VIRTUAL KEY FORCE – A NEW FEATURE FOR KEYSTROKE

D. SHANMUGAPRIYA*, DR. G. PADMAVATHI**,
Avinashilingam Institute for Home Science and Higher Education for women, Coimbatore, India
*Lecturer, Dept. of Information Technology, shanmugapriya.adu@gmail.com
** Prof and Head, Dept. of Computer science, ganapathi.padmavathi@gmail.com

Abstract

Securing the sensitive data and computer systems by allowing ease access to authenticated users and withstanding the attacks of imposters is one of the major challenges in the field of computer security. Traditionally, ID and password are most widely used method for authenticating the computer systems. But, this method has many loop holes such as password sharing, shoulder surfing, brute force attack, dictionary dttack, guessing, phishing and many more. Keystroke Dynamics is one of the famous and inexpensive behavioral biometric technologies, which will try to identify the authenticity of a user when the user is working via a keyboard. There are many features that can be acquired using keystroke a feature. Force of Key type is one of the features which can be obtained using a special force sensitive keyboard which is expensive. The virtual key force is measured without using any special key board which also improves the accuracy when the feature is used for classification.

***Keywords* – Keystroke; Back propagation neural network; Genetic Algorithm; Virtual Key force.**

1. Introduction

Almost all the people rely on computers at certain level in day today life. Many of these systems store highly sensitive, personal, commercial, confidential or financial data. Unauthorized access to such data will lead to loss of money or unwanted disclosure of highly confidential data that threats the security of Information. User Authentication prevents unauthorized access of information for providing information security. User authentication is the process of verifying claimed identity. This is done for the purpose of performing trusted communications between parties for computing applications.

User authentication is categorized into three classes [17] :

- Knowledge - based,
- Object or Token - based,
- Biometric - based.

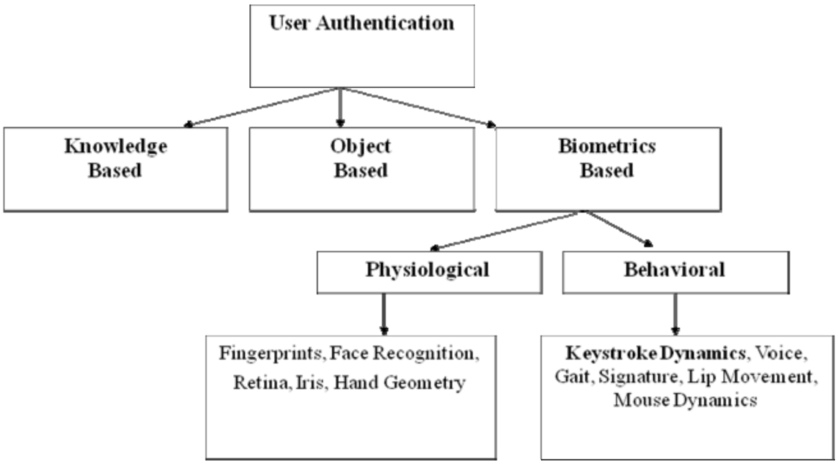
User Authentication
Knowledge Based
Object Based
Biometrics Based
Physiological
Behavioral
Fingerprints, Face Recognition, Retina, Iris, Hand Geometry
Keystroke Dynamics, Voice, Gait, Signature, Lip Movement, Mouse Dynamics

Figure 1. User authentication classification

User Authentication classification is given in figure 1. The knowledge-based authentication is based on something one knows and is characterized by secrecy. The object-based authentication relies on something one has and is characterized by possession. The Biometric-based user authentication is based on something you are and depends on behavioral and physiological characteristics of individuals. In knowledge-based and object-based approaches, passwords and tokens can be forgotten, lost or stolen. There are also usability limitations associated with them such as managing multiple passwords / PINs, and memorizing and recalling strong passwords which are not easy tasks. Biometric-based person recognition overcomes the above mentioned difficulties of knowledge-based and object based approaches.

Biometric authentication is further classified into Physiological and Behavioral types [17]. Physiological Biometric refer to what the person is, and Behavioral Biometrics are related to what a person does, or how the person uses the body. Keystroke dynamics is considered as a strong behavioral biometric based authentication system [1]. It is a process of analyzing the way a user types at a terminal by monitoring the keyboard in order to identify the users based on habitual typing rhythm patterns. Moreover, unlike other biometric systems, which may be expensive to implement, keystroke dynamics is almost free as the only hardware required is the keyboard. There are two approaches in keystroke authentication: Static and Dynamic. Static approach authenticates the user at logon time and Dynamic methods authenticates after logon. Static approach is used in this paper.

This paper is organised in such a way that it is divided into four sections. The first section gives a brief Introduction about Keystroke dynamics. The second section discusses the features. The next section discusses about the new feature. Results are given in fourth section and the final section concludes the paper.

2. Related works

The previous works on this topic are analyzed in the Table.1. The type of used measures for keystroke dynamics, the evaluation method and the data used for testing are analyzed.

Table 1: Analyses of previous works on keystroke dynamics

2. Features measured from Keystroke

Study	No of users	Evaluation method	Test data	Features used
Hwang,Cho, (2009)	25	Neural network	Different passwords	Duration, interval
Yu & Cho(2004)	21	Neural network	6-10 char Different passwords	Duration, interval
Obdait & Sadaun (1997)	15	Neural network	Average 7 character Different passwords	Dwell time
Obaidat, Macchairolo	6	Neural network	Phrases	Flight time
Revett (2007)	50	Neural network	6-15 char Different passwords	-
Cho, et al. (2000)	21	Neural network	-	Duration, Interval
Lin (1997)	90	Neural network	6-8 Different passwords	Duration, latency
Brown & Rogers (1994)	-	Neural network	15 character names	Flight time
Joshi (2007)	43	Neural network	-	Key hold (Duration)

Keystroke data can be obtained by measuring the pressing and releasing time of keys. There are many features that can be measured from the keystrokes. They are Duration, Latency, Digraph, Tri-graph, Pressure of keystroke, Force of Keystroke. Difficulties of typing text, Frequency of word errors, Typing rate, etc. All the features are not useful and widely used. For measuring Pressure and Force of keystroke special type of pressure or force sensitive keyboard is required. Difficulties of typing text, frequency of word errors, typing rate are useful for long text. Since user will be providing only password these features are not suitable. Therefore the timing feature such as Duration or Dwell time, Latency or Flight time, Digraph, Tri-graph are frequently measured from keystroke which is shown in figure 2.

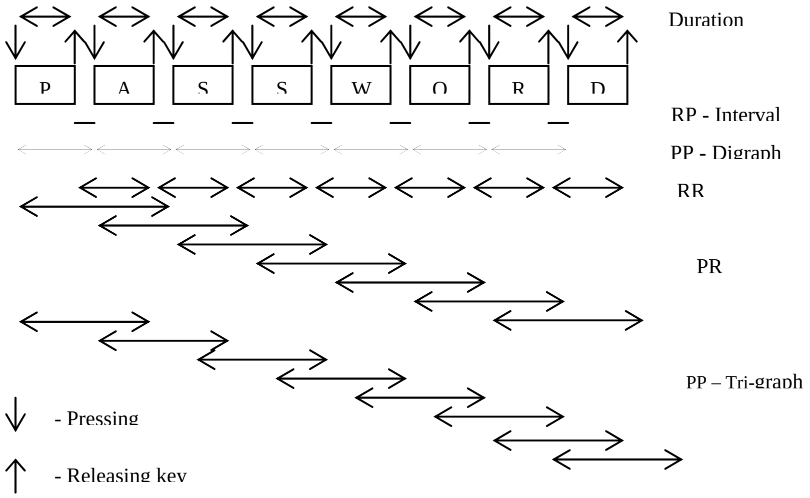

Figure 2. Timing Features of keystroke

Duration or Dwell time or Hold time It is the time to measure how long a key is pressed until it is released. It can be calculated as

Duration = release of same key – press of same key.

Flight time or latencies

Release-press (RP): It is the Interval between a key release and next key press time. It can be calculated as

RP= press time of next key – release time of a key

Press-Press (PP) It is the Interval between two successive key press.

PP=Press time of second key-press time of first key

Press-Release(PR) It is the Interval between pressing of one key and releasing of the next key

PR= duration of first key+ duration of next key +RP.

Release-Release(RR): It is the Interval between two successive key Release.

RR=Release time of second key-Release time of first key.

Digraph is the Elapsed time between the first key press and the second key press. It can be calculated from Press-Press Latency

Tri-graph is the elapsed time between the first key press and the Third key press.

Tri-graph= duration of first key+ duration of second key +RP between first and second key + RP between second and third key.

3. Proposed Feature-Virtual Key force

The virtual key force is calculated based on the typing speed and behavior of the user on the key board. It measures the time taken by the user between releasing one key and pressing another key. It is based on the fact that each user has different typing speed and each user takes their own time to release and press another key. The usage of keys and the typing speed and force is different for different users. Also the time interval taken for the release of one key and press of another key is different. Consider a user typing a word which consists of ten letters, hence there exists nine time intervals between the release of one key and press of another key. The average typing speed of the user can be calculated based on these time intervals. Virtual key force can be determined from the key complexity. The key complexity can be calculated as follows

- According to the complexity of usage of the keys, key complexity can be determined. It is based on the key position and distance.
- It means that the middle row keys (i.e., the keys from A to L) on the keyboard which are easy to handle by all the users is taken as 0. The key complexity of remaining keys is taken as 1.

In the figure 3, for the keys T,H,E the complexity label is assigned as CL=(0,1).i.e the distance from T and H is nearer(0) and the distance between H and E is longer(1).

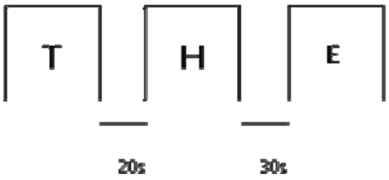

Figure 3. Timing intervals between Keys

Based on the key complexity and the average time interval taken between releasing a key and pressing another key, following algorithm which is shown in Figure 4. have been formulated:

```
Algorithm: Virtual Key Force (VKF)
if (key distance is nearer || longer && time interval is below average)
                                   VKF=3 (low)
else if (key distance is nearer && time interval is above the average)
                                   VKF =2 (medium)
else if (keys are longer and the average time interval is above the average)
                                   VKF =1 (high)
end
```

Figure 4. Virtual Keys Force Algorithm

4. Results and Discussions

KSP Data Set is used for evaluation of the result [30]. This dataset represents the typing of 103 individuals on three different words. (drizzle, jeffrey allen and pr7q1z). Each user typed the words anywhere from 7 to 503 entries (with an average of 26 entries per user). The data set contains the pressing and releasing timing of each password character. From the obtained press and release time, Dwell time, Flight Time, Di-graph and Tri graph are calculated. After calculating the features, the proposed Feature – Virtual Key force is calculated according to the algorithm shown is Figure 4 and is added to the dataset. The obtained features are preprocessed using Z-score Normalization method. The performance of the proposed feature is tested with Genetic Algorithm and Back propagation neural network. The accuracy obtained for all the three passwords with the new feature and without using new feature is tabulated below. Table 2 gives the accuracy obtained without new feature and Table 3. gives the accuracy obtained with the new feature – Virtual Key Force.

Table 2: Accuracy Obtained without VKF

Passwords	Accuracy (%)
drizzle,	89.63504
jeffrey allen	89.8893
pr7q1z	89.92806

Table 3: Accuracy Obtained with VKF

Passwords	Accuracy (%)
drizzle,	90.8759
jeffrey allen	90.7011
pr7q1z	90.43166

From the above table, it is shown that the accuracy has been improved more than 1% by introducing the new feature. The training time and testing time are also tested and given in the Figure 5 and Figure 6.

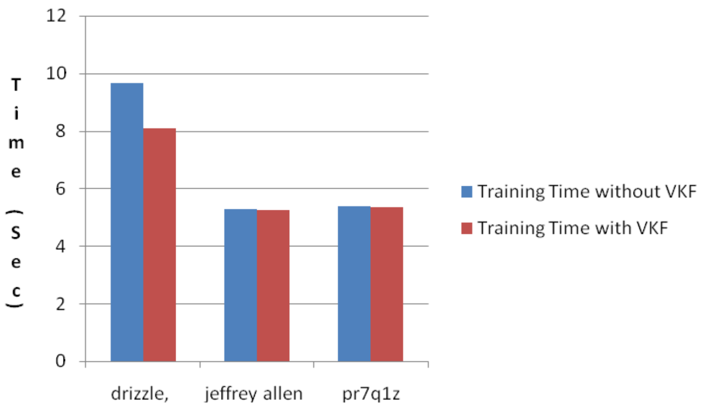

Figure 5: Training Time taken without and with VKF

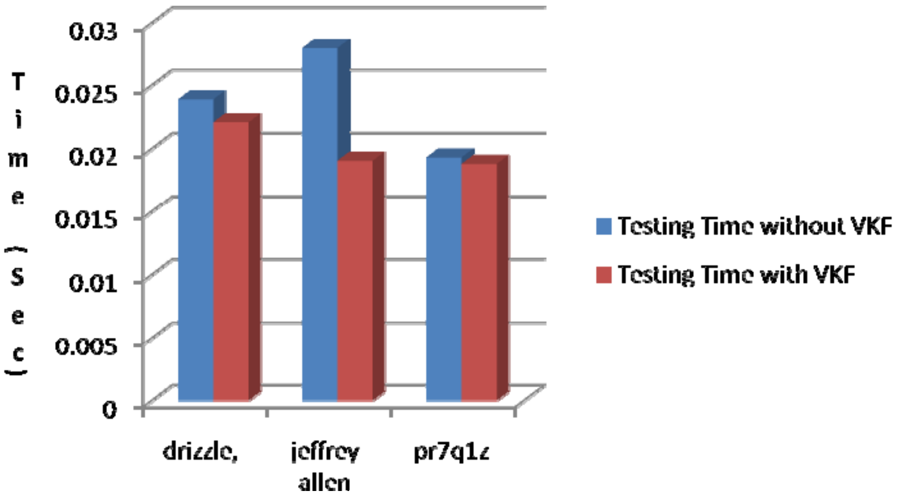

Figure 6: Testing Time taken without and with VKF

From the above figures 5 and 6, it is shown that the training and testing times are also reduced.

5. Conclusion

The new feature – Virtual Key force has been introduced which improves the accuracy and also reduces the training and testing time. The accuracy can further be improved using other Bio inspired computing techniques such as particle swarm optimization and Ant colony optimization techniques.

References

[1] Ahmed Awad E. Ahmed, and Issa Traore (2005), *Anomaly Intrusion Detection based on Biometrics*, Proceedings of 6th IEEE Information Assurance Workshop: 452- 453.

[2] Anil K. Jain, Arun Ross and Salil Prabhakar, (2004), *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.

[3] Attila Meszaros, Zoltan Banko, Laszlo Czuni, (2007), *Strengthening Passwords by Keystroke Dynamics*, IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 6-8.

[4] Benny Pinkas (2002), *Securing Passwords Against Dictionary Attacks*, Proceedings of the 9th ACM conference on Computer and communications security**,** 161 - 170

[5] Bergando et al, *User Authentication through keystroke Dynamics*, ACM transaction on Information System Security" Vol.No. 5, Nov 2002, pg 367-397

[6] Brown, M., Rogers, J. (1993), User *Identification via Keystroke Characteristics of Typed Names using Neural Networks*. International Journal of Man-Machine Studies, vol. 39, pp. 999-1014

[7] Cho et al, (2000), *Web based keystroke dynamics identity verification using neural network*, Journal of organizational computing and electronic commerce, Vol. 10, No. 4, 295-307

[8] Clarke, N. L. and Furnell, S.M. (2007), *Authenticating mobile phone users using keystroke analysis*, International Journal of Information Security, 6 (1): 1-14.

[9] Downland, P. and Furnell, S. (2004), *A long-term trail of keystroke profiling using digraph, trigraph and keyword latencies*. In proceedings of IFIP/SEC 19th International Conference on Information Security pages 275-289

[10] Enzhe Yu, Sungzoon Cho, (2004) ,*Keystroke dynamics identity verification and its problems and practical solutions*, Computers & Security

[11] Glaucya C. Boechat, Jeneffer C. Ferreira, and Edson C. B. Carvalho, Filho, (2006), *Using the Keystrokes Dynamic for Systems of Personal Security*, Proceedings Of World Academy Of Science, Engineering And Technology, Volume 18.

[12] Gunetti and Picardi, (2005), *Keystroke analysis of free text", ACM Transactions on Information and System Security*, volume 8, pages 312–347.

[13] Guven, A. and I. Sogukpinar (2003), *Understanding users' keystroke patterns for computer access security*, Computers & Security 22, 695–706.

[14] Hyoungjoo Lee, Sungzoon Cho, (2007), *Retraining a keystroke dynamics-based authenticator with impostor patterns*. Computers & Security 26(4): 300-310.

[15] John A. Robinson, Vicky M. Liang, J. A. Michael Chambers, and Christine L. MacKenzie, (1998), "*Computer User verification Using Login String Keystroke Dynamics*, IEEE transactions on systems, man, and cybernetics—part a: systems and humans, Vol. 28, No. 2.

[16] Joyce R., Gupta, G. (1990), *Identity Authentication Based on Keystroke Latencies*, Communications of the ACM, vol. 39; pp 168-176.

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

[18] Leggett, J., Williams, G., Usnick, M. (1991). *Dynamic Identity Verification via Keystroke Characteristics*. International Journal of Man-Machine Studies.

[19] Mohammad S. Obaidat, Balqies Sadoun,(1997), *Verification of computer users using keystroke dynamics*, IEEE Transactions on Systems, Man, and Cybernetics, Part B 27(2): 261-269 .

[20] Monrose, F., Reiter, M., Wetzel, S., (2001*), Password Hardening Based on Keystroke Dynamics*, IIJS, 1-15

[21] Monrose, F., Rubin, A., *Authentication via Keystroke Dynamics*, Proceedings of the 4th ACM Conference on Computer and Communications Security, p 48-56, April 1997

[22] Monrose, R., Rubin, A. (1999), *Keystroke Dynamics as a Biometric for Authentication,* Future Generation Computer Systems, 16(4) pp 351-359.

[23] Napier, R., Laverty, W., Mahar, D., Henderson, R., Hiron, M., Wagner, M. (1995). *Keyboard User Verification: Toward an Accurate, Efficient and Ecological Valid Algorithm*. International Journal of Human-Computer Studies, vol. 43, pp213-222.

[24] Obaidat, M. S., Sadoun, B. (1997). *Verification of Computer User Using Keystroke Dynamics*. IEEE Transactions on Systems, Man and Cybernetics – Part B: Cybernetics, Vol. 27, No.2.

[25] Ord, T., Furnell, S. (2000). *User Authentication for Keypad-Based Devices using Keystroke Analysis,* MSc Thesis, University of Plymouth, UK.

[26] Pin Shen Teh Teoh, A. Thian Song Ong Han Foon Neo (2007), *Statistical Fusion Approach on Keystroke Dynamics*, Third International IEEE Conference on Signal-Image Technologies and Internet-Based System.

[27] S Bleha and M S Obaidat, (1993), *Computer user verification using the perceptron,* IEEE Trans. Systems, Man, and Cybernetics, vol. 23, no. 3, pp. 900–902.

[28] Seong-soeb Hwang, Sungzoon cho, Sunghoon park, (2009), *Keystroke dynamics based authentication for mobile phones*, Computers & Security pages 85-93.

[29] Sogukpinar. I, Yalcin (2004), *User identification at logon via keystroke dynamics*, Journal of Electrical and Electronics Engineering, Vol. 4, No. 1, 995-1005

[30] http://jdadesign.net/2010/04/pressure-sensitive-keystroke-dynamics-dataset/