View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Electronic archive of Tomsk Polytechnic University

KEYSTROKE DYNAMICS APPLICATION FOR USER AUTHORIZATION

E.S. Gorokhova, E. A. Kochegurova, E.E. Luneva
Tomsk Polytechnic University
esg8@tpu.ru

Introduction

Protection information from illegal access is becoming more and more relevant issue. User recognition often uses biometrical characteristics. Biometrics refers to metrics related to human characteristics [1-4]. Biometric identifiers are often categorized as physiological versus behavioral characteristics. The first group consists of unique characteristics which were gotten by human since a birth. For example, it might be DNA, finger-prints or iris. On the other hand, behavioral characteristics are gotten during a lifetime and can be changed due to age or external factors. Examples include handwriting, voice and gait.

Keystroke dynamics are also can be used as biometric tool for user authentication [5-6]. As a behavioral characteristic, keystroke dynamics change during a lifetime for every user. Usually it stabilizes after 6 months of work with a computer [7]. One of the advantages of using keystroke dynamics for authentication is that we can check user's password and characteristics of keystroke dynamics at the same time. Moreover, it is possible to keep monitoring of these characteristics in order to determine change of users. One more advantage is that deployment of keystroke dynamics recognition system is cheap since it doesn't require purchasing any additional devices, only keyboard is needed. Development of keystroke dynamics recognition methodology helps to improve accuracy and efficiency of user authentication systems. Keystroke dynamics include a wide range of characteristics [8-9]:

- Dwell time;
- Flight time;
- Overlapping of keys presses;
- Amount of mistakes made by user during typing;
- Rhythm;
- Typing speed;
- Features of use command keys, for example using Left or Right Shift for capitalizing letters.

Dwell time is a period, during which a key is in pressed state. It is usually measured in milliseconds.

Overlapping occurs when one key is not left and another key is already pressed. Increasing of speed leads to increasing a number of overlapping of key pressed.

Flight time is time from the moment when one key is left and the next key is not pressed yet.

Figure 1 illustrates described characteristics of keystroke dynamics. Here piece 3 mean dwell time of keys "D". Piece 2 is flight time. Grey pieces mean overlapping during typing, for example piece 1 mean overlapping of keys "G" and "O".

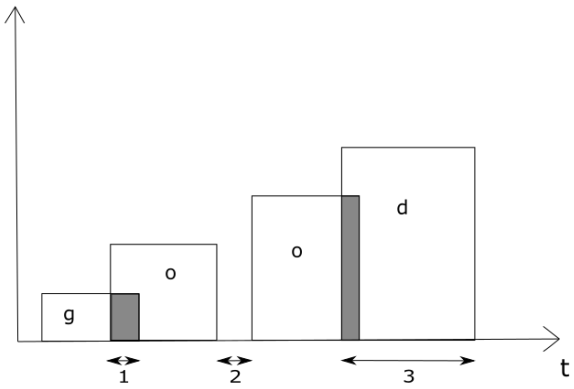

Fig. 1. Keystroke dynamics characteristics

In most cases practical researches investigate three first characteristics independently: dwell time, flight time and overlapping. Nevertheless, they all influence on each other and may identify user. That is why using vector criteria for keystroke dynamics, built from separate characteristics, make sense. This research focuses attention on making vector criteria and investigating its applicability for user recognition.

System description

Developed application consists of two components: client and server [10-11]. The client component is responsible for collecting data about user's keystroke dynamics. UI allows inputting text in this program itself or in any other application such as text editor or browser. Usually a user isn't informed about monitoring his keystroke dynamics.

The feature of this system is an opportunity to analyze any phrase, not a fixed one. Content and meaning of the phrase are not important; the only limitation is about the length, which must be more than 200 symbols. This limitation is caused by necessity to decrease statistical errors. The data are transferred between the client and the server components via TCP-sockets for security reasons. The server computes average dwell time for every key, and then determines if overlapping occurred. This information is recorded as a sample of user keystroke dynamics into database. There is an example of representation of keystroke dynamics for two users below. It shows significant divergence between them.

Table 1. Samples of keystroke dynamics

	User1		User2	
Key	Dwell time with overlapping, ms	Dwell time without overlapping, ms	Dwell time with overlapping, ms	Dwell time without overlapping, ms

A	123,77	106,85	127,75	210,81
B	90	105,5	67	88
C	100,5	105	113,42	116,25
D	131,75	174	96	196,5
E	99,42	131,5	110,85	121

Dwell time with and without overlapping is shown in the table for some keys from English keyboard layout. The database stores records about keystroke dynamics of each known user. Then a new sample comes to the server, it is added to record list of the corresponding user. In case the record list becomes too long (more than 10 samples), the oldest sample is removed from the list. This is how the first function of the server - collecting statistics about users keystroke dynamics and filling the database - is implemented.

Another function of the server is user recognition with a heuristic authentication algorithm.

Authentication algorithm

For authentication purpose, keystroke dynamics of user's input is compared with samples from the database. The following situations are possible:

The following variable parameters should be determined to create the timetable:

- User's new sample of keystroke dynamics is similar to one of the samples from the database. We call two samples similar if distance between the characteristic vectors of these samples does not exceed a certain error rate. Otherwise, these samples will be called not similar. So, if the sample is similar to one of the available, the system identifies the user and adds the new sample of keystroke dynamics to the list of records for that user in the database;
- User's new sample is not similar to any of available samples. In this case, an authentication error occurs and the user is unidentified.

Results and discussion

The experiment was made for keystroke dynamics samples of 10 different users. We asked users to type any text as they usually do. During typing the system was measuring dwell time for every key. After that the server component calculated average dwell time for each key and for every user. Then all the samples of keystroke dynamics were compared with each other, taking into account their belonging. Euclidean and Manhattan distances were calculated with respect to weight coefficients described above and also without them.

During the experiments value of error rate has been changing from 0.1 to 20 ms. In order to determine the best one, total amount FRR and FAR errors was calculated for each value.

In general, the results were quite similar for the four methods of comparing keystroke dynamics samples. Total errors amount is smaller for both analyzed distances with weight coefficients. At the same time, Manhattan distance was slightly more efficient. The best result for the algorithm in this experiment was 87,7% accuracy. That means the algorithm needs to be improved in order to increase correct identification rate.

Conclusion

In this article using of keystroke dynamics was considered as a tool of biometric authentication. The methods of samples comparison were investigated and compared in order to find the most efficient one. The application for keystroke dynamics analysis and recognition was developed. Experiments of user authentication have been made, and the results of the algorithms work were analyzed with the help of errors of the first and second kind.

The reported study is supported by the Ministry of Education and Science of Russian Federation (project #2.3649.2017/4.6).

References

1. Leggett, J., Williams, G., Usnick, M., Longnecker, M.: Dynamic identity verification via keystroke characteristics. *International Journal of Man-Machine Studies*. 35(6), 859 – 870 (1991).
2. Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., Senior, A. W. *: Guide to Biometrics*. Springer Verlag, Berlin (2004).
3. Ilonen, J.: Keystroke Dynamics. Lappeenranta University of Technology (2008).
4. Jain, A. K., Bolle, R., Pankanti, S.: *Introduction to Biometrics*, Springer Verlag, Berlin (2002).
5. Bergadano, F., Gunetti, D., and Picardi, C.: User authentication through keystroke dynamics. *ACM Transactions on Information and System Security*. 5(4), 367–397 (2002).
6. Karnan, M., Akila, M., Krishnaraj, N.: Biometric personal authentication using keystroke dynamics: A review. *Applied Soft Computing*. 11(2), 1565-1573 (2011).
7. Ivanov A.I. Neyrosetevye algoritmy biometricheskoy identifikatsii lichnosti.ó Seriya ´Neyrokompíyutery i ikh primenenieª. Kn. 15. ó M.: *Radiotekhnika*, 2004. ñ s. 22-50.
8. Olzak, T.: Keystroke Dynamics: Low Impact Biometric Verification (2006).
9. Pisani, P. H., Lorena, A. C.: A systematic review on key-stroke dynamics. *Journal of the Brazilian Computer Society*. 19(4), 573-587 (2013).
10. Kochegurova, E. A., Gorokhova, E.S., Mozgaleva, A. I.: Development of the Keystroke Dynamics Recognition System. *Journal of Physics: Conference Series*. 803 (1), (2017).
11. Stefan,D., Yao, D.: Keystroke-Dynamics Authentication Against Synthetic Forgeries. In International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom) (2010).