Intelligent Pressure-Based Typing Biometrics System

Azweeda Dahalan[1], M.J.E Salami[1], W.K. Lai[2], and Ahmad Faris Ismail[3]

[1]Mechatronics Dept. Faculty of Engineering,
International Islamic University Malaysia (IIUM),
Jalan Gombak, 53100 Kuala Lumpur Malaysia
aweedd@yahoo.com
momoh@iiu.edu.my
[2]Technology Research Group MIMOS Bhd.,
Technology Park Malaysia, 57000 Kuala Lumpur, Malaysia
lai@mimos.com
[3]Faculty of Engineering
International Islamic University Malaysia (IIUM),
Jalan Gombak, 53100 Kuala Lumpur Malaysia
faris@iiu.edu.my

Abstract. The design and development of a real-time enhanced password security system, based on the analysis of habitual typing rhythms of individuals, is discussed in this paper. The paper examines the use of force exerted on the keyboard and time latency between keystrokes to create typing patterns for individual users. Pressure signals which are taken from the sensors underneath the keypad are extracted accordingly. These are then used to recognize authentic users and reject imposters. An experimental setup has been developed to capture the pressure signal information of the users' typing rhythm. Neuro-fuzzy system is employed as the classifier to measure the user's typing pattern using the Adaptive Neural Fuzzy Inference System toolbox (ANFIS) in MATLAB.

1 Introduction

Security of an information system depends to a large extent on its ability to authenticate legitimate users. Other factors, such as the ability of the information system to withstand attacks of various kinds are also important. Confidence in its ability to provide adequate authentication is, however, waning. This is largely due to the wrongful use of passwords by many users.

In this paper, the development of hardware and software methodology that improves security by using pressure-based typing-biometrics has been discussed. This is based on the conventional password or PIN system with an extra dimension of keystrokes dynamic; time latency, pressure exerted on the keyboard and the consequence analysis of the user keystrokes' patterns. Each user has a unique way of using the keyboard to enter a password; for instance, each user types the characters that constitute the password at different pressure and/or speed. Not only must an

M.Gh. Negoita et al. (Eds.): KES 2004, LNAI 3215, pp. 294–304, 2004.

intruder know the correct password using this technique, but he or she must also be able to replicate the amount of pressure, rate of typing and time intervals between each key pressed to gain access to the information. A neuro-fuzzy based classifier is proposed here for measuring the user typing biometrics. The combination of both neural network and fuzzy logic mechanism is needed to increase the system's ability in learning and making decision on pattern matching. The hardware design that has been developed generates the pressure signal from the sensors placed underneath the keypad.

This paper describes the design and development of the enhanced password security system through pressure-based typing biometrics. The system that has been developed is used to verify authentic users and reject imposters. Experiment has been conducted to examine the acceptance rate of authorized user and rejection rate of imposters.

2 Biometric Systems

The term 'biometrics', refers strictly speaking to a science involving the statistical analysis of biological characteristics [5]. In this application, biometrics is used in the context of analyzing human characteristics for security purposes. In general, biometric authentication procedures use the features of an individual that are unique to that individual in order to identify him or her, e.g. fingerprint or iris. Similarly, typing biometrics uses the individual unique typing pattern or behavior to separate an authentic user from an imposter. The action of typing the password can be analyzed with respect to its physiological characteristics. The keystrokes pressure, the latency time between keystrokes, key displacement and key displacement duration are some of the quantifiable components [6].

Concepts of Typing Biometrics

The typing biometric that has been developed is based on the current password system with an extra dimension of keystrokes dynamics. Not only must an intruder know the correct password using this system, but the user must also be able to replicate the pattern of the force exerted and the rate of time interval of each key pressed to gain access to the system. It is most likely that, even if an unauthorized person is able to guest the correct password, they will not be able to type it with the proper rhythm unless they have had the ability to hear and memorize the correct user keystrokes.

In our approach, when a new user requests access to the system, or when an existing user's password is expired, the access-control system asks the user to type in the user login and a new password. The system then asks the user to re-enter the user login and password to verify the previous inputs. Based on the typing patterns displayed on entering and re-entering the information, the typing biometrics methodology computes a typing template for the user. This user identification would then be saved with the associated template, along with the normal user login and password pair.

On subsequent attempts to access the system, the user goes through the normal password authentication procedure that is, entering the user login and password. At the same time, the system monitors the user's typing patterns and computes a typing template based on the user login and password just entered. It then compares this template with the template previously determined for this user. If the new password and typing template, match those saved by the authentication mechanism, the system grants access to the user.

If the password does not match, the normal password-authentication mechanism, without consulting the biometric component, will reject the user or ask the user to re-enter the authentication information. If the password does match, the biometric component will provide a supporting recommendation that verifies the legitimate user.

If the user login and password are correct, but the new typing template does not match the reference template, the security system has several options, which will be devised accordingly. A typical scenario might be that the system advises the network administrator that the typing pattern for a newly entered user login and password is not what the system expects it to be and that a security breach might be possible. The security administrator then closely monitors the session to ensure that the user does no unauthorized activity. Figure 1 illustrates the basic process for the proposed system.

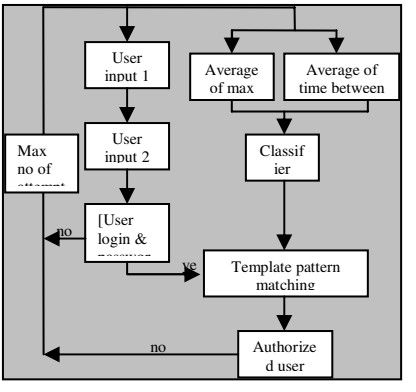

Fig. 1. Reinforced Password Authentication With Supporting Typing Biometrics

3 System Design

The overall system block diagram is shown in Figure 2 above. The alphanumeric keyboard with the additional pressure sensors, measures the user's biometric data during the process of identifying oneself. The data received are then passed to the LabView data capture system for further processing. The intelligent classifier will then do the recognition process. To make the recognition task possible, the reference value of each user's biometric data is stored in the local database.

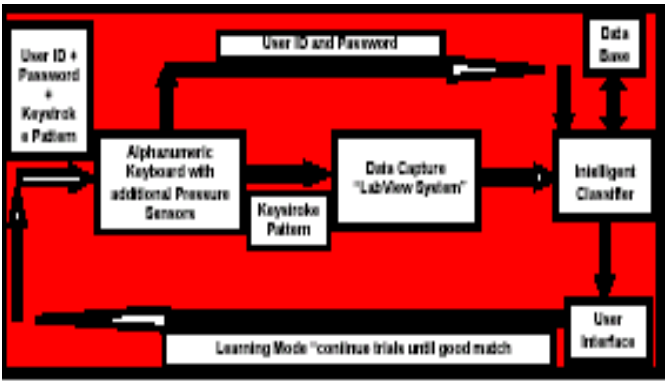

Fig. 2 . Overall System Block Diagram

Input Processing

The hardware design of the system has been carried out to achieve desired results with minimal hardware component utilization. The DAQ capture system constitutes of sensors, DAQ hardware, interface card and signal conditioning circuit in addition to the PC unit. The biometric sensors of the system are the Flexiforce Force sensors and these can also provide more specific information than just the force applied, hence using data acquisition and analysis one can examine each signal pattern and monitor the time duration which will enhance the system sensitivity and precision. The system uses the circular buffer technique for data acquisition whereby data is continuously acquired into a circular acquisition buffer at the same time that the VI reads the acquired data and processes it. The DAQ hardware has been configured in LabView to begin taking data when the incoming signal is on the rising slope and when the amplitude reaches 1.2V, signal is initiated on the keyboard.

The software design for the system is comprises the following parts:

(i) Graphical User Interface

The GUI of the system is developed with JAVA programming language. Users would have to train the system with the typing patterns. Once the system has been trained, it may then be used to authenticate users.

(ii) Login and Password (Enrolment)

A simple graphical user interface had been developed using MATLAB GUI(Graphical User Interface), to capture the user's login and passwords. The data captured are saved and will be transferred to the database and the intelligent classifier.

(iii) Intelligent Classifier

The pattern recognition process of the system is done by the intelligent classifier. Neuro-fuzzy system is employed as the classifier which is developed using Adaptive Neuro Fuzzy Inference System (ANFIS) from Matlab software toolbox.

(iv) Database

The system database is developed in the MySQLadmin Ver.4 using the text file format.

4 Experimental Setup

To determine the efficiency of this typing-biometrics authentication system, an experiment has been performed to satisfy these objectives:

- How successful does the system confirm that a user is the authorized person (acceptance rate)?
- How successful does the system identify an impostor (rejection rate)?

Basically, each user had to register as the authorized user by entering his or her user login and password information in the experimental system. It is required that the users enter passwords of 4 or more digits. It has been found that a user's initial typing pattern is very fuzzy and inconsistent for each attempt. For the system to be effective, it had to obtain a typing template, for reference purposes, that truly reflect the user's typing pattern. So the users would be given sufficient time to get used to their typing rhythm for their selected passwords until the typing patterns are stabilized into a recognizable pattern so that the database could be built.

After the database has been built to achieve the objectives, the system is tested to the other (public) users to access. To test for the first objective of the project, the authorized user is required to enter their authentication information in the session while for the second objective; we had the public user (impostor) to type in the authorized user's authentication information. The performance of the biometric system will be discussed later by observing the 'acceptance rejection rate' obtained from the experiment.

5 Data Analysis and Result

Based on the analysis of the data collected, some interesting observations are noted. Here, it was realized that some of the users themselves are not consistent. This inconsistency leads to two major problems: firstly, the inconsistent accounts were having a high number of unauthorized accesses as compared to the others. Secondly, as the pattern is very 'random', to the extent that the user could not get access to his/her account.

Since the typing biometric is a behavioral technique, there are many internal and external factors that can affect the typing pattern thus causing inconsistencies. One of these is the mood of the user when typing. Since the pattern depends on mood, the typing pattern would be different for happy, sad, upset or nervous individual. Typing skills is another factor. A skilful typist usually will not be affected much by their moods, as compared to non-skilful ones. The physical position of the user while typing can also obviously changes the keystrokes pattern typed. Therefore, it is also important that these external factors be supervised and controlled to get a consistent keystrokes pattern.

A signature or a component of a signature is visualized using the software FAMOS, by plotting the pressure value (voltage) versus the time from the computer system. The peak-point in the plot represents each keystroke pressed. A sample curve for a user with password is shown in Figure 3 and the training set comprises 11 trials recorded during the training phase is as shown in Figure 4.

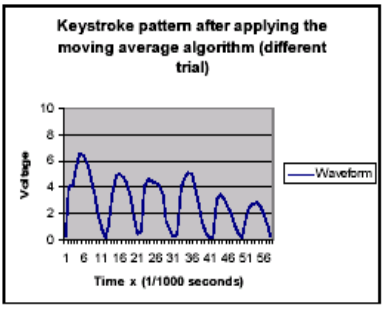

Fig. 3. Pressure Pattern for One Password

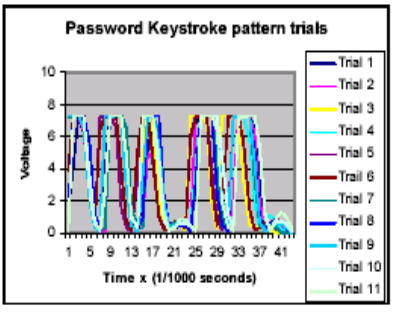

Fig 4. Training database of 11 trials for one password

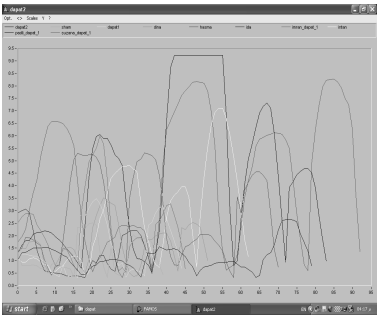

Fig 5. The Typing Pattern of 10 Public Users and User 1

From the Figure 4 above, it can be observed that a user has a consistent typing rhythm, where, a general pattern is easily recognizable from the graph obtained. From Figure 5, it can be observed that when the public users (impostors) attempt to access User 1 account, the patterns generated were far from being similar to the expected one.

6 Neuro-Fuzzy Classifier

The main objective of having neuro-fuzzy system is to automatically create or improve fuzzy system by means of neural network methodology. Neural network can be trained to capture the behavior and adapt to change of the human expert while controlling a system. In this case, the network mimics the system input-output mapping without providing any explanation to its operation. The benefit to have such system is its interpretability even after the training. The system can perform inferencing and able to make decision. It is also considered as model free system, since it doesn't require a mathematical model of the system.

Fuzzy Inference System (FIS)

Since the objective is to uniquely classify the user typing patterns, the output will be the classification of these patterns. This will be done along with a password to differentiate any user.
FIS uses two inputs to classify users' keystrokes patterns.

i) The average amount of force exerted on each button pressed.
ii) The time duration of pressing a key, in other words the amount of time a user takes to press and release button when typing, measured in clock cycles.

Based on the experimental setup, most of the pressure exerted by very highly experienced user is less than that of the less experienced user. The typing biometrics methodology uses these sets: very short (VS), short(S), moderately short (MS) and somewhat short (SS). The time interval between successive characters might be somewhat short for an inexperience user or very short for the experience user. Hence, the same sets as for the pressure is applied for the time interval. Regarding the output, the classification might be low for typing patterns displayed by inexperienced user or very high patterns displayed by an experience user. The output of the FIS is an array of constants, which after fine-tuning has resulted in the Fuzzy Associative Memory (FAM) table shown in Table 1.

Table 1: FAM Table

	VS	S	MS	SS
VL	1	0.90	0.55	0.25
L	0.95	0.875	0.35	0.20
ML	0.75	0.50	0.30	0.09
SL	0.65	0.40	0.1	0.01

ANFIS Training

The two ANFIS parameter optimization method options available for FIS training are hybrid (the default, mixed least squares and backpropagation) and backpropagation. The Error Tolerance is used to create a training stopping criterion, which is related to the error size. The training stops after the error remains within this tolerance. The

error tolerance is set to 0 since we don't know how the training error is going to behave, hybrid method for the parameter optimization and the number of training epoch to 100.

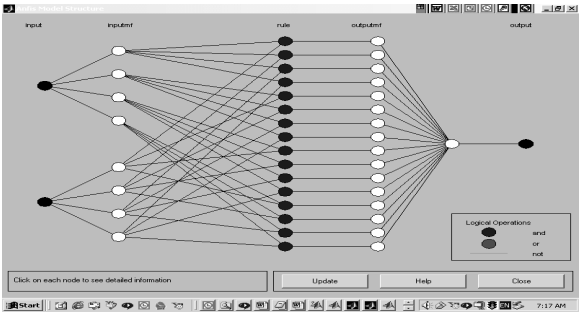

Fig. 8. ANFIS Model Structure

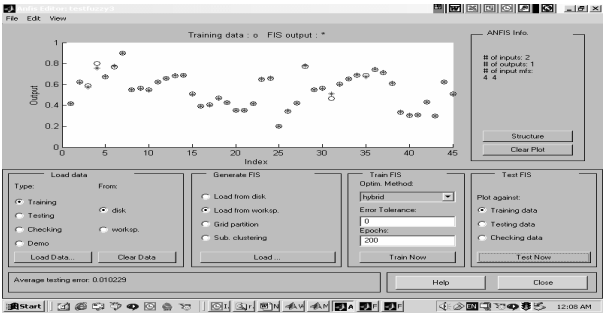

Fig. 9. Training data vs Fuzzy output after training

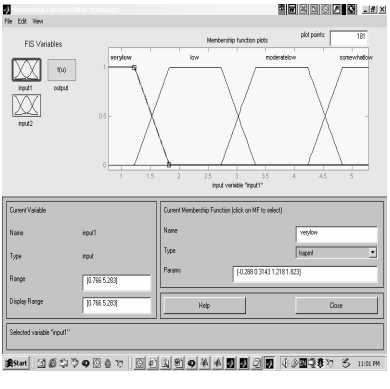

Fig. 10. Final Membership Function for Pressure

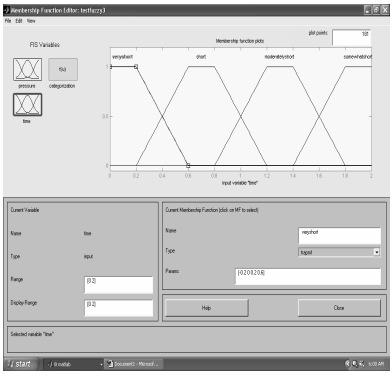

Fig. 11. Final Membership Function for Time

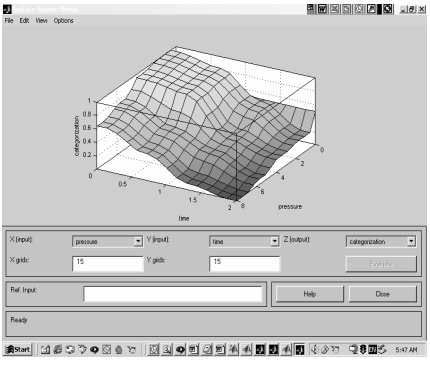

Fig. 12. Surface Output for FIS after Training

The training error is the difference between the training data output value, and the output of the fuzzy inference system corresponding to the same training data input value, (the one associated with that training data output value). The training error records the root mean squared error (RMSE) of the training data set at each epoch. The model structure represents the graphical representation of the Fuzzy Inference System input/output structure after being loaded into the ANFIS toolbox. Testing of training data against the trained FIS is done as shown below. The final result is a good fit of the original data.

FIS Membership functions after ANFIS training

Table 2. below shows the authentication information and the authentication system's performance. The third column represents the extent to which the system successfully identified the authorized user's typing patterns as belonging to the user. While the fail-rejection rate column shows the degree to which the system failed to reject the unauthorized user.

No of user	User ID	User Password	Acceptance Rate	Fail-Rejection Rate
User 1	jamal	jamal2	72	4
User 2	aswad	kadoko	80	0
User 3	azizul	sayapo	78	2
User 4	dillah	fafada	71	4
User 5	huss	asdhjk	70	4
User 6	ina	poltas	75	1
User 7	linda	1aslop	70	3
User 8	riza	kadoka	77	0
User 9	nurul	batamm	80	0
User 10	yon	1234ty	75	5

7 Conclusion and Recommendation

A system and algorithm for biometrics authentication based on pressure patterns has been discussed. The system is composed of pressure pattern acquisition, signal preprocessing, feature extraction and classifier design. The major part of the experiment was focused on collecting and identifying training data which consist of the pressure pattern and time duration, a necessary step for developing a neuro-fuzzy training scheme. The training data should be well distributed to prevent spurious ANFIS surface. In general, this type of modeling works well if the training data presented to ANFIS for training (estimating) membership function parameters is fully representative of the features of the data that the trained FIS is intended to model. For the result of training data versus the trained FIS output, the final result is a good fit of the original data. The trained FIS captured the features of this data set very well. Sometimes, the error is sufficiently large to indicate that either more data are needed for training, or to modify the membership function choices (both the number of membership functions and the type). The results of this study are strong indication that the neuro-fuzzy technique is significantly better than that of fuzzy logic system classifier. Combining fuzzy logic with neural network could increase the system's ability to learn the user's keystrokes patterns. The research results show that the system can identify authorized and unauthorized users. Various conditions, however, might influence its accuracy.

The results are only a first attempt to realize the application of password authentication through neuro-fuzzy pressure-based typing biometric system; further research is necessary. First, the hardware part of the system can be improved by designing a more ergonomic keyboard structure and secondly online training and testing processes can be applied for the software part which will give reliable and more accurate result.

References

1. William G.De Ru, Jan H.P. Eloff, "Enhanced Password Authentication through Fuzzy Logic", IEEE Expert 12(6): 38-45 (1997).

2. Wong, Fadhli M.H, Ainil Sufreena M.S., A. Faris, W.K. Lai, Ong C.S, "Enhanced User Authentication Through Typing Biometrics with Artificial Neural Network and K-Nearest Neighbor Algorithm" , Proc. 35th Asilomar Conference on Systems, Signal and Computers California USA, 1-3 , 2002.
3. Zhu Yong, T.Tan, Wang Y.H, "Biometric Personal Identification Based on Iris Patterns", National Laboratory of Pattern Recognition, Beijing, 1999.
4. Kwan H.K., Cai Y., "A Fuzzy Neural Network and its Application to Pattern Recognition", IEEE Transactions on Fuzzy Systems, Vol. 2, No.3, August 1994.
5. Garzon M.H, P. Ankaraju, Evan D., R. Kozma, "Neurofuzzy Recognition and Generation of Facial Features in Talking Heads", Computer Science, Memphis.
6. S.R. Jang, "ANFIS: Adaptive Network Based Fuzzy Inference Systems (1993)," IEEE Transactions on System, Man and Cybernatics 23:3, 665-685.
7. Jang, J.S., and Gulley N., "Fuzzy Logic Toolbox for use with MATLAB", the Mathworks, INC. Natick, MA, 1995.
8. Jang, J.S., and Sun C.T., "Neuro-Fuzzy Modeling and Control", Proc. Of the IEEE, Vol.83, No.3, March 1995, 378-406.
9. Chin T.L. and Lee George C.S, "A Neuro-Fuzzy Synergism to Intelligent Systems", Prentice Hall, 1995, 661-670.
10. Lefteri H.T, Robert E. U., "Fuzzy and Neural Approaches in Engineering", John Wiley & Sons, Inc. 1997, 471
11. J.C. Bezdek and S.K. Pal, Eds. "Fuzzy Models for Pattern Recognition", Piscataway, NJ:IEEE Press, 1992.
12. A. Kandel, "Fuzzy Techniquess in Pattern Recognition". New York: Wiley, 1982.
13. T. Yamakawa and S. Tomoda, "A Fuzzy Neuron and its Application to Pattern Recognition", in Proc. Third Int. Fuzzy System Associat. Congress Japan, 1989, pp: 30-38.