Design and Development of a Biometric System Using Mouse Gesture Dynamics

Chethan D C[1]
Dept.of ECE IVth sem M.tech (DECE) Akshaya
Institute of Technology
Tumkur, India

Mr.Sundaresh M P[2]
Lecturer Dept. of ECE
Akshaya Institute of Technology
Tumkur, India

Abstract— **Mouse gesture dynamics is a special type of behavioral biometric authentication technique. This approach extracts and analyses the mouse movement characteristics by using a computer mouse as a pointing device. In general, there are two types of authentication i.e. continual authentication and static authentication. Continual authentication system has been widely used and evolution of such system is much faster when compared to static authentication based system. Signature drawn by the user as input for the static authentication and mouse lock method are the only two existing mouse based static authentication systems. In order to improve the efficiency of static authentication based system, we are introducing a new model to make the system with much higher efficiency and robust. In this new approach user draws, at long time, a few gestures from which the gestures are collected and analyzed for authentication purpose. Existing gestures based authentication systems uses other input devices such as stylus but we use mouse as our input device for capturing the gestures. The captured gestures are analyzed using a hidden markov model classifier. Mouse gesture dynamic system yields impressive FAR of 5.2% (False Acceptance Ratio) and FRR of 4.5 % (False Rejection Ratio) compared to the existing mouse based static authentication systems. This Improvement in both accuracy and validation compared to existing mouse dynamic approaches that could be considered adequate for static authentication. To the best our knowledge, our work is the first to present an accurate static authentication scheme based on mouse gesture dynamics.**

Index Terms—component Behavioral biometric, Mouse dynamics, Mouse dynamics analysis framework

I. INTRODUCTION

The primary focus of designing the biometric system is to provide the very accurate authentication .In the last two decades, with the rapid development in the computerized services like online banking, trading and many others, the number of hacking and identity theft incidents are increasing enormously. Token based authentication is simple but not foolproof. To overcome the problem with token based authentication system, Biometric systems were emerged. But biometric properties cannot be kept secret due to many factors. This limits the scope of biometrics in day-to-day life. Another reason for limited usage of biometric system is the reliance on special purpose devices for biometric data collection and verification.

Hence we are developing a prototype for new category of behavioral biometrics that is gaining great attention in recent days is Mouse gesture dynamics. Mouse dynamics deals with extracting the features related to the mouse movements and analyzing them to extract a signature, which is unique for every individual and can be used to discriminate different individuals. The aim of mouse dynamics biometric technology is its ability to continuously monitor the legal and illegal users based on their usage of a computer system. This is referred to as continuous authentication. Continuous authentication is very useful for continuous monitoring applications such as intrusion detection. This paper first identifies the user movements or characteristics when the user interacts with the mouse, results in the generation of mouse gestures and checks every time when the user make session and provides authentication to the users. The mouse gestures is drawned in uni-stroke.

A mouse gesture results from the combination of computer mouse movements and clicks in a way that the software recognizes as a specific command. Biometrics refers to the identification of humans by their characteristics or traits. Biometric identifiers are characterized as physiological and behavioral characteristics. A physiological biometrics is related to voice, DNA, hand prints. A behavioral biometrics is related to the behavior of the persons. A biometric system involves 2 phases, enrollment phase and verification phase. In the enrollment phase, user will draw a set of gestures several times on a computer monitor using mouse. The features are extracted from the captured data, analyze them and train the neural network that is later used for identification. In the verification phase, the user will be asked to replicate a subset of gestures drawn during the enrollment phase for authentication.

Mouse gesture dynamics deals with biometric authentication. The mouse gesture dynamics uses a hidden markov model for classification. In the existing graphical password sahemes, the user is not only excepted to memorize and remember the graphical passwords, the user has to hide the passwords during the login process to avoid surfing attacks. The mouse dynamics proposed schemes depends on the user biometric information and the user need not to memorize the gestures. There are only two mouse dynamics based biometric systems techniques available for static authentication due to the complexity or challenges. One of the methods proposed by Syukri etal uses the signature drawn by the user as input during the static authentication process. The other method proposed by Revett etal uses mouse lock method for static authentication. In the proposed approach, the user draws the gesture at login time which are collected and analyzed for authentication purpose. Existing gestures based authentication systems uses other input devices such as stylus but in this paper, mouse is used as input device for capturing the gestures.

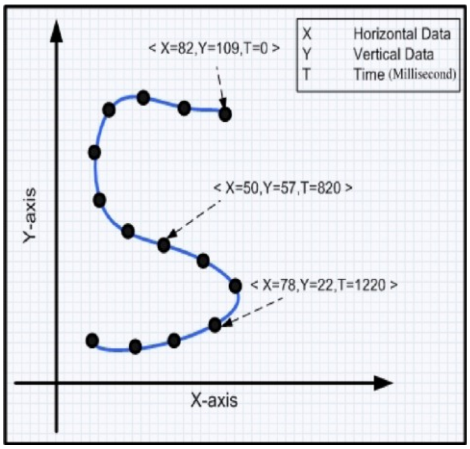

Fig.1. Example of a drawn gesture involving n = 14 data points.

II. SYSTEM DESIGN

The fig 2 clearly shows the actual flow diagram of capture and analysis of mouse gestures .This approach allows user to draw one or several gestures and asking them to replicate the gestures a certain number of times. The produced replications are then compared against templates produced by the user during the enrollment phase.

The raw data collected from the drawing area consists of the horizontal coordinate (x-axis), vertical coordinate (y-axis) and the elapsed time in milliseconds at each pixel. Each gesture replication for a given gesture is defined as a sequence of data points. Each data point is represented by a triplet <x, y, t> indicates X-coordinate, Y-coordinate and elapsed time respectively. The j^{th} replication of a gesture G is represented as a sequence Gj $_=$ $\{< x1j, y1j, t1j >, < x2j, y2j, t2j >, < xnj, ynj, tnj >\}$, where n is the gesture size(GS) and each $< xij, yij, tij >$ where $(1 \leq i \leq n)$ is a data point. The main aim is to differentiate between individuals based on their behavioral biometrics while drawing mouse gestures.

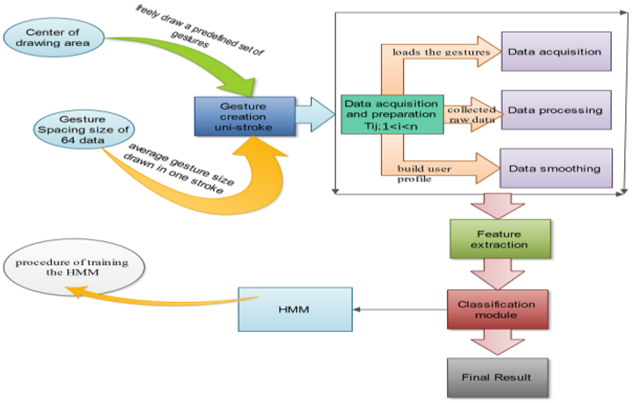
Center of drawing area
freely draw a predefined set of gestures
Gesture Spacing size of 64 data
average gesture size drawn in one stroke
Gesture creation uni-stroke
Data acquisition and preparation Tij;1<i<n
loads the gestures
collected raw data
build user profile
Data acquisition
Data processing
Data smoothing
Feature extraction
Classification module
HMM
procedure of training the HMM
Final Result

Fig.2. Flow Diagram for capture and analysis of Mouse Gestures

The mouse dynamics analysis framework involves four modules.

a) Gesture creation module.
b) Data acquisition and preparation module.
c) Feature extraction module.
d) Classification module.

A. Gesture Creation Module

The gesture creation module is a simple drawing application where the user is asked to freely draw a set of gestures. Te main aim of this module is to make the user to draw the gestures in their own way to replicate them later. The gestures are not tied to any language and they do not necessarily have a meaning. The gestures should be in uni-stroke. For each gesture three parameters are collected namely horizontal coordinate, vertical coordinate and elapsed time in milliseconds.

B. Data Aquition and preparartion module

Data acquisition: The data acquisition component loads the gestures, created initially by the user using the gesture creation module and presents them to the user to replicate. The data acquisition module records the user interaction while drawing the gestures.

Data preprocessing: The data acquisition module preprocesses the collected raw data from the computer mouse in such a way that some noise patterns are ignored or dropped.

After preprocessing the raw data, the data acquisition module applies two types of normalizations for the input data. The first is normalization and the second is size normalization. The center normalization shifts the gesture to the center of the drawing area as implemented in the gesture creation module. Then normalize the size so that the final size of the gesture is equal to the size of the template gesture to compare the two gestures. The normalization can be applied by accepting gestures which is drawn by the users whose size is greater than or equal to the size of the template gesture. If the gesture size is bigger than the template size, then the k-means algorithm is used to cluster the data points into 64 clusters. The Euclidean distance is a distance measure between the data points in three dimensions <x, y, t> is used. Then the centroids of the 64 clusters are used to form the new gesture.

Outlier removal and data smoothing: Data smoothing is used to eliminate noise and extract the real patterns from the data. The smoothing is used to smooth the data among the different replications obtained for each users. In general, human beings cannot draw the same gesture with the same exact details twice. This results in some variability in the replicas produced by the same user for the same gesture. Data smoothing will smooth such variability and minimize its effect on the learning process. The weighted least-squares regression (WLSR) method to smooth the data

The Peirce’s criterion [21] is used to eliminate the outliers. Peirce’s criterion method is a robust statistical based method that does not make any assumptions about the data. Peirce’s criterion deals with the data that has several suspicious values.

Peirce’s criterion determines outliers by computing the maximum allowable deviation from the sample mean. Given m the sample size, n is the number of outliers and R is the ratio between the maximum allowable deviation to the standard deviation. The maximum allowable deviation is calculated by $dmax = R \times \sigma$, where σ is the standard deviation of the sample and xi is a data item which is considered as an outlier if $|x_i - x_m| > d_{max}$, where x_m is the sample mean. Using the Peirce's criterion method and starting from n=1, the outliers are removed sequentially by incrementing the number of possible outliers, while keeping the original values of mean, standard deviation and sample size. The process is repeated until no other data item needs to be eliminated.

The outlier removal and data smoothing steps are applied only to horizontal coordinates and vertical coordinates data. The vector is constructed to aggregate the same occurrence of the first data point from each of the different replications. Then apply the Peirce's criterion method and WLSR method to the data in the vector to produce clean and smoothed data. Repeat the process for each of the remaining data points of the gesture. The smoothing occurs only on the training samples and not on the test data.

C. Feature Extraction Module

The feature extraction module extracts the features from the raw data. Features selection is made by analyzing sample data and identifying the features. The feature extraction module extracts the features from the raw data. Features that are obtained from the vector of data points they are intercepted between two mouse clicks can be used. The complete list of the extracted features is provided in Table 1. Figure 2 defines the angle of the tangent with the x-axis and the length of the path from the origin.

TABLE I: Feature Extracted From Raw Data

Feature Description	Notation
Horizontal coordinate	x
Vertical coordinate	y
Absolute time	t
Horizontal velocity	hv
Vertical velocity	vv
Tangential velocity	tv
Tangential acceleration	ta
Tangential jerk	tj
Path from the origin in pixels	l
Slope angle of the tangent	θ_i
Curvature	c
Curvature rate of change	δc

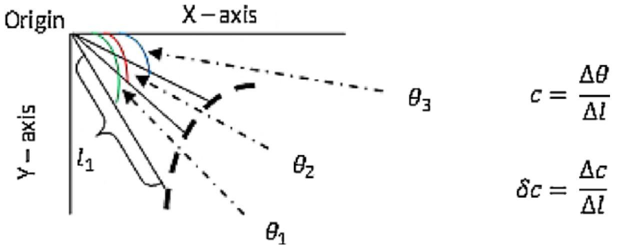
Origin
X – axis
Y – axis
l_1
θ_3
θ_2
θ_1
$c = \frac{\Delta\theta}{\Delta l}$
$\delta c = \frac{\Delta c}{\Delta l}$

Fig. 3: Angle of curvature and its rate of change for a portion of a drawn gesture

D. Classification Module

In order to classify the gestures, first we tried out with the Principle Component Analysis (PCA), yielding very poor performance. The feed-forward back propagation multilayer network was tried. The training steps of this network were exhaustive and time consuming. The training process is stopped when it exceeds five hours (on a computer system with a 2GHz Core 2 Duo CPU and 2GB RAM) for only a population of two users.

A new technique called Hidden Markov Model (HMM) is used here for comparison and recognition of mouse gestures. HMM is the best classifier for online handwriting recognition, speech recognition, gesture recognition and language modeling .HMM is the first best tools that have been created for easily generating and modifying test suites of data. After the training has been generated and stored as a test suite, the HMM recognizer program instantiates a new codebook of specified size and a set of HMMs (one per gesture) with a specified number of states. The HMM's immediately tested on the training data to verify the accuracy of training. The system can be worked for many hours. This will yield good results in recognition of mouse gestures.

a. EXPERIMENTAL RESULTS

We present, in this section, the experimental evaluation of the proposed framework. We start by describing the experimental conditions and procedures, and then present, analyze, and discuss the obtained results.

a. Apparatus

All the participants used the same Dell Inspiron laptop to enrol in our experiments. The hardware configuration of the laptop was an Intel Core 2 Duo processor clocked at 2 GHz, with 4GB of physical memory, running Microsoft Windows 7 configured with a resolution 1440×900 native screen resolution. All the participants used a Microsoft Explorer optical mouse to replicate the different gestures; even the same mouse pad was used during the experiment. The sampling rate was 125 Hz, which is the Microsoft Windows XP/Vista/7 OS default sampling rate for USB based mouse devices. The software involved in our experiments was already deployed on the laptop. The software, written in JAVA, consisted of a gesture creation tool and an enrolment tool. The gesture creation tool is used to create the gesture templates and store them with the user credentials in a database. The enrolment tool loads the templates from the database and allows the participant to enrol against them. The replications resulting from the enrolment are stored in the replications database.

b. Participants

The main objective of our experiment was to be able to recognize individuals based on their mouse gestures. Ideally, the system should be able to recognize, with a high degree of accuracy, the behaviour of each user while replicating a specific gesture. To achieve such a goal, 20 volunteers were involved in our experiment. The participants were from various backgrounds, with ages ranging from 18 to 56 years old. Participants' skill levels ranged from novice users using computers only occasionally to individuals using computers on a regular basis as part of their professions (e.g., university faculty members, students, engineers). Participants in the experiment were divided into two groups: a group of 15 individuals representing legal users and a group of five individuals representing impostors.

c. *Method and Data*

The gestures drawn here should be unistroke. 15 Legal participants asked to draw few gesture templates first, which are the combinations of line, angles and curves. Then ask them to replicate the same gesture number of time. Likewise allow the 5 impostors to forge the legitimate user's gesture minimum times.

d. *Evaluation Process*

During the evolution process we sre going to calculate the FAR (False Acceptance Ratio) and FRR (False Rejection Ratio). The global FRR is computed as the ratio between the total number of false rejections over all the test trials and the total number of test trials *n*

$$FRR = \frac{\sum_{j=1}^{n} count(\{FR\}_j)}{n} \times 100$$

Where number of replications j ($1 \leq j \leq n$) is the test trial index.

The global FAR is computed as the ratio between the total number of false acceptances over all the test trials and the total number of test trials *N*

$$FAR = \frac{\sum_{j=1}^{N} count(\{FA\}_j)}{N} \times 100$$

Where number of replications j ($1 \leq j \leq n$) is the test trial index.

e. *Evaluation Results*

We applied the above-mentioned evaluation method number of times separately for each gestures involved in our experiment, and computed global FRR and FAR. We observed an improvement in performance with FRR of 4.5% and FAR of 5.2%. This is the huge improvement when compared to handwriting biometrics. This improves the accuracy of authentication process and avoids biometric information from the attacks.

IV. CONCLUSION

In this paper, we highlighted the challenges faced by mouse dynamics biometric technology when it is applied to authentication and proposed a new mouse dynamics analysis framework to train the data that gave good results. The proposed framework uses hidden markov model for classification and uses Peirce's criterion and weighted least -square s regression methods for outlier removal and data smoothing.

In the future work, we intended to enhance the accuracy using various techniques. Since the proposed system is entirely software based, integrating in a complex system environment such as e-commerce or e-learning portals should be straightforward from an implementation perspective. The verification time should be much faster in order to train the gestures. One of the challenges is the protection of systems against security attacks. Like other biometric techniques, mouse dynamics can be the target of reply attacks. Such threats can be mitigated by strengthening the protection of biometric templates using various techniques. Mouse dynamics can also be a target of generative attacks through forgeries. In our feature work, we planned to strengthen our system by investigating the impact of generative attacks against it.

V. REFERENCES

[1] S. Cimato, M. Gamassi, V. Piuri, R. Sassi, and F. Scotti, "Privacy-aware biometrics: design and implementation of a multimodal verification system," in *Proc. Annu. Comp. Sec. Apps. Conf.*, 2008, pp. 130–138.

[2] D. Lopresti, F. Monrose., and L. Ballard, "Biometric authentication revisited: Understanding the impact of wolves in sheep's clothing," in *Proc. 15th USENIX Sec. Symp.*, 2006.

[3] M. S. Obaidat and N. Boudriga, *Sec of e-Sys and Comp Networks*. Cambridge, MA: Cambridge Univ. Press, 2007.

[4] M. Obaidat and B. Sadoun, "Verification of comp. users using keystroke dynamics," *IEEE Trans. Syst., Man, Cybern.*, vol. 27, no. 2, pp. 261–269, Apr. 1997.

[5] H. Gamboa and A. Fred, "A behavioral biometric system based on human-comp. inter," in *Proc. Conf. Biometric Tech. Human Identification*, vol. 5404. 2004, pp. 381–392.

[6] A. A. E. Ahmed and I. Traor´e, "A new biometric tech. based on mouse dynamics," *IEEE Trans. Dependable Secure Comput.*, vol. 4, no. 3, pp. 165–179, Jul.–Sep. 2007.

[7] M. Pusara and C. E. Brodley, "User reauthentication via mouse movements," in *Proc. ACM Workshop Visualization Data Mining Comp. Sec. (VizSEC/DMSEC)*, 2004, pp. 1–8.

[8] N. Zheng, A. Paloski, and H. Wang, "An efficient user verification system via mouse movements," in *Proc. 18th ACM Conf. Comp. Commun. Sec.*, 2011, pp. 139–150.

[9] K. Revett, H. Jahankhani, S. de Magalhaes, and H. M. D. Santos, "A survey of user authentication based on mouse dynamics," in *Proc. ICGeS, CCIS'12*, 2008, pp. 210–219.

[10] P. Oel, P. Schmidt, and A. Shmitt, "Time prediction of mouse-based cursor movements," in *Proc. Joint AFIHM-BCS Conf. Human Comp. Inter.*, vol. 2. Sep. 2001, pp. 37–40.

[11] A. A. E. Ahmed and I. Traor´e, "System and method for determining a comp. user profile from a motion-based input device," U.S. patent 10/555408, PCT/CA2004/000669, 2003.

[12] A. Nazar, I. Traor´e, and A. Ahmed, "Inverse biometrics for mouse dynamics," *Int. J. Artif. Intell. Pattern Recognit.*, vol. 22, no. 3, pp. 461–495, May 2008.

[13] A. F. Syukri, E. Okamoto, and M. Mambo, "A user identification system using signature written with mouse," in *Proc. 3rd Australasian Conf. Inform. Sec. Privacy*, 1998, pp. 403–414.

[14] S. Patel, J. Pierce, and G. Abowd, "A gesture-based authentication scheme for untrusted public terminals," in *Proc. UIST*, Oct. 2004.

[15] L. L. Lee, T. Berger, and E. Aviczer, "Reliable online human signature verification systems," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 18, no. 6, pp. 643–647, Jul. 1996.

[16] R. Plamondon and S. N. Srihari, "Online and off-line handwriting recognition: A comprehensive survey," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 22, no. 1, pp. 63–84, Jan. 2000.

[17] R. R. M. Roberts, R. A. Maxion, K. S. Killourhy, and F. Arshad, "User discrimination through structured writing on PDAs," in *Proc. 37th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw.*, 2007, pp. 378–388.

[18] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," in *Proc. 8th Conf. USENIX Sec. Symp. (SSYM)*, 1999, p. 1.

[19] C. Varenhorst. (2004). *Passdoodles: A Lightweight Authentication Method* [Online]. Available: http://people.csail.mit.edu/emax/papers/varenhorst.pdf

[20] S. Lloyd, "Least squares quantization in pcm," *IEEE Trans. Inform. Theory*, vol. 28, no. 2, pp. 129–137, Mar. 1982.

[21] S. Ross, "Peirce's criterion for the elimination of suspect experimental data," *J. Eng. Tech.*, vol. 20, no. 2, 2003.

[22] F. Azam, "Biologically inspired modular neural networks," Ph.D. dissertation, Virginia Polytechnic Instit. State Univ., Blacksburg, 2000.

[23] T. Kohonen, *Self-Organizing Maps* (Springer Series in Information Sciences, vol. 30), 3rd ed. Berlin, Germany: Springer, 2001.

[24] M. Gamassi, M. Lazzaroni, M. Misino, V. Piuri, D. Sana, and F. Scotti, "Accuracy and performance of biometric systems," in *Proc. Instrum. Meas. Tech. Conf.*, 2004, pp. 510–515.

[25] S. Bengio and J. Mariethoz, "A statistical significance test for person authentication," in *Proc. Odyssey: Speaker Language Recognition Workshop*, 2004.

[26] R. Biddle, S. Chiasson, and P. C. V. Oorschot, "Graphical passwords: Learning from the first twelve years," School Comp. Sci., Carleton Univ., Ottawa, ON, Canada, Tech. Rep. TR-11-01, Jan. 2011.