Keystroke pressure based typing biometrics authentication system by combining ANN and ANFIS-based classifiers

Conference Paper · April 2009

DOI: 10.1109/CSPA.2009.5069216 · Source: IEEE Xplore

Hasimah Ali
Universiti Malaysia Perlis

Momoh Salami
International Islamic University Malaysia

2009 5th International Colloquium on Signal Processing & Its Applications (CSPA)

Keystroke Pressure Based Typing Biometrics Authentication System by Combining ANN and ANFIS-Based Classifiers

Hasimah Ali[1], Wahyudi[2], Momoh J. E. Salami[3]
School of Mechatronic Engineering, UNIMAP, Perlis, Malaysia[1]
Department of Mechatronics Engineering, IIUM, Kuala Lumpur, Malaysia[2,3]

Abstract— **Security of an information system depends to a large extent on its ability to authenticate legitimate users as well as to withstand attacks of various kinds. 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 design and development of keystroke pressure-based typing biometrics for individual user's verification which based on the analysis of habitual typing of individuals is discussed. The paper examines the use of maximum pressure exerted on the keyboard and time latency between keystrokes as features to create typing patterns for individual users. Combining both an Artificial Neural Network (ANN) and Adaptive Neuro-Fuzzy Inference System (ANFIS) are adopted as classifiers to verify the authorized and unauthorized users based on extracted features of typing biometric. The effectiveness of the proposed system is evaluated based upon False Reject Rate (FRR) and False Accept Rate (FAR). A series of experiment shows that the proposed system that used combined classifiers produces promising result for both FAR and FRR.**

I. INTRODUCTION

Almost all the activities rely on the use of computer technology. Thus, computer has become an integral part of nearly in every aspect of societal activities. The communication, aviation and financial services are already controlled by computer. People entrust with vital information such as medical and criminal records, manage transactions, pay bills and write personal letters. However, this increasing dependency on computers coupled with growing emphasis on global accessibility in cyberspace, has unveiled new threats to computer system security [1]. In addition, crimes and impostors in the cyberspace appear are almost everywhere. Crimes on the computer networks may cause serious damages, including communication blocking, perusal of classified files, commerce information destruction etc [2].

Traditional methods such as passwords and PINs are no longer adequate, as either of these can be cracked, possibly breaking to the computer system. Consequently, alternatives to traditional access control methods are in high demand. Although, a variety of authentication devices to verify a user's identity are in use, password technique has been and will remain the preferred method. Password authentication is an inexpensive and familiar paradigm that most operating systems support. However, the confidence in ability to provide highly secured authentication is weakening. This is largely due to the wrongful use of passwords by many users and to the inhibited simplicity of the mechanism which makes it susceptible to extraordinary intruder attacks. Methods are needed, therefore, to extend and enhance the life of password techniques [3].

A software methodology that improves security by using typing biometrics has been developed to reinforce password-authentication mechanisms [3].Typing biometric or keystroke dynamics is the analysis of a user's keystroke patterns. This relies on the fact that, each user has a unique way of using the keyboard to enter a password; for example, each user types the characters that constitute the password at different speeds. Willem et al. [3] employed fuzzy logic to measure the users typing biometric. In developing a scheme using keystroke dynamics for identity verification, it is very necessary to determine which keystrokes characterize the individual's key pattern.

Taking the advantages of habitual typing of individuals possesses, this paper has proposed the design and development of keystroke-pressure based typing biometric as authentication system by using an artificial neural-network (ANN) and adaptive neuro-fuzzy inference system (ANFIS) based classifiers to identify the authorized and unauthorized user. The paper examines the use of maximum pressure exerted on the keyboard and time latency between keystrokes as features to create typing patterns for individual users. Pressure signals which are taken from underneath the keypad are extracted accordingly. Both features are then used to recognize authentic users and to reject impostors. The performance of proposed system is evaluated based on False Rejection Rate (FRR) and False Acceptance Rate (FAR).

II. PROPOSED SYSTEM DESCRIPTION

Fig. 1 shows the hardware development of the proposed Biometric Authentication System (BAS) which is based on keystroke pressure-based typing biometric. The proposed system is sensitive to the pressure applied on each keystroke. It consists of the following devices:

1. Alphanumeric keyboard (Biokeyboard) embedded with force sensors to measure the pressure while typing.
2. Data Acquisition System (DAS) which consists of analog interface and DAQ hardware.

978-1-4244-4152-5/09/$25.00 ©2009 IEEE

3. PC/Central Processing Unit (CPU).

This system employs special force sensors to measure the exact amount of pressure a user exerts while typing, signal processing is then carried out to construct a waveform pattern for the password entered. The maximum pressure is extracted from the waveform pattern and it's used as one of the features to authenticate the user. In addition, the proposed system also measures the actual timing traces called "latency" (the time between keystrokes). The combination of both "maximum pressure and latency" is used for biometric analysis of the user [4]. This proposed system in general makes four possible decisions; the authorized person is accepted, the authorized person is rejected, the unauthorized person (impostor) is accepted and the unauthorized person (impostor) is rejected. The accuracy of the proposed system is then specified based on the rate in which the system makes the decision to reject the authorized person and to accept the unauthorized person. False Rejection Rates (*FRR*) is used to measure the rate of the system to reject the authorized person whereas the False Acceptance Rates (*FAR*) is measure the ability of the system to accept the unauthorized person. Both performances are can be expressed as,

$$FRR = \frac{NFR}{NAA} x100\% \quad (1)$$

$$FAR = \frac{NFA}{NIA} x100\% \quad (2)$$

NFR is referred to the numbers of false rejections and *NFA* is referred to the number of false acceptances respectively while *NAA* and *NIA* refer to the number of the authorized person attempts and the number of impostor person attempts respectively [4]. In this paper the main objective is to develop a system that would have both low *FRR* and *FAR* as well as to achieve both high usability and high security of the system.

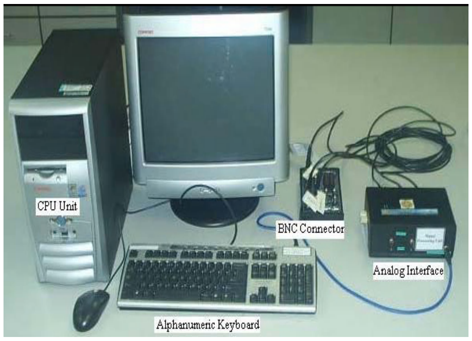
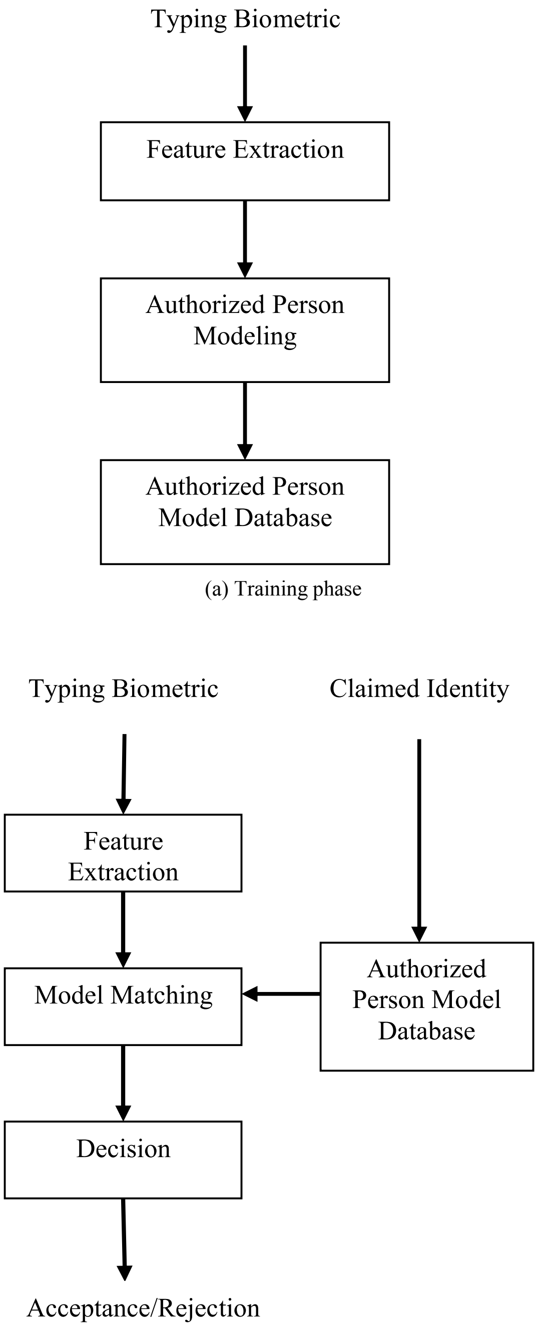


Fig. 1. Integration of biometric authentication system component.

III. Keystroke Pressure-Based Typing Biometric System

Most applications of keystroke dynamics are in field of verification. As other methods of biometric-based security system, there are two phases in the proposed system. First phase is training or enrollment phase as shown in Fig. 2(a) and second phase is testing as shown in Fig. 2(b).



(a) Training phase

(b) Testing phase

Fig. 2. Basic structure of keystroke pressure-based biometrics system

During the first phase, each person has to register as an authorized person by entering an appropriate information in the experimental system. Each of user passwords should consist of six (6) digits. Then the passwords that contain typing biometric data are extracted. The features extracted from typing biometric of the password are used to develop models of the authorized persons. The second phase in the proposed system is testing or operational phase as shown in Fig. 2(b). In the second phase, an attempt would be made to access the system when a user would be required to enter his/her password. At the same time, the system computes the person's typing for the password just entered. It then compares this with the claimed person model to verify his/her claim.

Features Extraction

Feature extraction is the process whereby unique data are extracted from the sample and a template is created. The templates for any two persons should differ whereas different samples for the same person should be identical [4]. As shown in Fig. 2, feature extraction is one of the important process in the proposed system. Feature extraction is the process of converting the biometric data to feature vector which can be used for classification.

There are several different features of the keystroke dynamics which can be used when the user presses the keyboard keys. Possible features include [7]:

1. Latency between consecutive keystrokes.
2. Duration of the keystroke, hold-time.
3. Overall typing speed.
4. Frequency of errors (how often the user has to use backspace).
5. The habit of using additional keys in the keyboard, for example writing numbers with the numpad.
6. The order that user press keys when writing capital letters, (is shift or the letter key released first?).
7. The force used when hitting keys while typing (requires a special keyboard).

In the proposed system, combine features of maximum pressure and latency are adopted as the features since this features combination is considerably the effective feature to be used in the keystroke-based authentication system [9]. The alphanumeric keyboard with additional press sensor, measures the person's biometric data during the process of identifying oneself.

IV. PATTERN CLASSIFICATION TECHNIQUES

A. Artificial Neural Network (ANN)

Artificial neural network (ANN), which is one of the approaches in artificial intelligence (AI), can be regarded as functional imitation of the human brain function [5]. They are based on simulated nerve cells or neurons, which are joined together in a variety of ways to form networks. The main feature of the ANN is the ability to learn effectively from the data. Hence, the ANN is used in the proposed system in order to develop the person model based on his/her typing biometric data. In general, an ANN is characterized by its architecture, learning algorithm, and activations function. The architecture describes the connections between the neurons. It consists of an input layer, an output layer and several hidden layers in between. Multilayer Feedforward Network (MFN) is very popular amongst the available architecture of the ANN. Because of this popularity, therefore the keystroke pressure-based typing biometric of person model is developed based on the MFN. The back-propagation learning algorithm is one of the most important historical developments in neural network [6]. MFN trained with back-propagation algorithm has been widely used in many engineering application due to its capability. An example of MFN is shown in Fig. 3. MFN generally consists of three main parts. The first part is the input layer which distributes the input data to the processing elements in next layer. The second part shows hidden layers where the nonlinear behavior comes from while the third part displays the output layer. Input and output are directly accessible while the hidden layers are not. Each layer contains several processing which are generally called neuron. In Fig. 3, it is shown that the MFN structure has input $x1, x2 \ldots, xn$ and output y. The connections between the neurons of the different layers are called weight and bias.

The output of neuron j in the hidden layer is given by

$$h_j = f\left(\sum_{i=1}^{m} w_{ji} x_i + b_j \right) \tag{3}$$

where w_{ij} and b_i are the hidden layer neuron weights and bias. In addition, $f\ (.)$ is the activation function which may be threshold, tansig or any other functions.

Then, the output of the network is,

$$y = f\left(\sum_{i=1}^{k} w_{0i} h_i + b_0 \right) \tag{4}$$

where $f(.)$, w_{oi} and b_o are the output layer neuron activation function, weights and bias respectively. The learning process of MFN is carried out using input-output data to update the weights and biases.

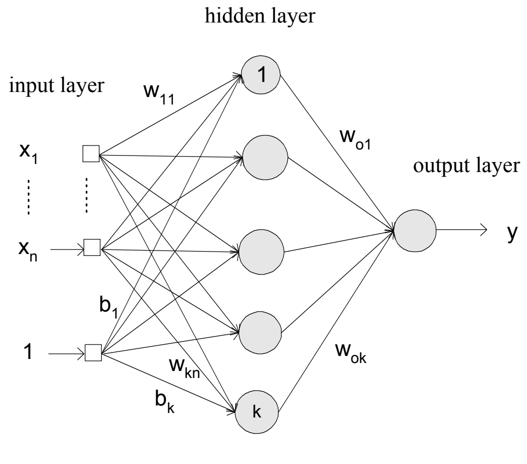


Fig. 3. A multilayer feedforward neural network

The output training data d is referred to as the target output of the neural network. The data is used to train the network until the output of neural network is stable and close to the target output. Back-propagation algorithm is the most popular learning algorithm for the MFN. The back-propagation algorithm is basically an iterative learning algorithm for minimizing the following mean square error (MSE) based on the set of N given training data pattern:

$$E = \frac{1}{2} \sum_{n=1}^{N} (d_i - y_i)^2 \qquad (5)$$

The weights of the MFN are iteratively and continuously updated until the MSE between the network output and the desired output is as small as acceptable for the desired case [5]. The weights are updated to get a minimum E with the use of the gradient descent method. The weight update equation is given by,

$$w_{ij}(t+1) = w_{ij}(t) + \eta \left(\frac{\partial E}{\partial w_{ij}} \right) \qquad (6)$$

where η represents the learning rate constant, *wij(t)* is the old weight and *wij(t+1)* represent the new updated weight. The weights are updated through iterations called epochs [5]. The epochs are continued until the error between the desired and actual outputs is as small as desired.

In summary, the process of developing keystroke model based on the maximum force and latency data using MFN are as follow:

1. Typing biometric was required for each person as data collection and these are analyzed for feature extraction.
2. Number of inputs, neurons, hidden layers and activation functions would determine the structure of the ANN.
3. ANN is trained, using the input pattern and desired output.
4. Validation of the trained ANN is done.

B. *Adaptive Neuro-Fuzzy Inference System (ANFIS)*

ANFIS (Adaptive Neuro-Fuzzy Inference System) is an architecture which is functionally equivalent to a Sugeno type fuzzy rule base [6,8],. Loosely speaking, ANFIS is a method for tuning an existing rule base with a learning algorithm based on a collection of training data. Besides, ANFIS is an approach that integrates the interpretability of a fuzzy inference system with the adaptability of a neural network. Moreover, because ANFIS has much less tunable parameters than traditional neural networks, it has the advantage of being significantly faster and more accurate than many ANN-based methods.

The structure of ANFIS has 5 layers and it uses Sugeno fuzzy inference model to be the learning algorithm. There are two inputs, *x* and *y*, and one output *z* in the simplest form structure of fuzzy inference system. In the first order of Sugeno fuzzy inference model, the typical fuzzy if-then rule can be expressed as:

Rule 1: If x is A_1 and y is B_1, then
$f_1 = p_1x + q_1y + r_1$
Rule 2: If x is A_2 and y is B_2, then
$f_2 = p_2x + q_2y + r_2$

These parameters p_1, p_2, q_1, q_2, r_1 and r_2 are linear, whereas A_1, A_2, B_1 and B_2 are nonlinear. The equivalent architecture of ANFIS is shown in Fig. 4. The five layers in ANFIS are fuzzification, production, normalization, defuzzification, and aggregation layer in order. The following concepts are the input-and-output relationships of each layer.

Layer 1 (Fuzzification layer)

A_1, A_2, B_1 and B_2 are the linguistic expressions which are used to distinguish the membership functions (MFs). The relationships between the input-output and MFs are:

$$O_{1,i} = \mu_{A_i}(x) \quad \text{for } i = 1, 2 \qquad (7a)$$

$$O_{1,j} = \mu_{B_j}(y)\text{, for } j = 1, 2, \qquad (7b)$$

$O_{1,i}$ and $O_{1,j}$ denote the output function of the first layer, $\mu_{A,i}(x)$ and $\mu_{B,j}(y)$ denote MFs. The membership function adopts bell-shape with maximum and minimum equal to 1 and 0, respectively.

$$\mu_{A_i}(x) = \frac{1}{1 + \left| \frac{x - c_i}{a_i} \right|^{2b}} \qquad (8)$$

where $\{a_i, b_i, c_i\}$is the parameter set. As the values of these parameters change, the bell-shaped functions vary accordingly. In fact, any continuous and piecewise differentiable functions such as trapezoidal or triangular–shaped membership function are also qualified candidates for node functions in this layer. Parameters in this layer are referred to as *premise parameters*.

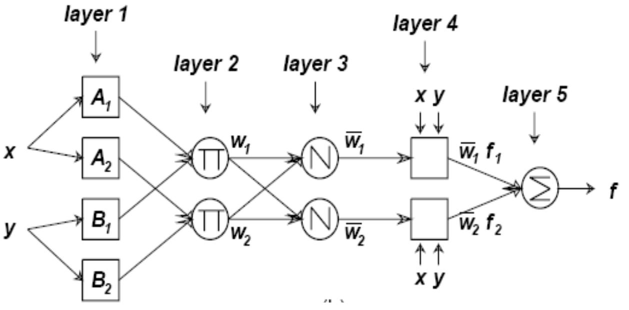


Fig. 4. ANFIS architecture

Layer 2 (Production layer)

Every node in this layer is marked as symbol Π . The outputs are w_1 and w_2 , the weight functions of the next layer. They can be shown as:

$$O_{2,i} = w_i = \mu_{A_i}(x)\mu_{B_i}(y)\text{, } i = 1, 2. \qquad (9)$$

$O_{2,i}$ is the output function of the second layer.

Layer 3 (Normalization layer)

The node is marked as **N**, and it is used to normalize the weight functions. The function is:

$$O_{3,i} = \overline{w_i} = \frac{w_i}{w_1 + w_2} \quad , \; i=1, 2. \qquad (10)$$

$O_{3,i}$ is the output function of the third layer. For convenience, outputs of this layer are called *normalized firing strengths*.

Layer 4 (Defuzzification layer)

Being an adaptive node, $\overline{w_i}$ is output and $\{p_i, q_i, r_i\}$ is the parameter set in this layer. The relationship between input and output is:

$$O_{4,i} = \overline{w_i} f_i = \overline{w_i}(p_i x + q_i y + r_i) \qquad (11)$$

$O_{4,i}$ is the output function of the fourth layer. Parameters in this layer are referred to as *consequent parameters*.

Layer 5 (Total output layer)

The single node in this layer is a fixed node labeled $\sum$, the summation of all inputs. It can be expressed as:

$$\text{Overall output } O_{5,1} = \sum_i \overline{w_i} f_i = \frac{\sum_i w_i f_i}{\sum_i w_i} \qquad (12)$$

$O_{5,i}$ is the output function *f* of the fifth layer.

Thus, an adaptive network has been constructed which is functionally equivalent to a Sugeno fuzzy model.

The main objective of the ANFIS is to optimize the ANFIS parameters. The ANFIS design consists of two steps. The first step is the design of the premise parameters and the other is consequent parameters training. Several methods have been proposed for designing the premise parameter such as grid partition, fuzzy c-means clustering and subtractive clustering. Once the premise parameters are fixed, the consequent parameters are then obtained based on the input-output training data [10].

IV. Architecture for Proposed Combining ANN and ANFIS-Based Classifiers

The ultimate goal of combining classifiers is to achieve the best possible classification performance. The pattern recognition process of the system is done by the intelligent classifiers. Artificial Neural–Network (ANN) and Adaptive Neuro-Fuzzy System (ANFIS) are employed as the classifiers to perform the classification of individually users for dynamic keystrokes analysis.

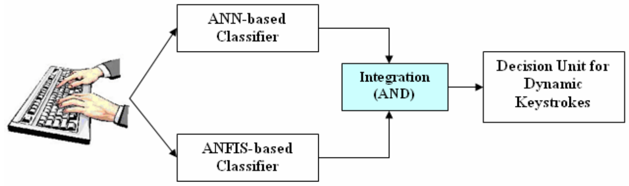


Fig. 5. Architecture proposed for combining classifiers.

In decision unit, both the ANN and ANFIS-based classifiers are modeled from the extracted features. The system will decide either to accept or to reject based on logical AND operator at decision unit. The system will accept if condition of both classifiers agrees, otherwise the system will reject. The effectiveness of the proposed system is evaluated based on False Rejection Rate (FRR) and False Acceptance Rate (FAR).

IV. Results

A. Experimental setup

To evaluate the effectiveness of the proposed keystroke pressure-based typing biometric authentication system, a group of five (7) persons is used as data collection in the experiment. Three (5) persons are considered as authorized person and the other two (2) persons are assumed as imposters. Each person has been required to type six characters of their own password for 200 times, 100 sets are used for training whereas the rest are used for testing data. So, each typed character of the password has maximum pressure and latency (time between keystroke). For example, when the password "asd123" were entered, then the time duration between the letter pairs (a-s), (s-d), (d-1), (1-2) and (2-3) would be computed. In addition, each character has its own maximum pressure. Here, each typed character of the password consists of five latency and six maximum force features, resulting in eleven features for each user [10].

The performance of biometric systems is usually described by two error rates: (*FRR*) and (*FAR*). Hence, the effectiveness, of the proposed system in testing (operational) phase is evaluated based upon *FRR* and *FAR*. The *FAR* is calculated based on the close set and open set. In the close set, the typing biometric of an authorized person makes up the distinguished typing biometric of the other authorized person. On other hand, the open set is referred as typing biometric of the impostors.

B. Training and testing performances for combining classifiers

For training ANN-based models, MFN with single hidden layer is used for developing user models based on extracted features. The initial weights and biases of the MFN are randomly selected. The goal of the Mean Square Error (MSE) is set at first as 10^{-7}. The activation function for all of the layers is tan-sigmoid transfer function. The ANN is trained using back propagation learning algorithm with a learning constant of 0.05.

Whereas, for ANFIS training, the first step is to design the structure of the ANFIS that allows the ANFIS to learn from the input-output data available so that the consequent parameters are obtained. The premise parameters are determined in order to design the ANFIS structure. Here the subtractive clustering method is used with varied radius parameters. Once the premise parameters are obtained, the ANFIS model is trained by using hybrid learning algorithm for ten (10) iterations.

Table II and III show the training and testing performance results of the combined classifiers (ANN and ANFIS-based classifiers) for the proposed system. Based on the results of Table II, all users give perfect classification rates. Since that, there are no errors in categorizing the individual users and its average training time is less than 1 second.

The result obtained by combining classifiers of ANN and ANFIS-based classifiers show the excellent results of False Rejection Rate (FRR). Thus, it indicates that the proposed system gives convenient for authorized users to access the system. Whereas, FAR for close set shows excellent results which is 0%. It means that other authorized users cannot use authorized user's password the system.

Besides, the FAR value for open set shows good result which is about 3.8% averagely. The first and fifth users give the maximum value of false acceptance rate (FAR) which is about 7% and 11% respectively. The poor performance that shows by first and fifth users are assumed due to lack of consistency of data in which there are possibility for impostors to break into the system once they obtain user's password. In terms of security, high FAR indicates possibility of imposters being able to access secured information. However, further improvement has to be done to improve the FAR for open set so as to enhance the level of security of the system.

TABLE I
TRAINING PERFORMANCES OF COMBINING CLASSIIERS

Authorized User	Training Time(sec)	Classification Rate (%)
User 1	0.9063	100
User 2	0.7344	100
User 3	0.9688	100
User 4	1.0313	100
User 5	0.9063	100
Average	***0.9094***	***100***

TABLE II
TESTING PERFORMANCES OF COMBINING CLASSIFIERS

Authorized User	FRR (%)	FAR (%) Close Set	FAR (%) Open Set
User 1	0	0	7
User 2	0	0	0
User 3	0	0	0
User 4	0	0	1
User 5	0	0	11
Average	***0***	***0***	***3.8***

V. CONCLUSIONS

This paper has examined development of keystroke pressure-based biometrics authentication system for security. The combining features of maximum pressure with latency are considerably more effective way to verify the authorized person due to unique typing biometric of each individual. Combining both an Artificial Neural Network (ANN) and Adaptive Neuro-Fuzzy Inference System (ANFIS)-based classifiers has the greatest promising result for improving accuracy in order to verify the authorized user as compared to standalone classifier. A series of experiment shows that the proposed system was achieved the best result, since it gives excellent result for false rejection rate (FRR) and false acceptance rate (FAR) of the close set condition. However, further study has to be done to improve the FAR for open set condition as well as enhance the level of security of the system.

REFERENCES

[1] W. E. Eltahir, W. K. Lai, Momoh Jimoh E. Salami. Ahmad Faris, "Design of a pressure based typing biometric authentication system", Proceeding of the eight's Australian and New Zealand Intelligent Information System Conference ANZIIS, 10-12 December 2003, Sydney AU.

[2] D. T. Lin, "Computer-access authentication with neural network based keystroke identity verification", International Conference on Neural Networks, Houston, Texas, USA (1997), 174-178.

[3] G. De William, Jan H.P, "Enhanced password authentication through fuzzy logic", IEEE Expert 12(6): 38-45 (1997).

[4] D. Zhang, *Automated Biometric Technologies and System*, Kluwer Academic Publishers, 2000.

[5] Wahyudi, Syazilawati, Albdulghani Albagul, "Intelligent voice – door access control system for Building Security", in press.

[6] C. T. Lin,C. S. George Lee *Neural Fuzzy System: A Neuro-Fuzzy Synergism to Intelligent Systems*, Prentice Hall,1996.

[7] J. Ilonen, "Keystroke dynamics", in Advanced Topics in Information Processing 1-Lectures, 2003.

[8] Jang, J. S. R., Sun, C. T., & Mizutani, E. (1997). *Neuro-Fuzzy and Soft Computing*. Prentice Hall, Upper Saddle River, NJ, USA.

[9] H. Ali, Wahyudi, M. J. E. Salami, "Keystroke pressure-based typing biometrics authentication system using artificial neural network", Proceeding 1st International Conference on Control, Instrumentation and Mechatronics Engineering, Johor Bahru, Malaysia, pp. 407-412 92007)

[10] H. Ali., Wahyudi & Momoh J. E. Salami. (2007, August). *Keystroke Pressure-Based Typing Biometrics Authentication System Using Adaptive Neuro-Fuzzy Inference System (ANFIS)*. International Conference on Instrumentation, Communication and Information Technology (ICICI 2007), Bandung, Indonesia