

Unlock A Device with Pressure and Rhythm Based Password

E. AYDEMİR, F. TOSLAK


Abstract— When people open their doors, they usually use the keys they carry in their pockets. As an alternative to these used keys, it is possible to open the doors which are authorized with RFID-enabled key holders or ID cards. But it seems that different alternatives have not been developed much. Moreover, none of them carries the sensory understanding dimension of the person and it is not possible to determine whether or not the entrance request has been made by that person. In this study, both the identification of the person and the opening of the door are ensured by considering both the stroking rhythm and the stroke force of a buttoner placed in the door. Thus, it is possible to open the door according to the person's identity and authority without carrying any object beside it, and it will have a unique original value. The milliseconds between each stroke for the stroke of the quill are recorded in the generated database. Comparison is made with the data obtained in the next stroke and the person is used for verification. In addition, the pressure data of the person is also kept in the database for each stroke and compared. In the study, the data of two different people were recorded in the system and the information of the people using the subjective button was recorded. Then, in addition to these two different people, a total of 15 people, including 13 different people, were allowed to use the system. In total, 50 door opening requests data were recorded and 87.5% success rate was obtained.

Index Terms— Rhythm, Pressure, Button, Password, Door Lock, Key Stroke.


I. INTRODUCTION

MANY DIFFERENT methods are used by people to unlock any locked device. Some of them are performed by carrying a device on people. For example, key, card, RFID keychain. Biometric solutions are also used to unlock locked devices. Fingerprint, face recognition, eye recognition, speech recognition and keystrokes are some of these. Carrying a device on people will be reduce in the future because of forgetting, loosing and being damaged reasons.

EMRAH AYDEMİR, is with Department of Computer Engineering, Kirsehir Ahi Evran University, Kirsehir, Turkey, (e-mail: emrah.aydemir@ahievran.edu.tr).

 <https://orcid.org/0000-0002-8380-7891>

FERHAT TOSLAK, is with Department of Computer Technologies, Kirsehir Ahi Evran University, Kirsehir, Turkey, (e-mail: ferhattoslak@ahievran.edu.tr).

 <https://orcid.org/0000-0003-1054-379X>

Manuscript received December 25, 2018; accepted February 06, 2019.
DOI: [10.17694/bajece.502550](https://doi.org/10.17694/bajece.502550)

The applications such as fingerprint, face recognition and eye retina, which are among the biometric solutions, cannot become widespread because they do not want to share their most special knowledge in various places. Likewise, in systems with critical data, software is used to protect confidential data and to provide locking. This software is used in computers and mobile devices and other special devices. These software use drag, move, enter PIN code, enter password, drawing pattern, fingerprint, face and voice recognition methods.

In this study, the key stroke dynamics within the biometric solutions developed among the unlocking systems was developed. An extra feature of the key stroke is considered and the stroke intensity is taken into consideration. In this way, it will not be necessary for people to carry any objects in the opening of the locked devices, and people who worry in the very special information held in fingerprint, eye and face recognition systems will be eliminated. In the literature there is also a patent that includes a comparison with a code generated from variations between hit force and stroke times in touch or touch systems [1]. Here, the person will be asked to stroke a button with a rhythm that he / she chooses. The time between each of these strokes and the force of each stroke will provide to unlock the locked system. Thus, the key stroke dynamics system in the literature will be improved and become safer and more effective. In addition, with just one button, the operation and reliability of this system will be tested and presented to the literature.

II. KEYSTROKE DYNAMICS

Computer users use their own unique rhythm while typing text with the keyboard. This method is called keystroke dynamics [2]. This method assumes that every person has the use of a keyboard in unique rhythm, just like the differences in characters in signatures. Keystroke dynamic is the data processing method that analyzes the typing in keyboard inputs. Stroke and pulling moments are considered. With the data of these moments, various algorithms are generated as a result of the calculation [4, 5]. Fig. 1 shows the graph of the key stroke and release times on the keyboard when writing the same text ("Computer") of the same person at different times. The similarity of keystroke dynamics can be easily seen from the graph. Fig. 2 shows the status of the keystroke dynamics that occur at the time when different people write the same text. Although the text is the same, it can be seen that it contains many differences.

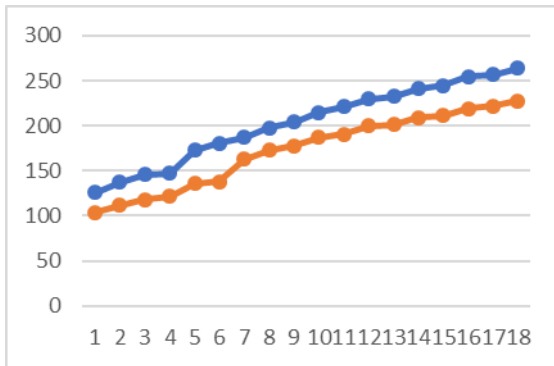


Fig 1. Same person writing the same text.

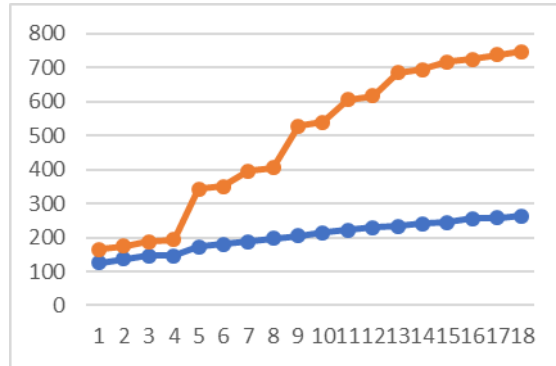


Fig 2. Different people writing the same text

Compared to other physical and biometric solutions, keystroke dynamics methods are not the most reliable identification method. Keystroke dynamics will be insufficient to become an independent biometric authentication factor. But using both the traditional applications and keystroke dynamics method will increase the security level of the unlocking systems [6]. The usability of the rhythm factor applied to mouse clicks has been investigated and it has been seen that it may be a secondary identification factor for general password applications [7, 8]. Providing a value indicating the reliability of the rhythm-based password to the user will also be useful in increasing the user's own reliability [9]. In addition to the existing password entries, the input rhythm of a given word is also used to increase the password security [10].

III. FORCE SENSITIVE KEYSTROKE DYNAMICS

The force-sensitive keystroke dynamics is a data processing method that analyzes the user's keystroke dynamics via a keyboard or a button, as well as the pressure values generated by the keystroke. Fig. 3 and Fig. 4 shows the pressure values for the force-sensitive keystroke dynamics and the time-to-break data. Even though two different people try the same rhythms, the data is different. Therefore, considering the pressure values in the keystroke dynamics, it is thought that the security level will increase even more and the person will be better acquainted.

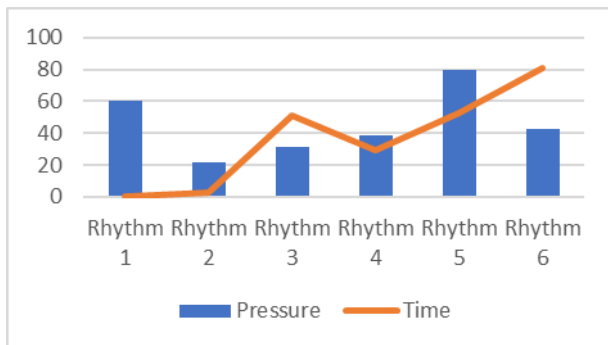


Fig 3. Pressure and time values of person A

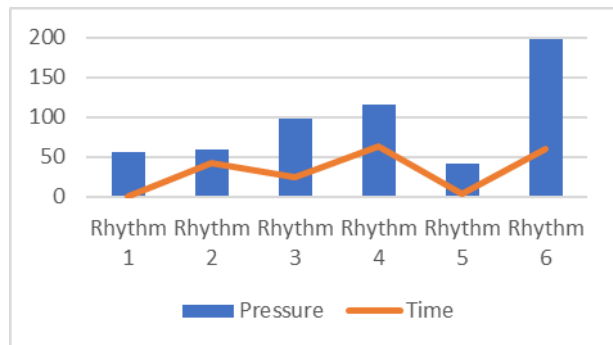


Fig 4. Pressure and duration values of Person B.

IV. DOOR LOCK DESIGN WITH FORCE SENSITIVE BUTTON

In this study, a button is designed to apply the force-sensitive keystroke dynamics method. Under this button there is a sensor that measures the pushing force and returns the pressure value. A resistor is connected to this sensor and connected to the LattePanda device with other connections. The LattePanda device comes with Windows 10 64 bit installed and also with Arduino software installed. Fig. 5 below shows the connections visually.

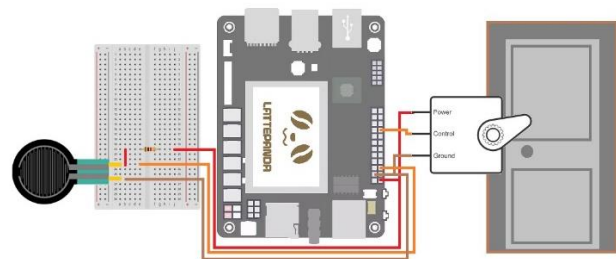


Fig 5. Door Lock Design with Force Sensitive Button.

The pressure values from Arduino were obtained with a program written in C#. One timer was added to receive data from Serialport, and the data on one port per millisecond was read and processed. The button pressure values come from the port. Data were processed with the following formulas considering the incoming values and the time of arrival.

$$\bar{t}_j = \frac{\sum_{i=1}^n t_i - t_{i-1}}{n} \tag{1}$$

$$\bar{P}_j = \frac{\sum_{i=1}^n P_i}{n} \tag{2}$$

n =number of attempts

t =duration of stroke

\bar{t} = average stroking time

j =number of rhythms

P =value of pressure

\bar{P} =average pressure

\bar{P}_j = average pressure for rhythm j .

\bar{t}_j = j . average duration for rhythm j .

In each stroke, the pressure and time values are obtained from the designed embedded system. Each stroke here is called rhythm. Values are kept in tables in a created database. The person definitions table records the highest-pressure value of each person and the duration of that stroke. Finger stroke begins to be read by the force applied to the first stroke of the finger, and as the pressure exerted by the finger on the unit area increases, the amount of force is increased. The highest force value was taken into consideration. Before registering these datas, the person is asked to try at least three times for the special stroke. The average of these trials is kept in the person definitions table. Here the number of attempts made by the person must be directly proportional to the consistency of his / her own special stroke. In other words, the higher the number of trials, the closer the values should be printed. All input requests are recorded in a table regardless of whether the entry is successful or not. Fig. 6 below shows the structure of the tables.

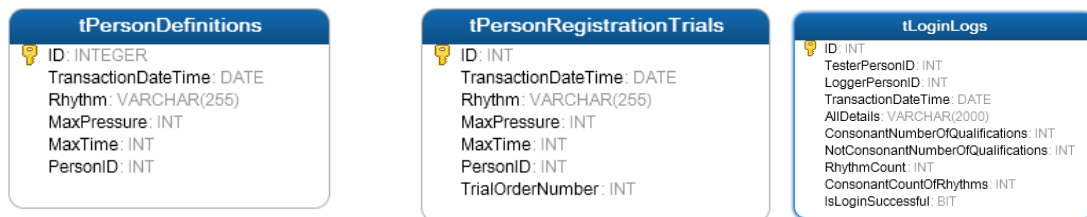


Fig 6. Database Table Designs

Here, the pressure values rise from the first touch of the finger to the completion of the touch. Therefore, the highest value between the values is the actual value of the stroke. Similarly, the time information is obtained from the first touch of the finger when stroking time is obtained but the time information is taken into consideration when the maximum pressure value is reached.

First of all, the records with the same number of rhythms are filtered from the input information registered in the input requests. Then comparisons are made with the pressure and duration information in each of these rhythms. A maximum of 25% difference between each is acceptable. If the difference is higher, a failure occurs and other conditions continue to be compared. A maximum of 10% failure is expected in the total number of events. If a higher failed situation is obtained, no entry is allowed.

V. RESULTS

In the study, identification data of two people were recorded and transactions were made. In addition to the real people, 13 people tried to do the same by attempting the identification stroke of these two people. This total of 13 people has made 29 attempts. The real people made 21 attempts. Table I below shows the data for this situation.

TABLE I
OVERVIEW OF DATA

Informations	Number
Number of total people	15
Number of real people	2
Real People Trial Count	21
Other people Trial Count	29

Two people recorded their strokes dynamics primarily in the system. While there are five rhythms in the strokes dynamics of an EA-coded person, there are four rhythms in the strokes dynamics of an FT-coded person. The data and data generated from these strokes are as follows on Table II and Fig. 7.

TABLE II
The Force-sensitive Stroke Dynamics Data of the People Registered to the System

Rhythm	Intensity	Duration	Name of Person
1. rhythm	89	0	EA
2. rhythm	56	73	EA
3. rhythm	87	31	EA
4. rhythm	87	50	EA
5. rhythm	134	81	EA
1. rhythm	74	0	FT
2. rhythm	105	53	FT
3. rhythm	99	52	FT
4. rhythm	45	123	FT

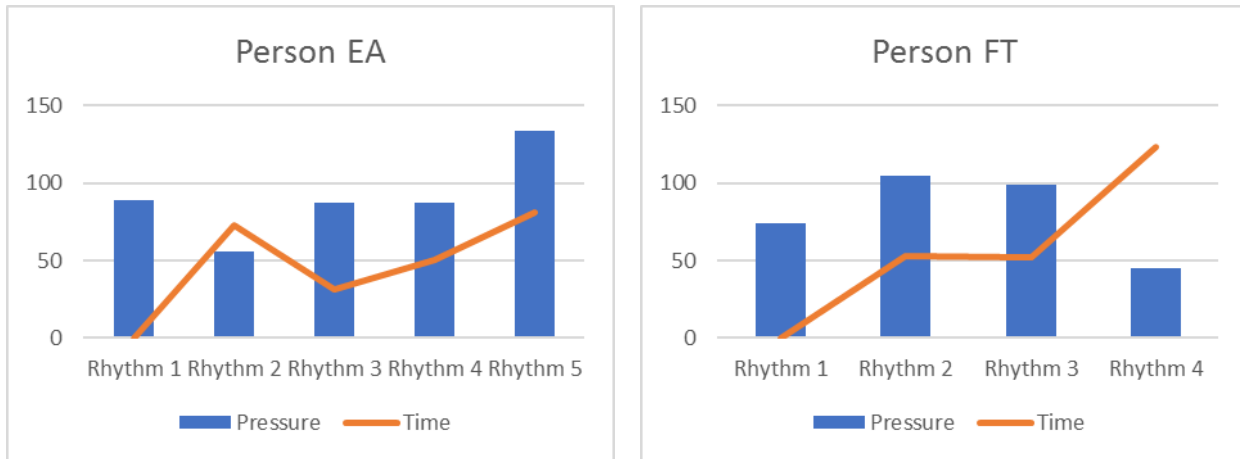


Fig 7. Force Sensitive Stroke Dynamics Data Chart of Registered People in the System.

The key strokes dynamics of two people with EA and FT codes differ from each other in terms of intensity and duration, while the number of rhythms is five in one and four in the other. Therefore, it is checked whether the number of rhythm matches. The number of rhythms is not negative and the

demand is negative. The Table III shows the data of people attempting to login. These data include both natural people and strokes, and try to match the results. In addition, several people tried to teach how they stroked and experimented.

TABLE III
Trial Data of People

ID	Person Who Try	Real Person	Process Date	Number of Correct Attributes	Number of Incorrect Attributes	Number of Rhythm	Number of People who Match Rhythm	Input Success Status.
1002	EA	EA	03.04.2018 10:29	8	1	5	1	1
1003	FT	FT	03.04.2018 11:17	7	0	4	1	1
1004	FT		03.04.2018 11:17	0	0	5	1	0
1005	FT		03.04.2018 11:18	0	0	5	1	0
1007	FT		03.04.2018 11:19	0	0	6	0	0
1008	FT		03.04.2018 11:20	0	0	5	1	0
1009	FT		03.04.2018 11:21	0	0	8	0	0
1010	FT	FT	03.04.2018 11:21	6	1	4	1	1
1011	FT		03.04.2018 11:22	0	0	5	1	0
1013	EA	EA	03.04.2018 11:23	9	0	5	1	1
1014	FT		03.04.2018 11:25	0	0	6	0	0
1017	FT		03.04.2018 12:37	0	0	5	1	0
1018	FT	FT	03.04.2018 12:38	6	1	4	1	1
1019	EA		04.04.2018 11:09	0	0	5	1	0
1020	EA	EA	04.04.2018 11:09	8	1	5	1	1
1021	EA	EA	04.04.2018 11:11	9	0	5	1	1
1022	KAK		04.04.2018 11:12	0	0	5	1	0
1023	KAK		04.04.2018 11:13	0	0	5	1	0
1024	KAK	EA	04.04.2018 11:13	8	1	5	1	1
1025	MÖ		04.04.2018 11:14	0	0	5	1	0
1026	HÇ		04.04.2018 11:16	0	0	5	1	0
1027	İY	EA	04.04.2018 11:16	8	1	5	1	1
1028	EA	EA	04.04.2018 11:17	9	0	5	1	1
1029	FA		04.04.2018 11:17	0	0	5	1	0
1030	FA		04.04.2018 11:18	0	0	4	1	0
1031	FA	EA	04.04.2018 11:18	8	1	5	1	1
1032	EA	EA	04.04.2018 11:19	8	1	5	1	1
1033	FT		04.04.2018 11:20	0	0	8	0	0
1034	ŞÖ		04.04.2018 14:44	0	0	2	0	0
1035	ŞÖ		04.04.2018 14:45	0	0	3	0	0
1036	BT		04.04.2018 14:45	0	0	5	1	0
1037	BT		04.04.2018 14:45	0	0	5	1	0
1038	EA	EA	04.04.2018 14:46	8	1	5	1	1
1039	HCP		04.04.2018 15:09	0	0	8	0	0
1041	EA	EA	04.04.2018 15:10	8	1	5	1	1
1042	HCP		04.04.2018 15:10	0	0	5	1	0

When the above table is examined, it has been seen that the total of 50 attempts from 32 attempts failed due to various reasons such as rhythm incompatibility. EA-coded person's own attempt to perform an experiment with eight deviations in a part of the success of the rhythm despite the high level of deviation despite the failure seems to be failing. This means that 87.5% success has been achieved. Again, FT coded person's three of the three attempts were successful. However, as a result of the EA-coded person's strokes dynamics, all of the 22 entry attempts of the people were able to capture the number of rhythms and failed because they could not approach the sensitivity and intensity of the stroke. 10 experiments did not catch the number of rhythms. Six people were shown the accuracy and severity of strokes and their experiments were successful.

VI. CONCLUSION

Various methods such as voice, face recognition and fingerprint reading used in the data entry offer distinctive access to people. However, the use of such systems may not be sufficient because of cost and being insufficient alone the result of some disadvantages. In this study, the password entry in the access systems which are actively used today is taken into consideration. These password entries are made through a touch screen or physical key systems of numerical or alphabetical values. In this study, it is discussed to unlock a locked system with a single button, considering both the stroking force and the rhythms generated by the times between the strokes. As a result of the study, it was seen that the people who registered in the system had repeated their stroking style very well and others could not achieve success either because of the stroke time or the stroke force. It is seen some people achieve success by looking carefully or being thought and some people did not achieve success although they were thought several times. In the literature, there is a patent intended rhythmized strokes which considered the keystroke duration differences. [11]. In this patent study, similar to the study here, the vector graphics consisting of time between keys are compared and processed. However, the impact force is not considered. In addition, another application of the study with a single button with the stroke rhythm validation study was performed and 83.2% accuracy was achieved. 19.4% of those who hear the stroking, copied successfully the shape of the stroke [12]. In this study, the accuracy rate is 87.5%. In another study, a similar situation was adapted to mobile applications and proved to be very reliable [13, 14]. Again, in mobile applications, the error rate was reduced from 13% to 4% by applying rhythm-based keystroke dynamics to the password entries [15]. The system presented in this study may not be as cheap as relying only on the rhythm of keystroke dynamics because of the need for extra hardware [16-17], but it appears to directly affect the reliability coefficient.

It would be useful to apply this study to more diverse user groups and to test for more recorded force-sensitive keystroke dynamics when there are contact data. It is thought that the comparison of different studies to be made by changing the threshold value and the reliability of such studies will be compared.

REFERENCES

- [1] G.J. Anderson. U.S. Patent No. 6,509,847. Washington, DC: *U.S. Patent and Trademark Office*. 2003.
- [2] Y. Zhong, Y. Deng, A.K. Jain. "Keystroke dynamics for user authentication", 2012 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW 2012). Rhode Island, USA, 2012.
- [3] M.S. Obaidat, B. Sadoun. "Keystroke dynamics-based authentication. Biometrics". *US: Springer*, 1996, pp 213-229.
- [4] R. Giot, M. El-Abed, C. Rosenberger. "Keystroke dynamics with low constraints svm based passphrase enrollment". In *Biometrics: Theory, Applications, and Systems*, 2009. BTAS'09. IEEE 3rd International Conference on IEEE. 2009.
- [5] S.S. Bender, H.J. Postley. U.S. Patent No. 7,206,938. Washington, DC: *U.S. Patent and Trademark Office*. 2007.
- [6] P.S. Teh, A.B.J. Teoh, C. Tee, T.S. Ong. "Keystroke dynamics in password authentication enhancement". *Expert Systems with Applications*, vol. 37. 12, 2010, pp 8618-8627.
- [7] T.Y. Chang, C.J. Tsai, Y.J. Yang, P.C. Cheng. "User authentication using rhythmic click characteristics for non-keyboard devices". In *Proceedings of the 2011 International Conference on Asia Agriculture and Animal IPCBEE*, Singapore, 2011.
- [8] T.Y. Chang, Y.J. Yang, C.C. Peng. "A personalized rhythm click-based authentication system". *Information Management & Computer Security*, vol. 18. 2, 2010, pp 72-85.
- [9] D.L. Ashbrook, F.X. Lin, S.M. Whtie. *U.S. Patent Application* No. 13/092,383, 2012.
- [10] Y.V. Fedorova, T.R. Ruddy, M.S. Nunuparov. U.S. Patent No. 7,536,556. Washington, DC: *U.S. Patent and Trademark Office*, 2009.
- [11] G.R. Hird. *U.S. Patent Application* No. 13/484,836, 2013.
- [12] J.O. Wobbrock. "Tapsongs: tapping rhythm-based passwords on a single binary sensor". In *Proceedings of the 22nd annual ACM symposium on User interface software and technology*. New York, USA, 2009.
- [13] Y. Chen, J. Sun, R. Zhang, Y. Zhang. "Your song your way: Rhythm-based two-factor authentication for multi-touch mobile devices". In *Computer Communications (INFOCOM)*, 2015 IEEE Conference on. Kowloon, Hong Kong, 2015.
- [14] J.D. Lee, Y.S. Jeong, J.H. Park. "A rhythm-based authentication scheme for smart media devices". *The Scientific World Journal*, vol. 2014, 2014.
- [15] S.S. Hwang, S. Cho, S. Park. "Keystroke dynamics-based authentication for mobile devices". *Computers & Security*. vol. 28. 1-2, 2009, pp 85-93.
- [16] T. Tuncer, and Y. Sönmez. "Block based data hiding method for images." *European Journal of Technique* 7.2 (2017): 85-95.
- [17] F. Cherifi, B. Hemery, R. Giot, M. Pasquet, C. Rosenberger. "Performance evaluation of behavioral biometric systems". In *Behavioral Biometrics for Human Identification: Intelligent Applications*, 2010, pp 57-74.

BIOGRAPHIES

EMRAH AYDEMİR Elazığ, in 1987. He received the M.S. degrees in computer teaching from the University of Elazığ Firat, in 2012 and the Ph.D. degree in informatics from Istanbul University, Turkey, TR, in 2017.



From 2012 to 2015, he was an Expert with the Istanbul Commerce University. Since 2017, he has been an Assistant Professor with the Computer Engineering Department, Kirsehir Ahi Evran University. He is the author of three books, more than 10 articles, and more than 40 conference presentation. His research interests include artificial intelligence, microcontroller, database and software.



FERHAT TOSLAK Karaman, in 1987. He received the B.S. in computer teaching from the University of Suleyman Demirel, Isparta, in 2010 and he is student in computer engineering from Inonu University, Turkey, TR.

From 2011 to 2016, he was a Research Assistant with the Sirnak University. Since 2016, he has been a Lecture with the Computer Technology Department, Kirsehir Ahi Evran University.