AUSTRALIAN JOURNAL OF BASIC AND APPLIED SCIENCES

ISSN:1991-8178 EISSN: 2309-8414
Journal home page: www.ajbasweb.com

A Comprehensive Survey on Gesture Based Authentication Schemes in Smart Phones

[1]S. Milton Ganesh, [2]P. Vijayakumar and [3]L. Jegatha Deborah

[1]*University College of Engineering Tindivanam, Department of Computer Science and Engineering, Tindivanam, Tamilnadu, India*
[2]*University College of Engineering Tindivanam, Tamil nadu, India*
[3]*University College of Engineering Tindivanam, Department of Computer Science and Engineering, Tindivanam, Tamilnadu, India*

Address For Correspondence:
S. Milton Ganesh, University College of Engineering Tindivanam, Department of Computer Science and Engineering, Tindivanam, Tamilnadu, India
Tel : +91-9965490586; E-mail: softengineermilton@gmail.com

ARTICLE INFO

Article history:
Received 04 December 2015
Accepted 22 January 2016
Available online 14 February 2016

Keywords:
Gesture, authentication, security, authorization, survey, mobile

ABSTRACT

Background: The sensitive information present in the smart phones is enormous and providing security in terms of authentication plays a very important role to protect such information from attackers. Hence, it is very essential to analyze the impact of various attacks on the existing authentication schemes in order to devise a new efficient authentication protocol for smart phones. **Objective:** Among the several existing authentication schemes, gesture based authentication schemes are predominant because security is provided based on physiological and behavioral characteristics. To accomplish such analysis, a survey of the past and recent techniques on gesture based authentication schemes in smart phones is conducted. The identified issues are given as an overview in textual and tabular representations to provide a good insight to the current researchers. **Results:** This survey primarily focuses on parameters such as Equal Error Rate (EER) and other issues related to the classification algorithm. It is also analyzed from the survey that classification algorithms play a vital role in improving the accuracy of authentication. **Conclusion:** The concluding remarks are that very few research works have progressed in hand waving biometrics, which exhibits a promising future if Equal Error Rate and computational complexity are given utmost importance.

INTRODUCTION

With the rapid advancements in hardware miniaturization, the mobiles are rapidly evolving. Thus mobiles are used not only for text-messaging and making calls but for mobile banking (Pousttchi, K. and M. Schurig, 2004), mobile governance and emails. Thus, they are used for storing secure financial data and private data. A study from UK statistics shows that a mobile phone is stolen every three minutes (Monitor password survey, 2002). Whenever a user keeps a touch screen phone unlocked, then there is a possibility that whoever gets access to the touch screen phone will have a better chance to access the private, secret and sensitive information. Symantec conducted a recent study in North America by keeping nearly 50 smart phones unlocked. It is observed that approximately 96% of the people showed willingness to manipulate the phone. 86% of them tried to access the personal information while 50% tried to run remote admin and a 60% tried to access the emails and social networking sites (The symantec smartphone honey stick project). Therefore, it is very important to safeguard the information in the mobile phones.

Malicious people tend to abuse the mobile phones through many ways utilizing the information and services. For instance, a malicious user may review a legitimate user's information and involve in online transaction using the owner's identity. Using mobile phones, intruders may authenticate themselves as

To Cite This Article: S. Milton Ganesh, P. Vijayakumar and L. Jegatha Deborah., A Comprehensive Survey on Gesture Based Authentication Schemes in Smart Phones. ***Aust. J. Basic & Appl. Sci.,*** *10(2): 27-36, 2016*

legitimate users and enter a company's internal network. Thus mobile phone authentication must be given critical importance. If the intruder steals a mobile phone with the corporate data, then there is high risk that this data could be handed over to the competitors. That is, an intruder may handover the business technical or financial information in the wrong hands leading to financial or business loss to clients. These misuses might damage a company's reputation. Thus, using mobile phones in corporate offices may reduce the customer confidence and damage the relationships and may lead to huge financial loss.

It is observed that given physical access an expert hacker can gain privileged access (Baum, L.E. and T. Petrie, 1966) without breaking the screen lock. During mobile authentication, a well-trained classifier is used to verify the identity of a user. For ensuring the accuracy of the system, the imposter acceptance rates and the legitimate user rejection rates are calculated. The imposter acceptance rate is calculated with the assumption that the imposter has access to the password of the legitimate user. Golfarelli (1997) pointed out that a biometric authentication system can be evaluated by two criteria which depend on corresponding threshold values. The two criteria are False Rejection Rate (FRR) and the False Acceptance Rate (FAR). The percentage of the system rejecting legitimate users while they attempt to login is called as the False Acceptance Rate (FRR) and the percentage of imposters accepted by the system while they attacked is called as the False Acceptance Rate (FAR). Based on these two criteria, Equal Error Rate (EER) is calculated. EER value is obtained when FRR equals FAR. This value not only represents the entire system utility, but also serves as the criterion for comparing various authentication systems.

Though many authentication systems have been developed, current systems are focused on PIN/passwords or biometric authentication mechanisms. But they are susceptible to attacks in this modern internet world. Not only traditional passwords are broken but the biometrics systems too. But it is very difficult to copy a person's behaviour and hence authentication systems which provide security based on these approaches are promising ones. For example, authentication in behavioural biometrics is based on the unique behaviour of a person such as the way a person walks (Stevenage, S.V., 1999; Öberg, T., 1993; Nishiguchi, S., 2012), types (Saira, Z., 2009; Sudhir, D., 2015), moves the hand (Yang, L., 2015; Karitat, S., 2015; Guerra-Casanova., C., 2012), writes and behaves. Though human behaviour is likely to change under different circumstances during illness, stress and environmental factors, the impact of accuracy in authentication can be increased by regular examination and regularly updating the behaviour profile in the mobile database.. Moreover, behavioural biometrics tends to be applied in transparent mode which is more preferable to physiological countermeasures.

A. *Attacks on authentication:*

There are various attacks (Shahzad, M., 2013) to break the authentication in smart phones. Among the various attacks, shoulder surfing and smudging attacks are the two important attacks which are explained below.

1) Shoulder surfing attack:

An attacker infers the Password/PIN/Pattern through direct observation over someone's shoulder (*Tari, F., 2006*).

2) Smudging Attack:

An attacker guesses the Password/PIN/Pattern through oil residues left by the fingers of a legitimate user on the touch screens. A number of works in the literature have clearly shown that an attacker can nearly guess the password from the smudges left on the touch screens (*Aviv, A.J., 2010*).

B. *Types of Authentication:*

Authentication in smart phones can be broadly classified into three categories (*Meng, W., 2015*).

1) What you know:

Approaches based on password/ PIN/pattern are the earlier ones which still exist today and also the most prevalent ones among the mobile user community. But they have proven weakness from mobile users like forgetting the long or complex password/PIN (*Shepard, R.N., 1967*) and from attacker community such as shoulder surfing and smudging attacks (*Tari, F., 2006; Turk, M.A. and A.P. Pentland, 1991*).

2) What you have:

As the conventional password/PIN/pattern based approaches failed to provide enough authentication for secrecy, biometric authentication systems evolved over time. Biometric authentication systems based on fingerprints (*Derawi, M.P., Bours, 2013; Wegstein, J.H., 1982; Kawagoe, M. and A. Tojo, 1984; Federal Bureau of Investigation, 1984; 1936; Galton, F., 1892*), face (*Fathy, M.E., 2015; Turk, M.A. and A.P. Pentland, 1991; Nefian, A. and M. Hayes, 1999; Phillips, P.J., 2000; Eickler, S., 2000*), voice (*Rabiner, L., 1989; O'Shaughnessy, D., 1987; Jourlin, P., 1997; Baker, J.K., 1975; Jelinek, F., 1976; Poritz, A.B., 1982; Markel, J.D., A.H. Gray, Jr., 1976*), ear (*Yuan, L., 2005; AfredIannarelli, 1989; Burge, M., W. Burger, 2000*), palm

(*Chen, J., 2010; Cummins, H. and C. Midlo, 1961*), iris (*Thavalengal, S., 2015*), teeth (*Jain, A., 1999*) and other features were introduced. Biometrics tends to provide physiological features for authentication since a long time ago (*Kowtko, M.A., 2014; Wegstein, J.H., 1982; Kawagoe, M. and A. Tojo, 1984; Isenor, D.K. and S.G. Zaky, 1986; Hrechak, A.K. and J.A. McHugh, 1990; Grasselli, A., 1969; Hankley, W.J. and J.T. Tou, 1968; Cumins, H. and C. Midlo, 1943*). But they have been proved to be susceptible to attacks too. Fingerprints of German Chancellor were cracked from a photo. Thus fingerprints once considered unbreakable are valid no more. Face recognition could prove ineffective during fatal damages to the physiological parts of the body or due to low intensity of light. Without liveliness detection, face recognition could be cracked easily. Still, a number of researches are providing promising results today. But certainly, each physiological behavior is susceptible to be cracked in one way or the other.

3) ***What you are:***

There is a real need for authentication systems which are ultimately not replicable at all. Behavioral biometrics promises to provide authentication in this direction (Mayron, L.M., 2015). They exhibit patterns of human behavior such as gait (*Ferrero, R., 2015; Claudia, N., C. Busch, 2013; Watanabe, Y., 2014*), handwriting, touch dynamics which include features such as finger pressure (*Qiao, M., 2015; Saevanee, H., P. Bhattarakosol, 2009*), acceleration on the touch pad (*Sae-Bae, N., 2014; Sae-Bae, N., 2012; Monrose, F., 1999*), keystroke dynamics (*Matthias, T., F. Ortmeier, 2014; Georgios, K., 2014; Cristiano, G., 2014; Saevanee, H., P. Bhattarakosol, 2009*) such as key stroke time, inter key stroke time, hand waving gestures [91, 44, 31] such as palm movement, wrist movement and many other notable features. Authentication methods of this kind are called as gesture based ones which cannot be replicated easily. Combining one or more gestures provide improved accuracy as well. They avoid both shoulder surfing and smudging attacks to the maximum possible extent. But they suffer from providing low accuracy and the very high computational complexity of machine learning algorithms to match the input sample with the stored samples in the mobile phone database and may increase the authentication time of the smart phones.

In this line, the latest trends of authentication mechanisms use the behaviors of a user to unlock the phone. Compared to other authentication methods to unlock smart phones, only little research has been done in the gesture based arena.

Rest of the paper is organized as follows. Section 2 provides a survey on the most popular gesture based authentication techniques in smart phones today. Detailed discussion with comparative analysis is provided at the end of each section. Section 3 provides a discussion on the open research challenges in the area of gesture based authentication. Finally, Section 4 concludes the survey and provides future directions.

Survey:

In addition to the conventional password/PIN/pattern based authentication systems, biometric authentication provides security in two ways such as physiological characteristics and behavioral characteristics. Physiological biometric authentication is used for identification of a person based on retina, face, palm, fingerprints and others. But behavioral biometrics identifies a person based on the behavioral attributes of a user such as the way the user walks, types, moves. Biometric systems are implemented as pattern-recognition systems through which the authenticity of a person based on his behaviors is determined. The system consists of many phases. In the first phase, a user's biometric characteristics are enrolled in the database. During authentication, the user's behavioral traits are captured. They are then pre-processed and compared with the templates acquired in the training phase. Finally the users are accepted or rejected based on a threshold value. Thus the decision depends on the similarity of the collected sample with the ones in the database (Shahzad, M., 2013).

There are a number of behaviors which exhibit unique characteristics to distinguish users from one another. This includes keystroke dynamics, gait, touch dynamics, gestures on patters, hand waving biometrics and other gestures. Various authentication techniques based on the promising gestures are presented below.

A. Works on Keystroke dynamics:

Several recent research works (Jeanjaitrong, N., P. Bhattarakosol, 2013; Bhatt, S. and T. Santhanam., 2013) have directly or indirectly occupied themselves with keystroke dynamics in the realm of mobile devices. The rhythm with which an individual types the characters on keyboard or keypad is used for authentication (Monrose, R., A. Rubin, 1999; Gaines, R.S., 1980; Dvorak, A., 1936; Coover J.E., 1923; Harding D.W., 1933). It is one of the earliest gesture based techniques developed. They are categorized into three groups: those proposed for devices equipped with a hardware keyboard, touchscreen and motion sensors. Keystroke based authentication schemes using desktop computers have been proposed as early as 1985 to 1990 (Matthias, T., F. Ortmeier, 2014; Napier, R., 1995; Obaidat, M. and B. Sadoun, 1997). The first study achieved an EER of 6% with the digraph features of a normal keyboard (Umphress, D. and G. Williams, 1985). Current researches consider various digraph features of a mobile touchpad along with the other gestures. A survey on the recent

works on touch based authentication is given below and the comparison based on various parameters and also the advantages and disadvantages is presented in Table 1.

One of the latest works is done by Sudhir *et al*. (2015) on keystroke based analysis providing better results. Key hold time and digraph latencies such as press-press duration, release-press duration and release-release duration have been considered for the analysis. Statistical factors such as sum, weighted sum, product, OR Limit, AND Limit have been used to evaluate the inputs. This method outperforms the method proposed by Georgios Kambourakis (2014) *et al*. If combined with the biometric sensors in mobile phones, EER value can be enhanced further.

Georgios *et al*. (2014) proposed an approach based on key stroking patterns in touch screens of android mobile phones. Features considered for gesture based authentication are key stroking speed and distance which are derived from key hold time and inter key time. The features were classified and authenticated using three classifiers such as k-Nearest Neighbor (k-NN), Random Forest and Multi-Layer Perceptron (MLP) and the results proved that k-NN achieved the best performance with an EER of 12.5%.

Table 1: Comparison Of Recent Works On Keystroke Dynamics.

Algorithm Used	Author	Parameters Considered	Advantages	Disadvantages
A new algorithm combining methods from statistics	Sudhir *et al*. (2015)	Key hold time, Digraph latencies	EER of 0.806% was achieved	Less Accuracy
k-NN, Random Forest, MLP	Georgios *et al*. (2014)	Keystroking speed and distance based on Key hold time, inter key time	Minimum EER is 12.5%, FAR is 3.5%	Less Accuracy
J48	Matthias *et al*. (2014)	Swipe pad dynamics such as digraph, key hold time, straightness of curves	FAR is 11% and FRR is 16%	Less Accuracy
k-NN	Cristiano *et al*. (2014)	Sensor data from accelerometer and gyroscope were considered	EER is 0.08%	Accuracy may vary under different postures of authentication.
Probabilistic Neural Network (PNN)	Saevanee and Bhattarakosol *et al*. (2009)	Inter key time, key hold time and finger pressure	EER of 9%	The EER achieved is lesser. Also finger pressure sensor not available in all phones.
Fuzzy classifier with PSO, GA algorithms	Saira *et al*. (2006)	Key hold time, digraph time such as Horizontal Digraph, Vertical Digraph, Non-Adjacent horizontal Digraph, Non-Adjacent Vertical Digraph, error rate.	EER of 2%	Fuzzy classifier with PSO, GA algorithms needs intensive computational load on mobile devices with low capability.

Matthias *et al*. (2014) achieved an FAR of 11%, FRR of 16% for touch screen authentication using swipe pads in touch screen mobile phones. Many algorithms such as J48, KSTAR, MLP, RBFN, BayesNet and Naïve Bayes were used for classification during the authentication. J48 outperformed them all. Classifiers such as ANN, SVM could be implemented to achieve more FAR, FRR.

Cristiano *et al*. (2014) proposed an approach in which keystroke dynamics were evaluated based on the inputs from accelerometer sensors and the gyroscope. Accelerometer sensor sensed the movement of the phone in x, y, z axes and gyroscope sensed the phone inclination angle. Combining the input from both the sensors when the user authenticates the phone by typing the keys, an EER of 0.08% was achieved which is relatively far better than other works. K-NN classifier was used for classification. The metrics observed from accelerometer and gyroscope may change for a person under different postures. A thorough analysis in this angle could further improve the accuracy of the algorithm.

According to the research of Saevanee and Bhattarakosol *et al*. (2009), an EER of 9% can be achieved by using the factors such key hold time, key interval time combined with finger pressure. Probabilistic neural networks were employed to classify the input from the user to be used for user authentication. When finger pressure alone was considered for authentication, the accuracy was 99% which when combined with the keystroke dynamics, the accuracy of the result dropped to 90%. Limitation of this method is that finger pressure sensors are not widespread among all the touch screen mobiles.

Saira *et al*. (2006) proposed an earlier approach in 2006. During the sample collection phase, Fuzzy classifier is used to store the samples in the mobile database. The fuzzy classification system was made to evolve through the bio-inspired algorithms such as PSO and GA. An eight character PIN is used for the authentication purpose. Features which were considered for classification include key hold time, digraph time such as Horizontal Digraph, Vertical Digraph, Non-Adjacent horizontal Digraph, Non-Adjacent Vertical Digraph, error rate. As a result, an EER of 2% has been achieved. This implementation could be further improved to support more characters and also ANN or SVM could be used to reduce the computational overhead incurred using PSO-GA based Fuzzy classifier.

B. Works on Gait Authentication:

Mobile authentication using gait recognition is relatively a new area of research and the previous works on gait based approaches focused on machine vision techniques [69]. Video or a sequence of images is processed to extract gait patterns of the user. But recent research works focus on sensors to recognize the gait patterns of a user (Ferrero, R., 2015; Claudia, N., C. Busch, 2013; Watanabe, Y., 2014). This direction significantly differs from vision-based methods in terms of technology. Instead of the camera, a physical device attached to the body is used to collect the gait patterns. Usually accelerometers are used as a sensor which is a inbuilt component of smart phones and hence the need for an external sensor is avoided. A primary advantage of the sensor-based gait

biometric over other types of biometrics is that it enables unobtrusive user authentication. Gait patterns combined with other gestures could yield high accuracy in terms of reduced EER values. A comparison of the recent works on gait authentication is presented in Table 2 and is discussed below.

Ferrero *et al*. (2015) identified a procedure for analyzing gait using the embedded accelerometer in mobile phones. The smart phone has been kept near the hip of a user in many ways. Noise from the received signal is removed using filters and analysis is done using statistical measures as averaging, RMS, Correlation. Dynamic Time Warping Algorithm (DTW) has been used for comparing the acceleration patterns. An EER of 7% was achieved as minimum and 33% as maximum.

Unlike previous approaches, an approach proposed by Watanabe (2014) considered linear as well as angular or rotational movements of the phone for gait authentication. So, inputs from gyroscope and electromagnetic compass were taken for the classification. Authentication was tried using many algorithms such as J48, Radial Basis Function (RBF), Neural Networks (NN) and Random Forest (RF). Of these, RBF out-weighed others with an EER of 9.38% for FAR. But FRR received by all the algorithms were poor and hence need to be improvised. A recent research on gait-based authentication was proposed by Claudia and Busch (2013) which showed a promising future in this direction. The smart phone with the accelerometer sensor was kept at the right hip of 48 users and the whole test was conducted for 2 days. Unlike previous works, the experiment was conducted not only on flat floors but on stairs as well. Hidden Markov model introduced in 1960s (Nickel, C., 2011; Rabiner, L. and B. Juang, 1986; Markel, J.D., A.H. Gray, Jr., 1976) with more refinements classified the training samples with features in x, y, z directions and also based on the magnitude of acceleration of the participants. Data collected for 33s produced an EER of nearly 6.15% which has to further improved under more walking scenarios.

Another work on gait identification using smart phones was by Derawi and Bours (2013). Five participants walked at different speeds and the corresponding training samples were stored in the database. Gait features were captured using the accelerometer readings in three perpendicular axes as x, y, z and the magnitude of motion was found using the Euclidean method. Authors believe that the magnitude of motion does not depend on the orientation of the phone but on the location of the phone which is contrary to the approach of Watanabe.Y. Approximately 150 samples were collected per second and Weight Moving Average (WMA) filter was used for the noise removal. The raw data was converted to cycles, pre-processed and the samples were identified. An accuracy of 99% was achieved with the test conducted on 20 users. Dynamic Time Warping algorithm (DTW)was used for classification of training samples and for the authentication of the rightful users. Disadvantages of this approach include the accuracy which has to be tested with more training samples.

A work on gait based authentication by Davrondzhon *et al*. (2016) uses a motion recording device consisting of accelerometers on the leg of mobile users. The accelerometers kept at perpendicular axes collect the gait data in three perpendicular axes as vertical, backward-forward and sideways. Gait data was processed in cycles and the classification and training has been done using statistical measures such as mean of cycles, variance of cycles. An EER of 5.9% was achieved which outperforms many other methods.

A work on gait based authentication is from Thang *et al*. (2015). This is a novel work which verifies the user through a stored key which has been biometrically encrypted using gait templates collected through accelerometers. Gait data were collected from 34 volunteers which address both security and privacy and it is a novel work of its kind. A cryptographic key was encoded using BCH encoding scheme. During the training phase, fuzzy commitment scheme computes a hash code and a secret value for the key. The hash code and the secret value were stored and used during the authentication. During authentication, the collected gait templates were modelled to form a key and a hash value for the same is computed using the Fuzzy commitment scheme. If the computed hash value matches with the one in the database, then the user is authenticated.

Table 2: Comparison Of Recent Works On Gait Authentication In Mobile Phones.

Algorithm Used	Author	Parameters Considered	Advantages	Disadvantages
DTW	Ferrero *et al*. (2015)	Acceleration of the accelerometer in 3 perpendicular axes	Minimum EER of 7%. Maximum of 33%.	EER is low. Need to be tailored to low-grade accelerometers in mobile phones.
Radial Basis Function	Watanabe (2014)	Linear motion along with the angular motion of phone movement	FAR is 9.38% from RBF.	Very poor FRR. More training needed.
Hidden Markov Model	Claudia and Busch (2013)	Acceleration in all three dimensions and the magnitude of acceleration.	EER of 6.15% achieved	More testing under different scenarios need to be done. EER has to be improved.
Manhattan Distance method	Derawi and Bours (2013)	Linear motion in x, y, z axes	Low computational complexity	Less accuracy. It can be increased using DTW algorithm
Statistical measures such as mean, variance	Davrondzhon *et al*. (2016)	Vertical, backward-forward and sideways of legs.	EER of 5.9%	Less Accuracy. Also, Data from sensor manually fed to the mobile for authentication. Placement of sensors to be appropriate.
Fuzzy based cryptographic scheme	Thang *et al*. (2015)	A key cryptographically encrypted using gait templates is used for the authentication purpose.	FAR is 0% FRR is 16.18%.	FRR is not appropriate. More parameters and training samples needed.

C. Works on Gestures on Pattern Locks:

A graphical password, in terms of quick recollection ability and convenience providing more security is preferable to a text-based password on mobile phones (Jermyn, I., 1999; Angulo, J. and E.W. astlund, 2012). Only a very few works have progressed in adding gesture based authentication to password lock authentication

schemes. Though pattern locks are susceptible to smudge attacks and shoulder surfing attacks, combined with gestures they would prove to be a strong authentication technique to be implemented in smart phones. Recent works on some of the notable pattern based drawing approaches are compared in Table 3 which are discussed below in detail.

An android pattern lock layout proposed by Liu *et al*. (2015) have considered factors such as time, pressure, size, and angle which were used to build a statistical classifier for authentication. They achieved an EER of 3.03% with only 10 training samples. To enhance the achieved EER, outlier detection algorithm could be used in the future.

Alpar (2015) has put forward a pattern based approach in 2015 which compares three algorithms such as Artificial Neural Networks(ANN), Adaptive Neuro-Fuzzy Inference System(ANFIS) and Histogram Method for the pattern based unlocking technique. ANFIS achieved the best performance with an EER of 2.5% which was far better than the previous works in this line of research. The size of the pattern consists of only numbers and it could be increased in the future and required analysis needs to be done for ensuring the effectiveness of the algorithm.

Table 3: Comparison Of Some Of The Recent Works Of Gestures On Pattern Locks.

Algorithm Used	Author	Parameters Considered	Advantages	Disadvantages
Statistical classifier	Liu *et al*. (2015)	Graphical Keystroke features such as time, pressure, size and the new parameter angle keystroke feature	EER of 3.03% achieved with only 10 training samples	Outlier detection algorithm could be used to further enhance the EER
ANN, ANFIS, Levenberg–Marquardt, Histogram method	Alpar (2015)	Touch durations on each node	FAR is 0%, FRR is 16.5%, EER is 2.5% with ANFIS with just 10 training samples	Size of the pattern password is only 4. FRR need to be enhanced.
-	Zezschwitz *et al*. (2013)	Smudge attacks, speed of drawing a pattern	New proposals such as circular patterns to avoid smudge attacks.	Shoulder surfing not considered.
Random forest classifier	Angulo and Wastlund (2012)	Pattern parameters such as finger-in-dot time and finger in-between time	EER of 10.39% achieved	A better noise removal algorithm can be coupled. A good outlier algorithm could enhance the EER rate.
Dynamic Time Warping (DTW)	DeLuca *et al* (2012)	Password pattern extended to support pressure, coordinates, size, speed, time	Accuracy is 77% with FRR of 19% and FAR of 21%	Accuracy need to be increased.

Another approach to patter dynamics was put forward by Julio Angulo and Wastlund (2012). Random forest classifier was used to classify the input and it produced an EER of 10.39%. The result was conducted using 32 participants comprising of 12 women and 20 men in different age groups. This algorithm was compared with many other algorithms and it outperformed all of them. Parameters considered were finger-in-dot time, which is the time in milliseconds from the moment the participant's finger touches a dot to the moment the finger is dragged outside the dot area, and the finger-in-between-dots time, representing the speed at which the finger moves between two dots.

A view on the possible attacks on the pattern based locks is provided by Zezschwitz *et al*. (2013). Grid based patterns are more susceptible to smudge attacks and hence new patterns such as circular ones have been proposed. Twenty four participants were put to test on four types of patterns proposed and 192 samples collected. The best one was the pattern with nine colors arranged in a circle in which the authentication technique was to drag the colors to the centre in the correct order. Speed of drawing the pattern was considered for authentication. Limitation of this approach is that a classifier such a support vector machines or neural networks to be implemented for authentication.

Smudge attacks pose a major threat to android pattern locks. The Aviv *et al*. (2010) has studied the effect of smudge attacks on the android patterns under various lighting situations and camera angles in an attempt to extract the recent user input. It is also inferred that an attacker might have many images of a recently used pattern and combine them to produce the near correct pattern.

DeLuca *et al* (2012) proposed a novel method to improvise the simple pattern lock of smart phones. The experiments were conducted using 48 participants of different age groups. An android application was developed which sensed the users' finger pressure on the touch screen along with the area which the finger is touching. Dynamic Time Warping algorithm was used for data analysis. The results suggest that it is possible to distinguish users based on many features alongside the password match.

D. Works on Touch Dynamics:

With the rapid advancements in mobile phones, touchscreens have recently become an indispensable way of providing input. They are electronic displays and users control them using single-touch or multi-touch gestures. It has been estimated that the global touch screen shipments may reach 1.75 billion in 2013, with approximately 73% are to be for handsets, and it will increase by 14.2% per year. Touch dynamics refers to collecting detailed information about individual touches such as touch duration and touch direction based on single-touch or multiple-touch gesture. Table 4 discusses about the pros and cons of some of the most useful works in the direction of pattern based gesture authentication schemes. Schemes mentioned in the Table are discussed below.

Jain and Kanhangad (2015) have proposed a recent study on touch screen gestures based on the parameters such as touch finger area, readings of the accelerometer sensor and orientation sensor, the co-ordinates of touch gestures. Seven gestures such as left to right swipe, right to left swipe, scroll up, scroll down, zoom in, zoom out and single tap have been used for the authentication purpose. Two other parameters include curvature of the swipe and curvature at the touch point of swipe. DTW algorithm is used for the classification of training samples and authentication purpose. The scores of the different inputs are fused and the authentication identification is performed using Hausdorff distance method. A very low EER of 0.31% is achieved using this approach.

A total 22 of multi-touch gestures including pinching, swiping, circular movement were proposed by Sae-Bae *et al*. (2014) which provides more accuracy then her previous work in 2012. The gestures for identification were palm movement and fingertip movement in different angles and directions comprising the 22 distinguishable ones. The best performance was 4.03% using multi-touch gesture and it is verified that gestures can be recalled more easily in time. Limitations of this approach include computational complexity of the method proposed and the lesser accuracy.

An attempt by Zhao *et al*. (2014) with 78 participants has given a promising future in touch dynamics which provides more accuracy than the previously proposed Graphic Touch Gesture Feature(GTGF) scheme. Features extracted include x, y coordinates of finger touch points, pressure values and time stamps of the touch gestures on the touch screen. Novelty of the proposed method based on Statistical Touch Dynamics Images(STDI) is that authentication for multiple users can be done. To reduce the computation complexity in mobile phones, STDIs of the same user are first separated using the previously proposed GTGF scheme and the comparison for authentication is done later. The EER values range from 11.28% to 12.14%.

Shahzad *et al*. (2013) proposed a scheme with both single-touch and multi-touch behavior through touch dynamics authentication which provided an EER of 0.5%. Novelty in the proposed work includes swiping or pinching in screens. A total of 50 volunteers were tested collecting 15009 gesture samples with the test done on only 3 types of gestures out of 25 supported gestures. A user has to provide 25 to 30 samples to input the behavior of a user for two or three days. During this time, usual pin/password/pattern authentication was used. Features identified for classification include finger velocity, device acceleration, and stroke duration. Support vector distribution estimation (SVDE) is used for classification and authentication of users.

Another investigation is done by Meng *et al*. (2013) which supports both multi-touch and single-touch behaviors. Gestures were identified for user authentication which includes average touch speed per direction, fraction of touch movements per direction, average touch time and a number of touch events. 20 users were tested for 120 sessions of 10 minutes each which provided an EER of 3.34% using the hybrid model of Particle Swarm Optimization (PSO) and an RBFN classifier. The proposed method outperforms the classification using other algorithms such as J48, Naïve Bayes, Kstar, Radial Basis Feed-Forward Networks (RBFN), Back Propagation Neural Networks (BPNN). The limitation of this approach is that it needs more computational complexity in battery powered smart phones.

Table 4: Discussion Of Pros And Cons Of Some Of The Recent Works In Touch Dynamics Authentication.

Algorithm Used	Author	Parameters Considered	Advantages	Disadvantages
Hausdorff Distance Method	Jain and Kanhangad (2015)	Co-ordinates of touch area, finger area, accelerometer and orientation sensor readings	EER of 0.31% achieved	More testing needed to check the consistency of EER value.
Dynamic Time Warping Algorithm	Sae-Bae *et al.* (2014)	Palm movements, finger movements	EER is 4.03%	Accuracy is less. More computational overhead.
Statistical classifier	Zhao *et al.* (2014)	Coordinates of finger touch points, pressure values and time stamps	Best EER is 11.28%	Accuracy is less.
Support Vector Distribution Estimation (SVDE)	Shahzad *et al.* (2013)	Finger velocity, device acceleration, stroke time	EER is only 0.5% which is very low. Overcomes both shoulder surfing and smudging attacks.	More training need to be under different postures.
Hybrid PSO-RBFN	Meng *et al.* (2013)	Touch speed, touch velocity, finger movement direction	EER is 2%, FAR is 2.5%, FRR is 3.34%	More computational complexity due to hybrid algorithm
DTW	Sae-Bae *et al.* (2012)	Palm movements, finger movements	Best achieved EER was 5%	Accuracy is less.

An investigation done by Sae-Bae *et al*. (2012) revealed that multi-touch gestures provide more reliability than single-touch gestures. Both palm and finger movements were considered for the authentication. Palm movements could be static or dynamic during a gesture. Finger movements of fingers include parallel, closed where all fingers move towards the centre, opened, circular. Also, movement of all fingers and some fingers were taken into consideration. A best EER of 5% was achieved and the Dynamic Time Warping (DTW) has been used for the authentication purpose. The limitation of this approach is its less accuracy. This technique combined with inputs from sensors such as finger pressure, face recognition using on-board camera could further increase the accuracy of the algorithm.

E. Works on Handwaving Biometrics:

One of the recent gesture based authentication is hand waving biometrics. The authentication process is based on the features of a user's habits and motions, which is much harder to be replicated by intruders of

mobile phones. This approach seems to be very convenient to users as there is no necessity to remember any information to unlock the phone. A natural human machine interaction can be established through handwaving gestures in distinct features of human are identified and used for the authentication purpose. Also, time required to do the gesture would be very small compared to gait, keystroke based approaches. Obviously, this approach has its limitations as well. To extract the patterns from the accelerometer sensors and to classify them, a classifier with more computational complexity is needed. Some of the works on handwaving biometrics is discussed below and a comparison of them is in Table 5.

A more recent scheme proposed by Yang *et al*. (2015) is that each user exhibits unique handwaving gestures which may be used for strong authentication purposes while the user waves the phone for just 1 or 2 seconds. 200 participants gave training samples with each user waving the phone for ten seconds and it is repeated for 3 times. During waving, acceleration in x, y, z co-ordinates is collected under different postures such as standing, lying on bed and waving on the side using the built-in accelerometer. Support Vector Machine (SVM) was used for the classification and authentication purposes with the accuracy of false positive rate of around 15%, while the false negative rate is lower than 8%. But accuracy can be further improved by features from orientation sensors and face-recognition algorithms.

Table 5: Handwaving Biometrics – Survey On Recent Works.

Algorithm Used	Author	Parameters Considered	Advantages	Disadvantages
SVM	Yang *et al*. (2015)	Acceleration along x, y, z co-ordinates	FPR is around 15%, FRR is less than 8%	Requires intense computation and more training needed
K-Medoids	Karitat *et al*. (2015)	Acceleration along x, y, z co-ordinates	Matching done with template from the server. EER of 5.2%	Accuracy is less.
Global sequence alignment algorithm	Guerra-Casanova *et al*. (2012)	Acceleration along x, y, z co-ordinates	EER of 2.01% and 4.82%	Better classifier needed.

Another work on biometric authentication with hand motion gestures for mobile devices was proposed by Karitat *et al*. (2015). EER of 5.2% was achieved which is far better than the conventional update method with 12%. The experiment was conducted with 10 persons for 10 days. The metrics of each user were uploaded to a server where a clustering mechanism is imposed for classification. The 3D accelerations of the motion gestures are captured using the accelerometer, pre-processed and compared with the template from the server. The K-Medoids based clustering algorithm was used to generate the template for a cluster. Gestures used for authentication include wrist rotation, left-right, up-down, drawing a star and arm bending which consisted of free form gestures of the participants. Writing "123" and writing initials proved to be much better candidates to provide accuracy in both multi-user template and single-user templates when compared to other algorithms.

Another earlier approach to handwaving gesture is proposed by J. Guerra-Casanova *et al*. (2012). When a user waves a hand, acceleration on each of the three axes x, y, z is measured and is used for classification of the users and for the authentication purposes. A user has to be registered with the system by providing 3 training samples. Comparison is done using Global Sequence Alignment Algorithm which is a variation of the Dynamic Time Warping algorithm. A total of 100 users were put to test. Each user repeated his gesture 8 times with an acceleration rate of 100Hz. The best accuracy of 2.01% achieved when a database contained only true gestures. But the accuracy reduced to 4.82% when the database is provided with imposter samples. Advantages of this approach include no extra sensors needed and the disadvantage is that a better classifier is needed.

Survey Analysis:

Gesture based authentication schemes are convenient and establishes a natural interaction between human and mobile phones. Recent works on this direction give promising results that the schemes are likely to be implemented in mobile phones in the near future. But there are always challenges associated with good proposals. The challenges associated with gesture authentication techniques are in pre-processing the input data, classifying the pre-processed data and accordingly matching the input sample with the set of samples in the mobile database. In gait based approaches, pre-processing of input data from the accelerometer sensors consume intense computations (Ferrero, R., 2015; Claudia, N., C. Busch, 2013). In touch dynamics based schemes, classifying the input sample and matching needs more computation (Jain, A., V. Kanhangad, 2015; Shahzad, M., 2013). An open challenge is to select a suitable gesture scheme for the authentication of mobile phones. With the evolution of more convenient but computational intensive gestures, identifying the best algorithm is an open problem too. When a hybrid approach is proposed to increase the accuracy (Alpar, O., 2015; Meng Y., 2013), the computational complexity has to be addressed as well. Another challenge in this arena to be addressed is that the authentication of user should be possible under different postures and different contexts. In gait authentication schemes, very few works have been proposed in the literature to all the possible walking styles. Hand waving biometrics seems to be a very new area in gesture based authentication schemes and only a very few works have been done. So, it is a better area for research. It is hoped that this article could give more insights into some of the popular gesture based authentication techniques and open problems in the domain for the current researchers in this area.

Hand waving biometrics seems to be a more convenient and quick way to authenticate the smart phones. The literature portrays that very few works have progressed in this direction. Hence, we have planned to propose an authentication mechanism in hand waving biometrics based on K-Nearest Neighbour classification algorithm as it shows more guarantee in terms of accuracy and computational complexity.

Conclusion:

A review of the various popular authentication schemes for smart phones with their relative advantages and disadvantages have been presented in this survey paper. For each category of gesture based authentication schemes, a detailed analysis is provided with suitable explanations. Finally, a comparison of various authentication schemes with respect to important parameters is also provided to enhance the understanding of the literature. It is clearly identified that though gesture based authentications are secure, they demand low computational intense algorithms with more accuracy. This comprehensive survey shows that hand waving biometrics seems to have a promising future because it is very convenient and only a very few works have been found in the literature. In future, we would like to develop a new computational efficient authentication scheme with high accuracy based on the parameters used in the various existing schemes and compare its performance over the other schemes of its category.

REFERENCES

AfredIannarelli, 1989. Ear Identification. Forensic Identification Series, Paramount Publishing Company, Fremont, California.

Ailisto, H.J., M. Lindholm, J. Mantyjarvi, E. Vildjiounaite and S.M. Makea, 2005. Identifying people from gait pattern with accelerometers. Proceedings of SPIE, Biometric Technology for Human Identification, 5779(2): 7–14.

Alpar, O., 2015. Intelligent biometric pattern password authentication systems for touchscreens. Journal of Expert Systems with Applications, Elsevier, pp: 6286–6294.

Angulo, J. and E.W. astlund, 2012. Exploring touch-screen biometrics for user identification on smart phones. Journal of Privacy and Identity Management for Life, 375: 130–143.

Antal, M., L.Z. Szabo, 2015. An Evaluation of One-Class and Two-Class Classification Algorithms for Keystroke Dynamics Authentication on Mobile Devices. 20th International Conference on Control Systems and Computer Science (CSCS), Bucharest, IEEE, pp: 343-350.

Aviv, A.J., K. Gibson, E. Mossop, M. Blaze and J.M. Smith, 2010. Smudge attacks on smartphone touch screens. Proc. 4th USENIX Conf. on Offensive technologies, pp: 1–10.

Baker, J.K., 1975. The Dragon System- An Overview. IEEE Trans. On Acoustics Speech Signal Processing, 23(1): 24-9.

Baum, L.E. and T. Petrie, 1966. Statistical inference for probabilistic functions of finite state markov chains. The Annals of Mathematical Statistics, 37(6): 1554–1563.

Bhatt, S. and T. Santhanam., 2013. Keystroke dynamics for biometric authentication — A survey. IEEE International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME), Salem , India, pp: 17-23.

Burge, M., W. Burger, 2000. Ear Biometrics in Computer Vision. In the 15th International Conference of Pattern Recognition, pp: 822-826.

Chen, J., Y.S. Moon, M.F. Wong, G. Su, 2010. Palmprint authentication using a symbolic representation of images. Journal of Image and Vision Computing, Elsevier, 28(3): 343-351.

Claudia, N., C. Busch, 2013. Classifying Accelerometer Data via Hidden Markov Models to Authenticate People by the Way They Walk. Aerospace and Electronic Systems Magazine, IEEE, 28: 29-35.

Coover J.E., 1923. A Method of Teaching Typewriting Based on a Psychological Analysis of Expert Typing. National Educational Association, Addresses and Proceedings, 61: 561-567.

Cristiano, G., K. Majdanik, M. Conti, H. Bos, 2014. I Sensed It Was You: Authenticating Mobile Users with Sensor-Enhanced Keystroke Dynamics. Proceedings of 11th International Conference, DIMVA 2014, Egham, UK, July 10-11, Springer, pp: 92-111.

Cumins, H. and C. Midlo, 1943. Finger Prints, Palms and Soles. Dover.

Cummins, H. and C. Midlo, 1961. Palms and Soles: An Introduction to Dermatoglyphics. Dover Publications, New York.

Davrondzhon, G., K. Helkala, T. Søndrol, 2016. Biometric Gait Authentication Using Accelerometer Sensor. Journal of Computers, Academy Publisher, 7(1): 51-59.

DeLuca, A., A. Hang, F. Brudy, C. Lindner, H. Hussmann, 2012. Touch me once and I know it's you! Implicit Authentication based on Touch Screen Patterns. 26th IEEE International Conference on Advanced Information Networking and Applications Workshops (WAINA), Fukuoka, pp: 704-707.

Derawi, M.P., Bours, 2013. Gait and activity recognition using commercial phones. Journal of Computers and Security, Elsevier, 39:137-144.

Dvorak, A., N. Merrick, W. Dealey and G. Ford, 1936. Typewriting Behavior, American Book Company, NewYork, USA.

Eickler, S., S. Mwuller, G. Rigoll, 2000. Recognition of JPEG compressed face images based on statistical methods. Image Vision Computing, 18(4): 279– 287.

Fathy, M.E., V.M. Patel, R. Chellappa, 2015. Face-based Active Authentication on mobile devices. International Conference on Acoustics, Speech and Signal Processing (ICASSP), South Brisbane, QLD, IEEE, pp: 1687-1691.

Federal Bureau of Investigation, 1984. The Science of Fingerprints: Classification and Uses. Washington, D.C.: GPO.

Ferrero, R., Dipt. Di Automе Inf., P. di Torino, F. Gandino, B. Montrucchio, M. Rebaudengo, 2015. On gait recognition with smartphone accelerometer. 4th Mediterranean Conference on Embedded Computing (MECO), Budva, June 14-18., IEEE, pp: 368-373.

Gafurov, D., E. Snekkenes, T.E. Buvarp, 2006. Robustness of biometric gait authentication against impersonation attack. First International Workshop on Information Security (IS'06), On The Move Federated Conferences(OTM'06), Montpellier, France, Springer LNCS.

Gaines, R.S., W. Lisowski, S.J. Press and N. Shapiro, 1980. Authentication by keystroke timing: Some preliminary results. Rand Report R-256- NSF. Rand Corporation.

Galton, F., 1892. Finger Prints. Mcmillan, London.

Georgios, K., D. Damopoulos, D. Papamartzivanos and E. Pavlidakis, 2014. Introducing touchstroke: keystroke-based authentication system for smartphones. Security Comm. Networks, John Wiley and Sons Pvt. Ltd.

Golfarelli, M., D. Maio., D. Malton, 1997. On the error-reject trade-off in biometric verification systems. IEEE Transactions onPattern Analysis and Machine Intelligence, 19(7): 786–796.

Grasselli, A., 1969. On the Automatic Classification of Finger-prints-Some Considerations of the Linguistic Interpretation of Pictures. Methodologies of Pattern Recognition, S. Watanabe, ed., Academic Press, pp: 253-273.

Guerra-Casanova., C., Sánchez-Ávila, G. Bailador, A. de Santos Sierra, 2012. Authentication in mobile devices through hand gesture recognition. International Journal of Information Security, Springer, 11: 65-83.

Hankley, W.J. and J.T. Tou, 1968. Automatic Fingerprint Interpretation and Classification via Contextual Analysis and Topological Coding. Pictorial Pattern Recognition, (Thompson Book Co., Washington D.C.).

Harding D.W., 1933. Rhythmization and speed of work. British Journal of Psychology 23: 262-278.

Hrechak, A.K. and J.A. McHugh, 1990. Automated fingerprint recognition using structural matching. Pattern Recognition, 28(8).

http://www.techworm.net/2014/12/fingerprint-of-german-defence-minister-copied-hacker-chaos-computer-club.html

Isenor, D.K. and S.G. Zaky, 1986. Fingerprint identification using graph matching. Pattern Recognit., 19(2).

Jain, A., V. Kanhangad, 2015. Exploring orientation and accelerometer sensor data for personal authentication in smartphones using touchscreen gestures. Journal of Pattern Recognition Letters, Elsevier.

Jain, A., L. Hong, Y. Kulkarni, 1999. A multimodal biometric system using fingerprint, face and speech. Proc. of Audio-and Video based Biometric Person Authentication.

Jeanjaitrong, N., P. Bhattarakosol, 2013. Feasibility study on authentication based keystroke dynamic over touch-screen devices. 13th International Symposium on Communications and Information Technologies (ISCIT), SuratThani , IEEE, pp: 238 – 242.

Jelinek, F., 1976. Continuous Speech Recognition by Statistical Methods. Proc. IEEE, 65: 532-556.

Jermyn, I., A. Mayer, F. Monrose, Reiter, M.K. Rubin, 1999. The design and analysis of graphical passwords.In Proceedings SSYM 1999,USENIX Association.

Jourlin, P., J. Luettin, D. Genoud, H. Wassner, 1997. Acoustic-labial speaker authentication. Pattern Recognition Letter, 18: 853-858.

Juang, B.H., 1984. On the Hidden Markov Model and Dynamic time Warping for Speech Recognition-A Unified View. AT&T B.L.T.J., 63(7):1213-1243.

Karitat, S., K. Nakamurat, K. Konott, Yoshimichitottt, N. Babaguchit, 2015. OWNER Authentication For Mob Ile Devices Using Motion Gestures Based On Multi-Owner Template UPDATE. International Conference on Multimedia & Expo Workshops (ICMEW), IEEE, pp: 1-6.

Kaufman, L. and P.J. Rousseeuw, 1987. Clustering by means of Medoids, in Statistical Data Analysis Based on the UNorm and Related Methods, Noth Holland.

Kawagoe, M. and A. Tojo, 1984. Fingerprint pattern classification. Pattern Recognit., 17(3): 295–303.

Kowtko, M.A., 2014. Biometric authentication for older adults. Systems, Applications and Technology Conference (LISAT) Long Island, Farmingdale, NY,USA, IEEE, pp: 1-6.

Lahy J.M., 1924. Motion Study in Typewriting, World Peace Foundation, Boston.

Liu, C.L., C.J. Tsai, T.Y. Chang, W.J. Tsai, P.K. Zhong, 2015. Implementing Multiple Biometric Features for a Recall-Based Graphical Keystroke Dynamics Authentication System on a Smart Phone. Journal of Network and Computer Applications, Elsevier, pp: 128-139.

Mantyjarvi, J., M. Lindholm, E. Vildjiounaite, S.M. Makela, H.J. Ailisto, 2005. Identifying users of portable devices from gait pattern with accelerometers. IEEE International Conference on Acoustics, Speech, and Signal Processing.

Markel, J.D., A.H. Gray, Jr., 1976. Linear Prediction of Speech. Springer-Verlag, New York.

Matthias, T., F. Ortmeier, 2014. Toward mobile authentication with keystroke dynamics on mobile phones and tablets. 27th International Conference on Advanced Information Networking and Applications Workshops.

Mayron, L.M., 2015. Biometric Authentication on Mobile Devices. Journal of Security & Privacy, IEEE, 13: 70-73.

Meng Y., D.S. Wong, R. Schlegel, L.F. Kwok, 2013. Touch Gestures Based Biometric Authentication Scheme for Touchscreen Mobile Phones. 8th International Conference(Inscrypt 2012), Beijing, China, Springer-Verlag, pp: 331-350.

Meng, W., D.S. Wong, S. Furnell, J. Zhou, 2015. Surveying the Development of Biometric User Authentication on Mobile Phones. Communications Surveys & Tutorials, IEEE, pp: 1268-1293.

Monitor password survey, 2002 NTA - http://www.outlaw.com/page-3193, Last visit: 04.09.2006.

Monrose, F., M.K. Reiter and S. Wetzel, 1999. Password hardening based on keystroke dynamics. Proc. 6th ACM Conference on Computer and Communications Security (CCS), pp: 73-82.

Monrose, R., A. Rubin, 1999. Keystroke dynamics as a biometric for authentication. Future Gener.Comput.Syst., 16(4): 351–359.

Napier, R., W. Laverty, D. Mahar, R. Henderson, Hiron, M. Wagner, 1995. Keyboard user verification: toward an accurate, efficient and ecologically valid algorithm. Int. J. Hum. – Comput. Stud., 43: 213–222.

Nefian, A. and M. Hayes, 1999. An Embedded HMM-based Approach for Face Detection and Recognition. IEEE International Conference on Acoustic Speech and Signal Processing.

Nickel, C., C. Busch, S. Rangarajan, M. Mobius, 2011. Using Hidden Markov Models for Accelerometer-Based Biometric Gait Recognition. IEEE 7th International Colloquium on Signal Processing and its Applications (CSPA), pp: 58-63.

Nishiguchi, S., M. Yamada, K. Nagai, S. Mori, Y. Kajiwara, T. Sonoda, K. Yoshimura, H. Yoshitomi, H. Ito, K. Okamoto, T. Ito, S. Muto, T. Ishihara and T. Aoyama, 2012. Reliability and validity of gait analysis by android-based smartphone. Telemedicine and e-Health, 18(4): 292–296.

O'Shaughnessy, D., 1987. Speech Communication - Human and Machine. Addison-Wesley, New York.

Obaidat, M. and B. Sadoun, 1997. Verification of computer uses using keystroke dynamics. IEEE Trans. Syst. Man Cybern. – Part B:Cybern, 27(2): 261–269.

Öberg, T., A. Karsznia, K. Öberg, 1993. Basic gait parameters: reference data for normal subjects, 10-79 years of age. Journal of rehabilitation research and development, 30(2): 210–223.

Phillips, P.J., A. Martin, C.L. Wilson, M. Przybocki, 2000. An introduction evaluating biometric systems, Computer, 33(2): 56–63.

Poritz, A.B., 1982. Linear Predictive Hidden Markov Models and the Speech Signal. Proc. ICASSP '82, Paris, France, pp: 1291-1294.

Pousttchi, K. and M. Schurig, 2004. Assessment of today's mobile banking applications from the view of customer requirements. 37th Annual Hawaii International Conference on System Sciences (HICSS'04).

Prathap, C., S. Sakkara, B.P. Pradeep Kumar, 2015. Analysis of algorithm models for Gait Recognition. The International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO), IEEE, pp: 1-6.

Qiao, M., S. Zhang, A.H. Sung and Q. Liu, 2015. A Novel Touchscreen-Based Authentication Scheme Using Static and Dynamic Hand Biometrics. 39th Annual International Computers, Software & Applications Conference (COMPSAC), Taichung, Taiwan, IEEE.

Rabiner, L. and B. Juang, 1986. An introduction to hidden Markov models. ASSP Magazine, IEEE, 3(1): 4–16.

Rabiner, L., 1989. A tutorial on hidden Markov models and selected applications in speech recognition. Proc. IEEE, 77(2): 257-286.

Sae-Bae, N., K. Ahmed, K. Isbister and N. Memon, 2012. Biometric-Rich Gestures: A Novel Approach to Authentication on Multi-touch Devices. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12), New York, NY, USA, ACM, 977-986.

Sae-Bae, N., N. Memon, K. Isbister, K. Ahmed, 2014. Multitouch Gesture-Based Authentication. TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE, 568 – 582.

Saevanee, H., P. Bhattarakosol, 2009. Authenticating User Using Keystroke Dynamics and Finger Pressure. 6th international conference on Consumer Communications and Networking Conference CCNC, Las Vegas, NV , Jan 10-13, IEEE, 1-2.

Saira, Z., M. Shahzad, S.A. Khayam1, M. Farooq, 2009. Keystroke-Based User Identification on Smart Phones. Proceedings of the 12th International Symposium on Recent Advances in Intrusion Detection RAID'09, Springer-Verlag, pp: 224-243.

Shahzad, M., A.X. Liu, A. Samuel, 2013. Secure Unlocking of Mobile Touch Screen Devices bySimple Gestures – You can see it but you can not do it. Proceedings of the 19th annual international conference on Mobile computing & networking(MobiCom '13), New York, NY, USA, ACM, 39-50.

Shepard, R.N., 1967. Recognition memory for words, sentences, and pictures. Journal of Verbal Learning and Verbal Behavior, 6(1): 156-163,

Stevenage, S.V., M.S. Nixon, K. Vince, 1999. Visual Analysis of Gait as a Cue to Identity. Applied Cognitive Psychology, (13): 513–526

Sudhir, D., P. Kundra, A. Kanchan, P. Kap, 2015. Mobile Authentication using Keystroke Dynamics. International Conference on Communication, Information & Computing Technology (ICCICT), Jan. 16-17, Mumbai, India, IEEE, pp: 1-5.

Tari, F., A.A. Ozok and S.H. Holden, 2006. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. Proc. Of SOUPS, pp: 56-66.

Thang, H., DeokjaiChoi, T. Nguyen, 2015. Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme. Internal Journal of Information Security, Springer, pp: 1-12.

Thavalengal, S., P. Bigioi, P. Corcoran, 2015. Iris authentication in handheld devices - considerations for constraint-free acquisition. Transactions on Consumer Electronics, IEEE, 61(2).

The symantec smartphone honey stick project.

Turk, M.A. and A.P. Pentland, 1991. Face Recognition Using Eigenfaces. Proc. IEEE Conf. Computer Vision and Pat ern Recognition (CVPR 91), pp: 586–591.

Umphress, D. and G. Williams, 1985. Identity verification through keyboard characteristics. International Journal of ManMachine Studies, (23): 263–273.

Venkataramani, K., S. Qidwai and B. VijayaKumar, 2005. Face authentication from cell phone camera with illumination and temporal variations. IEEE Trans. on Systems, Man and Cybernetics, 35(3): 411-418.

Vildjiounaite, E., S.M. Makela, M. Lindholm, R. Riihimaki, V. Kyllonen, J. Mantyjarvi and H. Ailisto, 2006. Un-obtrusive multimodal biometrics for ensuring privacy and information security with personal devices. Pervasive, Springer LNCS, pp: 187–201.

Watanabe, Y., 2014. Influence of Holding Smart Phone for Acceleration-Based Gait Authentication. Fifth International Conference on Emerging Security Technologies (EST), Alcala de Henares, IEEE, pp: 30-33.

Wegstein, J.H., 1982. An Automated Fingerprint Identification System. National Bureau of Standards Special Publication 500-89,republished by National Technical Information Service, U.S. Dept. Commerce, Springfield, VA.

Yang, L., Y. Guo, X. Ding, J. Han, 2015. Open Sesame: Unlocking Smart Phone through Handwaving Biometrics. Transactions On Mobile Computing, IEEE, pp: 1044–1055.

Yuan, L., Z. Mu, Z. Xu, 2005. Using Ear Biometrics for Personal Recognition. Proceedings of the International Wokshop on Biometric Recognition Systems (IWBRS), Beijing, China, Springer.

Zezschwitz, E.V., A. Koslow, A.D. Luca, H. Hussmann, 2013. Making graphic-based authentication secure against smudge attacks. Proceedings of the international conference on Intelligent user interfaces(IUI '13), Santa Monica, CA, USA, ACM.

Zhao, X., T. Feng, W. Shi, 2013. Continuous mobile authentication using a novel graphic touch gesture feature. Proc. IEEE Int. Conf. Biometrics, Theory, Appl. Syst., Washington, DC, USA, pp: 1–6.

Zhao, X., T. Feng, W. Shi, L.A. Kakadiaris, 2014. Mobile User Authentication Using Statistical Touch Dynamics Images. Transactions on Information Forensics And Security, IEEE, 1780 – 1789.