Enhanced Authentication Mechanisms for Desktop Platform and Smart Phones

Dina EL Menshawy, Hoda M. O. Mokhtar, Osman Hegazy
Information Systems Department
Faculty of Computers and Information, Cairo University
Cairo, Egypt

***Abstract*— With hundreds of millions using computers and mobile devices all over the globe, these devices have an established position in modern society. Nevertheless, most of these devices use weak authentication techniques with passwords and PINs which can be easily hacked. Thus, stronger identification is needed to ensure data security and privacy. In this paper, we will explain the employment of biometrics to computer and mobile platforms. In addition, the possibility of using keystroke and mouse dynamics for computer authentication is being checked. Finally, we propose an authentication scheme for smart phones that shows positive results.**

Keywords- Biometrics; Keystroke; Mouse; Authentication; Smart Phones; Touch Screens; Touch Pressure; Touch Contact Size.

I. INTRODUCTION

Today we are witnessing a tremendous increase in the use of computers and smart phones for storing sensitive information and accessing on-line services. These devices have become important tools in many people's daily activities, and are consequently used for many purposes including: communication, entertainment, storing confidential personal and business information. Therefore, the hacking of a computer or a mobile device can have negative implications like the invasion of privacy, the opportunity to impersonate user, and even severe financial loss. Current user authentication for computers and mobile phones is provided by the personal identification numbers (PIN) and passwords which have a number of inherent weaknesses such as the ease of figuring out one's PIN. In general, there are three levels of computer security mechanisms: the first mechanism depends on something a person carries, such as an ID badge with a photograph, while the second scheme relies on something a person knows, such as a password. Finally, the third approach is related to a person's human attributes, such as fingerprint and/or signature [1]. The increasing need for improving security systems led to more research in the application of biometrics in authentication systems. The term biometrics originates from the Greek words bios (life) and metrikos (measure). Biometrics refers to the identification of a person based on his/her physiological or behavioral characteristics. People have personal characteristics that uniquely identify them such as hand signature, fingerprint and voice. In general, biometrics is mainly divided into two categories, namely, physiological biometrics and behavioral biometrics. *Physiological biometrics* identifies a person based on his/her physiological characteristics such as eye retina, whereas *behavioral biometrics* relies on detecting the behavioral attributes of the user, such as keystroke dynamics [2]. Biometrics became popularly used as a tool for security because of its universality and distinctiveness. Mainly, there are two capabilities of biometrics which are identification and verification. Identification is the process of determining a person's identity; whereas verification ensures that the person requesting the access is the one he claims to be [3]. A biometric system consists of several modules, the main components are: a sensor module, a feature extraction module, and a classification module. The sensor module captures the trait, and then the feature extraction module extracts a feature set from the captured data. After that, the classification module compares the extracted feature set with reference feature sets to validate a claimed identity [1]. Finally, a biometric based authentication system can be evaluated using either a genuine test or an impostor test, described as follows:

- The genuine test (or False Rejection Rate (FRR)): when the user enters an input that is far away from his own template.
- The impostor test (or False Acceptance Rate (FAR)): when the user enters an input that is very similar to another user's template [1].

The main contribution of this work can be summarized as follows:

1. Explored the use of machine learning techniques in biometric authentication for both desktop application and smart phones.
2. For desktop platform, we examined the employment of neural networks and k-means clustering with focus on only two types of behavioral biometrics; keystroke and mouse data.
3. Also, we constructed a multi-modal biometric system based on both keyboard and mouse data. Fusion at the feature level was examined for a better degree of accuracy. Feature level was accomplished by merging both forms of data to create a new behavioral feature vector.
4. For smart phones, we proposed an authentication mechanism based on different metrics. Again, neural networks and k-means clustering were implemented on the collected data. The investigations examined

other behavioral biometrics which is: key hold times, latencies, finger pressure and finger contact size.

The rest of the paper is organized as follows: we present in Section 2 a comparison between uni-modal and multimodal biometric systems. Section 3 discusses related work to the study of biometrics for computer and mobile phones authentication. Section 4 introduces the behavioral biometrics and discusses the types of data that will be used in the experiments. Section 5 presents the machine learning techniques used in our research. Section 6 describes our experimental approach and results. Finally, Section 8 concludes the paper and Section 9 presents directions for future work.

II. Multi-Modal Biometric Systems

Biometric systems depending on a single source of information are called uni-modal systems, while systems depending on multiple resources are named multi-modal systems. Sometimes, uni-modal biometric systems do not attain the required performance because they are more susceptible to problems such as noisy data, intra-class variations, inter-class similarities, non-universality and spoofing. On the other hand, multi-modal biometric systems handle some of these problems. They solve the problem of non-universality as multiple traits will guarantee adequate population coverage. Moreover, they overcome the spoofing problem as it won't be easy for an imposter to spoof multiple biometric traits of a real user [4]. Fusion can be achieved by applying multi-modal systems, fusion refers to combining or making use of multiple biometric traits to enhance the classification accuracy. There are three various levels of fusion: the first type is at the feature level where feature sets arising from several sensors are fused. The second kind of fusion is at the match score level where the scores produced by classifiers related to different biometric traits are aggregated. The third level of fusion is achieved at the decision level where the final outputs of multiple classifiers are merged through certain techniques. In our research, we will build a multi-modal biometric system then we will apply the feature level fusion on behavioral biometrics.

In this paper, we investigate a crucial problem in biometric data, namely, mining biometric data. Data mining has become an increasingly popular activity in all areas of research, from business to science, and currently, in biometrics. Biometric verification is gaining more attraction because most of the systems based on it are easy to incorporate in ordinary computer use and without user interaction. Besides, they do not need extra devices for authentication. The challenge is to integrate machine learning techniques into biometrics verification leading to the evolution of the term biometric data mining. Hence, biometric data mining (BDM) is the application of knowledge discovery techniques to biometric information with the purpose of identifying underlying patterns [5].

III. Related Work

Recently a number of researches were conducted to explore the utilization of machine learning techniques in different biometric systems. Several works on keystroke biometrics have already adopted approaches based on different metrics, sampling methodologies and data analysis techniques. In [6], the authors proposed a benchmark testing suite composed of a database and a software that are publicly available for the research community to evaluate keystroke dynamics based systems. The software offers several functionalities, for example, it records timing information when a user enters a certain password. Also, the tool offers different types of keyboards to test typing evolution depending on this parameter. In [7], the authors designed, tested, and evaluated four different metrics related to keystroke analysis. The four metrics were key press duration, key press and release comparisons, relative keystroke speeds, and a metric based on shift key usage patterns. Each user typed the sentence"A quick brown fox jumps over the lazy dog" up to eleven times and the different metrics were recorded. In [8], the authors presented a design and an implementation of a remote authentication framework called TUBA for monitoring a user's keystroke-dynamics patterns and identifying intruders. They evaluated the robustness of TUBA through comprehensive experimental evaluation including two series of simulated bots. It was concluded that TUBA can be integrated with other anomaly detection systems to achieve remote monitoring and diagnosis of hosts with high assurance. In [9], the authors collected keystroke data in the form of digraphs when users enter a specific password, then rough sets were used to detect patterns in the typing rhythm. The analysis produced a sensitivity of 96%, specificity of 93% and an overall accuracy of 95%. On the other hand, some studies were done on using mouse movements as a biometric for authentication.

In [10], a user was asked to join the dots appearing on the screen, and then in the verification phase, the user should move the mouse in the same pattern as done in the enrollment step to check his/her identity. The testing was done in a classroom with students in the age group of 22-30. The error rate for this system was 20%. In addition, another study on using mouse biometrics was conducted in [11]. The k-nearest neighbor method was used to identify unknown mouse profile from a set of known user profiles; and the Euclidean distance was used to discover the nearest neighbor. A success rate of 92% for the first choice of the nearest neighbor was reached. Matching the second choice was 88% and matching second and third choices together was 80%. In [12], the paper investigated the effectiveness of user authentication using keystroke dynamics-based authentication (KDA) on mobile devices. A keystroke dynamics-based authentication mechanism was proposed with artificial rhythms and tempo cues for mobile user authentication. The novelty detector classifier was built. Then, subjects were asked to perform enrollment, login, and even intrusion to other subjects' accounts.

In [13], the authors investigated the authentication of users based upon three interaction scenarios: entry of 11-digit telephone numbers, entry of 4-digit PIN, and entry of text messages. The discussion focused upon the concept of keystroke analysis for users' authentication. The findings revealed the technique to be promising for certain users with average error rates below 5%. In [14], an application for the Android mobile platform was developed to collect data on the way individuals draw lock patterns on a touchscreen. Using a Random Forest machine learning classifier this method achieved an average Equal Error Rate (EER) of approximately 10.39%. In [15], six distinguishing keystroke features were used for user identification in smart phones. They optimized the front-end fuzzy classifier using Particle Swarm Optimizer (PSO) and Genetic Algorithms (GA) as back-end dynamic optimizers to adapt to variations in usage patterns. Finally, they provided a novel keystroke dynamics based PIN verification mode to ensure information security on smart phones.

IV. Behavioral Biometrics

Behavioral biometrics refers to a subset of biometrics which has to do with a person's behavior. Examples include keystroke dynamics, signature verification, and voice. Behavioral biometrics works on the characteristics that are developed naturally over time [2]. For instance, in keystroke dynamics, some features can be measured, for example, the typing speed, and the time taken between consecutive keystrokes. In the following discussion we will further elaborate two biometric types that will be later used in our experiments. Keystroke and mouse data will be shown in Sections 5.1 and 5.2 respectively. Also, the metrics that will be used in smart phones authentication will be presented. Finger pressure and finger contact area were considered distinguishable features across users which will be explored in Section 5.3.

A. Keystroke Dynamics

Keystroke dynamics means the pattern in which a user types characters, or numbers on a keyboard. Keystroke dynamics is used to define the person's identity because it resembles an individual's handwriting or signature. A user's keystroke rhythms are measured to generate a distinctive prototype of the user's typing patterns for use in authentication. One key advantage of using keystroke dynamics is that FRR and FAR can be fine-tuned by altering the acceptance threshold at the individual level. Also, keystroke movements can be captured constantly. Moreover, no additional hardware is needed to collect keystroke data, the keyboard is enough. Each user has a unique time for depressing and holding keys, as some people type certain words or characters faster than others. A lot of features can be derived from keyboard typing such as: duration time (the time of a key press), and latency (the time between"key up" and the next "key down") [16]. In this paper, different keyboard features are used to explore various attributes that are not common, the features are:

- The difference between two press events (PP).
- The difference between two release events (RR).
- The difference between one press and one release events (PR).
- The difference between one release and one press events (RP).
- The time to type the password: the total time taken to write a certain word or password [6].

B. Mouse Dynamics

Mouse dynamics is a recent behavioral biometric that is being used in authentication systems. Mouse dynamics means monitoring the users' activities through a human computer interface. It has been proven that user-based mouse movements can model the user's behavior. Features used to explain the users' behavior include drag and drop, click, and any other mouse movement. Moreover, we can compute some calculations such as the speed of moving the mouse across a certain distance. The key plus of using mouse dynamics to validate the identity of the user is that it does not need additional hardware to capture the users' behavior [17]. In addition, mouse dynamics is useful for continuous authentication since the user identity can be confirmed through the repeated mouse movements. In this paper, we focus on the following features to monitor mouse movements:

- Total time [T_{Total}]: time from when mouse button was first depressed to draw first segment until last segment was completed.
- Actual drawing time [T_{Draw}]: time excluding pauses when mouse button is released.
- Length [$Length_{tot}$]: total length of all drawn segments [18].

C. Finger Pressure and Finger Contact Size

We noticed that users of touch screens enter data in a characteristic manner as they exert different pressures and varying finger touch area. Therefore, we utilize both finger pressure and contact area as new biometric features for smart phones authentication. Analogous to keystroke studies but for smart phones with touch screens, two distinguishing features will be captured for all users:

- Finger pressure: the pressure of finger touch on the screen.
- Touch size: the contact area or the area pressed of the finger on the touch screen [19].

V. Biometric Based Authentication Techniques

In this paper, we employed neural networks and k-means clustering to study the accuracy and efficiency of behavioral biometrics for authentication in both desktop application and smart phones.

A. Neural Networks

A multilayer feed-forward neural network consists of an input layer, one hidden layer, and an output layer. In the hidden layer, each neuron performs a weighted summation of the inputs, which then passes a nonlinear activation function. The network output is formed by another weighted summation of the outputs of the neurons in the hidden layer. This summation on the output is called the output layer [20].

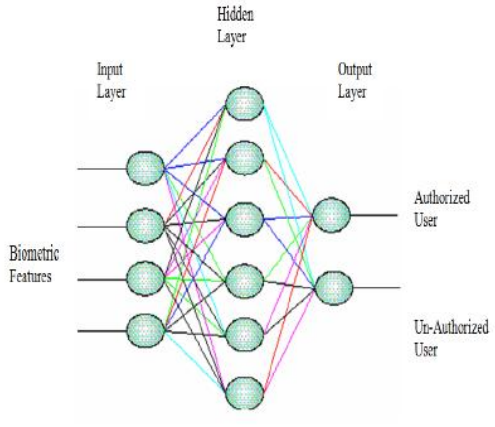


Figure 1: Multilayer Feed-forward Neural Network

B. K-means Clustering

The second machine learning technique used in this work is the traditional k-means clustering. Following the kmeans, the number of clusters is equal to the number of users. The main goal is to ensure that each user is correctly classified into a *single* cluster. When a user is classified into more than one cluster which will result in an in-accurate authentication, experiments can be repeated to ensure that the behavioral pattern does not change. K observations from the samples were selected at random as initial cluster centroid positions. Centroids were updated until they reached stable centers of clusters. A feature vector is created for each user. The aim is to partition N feature vectors into K disjoint subsets containing *Nj* feature vectors so as to minimize the sum-of-squares criterion [20]. Keystroke and mouse data denote the feature vector of a user in desktop platform while the finger pressure and finger contact size denote the feature vector of a user in smart phones.

VI. Experimental Setup And Results

The initial motivation for our research arose from the need to provide secure and unobtrusive methods for authenticating users of computers and mobile devices. The main objective is to have both low FRR and FAR as well as to achieve both high usability and high security of the system. In our research, the use of neural networks and k-means clustering will be investigated to mine behavioral biometric data and discover hidden features that help to increase verification accuracy.

Actually, mouse dynamics is used in GUI base applications, whereas a keyboard is essential for command line base applications so they are two related tools when dealing with computers. As a result, we will explore fusing those kinds of biometric data to construct an accurate multi-modal system. Also, a proposed scheme for smart phones authentication will be presented, the authentication will be based on finger touch pressure and finger contact size. The experimental details will be shown below:

A. Study of Behavioral Biometrics for Desktop Platform

In our proposed methodology, there are four important stages involved in keystroke and mouse dynamics based authentication system.

1. First, a user enrolls his/her feature vector.
2. Second, a preprocessing phase is done.
3. Third, neural networks were implemented using the feature vectors for each biometric trait on its own, then were applied on both keyboard and mouse data together. Here, we built three neural networks: the first one was based on keystroke data only, the second was based on mouse dynamics only. Last but not least, the third network worked on both forms of data together. Moreover, K-means clustering was implemented on the fused data.
4. Forth, the performance of the proposed system is evaluated.

The following sections clearly illustrate the experimental details:

1) Enrollment

We have conducted some experiments involving 20 participants, and collected experimental data over 3 weeks. Ages range from 18 to 30, and both males and females participants were involved to cover different ages and both genders along with different computer literacy or experience. A strong password was chosen containing capital and small letters, and numbers were used in the enrollment stage. All users were allowed to enter the same password several times to get used to typing it. Then, in the enrollment stage, each user typed the word ”DI19na25” twenty times and the keystroke features were recorded. Concerning mouse dynamics data, the 20 users were allowed to draw a line between 2 points and the mouse features were recorded.

Most literature work applied different machine learning technique on two keystroke features: duration of key hold and latencies. Here, we utilized a little bit features that may produce better results than those two features. We used PP, RR, PR, RP and total time to write a password. The definitions of those features were shown in a previous section. For example, when a user enters”DI19na25”, the four latency timings (PP, RR, PR, RP) were recorded for each pair of characters. Also, the total duration of writing the whole password is recorded. Concerning the mouse features, the following table clearly illustrates the used features:

Table 1: Mouse Features

ID	T_{Total}	T_{draw}	$Length_{tot}$
1	3.09	3.09	2008.6
1	3.09	3.09	2008.6
1	13.27	5.09	4016.5
1	27.92	7.68	6044.8

2) Preprocessing

As typing pattern of the same user varies from time to time although it is relatively unique for each user, normalization was done to improve the accuracy of classification. The normalization technique used was min-max as it has been shown to give good results. The preprocessing phase maps the feature vectors to fall into a small specified range. In the preprocessing phase, outliers were removed in order to improve the performance of the system [20].

3) Classification Using Neural Networks and Kmeans Clustering

In order to evaluate the feasibility of applying behavioral biometrics for authentication in secure systems, neural networks and K-means clustering were used in different experiments. We computed a profile for each member who will be later used as a reference in testing and evaluation. For both keyboard and mouse data, fifteen samples will be used for training and another five for testing. Neural networks were applied on keystroke and mouse data, each separately, and then fusion was done on the feature level. The feature vectors were classified using feed forward network. Feature level fusion is fulfilled by a concatenation of the feature sets acquired from several sensors. The main idea behind fusing more than one biometric trait is to improve the prediction rate. In this research, keyboard and mouse biometrics data are fused to form a single template. For example, if keystroke data is denoted by $\{X_1, X_2,...X_m\}$ while mouse data is expressed as $\{Y_1, Y_2,...Y_n\}$. The aim is to integrate both kinds of data to produce a new feature vector $Z = \{X_1, X_2,...X_m , Y_1, Y_2,...Y_n\}$ which better represents the user [21]. Three networks were built, the first one handled the keystroke data and the second network processed the mouse data. The fused feature vectors were fed into the third network. The networks were built in Matlab because it offers a great neural networks toolbox; also, it is relatively fast in testing.

4) Experimental Results

The three networks were run several times to compare the performance, it has been shown that fusing biometrics data achieves the best results, mouse data following it and keystroke attains the lowest accuracy. The numerical outputs are clearly presented in the following table:

Table 2: Recognition Accuracies of Three Networks

Data	Number of Characteristics	Accuracy (%)
Keystroke	33	54
Mouse	3	65
Fusion	36	72

FAR is computed as the percentage of imposters wrongly classified as legitimate users, and FRR is the percentage of legitimate users classified as imposters. In the testing phase, we divided the participants into 2 groups: a group of 10 representing authorized users, and the remaining 10 representing unauthorized users.

Also, FRR and FAR measures were calculated for each user then an average value was measured. The average FRR and FAR were 14 % and 17 % respectively. As fusion of both keystroke and mouse data gave promising results, k-means clustering was implemented to compare the performance with neural networks. The number of clusters was 20 as there were twenty participants, each cluster denotes a user. The whole samples were fed into the clustering algorithm. Twenty tests were run with random seeds, the tests resulted in an average accuracy of 79%.

B. Keystroke Dynamics for Smart Phones

Using Android 2.3.3 (API10) and Eclipse, we have developed a mobile application to collect data from different individuals about the way they type numbers on a smart phone. The handheld mobile device used in the experiment was a Samsung Galaxy Ace GT-S5830i with 832 MHz CPU and 158 MB memory.

The experimental approach is described as follows:

1. Let users practice typing PIN code until they can type smoothly.
2. Allow each user to type the PIN twenty times to create a database.
3. Classify the feature vectors using neural networks and clustering.
4. Test the biometric system using the error rates.

1) Enrollment

Twenty participants were enrolled in the experiment; each user was allowed to enter a PIN code. The PIN was chosen to be"9721" to avoid same horizontal and vertical alignment. The investigation required the participants to enter the PIN twenty times which will be used to create a reference profile. The first phase investigated the feasibility of authenticating mobile phone users based upon the traditional keystroke features used in computer authentication which are hold time of keys and latency between keystrokes. For example, when all users entered the PIN "9721", the time duration between the number pairs (9-7), (7-2) and (2-1) will be computed. Also, the duration time of holding each key will be recorded. In our case, each typed PIN consists of three latencies and four hold times features, resulting in seven features for each user. Again, min-max normalization is done in the pre-processing phase.

Since data entry on a standard numerical keypad on a PC differs from entering numerals on a mobile phone in terms of feel and layout, so a second phase of the study was implemented. This study seeked to evaluate the feasibility of using finger touch pressure and finger contact touch area as unique characteristics rhythms. Each user was allowed to practice by typing the PIN several times. In the enrollment phase, each user entered the PIN code 20 times to have a true profile for the typing pattern, and then finger pressures and contact area were recorded for each key. All erroneous trials were disregarded. Touch coordinates on button presses were supposed to be used in the experiments but when tried with different users, it has been shown that it cannot be used as a distinguishable feature. Screen location on touch screen of different users were similar so was not used in our investigations.

2) Classification Using Neural Networks and Kmeans Clustering

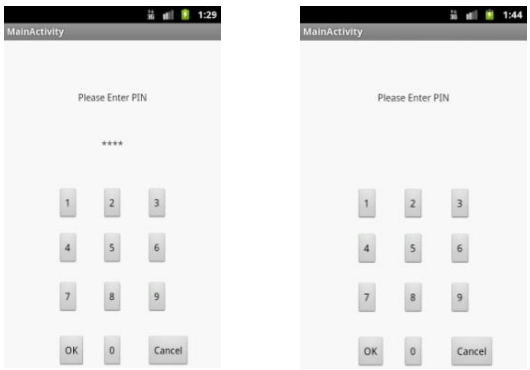
Neural networks and K-means clustering are again used but here in smart phones authentication.

In the first investigation, fifteen samples were used for training and the remaining five for testing. At first, a reference template was constructed for each user containing the hold times of entering the four keys and the latencies periods between the keys. Neural networks were applied on hold times and latencies, the feature vectors were classified using feedforward network.

In the second investigation, fifteen samples were used for training and the remaining five for testing. At first, a reference template was constructed for each user containing the finger touch pressures and finger contact sizes. Neural networks were applied on finger pressures and contact sizes, the feature vectors were classified using feedforward network.

The data was acquired by Android functions, the pressure value was obtained via the getPressure() method while the touch area was captured through the getSize() method. The pressure exerted on the device was obtained in kilopascals while the getsize() functions returns the size of the current contact area. This method returns the size in pixels corresponding to the area touched by the finger [22]. Both functions return a value ranging from 0 to 1 so there is no need for normalization.

Figure 2: Snapshots of Mobile APPLICATION



3) Experimental Results on Key Hold Times and Latencies

In the verification phase, we divided the participants into 2 groups: a group of 10 representing authorized users and the remaining 10 representing unauthorized users. The performance of biometric systems is usually evaluated by two error rates: (FRR) and (FAR).

Hence, FAR and FRR were calculated for each user, then an average was computed. The experiments produced relatively good results; FRR was 19% and FAR was 27%. A snapshot of the mobile application is shown in Figure 2, it shows the layout of buttons the user will use to enter the PIN.

4) Experimental Results on Finger Touch Pressure and Finger Contact Size

Again neural networks were used as in previous experiments resulting in 83% accuracy. FRR and FAR are then measured for each user then an average was computed. The FRR rate was 12% and FAR was 18%.

It has been shown that finger pressure and finger contact areas acted as distinguishable characteristics among users and provided better results than the traditional keystroke features used in computer authentication. Again as presented in the desktop experiment, k-means clustering was implemented on finger pressure and finger contact area data and resulted in 64% accuracy. To conclude, clustering had a better performance in desktop platform rather than neural networks while the opposite occurred in mobile platform.

VII. CONCLUSION

The investigations have shown that it is feasible to authenticate users based on behavioral biometrics. This study has demonstrated the ability of neural networks and k-means clustering to differentiate between computer users based on keyboard and mouse biometrics with a relatively good degree of accuracy. Each technique was applied on keyboard and mouse biometrics each separately, and then fusion of both kinds of data was implemented on the feature level. Different trials were conducted on a number of users and it has been shown that fusion of keyboard and mouse data produced the best results. Also, an authentication scheme for mobile users based on finger touch area and contact finger area was proposed. Before applying the proposed scheme, experiments were done on key hold times and latencies, which are the most commonly used features in keystroke authentication systems. After various experiments, it has been shown that finger pressure and contact size can act as unique features and resulted in better accuracy than the classical keystroke features applied in desktop authentication. This is can be due to that finger pressure and contact size are considered distinguishable among users using touchscreens rather than holding time and latency.

Keystroke analysis has proven to be a promising technique having achieved good results in both desktop and mobile platforms.

VIII. FUTUREWORK

For future work, we plan to explore other machine learning techniques to have a comparative study on different techniques. Also, a comparative research for various smart phones can be implemented as there is a massive evolving variety in touchscreens technology.

Experiments can be conducted on smart phones with different screen sizes to investigate wether screen size can influence finger touch actions which as a result, can affect the authentication accuracy. Also, investigations can be done on smart phones with stylus pens to examine the distinguishing features for those kinds of smart phones and discover if touch pressure and touch contact size can act as unique features or not.

ACKNOWLEDGMENT

We would like to thank Professor Walter Beagley, Professor of Psychology at Alma College for letting us use the Eye Lines Program to collect the data. Also, we gratefully appreciate Romain Giot, Mohamad El-Abed and Christophe Rosenberger for making their GREYCKeystroke software publicly available to help researchers to create keystroke

dynamics databases. Moreover, special thanks to all colleagues who devoted their time to assist us in data gathering.

REFERENCES

[1] J.M. Kizza, Ethical and Social Issues in the Information Age, Texts in Computer Science, Springer- Verlag, 2010.

[2] John Chirillo and Scott Blaul, Implementing Biometric Security, Wiley Pub.,2003, Vol. 14, 9780764525025.

[3] Dmitry O. Gorodnichy, Evolution and evaluation of biometric systems, IEEE Symposium on Computation Intelligence for Security and Defense Applications, 2009.

[4] Prof. V. M. Mane and Prof. (Dr.) D. V. Jadhav, Review of Multimodal Biometrics: Applications, challenges and Research Areas, International Journal of Biometrics and Bioinformatics (IJBB), Vol. 3, Issue 5, 2009.

[5] Jos Alberto Hernndez-Aguilar, Crispin Zavala, Ocotln Daz, Gennadiy Burlak, Alberto Ochoa and Julio Csar Poncem, Biometric Data Mining Applied to On-line Recognition Systems, InTech, 2011.

[6] Romain Giot, Mohamad El-Abed and Christophe Rosenberger, GREYC Keystroke: a Benchmark for Keystroke Dynamics Biometric Systems, IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2009.

[7] Edmond Lau, Xia Liu, Chen Xiao and Xiao Yu, Enhanced User Authentication Through Keystroke Biometrics, Massachusetts Institute of Technology, 2004.

[8] Deian Stefan, Xiaokui Shu and Danfeng (Daphne) Yao, Robustness of keystroke dynamics based biometrics against synthetic forgeries, Journal of Computers and Security 3 I, 2011.

[9] Kenneth Revett, Sergio Tenreiro de Magalhaes and Henrique Santos, DataMining a Keystroke Dynamics Based Biometrics Database Using Rough Sets, IEEE, 2005.

[10] Shivani Hashia, Chris Pollett and Mark Stamp, On Using Mouse Movements as a Biometric, San Jose State University, 2008.

[11] AdamWeiss, Anil Ramapanicker, Pranav Shah, Shinese Noble and Larry Immohr, Mouse Movements Biometric Identification: A Feasibility Study, Seidenberg School of CSIS, Pace University, 2007.

[12] Seong-seob Hwang, Sungzoon Cho, and Sunghoon Park, Keystroke dynamics-based authentication for mobile Devices, Journal of Computers and Security, 2009.

[13] N.L. Clarke, S.M. Furnell, Advanced user authentication for mobile devices, Journal of Computers and Security, 2007.

[14] Julio Angulo and Erik W?stlund, Exploring Touchscreen Biometrics for User Identification on Smart Phones, Karlstad University, 2011.

[15] Saira Zahid, Muhammad Shahzad, Syed Ali Khayam and Muddassar Farooq, Keystroke-based User Identification on Smart Phones, Springer Verlag, 2009.

[16] Michal Choras and Piotr Mroczkowski, Keystroke Dynamics for Biometrics Identification, Springer- Verlag, 2007.

[17] S.Benson Edwin Raj and A. Thomson santhosh, A Behavioral Biometric Approach Based on Standardized Resolution in Mouse Dynamics, IJCSNS International Journal of Computer Science and Network Security, Vol. 9, No. 4, 2009.

[18] http://www.alma.edu/el/, [accessed 10/09/2011].

[19] Meier, R., Professional Android 2 Application Development, John Wiley and Sons Inc., 2010.

[20] Jiawei Han and Micheline Kamber, Data Mining Concepts and Techniques, Elsevier, 2006, Second Edition, 81-312-0535-5.

[21] Arun Ross and Rohin Govindarajan, Feature Level Fusion Using Hand and Face Biometrics, SPIE Conference on Biometric Technology for Human Identifiication II, Vol. 5779, pp. 196-204, 2005.

[22] Ting-Yi Chang, Cheng-Jung Tsai, Jyun-Hao Lin, A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices, The Journal of Systems and Software, 2012.