2011 International Conference on Asia Agriculture and Animal
IPCBEE vol.13(2011) © (2011)IACSIT Press, Singapore

User Authentication using Rhythm Click Characteristics for Non-Keyboard Devices

Ting-Yi Chang [1], Cheng-Jung Tsai [2 +], Yu-Ju Yang [1] and Pei-Cheng Cheng [3]

[1] Graduate Institute of e-Learning, National Changhua University of Education
tychang@cc.ncue.edu.tw

[2] Graduate Institute of Statistics and Information Science, National Changhua University of Education
cjtsai@cc.ncue.edu.tw

[3]Department of Information Management, Ching Yun University
Email: pccheng@cyu.edu.tw

Abstract. Since some portable computational devices such as personal digital assistants and mobile phones have no computer keyboard, keystroke dynamics-based authentication (KDA) systems which combine password knowledge with typing characteristics to enhance the security of general password authentication systems cannot successfully work. In this paper, we adopt rhythms clicked by a mouse as another identifiable factor and mouse clicks can be replaced by a stylus on non-keyboard devices, numeral buttons on mobile phones, or fingers on touch screens to enhance system portability. Experimental results showed that the rhythm clicked by a mouse is able to function as the second identifiable factor in the general password authentication systems or as the standby identifiable factor in KDA systems.

Keywords: biometrics, user authentication, keystroke dynamics, click dynamics.

1. Introduction

Password authentication is one of the simplest and most common user authentication mechanisms used to provide basic computer security. In a general password authentication system, the validity of passwords is the main identifiable factor. However, most user-defined passwords are susceptible to password guessing attacks [3][4]. To guard against unauthorized account access, biometrics deals with the identification of individuals based on users' biological characteristics [11]. Keystroke dynamics, which does not require other special devices such as fingerprint, iris or signature scanners, is one of the biometric techniques. In earlier keystroke dynamics-based systems, many classifiers are used to achieve higher system accuracy. Statistics [2][8][9] [20], neural networks [13][15], fuzzy logic [6], support vector machines [8][14], *k*-nearest neighbor [8][10], and other classifiers [5][8][17] have all been developed into *keystroke dynamics-based authentication* (KDA) systems. Since some portable computational devices such as personal digital assistants and mobile phones have no computer keyboard, KDA cannot successfully work while the enrolment phase is implemented based on a standard desktop keyboard. Even the different types of computers, such as desktop and notebook, lead to significantly different typing performance [19], and therefore will affect system accuracy. Recently Kang et al. used artificial rhythms to improve the keystroke data quality [12]. However, users in their system must remember the locations of inserting pauses in his/her password, which is not an innate typing characteristic. Therefore, a personalized rhythm click dynamics-based authentication system is proposed in this paper.

[+] Corresponding author. Tel.: +886-4-7232105; fax: +886+4+7211290.
E-mail address: cjtsai@cc.ncue.edu.tw.

In previous studies, a common mouse was used as an input device to authenticate users. Hayashi, Okamoto and Mambo utilized drawing a circle and other figures with a mouse to authenticate the identities of users, and their system obtained an *average false rate* of 0.11 [7]. Syukri, Okamoto and Mambo utilized a signature written by a mouse to collect user's biometrics data resulting in an AFR of 0.055 [18]. Unfortunately, since users are not familiar with writing a signature using a mouse, they have to practice more than eighty times to achieve more consistency in the signing. It is also difficult to obtain the same accuracy as an actual signature. Recently, Ahmed and Traore used mouse movements to authenticate users and obtained a remarkable AFR of 0.0246315 [1]. In their scheme, the users install the data collection software on their machines and conduct their usual activities without any restriction. However, the data collected per user should be over a long period of time.

According to the above discussions, an efficient and feasible system to collect users' biometric data conveniently and precisely authenticate their identities is needed. In this paper we use a biometric -the personalized rhythm- as the second identifiable factor to authenticate users. We hypothesize each person clicks a mouse in a characteristic way, and then authenticate users by these click data. The data can be simply and conveniently captured by most devices, requires little time to collect, and quickly verify identities in the authentication. In the enrolment phase, ten samples are collected from each user since the user becomes impatient if providing more than ten samples [2]. Further, a statistical-fusion classifier [16] is used to examine the usefulness of the rhythm click-dynamics authentication system based on mouse clicks.

This paper is organized as follows. The architecture of the methodology as well as the evaluation approach and the data collection are described in Section 2. The experimental results are analyzed in Section 3. Finally, Section 4 is the conclusions.

2. Methodology

In the enrolment phase of our system, the user initializes an account and clicks the target rhythm several times. While the user is clicking, the click data is captured and then the system checks the number of clicks for the target rhythm. If the number is wrong, the user will be required to click again and the wrong data will be filtered out. Otherwise, the samples are created containing the features calculated using these click data. Finally, a template as well as other related information are computed and stored in a database. In the authentication phase, an unknown user tries to access our system and is required to enter the password and click the target rhythm. Here, we assume the user knows the password and he also clicks the correct target rhythm in the experiment. In other words, our system only uses the rhythm clicking characteristic with the designed classifier to determine whether an unknown user is allowed to access the system. Since legitimate users usually fail in the first attempt for authentication [2], our system gives user a second chance if he/she fails in the first attempt.

For experimental convenience and to facilitate the accuracy of our method, our system used a fixed and common target rhythm -"Encourage with Love" in Taiwan or "Rainbow Claps" in Singapore. The beats of this rhythm are 2-3-4-2 with a total length of 11, as shown in Fig. 1. Such a fixed and common rhythm provides higher accuracy than unfamiliar rhythms. As Fig. 1 shows, the first musical note from the left is a quarter note; the third musical note from the left is an eighth note; and the sixth musical note from the left is an eighth rest. The system requires the unknown user to click the same target rhythm in the authentication phase.

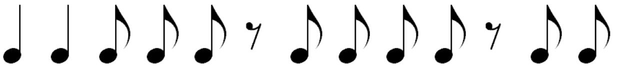


Fig. 1: The illustration of the target rhythm used in this paper

Click dynamics studies the way a user interacts with a mouse or a stylus. In this paper, a common mouse is used as an input device. A mouse event includes the mouse button down and up, and five features are produced. These features are conceptually similar to the features of keystrokes and explained as follows:

- *Down-Up* (DU) time: DU time is the interval between the same click being pressed and being released.

- *Down-Down* (DD) time: DD time is the interval between the click being pressed and the next click being pressed.
- *Up-Down* (UD) time: UD time is the interval between the click being released and the next click being pressed.
- *Up-Up* (UU) time: UU time is the interval between the click being released and the next click being released.
- *Down-Up*2 (DU2) time: DU2 time is the interval between the click being pressed and the next click being released.

DU time is a feature of any one click. DD, UD, UU, and DU2 time are the click latency features relating to any two consecutive clicks. The DU, DD, UD, UU, and DU2 time sets of the sample *s* account *a* are represented in Eq. (1), where *n* is a length of the target rhythm, and *C*(*i*) means the *i-th* click.

$$\begin{aligned}
&\mathrm{DU}_{a,\,s} = \{du_{c(1)}(a, s), du_{c(2)}(a, s), \ldots, du_{c(n)}(a, s)\},\\
&\mathrm{DD}_{a,\,s} = \{dd_{c(1)c(2)}(a, s), dd_{c(2)c(3)}(a, s), \ldots, dd_{c(n\text{-}1)c(n)}(a, s)\},\\
&\mathrm{UD}_{a,\,s} = \{ud_{c(1)c(2)}(a, s), ud_{c(2)c(3)}(a, s), \ldots, ud_{c(n\text{-}1)c(n)}(a, s)\},\\
&\mathrm{UU}_{a,\,s} = \{uu_{c(1)c(2)}(a, s), uu_{c(2)c(3)}(a, s), \ldots, uu_{c(n\text{-}1)c(n)}(a, s)\},\\
&\mathrm{DU2}_{a,\,s} = \{du2_{c(1)c(2)}(a, s), du2_{c(2)c(3)}(a, s), \ldots, du2_{c(n\text{-}1)c(n)}(a, s)\}.
\end{aligned} \tag{1}$$

In our system, the template is calculated by a statistical-fusion method. Average, maximum, minimum, standard deviation, and box plot with median, lower quartile, upper quartile, and interquartile range are used in this statistical-fusion classifier [16]. Finally, twenty-five students familiar with basic computer operation participated in our experiment. The sample collected by the 25 users click the target rhythm in accordance with their habit. Each user was asked to provide 30 samples of the target rhythm in accordance with his/her habit. The samples were collected over a period of six months to avoid the participants becoming impatient.

Four evaluation metrics, which are defined as follows, were used to evaluate our system.

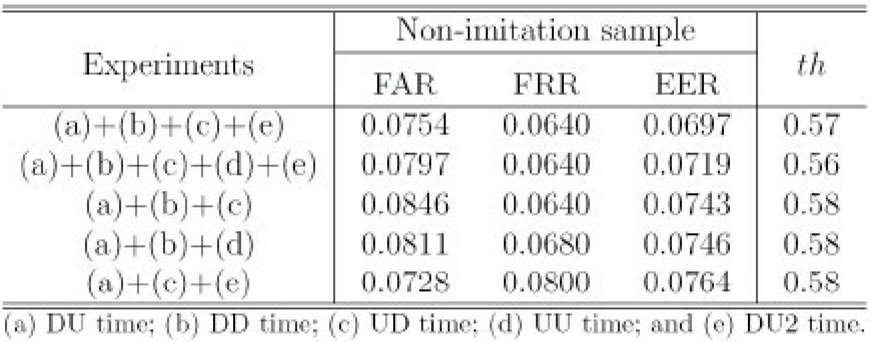
- *False Acceptance Rate* (FAR): the rate of the system accepting an impostor.
- *False Rejection Rate* (FRR): the rate of the system rejecting a legitimate user.
- *Average False Rate* (AFR): the simple average of FAR and FRR.
- *Equal Error Rate* (EER): the value at which FAR equals FRR, which is the most balanced performance index. In this paper, EER is defined as an average of FAR and FRR when both are at their closest [20].

FAR was calculated based on the results of each user attacking another. Each user took turns as a legitimate user, and other users as impostors to attack the legitimate user. Any user has a second attempt regardless of whether they were the legitimate user or impostor; therefore, the 30 samples for each user were divided into two groups. The first 15 samples were used as the major attempts and the 15 remaining samples were ready for use as the standbys if the user fails in the first major attempt. Then, a legitimate user has been attacked 24×15 times and the total number of attacks is 24×15×25. If the system accepts an attempt from an impostor, the wrong acceptance number is counted as 1. Finally, the total wrong acceptance number is divided by the total number of attacks, and the FAR is obtained. FRR was calculated by dividing 30 samples into three groups. The first 10 samples were used in the enrollment phase, and the second 10 samples and the third 10 samples were used as the major attempts and the standbys of authentication, respectively. In this situation, each user is a legitimate user and has a second attempt. Therefore, the total number of attempts is 10×25. If the system rejects an attempt from a legitimate user, the wrong refusal number is counted as 1. Finally, the total wrong refusal number is divided by the total number of legitimate invasions, and the FRR is obtained.

3. Results and Discussion

In this paper, five features are analyzed in our classifier to authenticate the identities of users. Several experiments combining the five features were performed. There is another important discovery in our experiment. We found that allowing a second attempt causes a slight increase in FAR and a marked decrease in FRR, which demonstrates the usefulness of the claim from Araujo et al. [2]. For the sake of brevity, Table 1 lists only the results of the top five EER with FAR and FRR. In Tables 1 and 2, parameter *th* is used in our classifier to determine the decision threshold and its value is between 0 and 1. If the score of a sample obtained from our classifier is greater than or equal to the decision threshold, our system considers this sample as legitimate. Table 2 lists the results of the top five AFR that are irrelevant to whether FAR and FRR are closest. As Tables 1 and 2 indicate, an experiment combining DU, DD, UD, and DU2 time has a better EER of 0.0697 and a better AFR of 0.0628 while the *th* value are 0.57 and 0.56, respectively. There are a reasonable amount of results showing the rhythm click-dynamics authentication system based on mouse clicks with the proposed classifier is feasible.

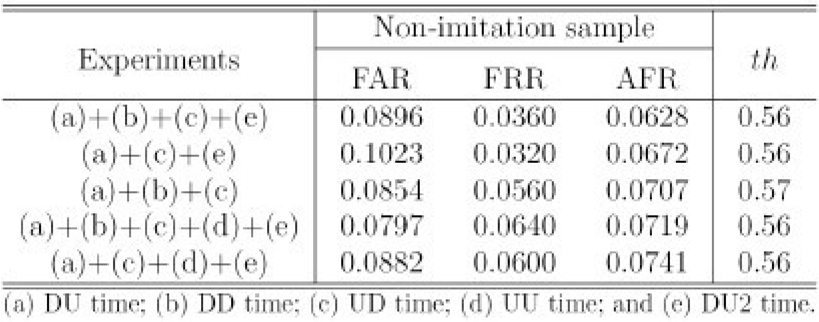
Table 1: The results of the top five EER with FAR and FRR



Experiments	Non-imitation sample			th
	FAR	FRR	EER	
(a)+(b)+(c)+(e)	0.0754	0.0640	0.0697	0.57
(a)+(b)+(c)+(d)+(e)	0.0797	0.0640	0.0719	0.56
(a)+(b)+(c)	0.0846	0.0640	0.0743	0.58
(a)+(b)+(d)	0.0811	0.0680	0.0746	0.58
(a)+(c)+(e)	0.0728	0.0800	0.0764	0.58

(a) DU time; (b) DD time; (c) UD time; (d) UU time; and (e) DU2 time.

Table 2: The results of the top five AFR with FAR and FRR



Experiments	Non-imitation sample			th
	FAR	FRR	AFR	
(a)+(b)+(c)+(e)	0.0896	0.0360	0.0628	0.56
(a)+(c)+(e)	0.1023	0.0320	0.0672	0.56
(a)+(b)+(c)	0.0854	0.0560	0.0707	0.57
(a)+(b)+(c)+(d)+(e)	0.0797	0.0640	0.0719	0.56
(a)+(c)+(d)+(e)	0.0882	0.0600	0.0741	0.56

(a) DU time; (b) DD time; (c) UD time; (d) UU time; and (e) DU2 time.

4. Conclusions

This paper examines the usefulness of the rhythm click-dynamics authentication system based on mouse clicks. For facilitating the accuracy of this paper, a fixed common rhythm which is very familiar for all participants was used. If each legitimate user adopts a personal rhythm as the target rhythm, it will significantly reduce the error rate since any impostor has to guess the target rhythm. Our experiment also has a reasonable amount of results with the classifier used in this paper, showing rhythms clicked by a mouse can act as the second identifiable factor in the general password authentication systems. Our system also increases portability. Our system can be applied to electronics with touch or numerical input pads and can also be used as the standby identifiable factor in the KDA systems to improve the security of the system.

5. Acknowledgements

This research was partially supported by the National Science Council of Republic of China under Grant No. NSC99-2221-E018-018 and NSC99-2221-E018-021.

6. References

[1] A. A. E. Ahmed and I. Traore, “A new biometric technology based on mouse dynamics,” *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 3, pp. 165–179, 2007.

[2] L. C. F. Araujo, L. H. R. Sucupira Jr., M. G. Lizarraga, L. L. Ling, and J. B. T. Yabu-Uti, “User authentication through typing biometrics features,” *IEEE Transactions on Signal Processing*, vol. 53, no. 2, pp. 851–855, 2005.

[3] T. Y. Chang, C. C. Yang, and M. S. Hwang, “Cryptanalysis of simple authenticated key agreement protocols,” *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E87-A, no. 8, pp. 2174–2176, 2004.

[4] T. Y. Chang, W. P. Yang, and M. S. Hwang, “Simple authenticated key agreement and protected password change protocol,” *Computers & Mathematics with Applications*, vol. 49, no. 5-6, pp. 703–714, 2005.

[5] M. Choras and P. Mroczkowski, “Keystroke dynamics for biometrics identification,” in *Adaptive and Natural Computing Algorithm*, pp. 424–431, Lecture Notes in Computer Science 4432, 2007.

[6] S. Haider, A. Abbas, and A. K. Zaidi, “A multi-technique approach for user identification through keystroke dynamics,” in *IEEE International Conference on System, Man, and Cybernetics*, pp. 1336–1341, 2000.

[7] K. Hayashi, E. Okamoto, and M. Mambo, “Proposal of user identification scheme using mouse,” in *Proceedings of the First International Conference on Information and Communication Security*, pp. 144–148, Lecture Notes in Computer Science 1334, 1997.

[8] S. Hocquet, J. Y. Ramel, and H. Cardot, “User classification for keystroke dynamics authentication,” in *Advances in Biometrics*, pp. 531–539, Lecture Notes in Computer Science 4642, 2007.

[9] D. Hosseinzadeh and S. Krishnan, “Gaussian mixture modeling of keystroke patterns for biometric applications,” *IEEE Transactions on Systems, Man, and Cybernetics-Part C: Applications and Reviews*, vol. 38, no. 6, pp. 816–826, 2008.

[10] J. Hu, D. Gingrich, and A. Sentosa, “A k-nearest neighbor approach for user authentication through biometric keystroke dynamics,” in *IEEE International Conference on Communications*, pp. 1556–1560, 2008.

[11] A. K. Jain, R. Bolle, and S. Pankanti, *Biometrics: Personal Identification in Networked Society*. New York, Boston, Dordrecht, London, and Moscow: Kluwer Academic, 2002.

[12] P. Kang, S. Park, S. S. Hwang, H. J. Lee, and S. Cho, “Improvement of keystroke data quality through artificial rhythms and cues,” *Computer & Security*, vol. 27, no. 1-2, pp. 3–11, 2008.

[13] H. Lee and S. Cho, “Retraining a keystroke dynamics-based authenticator with impostor patterns,” *Computers & Security*, vol. 26, no. 4, pp. 300–310, 2006.

[14] W. Martono, H. Ali, and M. J. E. Salami, “Keystroke pressure-based typing biometrics authentication system using support vector machines,” in *Computational Science and Its Applications*, pp. 85–93, Lecture Notes in Computer Science 4706, 2007.

[15] M. S. Obaidat and B. Sadoun, “Verification of computer users using keystroke dynamics,” *IEEE Transactions on System, Man, and Cybernetics-Part B: Cybernetics*, vol. 27, no. 2, pp. 261–269, 1997.

[16] C. C. Peng, T.Y. Chang, C.J. Tsai, J.W. Li, and M.L. Chiang, “A novel and simple statistical fusion method for user authentication through keystroke features”, *Journal of Convergence Information Technology*, vol. 6, no. 2, pp. 347-356, 2011.

[17] K. Revett, S. T. de Magalhaes, and H. M. D. Santos, “On the use of rough sets for user authentication via keystroke dynamics,” in *Progress in Artificial Intelligence*, pp. 145–159, Lecture Notes in Computer Science 4874, 2007.

[18] A. F. Syukri, E. Okamoto, and M. Mambo, “A user identification system using signature written with mouse,” in *Information Security and Privacy*, pp. 403–414, Lecture Notes in Computer Science 1438, 1998.

[19] G. P. Szeto and R. Lee, “An ergonomic evaluation comparing desktop, notebook, and subnotebook computers,” *Archives of Physical Medicine and Rehabilitation*, vol. 83, no. 4, pp. 527–532, 2002.

[20] P. S. Teh, A. B. J. Teoh, T. S. Ong, and H. F. Neo, “Statistical fusion approach on keystroke dynamics,” in *IEEE Conference on Signal-Image Technologies and Internet-Based System*, pp. 918–923, 2008.