Mouse Interaction based Authentication System by Classifying the Distance Travelled by the Mouse

Saurabh Singh
Invertis University
Bareilly, India

Dr. K.V.Arya
AVB Indian Institute of Information Technology
Gwalior, India

ABSTRACT
Behavioral biometric based systems as a solution of authentication challenge are appealing because of various reasons – unlike other password based or physiological property based systems, there is no chance of acquiring behavioral properties by someone else. In the proposed work, mouse interaction dynamics has been exploited for user authentication purpose. User's behavior on mouse is unique and can be taken as biometric property. A graphical panel has been designed for acquiring user pattern and a grouping approach has been applied to reduce the size of the pattern. Results are very encouraging and indicate that the designed graphical panel can effectively classify the legitimate users and imposters.

1. INTRODUCTION

Access to secure system is controlled by some authentication system which decides whether user is legitimate or imposter. This is established by the system in two ways – (i) Does user know something which is supposed to be known only by the genuine user? and (ii) Does the user own some unique characteristics of the legitimate user. In first case it is possible that an imposter can also know that something which is required to enter in a secure system. We are therefore, interested in second case. The characteristics of a person which can be used to authenticate a legitimate user are the physiological or behavioral characteristics [1, 2]. Physiological characteristics are those which are biologically owned by the user (face, finger prints, iris pattern etc.) and behavioral characteristics are those which includes user's habits (handwriting, keystroke dynamics, mouse interaction, gait etc.). Currently, the industry is oriented towards physical biometrics. Fingerprints are most commonly used authentication system because of its high accuracy [3]. Physical biometrics have number of drawbacks- these systems are expensive, no one can alter his/her physical biometric characteristics like passwords or behavior (for example one can change his/her typing rhythm but cannot change is fingerprints). Moreover most physical biometric systems require additional hardware devices [4]. Behavioral characteristics are very hard to copy and it is very difficult to generate them artificially.

In this paper we are concentrating on mouse interaction based authentication which is a behavioral biometric system. Rest of the paper is organized as follows: section 2 describes the related work done in the field, section 3 explains the proposed technique and section 5 gives conclusion and limitations.

2. RELATED WORK

Mouse dynamics include mouse movement, drag and drop, point and click etc. These actions can be used to generate a unique profile for user authentication purpose [5]. Pusara et al. [5] splits the mouse event data into two groups, mouse wheel movements and clicks. Click data is further divided into single and double click data. Weiss et al. [6] concentrated on button press and mouse drag data for a fixed pattern to gather features, and to create feature vector. They have designed a button panel (having 5*5 buttons) which has to be clicked by user in some pre defined order. All the data related to mouse activities have been collected and seven features are computed to form feature vector. The seven features described are size of curve, length of mouse curve, total time of the mouse curve, mouse speed over a pre defined action, angle of mouse movement, acceleration and mouse click duration.

Analysis done in this work is fixed pattern based that is the actions taken by the user were controlled by the system. The drawback of this system is that user cannot make his/her own choice of movements, this prevents the user to do actions in natural way but in a behavioral system, the behavior of the user must be natural at the time of data collection. In the proposed work the user is allowed to make any actions on the button penal and features are collected such a way a vector can be constructed.

3. PROPOSED TECHNIQUE

Any behavioral authentication system works on the basis of natural behavior of the user, if the behavior of the user is controlled or influenced by anything else, the accuracy of the identification system gets affected. In the proposed work, the system allows the user to behave naturally to collect features.

This section is further divided into 3 subsections, subsection 3.1 explains the feature extraction strategy we have followed in the technique. Subsection 3.2 describes how the

3.1 Feature Extraction Strategy and pattern construction

Study says that mouse speed increases with the distance travelled by the mouse [6] and highly dependent on the direction of the mouse movement. So, following hypothesis are made –

(H1a) Mouse speed increases with the distance travelled.

(H1b) Mouse speed is different in different directions considerably.

In the proposed work, speeds over different directions and over different distances have been collected to construct feature vector. Another hypothesis has been made to simplify the process of vector construction. In the proposed work distances travelled by the user are classified in three classes (1) Short (2) Long and (3) Very long and in eight directions. Therefore total 24 speeds (along 8 directions *3 Distances classes) may be collected to construct the feature vector.

(H2) Distances can be classified such that speeds in any one class are almost similar.

According to hypothesis H2 all the speeds that are collected are not taken. For example if [s1,s2,s3…..s24] is a feature vector where s1 is speed along direction 0 for short class distance, s2 is speed along direction 0 for long class distance, s3 is speed along direction 0 for very long class distance similarly s4, s5, s6 are speeds along direction 1 for the three classes and so on.

3.2 Design of experiment

To capture the features, a nine button panel was considered as shown in fig. 1 and distances between any pair of buttons on the panel are classified as follows:

Short- For the buttons adjacent (1-2, 1-5, 2-5, 2-6 etc.).

Long- For the buttons neither adjacent and nor at largest diagonals (1-3, 1-6 etc.).

Very Long- For the buttons that are at the ends on largest diagonals (1-9, 3-7).

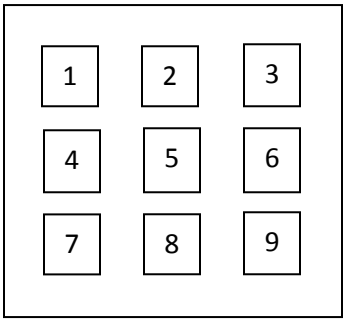

Fig. 1: The nine button panel used in the experiment

Profile vector is created by the features collected from the user. The maximum length of profile vector is twenty four (explained in section 3.1). Each feature in the vector is a speed calculated across any two buttons and along any one direction.

Speed is calculated against distance (short, long or very long) and direction (0 through 7). It is computed as the number of pixels travelled per millisecond. All speeds that are calculated by the formula are not considered as feature (H2), but only one speed is taken from each category (remember there are 24 categories), this reduces the vector size.

The login vector is created at login time and its features are ordered according to the profile that stored in the database. Now distance between the two vectors are calculated and classified as accepted or rejected.

3.3 Methodology

To establish the hypothesis H1a and H1b, five users participated in the experiment, who were asked to use the panel explained in 3.2. Users
are 3rd and 4th year undergraduate students of age group 22-25 years.

All users had considerable experience with computer system (more than 2 years). Participants were first asked to play a game having mouse interaction for five minutes to normalize their behavior with the mouse. A code (1-2-6-1-9) was given to all five users to click on the panel and button sequence wise average of distances and there corresponding speeds are calculated as shown in table 1. It clear from the table that average mouse speed is increasing with the speed this supports H1a. Similarly table 2 shows the speed dependency on the direction. The code given to participants was (7-8-6-3-5-4-8-4-7). Table 2 shows the direction wise average of speed of all users. This verifies H1b as it is clear that movements in right and upper directions are faster than the movements in lower and left directions.

Table 1: Speeds against distances

Button sequence	Average Distance(pixels)	Average Mouse speed(Pixels/milliseconds)
1-2	502.485	1.04723
2-6	712.871	1.43878
6-1	1218.458	1.92874
1-9	1481.287	2.47871

Table 2: Speeds against directions

Button sequence	Direction	Average Mouse speed(Pixels/milliseconds)
7-8	0	2.1265
8-6	1	1.3987
6-3	2	1.3125
3-5	3	1.0245
5-4	4	1.0356
4-8	5	1.2341
8-4	6	1.5672
4-7	7	2.5419

USER	1	2	3	4	5	6	7	8	9	10	Average
FAR	1.53	0.82	0.51	0.21	0.33	0.58	0.41	0.48	0.52	0.54	0.593
FRR	2.47	3.51	2.31	3.01	2.51	1.87	1.98	4.26	3.17	5.65	3.074

Table 3: Performance of the system

Table 1 also gives the basis of classification of the distances, it can be clearly seen that if distances are similar, corresponding speeds are also similar. Hence, this also supports H2.

4. RESULTS

To evaluate performance of the system, the same program (described in 3.2) was used and ten users having qualities described in 3.4 were asked to participate. Each participant registered themselves and everyone worked as an imposer for others to evaluate FAR (false acceptance rate). FAR is computed as the percentage of imposters wrongly classified as legitimate user and FRR is the percentage of legitimate user classified as imposter**s.** Table 3 shows the results obtained. Worst FAR is 1.53 and worst FRR is 5.65 which ensure the acceptability of the system. Low value of FAR is more important than FRR because the low value of FAR shows the strictness of secured system.

5. CONCLUSION AND LIMITATIONS

The paper proposes a new approach in behavioral biometric authentication system using mouse interaction. In the work a new idea of classifying the distances travelled by the mouse is presented with supporting results. The study was done on limited number of participants and it is possible that if different population is used results may vary from those presented here.

There are other aspects of mouse interaction behavior which are not studied here like mouse shape and size. These issues can also be explored in future work.

6. REFERENCES

[1] Anil K. Jain, Arun Ross and Salil Prabhakar2, "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and systems for Video

Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.

[2] Lawrence O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication", Proceedings of the IEEE, Vol.91, No. 12, Dec, pp. 2019-2040, 2003.

[3] P. Reid, "Biometrics for Network Security", Prentice Hall, Upper Saddle River, NJ, 2004.

[4] D. Polemi, Biometric techniques: review and evaluation of biometric techniques for identification and authentication — final report, and editors. Institute of Communication and Computer systems, National Technical University of Athens, 1995.

[5] M. Pusara and C. E. Brodley, User re-authentication via mouse movements, VizSEC/DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, ACM Press, Washington DC, USA, 2004, pp. 1--8.

[6] A. Weiss, A. Ramapanicker, P. Shah, S. Noble, and L. Immohr. "Mouse movements biometric identification : A feasibility study". In Proc. Student/Faculty Research Day, CSIS, Pace University, pages 1-8, May 2007.

[7] A. A. E. Ahmed and I. Traore, "Detecting computer intrusions using behavioral biometrics. Privacy, Security and Trust", 2005.