduced a new application of Local binary pattern (LBP) operators which successfully used in face recognition system to secure the digital fingerprint stored in Automated Fingerprint Identification System plus the embedding of watermarks using Arnold technique hidden in the fingerprint's image. The results indicated that this method was robust against commonly used image processing operations and in the process of compression JPG file, the fingerprint features did not change moreover still maintained a good visibility of the original one. Smith et al. (Smith et al., 2015b) considered the limitations of using current device and environment which could create the impact on the performance to detect face spoofing and found out appropriate ways to decrease the impact of these restrictions. As well as continued their study on replay attack in video analysis to defeat the attacks on consumer device (Smith et al., 2015a). Later, Abdal-Ghafour et al. (Abdal-Ghafour et al., 2016) paid attention to the enhancement technique for BAC on iris recognition in order to rapidly detect the attacks.

In addition, by reviewing related works, static authentication system with physical biometric is not strong enough. Thus, for future work, we identify that 1) using behavioral biometric such as voice, keystroke and touch dynamic can bring mobile's user more reliable. Moreover, by using the dynamic authentication with machine learning and deep learning techniques in authentication process can provide high trustworthy as it delivers user's real-time monitoring and verifying as shown in Figure 2.

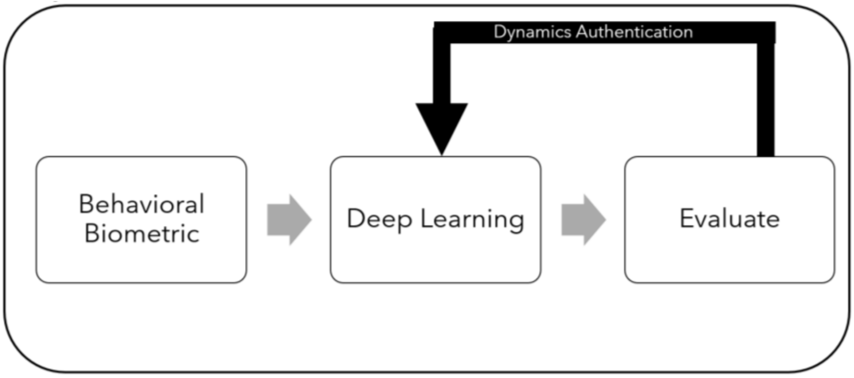

Figure 2 Dynamics authentication solution

2) applying multi-factor authentication for instance using only password. By using biometrics factor with traditional process may provide user more reliability in using their mobile device as shown in Figure 3.

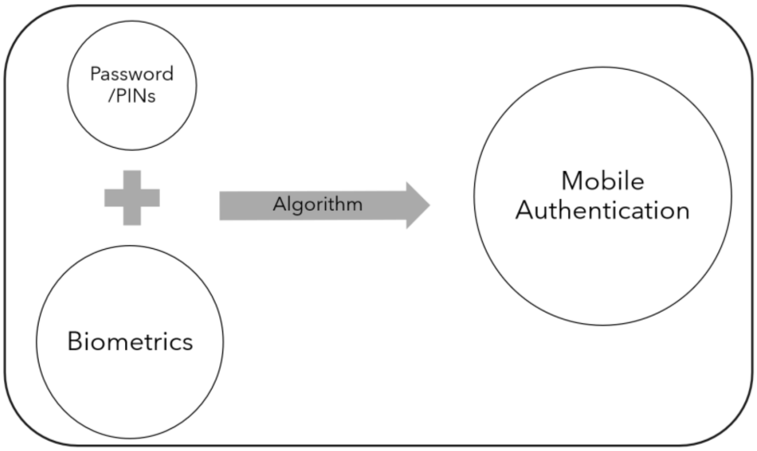

Figure 3 Muiti-factor authentication solution

CONCLUSIONS

In this paper, we presented the use of biometric authentication on mobile device based on existing research literature as it is generally used in people's everyday life. Mobile technology offers many convenient and benefit to life. However, with the change way of life, one of the most important things should be considered is the security. The problem of mobile user authentication has been concerned for over decade. Many researches applied methods to ensure the reliability and trust since password based and token based were found many points of failures. Biometric authentication makes the most of unique existing character in every human being as factor to verify. However, there are still many hard works on the accuracy rate of each method plus the tolerance to practical attacks available today.

ACKNOWEDGMENTS

This research was supported by Suan Dusit University and the Faculty of Science and Technology. We are thankful to our colleagues in the Department of Computer Science, who provided expertise and all comments that greatly assisted this work.

REFERENCES

Abdal-Ghafour, N. M., Abdel-Hamid, A. A., Nasr, M. E., & Khamis, S. A. (2016, 28-30 Nov. 2016). *Authentication enhancement techniques for BAC in 2G E-passport.* Paper presented at the 2016 12th International Conference on Innovations in Information Technology (IIT).

Ali, L. E., Luo, J., & Ma, J. (2016, 6-10 Nov. 2016). *Iris recognition from distant images based on multiple feature descriptors and classifiers.* Paper presented at the 2016 IEEE 13th International Conference on Signal Processing (ICSP).

Ali, M. L., Thakur, K., Tappert, C. C., & Qiu, M. (2016, 25-27 June 2016). *Keystroke Biometric User Verification Using Hidden Markov Model.* Paper presented at the 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud).

Alzubaidi, A., & Kalita, J. (2016). Authentication of Smartphone Users Using Behavioral Biometrics. *IEEE Communications Surveys & Tutorials*, 18(3), 1998-2026.

Benarous, L., Kadri, B., & Bouridane, A. (2017). A Survey on Cyber Security Evolution and Threats: Biometric Authentication Solutions. *Biometric Security and Privacy: Opportunities & Challenges in The Big Data Era, 371-411.* Cham: Springer International Publishin.

Ben-Asher, N., Kirschnick, N., Sieger, H., Meyer, J., Ben-Oved, A., M, S., . . . ller. (2011). *On the need for different security methods on mobile phones*. Paper presented at the Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services, Stockholm, Sweden. http://dl.acm.org/citation.cfm?doid=2037373.2037442

Bhatt, S., & Santhanam, T. (2013). *Keystroke dynamics for biometric authentication : A survey*. the 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering, 17-23.

Borah, T. R., Sarma, K. K., & Talukdar, P. H. (2015, 10-12 Sept. 2015). *Retina recognition system using adaptive neuro fuzzy inference system.* Paper presented at the 2015 International Conference on Computer, Communication and Control (IC4).

Buza, K. (2016). Person Identification Based on Keystroke Dynamics: Demo and Open Challenge. *The 28th International Conference on Advanced Information Systems Engineering.* Ljubljana, Slovenia.

Çeker, H., & Upadhyaya, S. (2015, 26-28 Oct. 2015). *Enhanced recognition of keystroke dynamics using Gaussian mixture models.* Paper presented at the MILCOM 2015 - 2015 IEEE Military Communications Conference.

Çeker, H., & Upadhyaya, S. (2016, 6-9 Sept. 2016). *User authentication with keystroke dynamics in long-text data.* Paper presented at the 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS).

Clarke, N. L., & Furnell, S. (2007). Authenticating mobile phone users using keystroke analysis. *International Journal of Information Security*, 6(1), 1-14.

Darojah, Z., & Ningrum, E. S. (2016, 28-30 July 2016). *The extended Kalman filter algorithm for improving neural network performance in voice recognition classification.* Paper presented at the 2016 International Seminar on Intelligent Technology and Its Applications (ISITIA).

Dholi, P. R., & Chaudhari, K. P. (2013). Typing Pattern Recognition Using Keystroke Dynamics. In V. V. Das & Y. Chaba (Eds.), *Mobile Communication and Power Engineering: Second International Joint Conference, AIM/CCPE 2012, Bangalore, India, April 27-28, 2012, Revised Selected Papers* (pp. 275-280). Berlin, Heidelberg: Springer Berlin Heidelberg.

El-Abed, M., & Charrier, C. (2012). Evaluation of Biometric Systems *New Trends and Developments in Biometrics* (149 - 169).

Elazhari, A., & Ahmadi, M. (2013, 8-11 Dec. 2013). *Interpolation of low resolution images for improved accuracy in human face recognition.* Paper presented at the 2013 IEEE 20th International Conference on Electronics, Circuits, and Systems (ICECS).

Fatima, J., Syed, A. M., & Akram, M. U. (2013, 9-9 Sept. 2013). *Feature point validation for improved retina recognition.* Paper presented at the 2013 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications.

Fatima, J., Syed, A. M., & Akram, M. U. (2013, 22-25 Sept. 2013). *A secure personal identification system based on human retina.* Paper presented at the 2013 IEEE Symposium on Industrial Electronics & Applications.

Feng, F., Li, X., & Wang, L. (2016, 14-17 Oct. 2016). *Design and implementation of identity authentication system based on fingerprint recognition and cryptography.* Paper presented at the 2016 2nd IEEE International Conference on Computer and Communications (ICCC).

Fudong, Li Clarke, N. Papadaki, M & Haskell-Dowland, P. (2013). Active authentication for mobile devices utilising behaviour profiling. *International Journal of Information Security*, 13(3), 229-244.

Gavrilescu, M. (2016). Study on using individual differences in facial expressions for a face recognition system immune to spoofing attacks. *IET Biometrics, 5*(3), 236-242. doi: 10.1049/iet-bmt.2015.0078

Hariyanto, Sudiro, S. A., & Lukman, S. (2015, 2-4 Dec. 2015). *Minutiae Matching Algorithm Using Artificial Neural Network for Fingerprint Recognition.* Paper presented at the 2015 3rd International Conference on Artificial Intelligence, Modelling and Simulation (AIMS).

Jain, A. K., Arora, S. S., Best-Rowden, L., Cao, K., Sudhish, P. S., Bhatnagar, A., & Koda, Y. (2016). *Giving Infants an Identity: Fingerprint Sensing and Recognition*. Paper presented at the Proceedings of the Eighth International Conference on Information and Communication Technologies and Development, Ann Arbor, MI, USA. http://dl.acm.org/citation.cfm?doid=2909609.2909612

Kakarwal, S. N., & Deshmukh, R. R. (2010, 19-21 Nov. 2010). *Analysis of Retina Recognition by Correlation and Covariance Matrix.* Paper presented at the 2010 3rd International Conference on Emerging Trends in Engineering and Technology.

Kang, W. M., Lee, K. W., Park, J. S., & Park, J. H. (2014). Design and Prototype Implementation of Smart-Phone Voice Locker Using Voice Recognition. In *Future Information Technology: FutureTech 2013*, 237-244, Berlin, Heidelberg: Springer Berlin Heidelberg.

Kekre, H. B., Sarode, T. K., Bharadi, V. A., Agrawal, A., Arora, R., & Nair, M. (2010). *Iris recognition using discrete cosine transform and Kekre's fast codebook generation algorithm*. Paper presented at the Proceedings of the International Conference and Workshop on Emerging Trends in Technology, Mumbai, Maharashtra, India. http://dl.acm.org/citation.cfm?doid=1741906.1741913

Kim, D. J., Chung, K. W., & Hong, K. S. (2010). Person authentication using face, teeth and voice modalities for mobile device security. *IEEE Transactions on Consumer Electronics*, 56(4), 2678-2685.

Kolly, S. M., Wattenhofer, R., & Welten, S. (2012). *A personal touch: recognizing users based on touch screen behavior*. Paper presented at the Proceedings of the Third International Workshop on Sensing Applications on Mobile Phones, Toronto, Ontario, Canada.

Latha, L., Pabitha, M., & Thangasamy, S. (2010, 12-13 Feb. 2010). *A novel method for person authentication using retinal images.* Paper presented at the 2010 International Conference on Innovative Computing Technologies (ICICT).

Lee, J.-W., Choi, S.-S., & Moon, B.-R. (2007). *An evolutionary keystroke authentication based on ellipsoidal hypothesis space*. Paper presented at the Proceedings of the 9th annual conference on Genetic and evolutionary computation, London, England. http://dl.acm.org/citation.cfm?doid=1276958.1277365

Liu, Q., Wang, M., Zhao, P., Yan, C., & Ding, Z. (2016). *A behavioral authentication method for mobile gesture against resilient user posture*. The 3rd International Conference on Systems and Informatics (ICSAI). Shanghai, China.

Marous, J. (2016). The biometric future of banking. Retrieved 4/28/2017, 2017, https://thefinancialbrand.com/61449/biometric-banking-password-trends/

Meng, W., Wong, D. S., Furnell, S., & Zhou, J. (2015). Surveying the Development of Biometric User Authentication on Mobile Phones. *IEEE Communications Surveys & Tutorials, 17*(3), 1268-1293. doi: 10.1109/COMST.2014.2386915

Meng, Y., Wong, D. S., & Kwok, L.-F. (2014). *Design of touch dynamics based user authentication with an adaptive mechanism on mobile phones*. Paper presented at the Proceedings of the 29th Annual ACM Symposium on Applied Computing, Gyeongju, Republic of Korea. http://dl.acm.org/citation.cfm?doid=2554850.2554931

Nguyen, H. P., Retrain, F., Morain-Nicolier, F., & Delahaies, A. (2016, 7-9 Dec. 2016). *Face spoofing attack detection based on the behavior of noises.* Paper presented at the 2016 IEEE Global Conference on Signal and Information Processing (GlobalSIP).

Nissenbaum, L. D. I. a. H. *Facial Recognition Technology: A survey of policy and implementation issues*. New York University.

Ortiz-Lopez, J., Galbally, J., Fierrez, J., & Ortega-Garcia, J. (2011, 18-21 Oct. 2011). *Predicting iris vulnerability to direct attacks based on quality related features.* Paper presented at the 2011 Carnahan Conference on Security Technology.

Padma, P., & Selvaraj, S. (2016). *A survey on biometric based authentication in cloud computing*. International Conference on Inventive Computation Technologies (ICICT), (pp. 1 - 5).

Pandey, A. K., & Pandey, R. (2015). *Application of Spectral Information in Identification of Real-Fake Face Images*. Paper presented at the Proceedings of the Sixth International Conference on Computer and Communication Technology 2015, Allahabad, India.

Pisani, P. H., Lorena, A. C., & Carvalho, A. C. (2015). Adaptive approaches for keystroke dynamics. *The International Joint Conference on Neural Networks.* Killarney, Ireland.

Rajput, M. R., & Sable, G. S. (2016). *IRIS biometrics survey 2010–2015*. IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). Bangalore, India.

Ranny. (2016, 23-26 May 2016). *Voice Recognition Using k Nearest Neighbor and Double Distance Method.* Paper presented at the 2016 International Conference on Industrial Engineering, Management Science and Application (ICIMSA).

Rasmus, E., & Green, R. (2012). *Improving face recognition with genealogical and contextual data*. Paper presented at the Proceedings of the 27th Conference on Image and Vision Computing New Zealand, Dunedin, New Zealand. http://dl.acm.org/citation.cfm?doid=2425836.2425897

Rathgeb, C., & Uhl, A. (2011). A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security, 2011*(1), 3. doi: 10.1186/1687-417x-2011-3

Sadi, K. A., Bouchair, I., Zebbiche, K., & Laadjel, M. (2014, 28-30 Aug. 2014). *Protecting digital fingerprint in Automated Fingerprint Identification System using Local Binary Pattern operator.* Paper presented at the 2014 International Conference on Signal Processing and Multimedia Applications (SIGMAP).

Sae-Bae, N., Ahmed, K., Isbister, K., & Memon, N. (2012). *Biometric-rich gestures: a novel approach to authentication on multi-touch devices*. Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in

Computing Systems, Austin, Texas, USA. http://dl.acm.org/citation.cfm?doid=2207676.2208543

Saevanee, H., Clarke, N. L., & Furnell, S. M. (2012). Multi-modal Behavioural Biometric Authentication for Mobile Devices. In D. Gritzalis, S. Furnell & M. Theoharidou (Eds.), *Information Security and Privacy Research: 27th IFIP TC 11 Information Security and Privacy Conference, SEC 2012, Heraklion, Crete, Greece, June 4-6, 2012. Proceedings* (pp. 465-474). Berlin, Heidelberg: Springer Berlin Heidelberg.

Schwartz, W. R., Guo, H., Choi, J., & Davis, L. S. (2012). Face Identification Using Large Feature Sets. *IEEE Transactions on Image Processing, 21*(4), 2245-2255. doi: 10.1109/TIP.2011.2176951

Seto, Y. (2015). Retina Recognition. *Encyclopedia of Biometrics*, 1321-1323. Boston, MA: Springer US.

Smejkal, V., & Kodl, J. (2018). Dynamic Biometric Signature - an Effective Alternative for Electronic Authentication. *Advances in Technology Innovation*, 3, 166-178.

Smith, D. F., Wiliem, A., & Lovell, B. C. (2015a, 23-25 March 2015). *Binary watermarks: a practical method to address face recognition replay attacks on consumer mobile devices.* Paper presented at the IEEE International Conference on Identity, Security and Behavior Analysis (ISBA 2015).

Smith, D. F., Wiliem, A., & Lovell, B. C. (2015b). Face Recognition on Consumer Devices: Reflections on Replay Attacks. *IEEE Transactions on Information Forensics and Security, 10*(4), 736-745. doi: 10.1109/TIFS.2015.2398819

Suciati, N., Anugrah, A. B., Fatichah, C., Tjandrasa, H., Arifin, A. Z., Purwitasari, D., & Navastara, D. A. (2016, 12-12 Oct. 2016). *Feature extraction using statistical moments of wavelet transform for iris recognition.* Paper presented at the 2016 International Conference on Information & Communication Technology and Systems (ICTS).

Tan, X., & Triggs, B. (2010). Enhanced Local Texture Feature Sets for Face Recognition Under Difficult Lighting Conditions. *IEEE Transactions on Image Processing, 19*(6), 1635-1650. doi: 10.1109/TIP.2010.2042645

Ushe, D., Tosa, Y., & Friedman, M. (2015). Simultaneous Capture of Iris and Retina for Recognition. *In Encyclopedia of Biometrics*, 1401-1407. Boston, MA: Springer US.

Vergara, D. (2019, 03 1). *Static vs behavioural: what's the future of biometric authentication*. Retrieved www.itproportal.com: https://www.itproportal.com/features/static-vs-behavioural-whats-the-future-of-biometric-authentication/

Wang, L., Bhattacharjee, N., Gupta, G., & Srinivasan, B. (2010). *Adaptive approach to fingerprint image enhancement*. Paper presented at the Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia, Paris, France. http://dl.acm.org/citation.cfm?doid=1971519.1971530

Wei, S., & Stevenson, M. (2008, 12-14 March 2008). *A playback attack detector for speaker verification systems.* Paper presented at the 2008 3rd International Symposium on Communications, Control and Signal Processing.

Yanushkevich, S.N., Gavrilova, M.L., Wang, P.S., & Srihari, S.N. (2007). Image Pattern Recognition - Synthesis and Analysis in Biometrics. *Image Pattern Recognition*.

Yoon, S. (2014). *Fingerprint Recignition: Models and Application.* (Doctor of Philosophy), Michigan State University. Retrieved http://biometrics.cse.msu.edu/Publications/Thesis/SoweonYoon_FingerprintRecognitionModelsandApplications_PhD14.pdf

Yu, S., Guo, S., & Stojmenovic, I. (2012, 25-30 March 2012). *Can we beat legitimate cyber behavior mimicking attacks from botnets?* Paper presented at the 2012 Proceedings IEEE INFOCOM.

Yu, S., Guo, S., & Stojmenovic, I. (2015). Fool Me If You Can: Mimicking Attacks and Anti-Attacks in Cyberspace. *IEEE Transactions on Computers, 64*(1), 139-151. doi: 10.1109/TC.2013.191

Zafeiriou, S., Atkinson, G. A., Hansen, M. F., Smith, W. A. P., Argyriou, V., Petrou, M., . . . Smith, L. N. (2013). Face Recognition and Verification Using Photometric Stereo: The Photoface Database and a Comprehensive Evaluation. *IEEE Transactions on Information Forensics and Security, 8*(1), 121-135. doi: 10.1109/TIFS.2012.2224109

Zirjawi, Nedaa Kurtanović, Zijad & Maalej, Walid. (2015). A survey about user requirements for biometric authentication on smartphones. *The 2015 IEEE 2nd Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE)*. 1-6. 10.1109/ESPRE.2015.7330160.