# Keystroke Patterns Classification using the ARTMAP-FD Neural Network

Chen Change Loy[1], Weng Kin Lai[1], and Chee Peng Lim[2]
[1] *Centre for Advanced Informatics, MIMOS Berhad, 57000 Kuala Lumpur, Malaysia*
*chenchange.loy@mimos.my, lai@mimos.my*
[2] *School of Electrical & Electronic Engineering, University of Science Malaysia, Engineering Campus, 14300 Nibong Tebal, Penang, Malaysia*
*cplim@eng.usm.my*

## Abstract

*This paper presents the development of a keystroke dynamics-based user authentication system using the ARTMAP-FD neural network. The effectiveness of ARTMAP-FD in classifying keystroke patterns is analyzed and compared against a number of widely used machine learning systems. The results show that ARTMAP-FD performs well against many of its counterparts in keystroke patterns classification. Apart from that, instead of using the conventional typing timing characteristics, the applicability of typing pressure to ascertaining user's identity is investigated. The experimental results show that combining both latency and pressure patterns can improve the Equal Error Rate (ERR) of the system.*

**Keywords:** Keystroke dynamics, typing biometrics, novelty detection, ARTMAP-FD, Fuzzy ARTMAP

## 1. Introduction

Keystroke dynamics, sometimes also known as typing biometrics is a type of behavioural biometric technology that authenticates individuals based on distinct keystroke patterns. The underlying assumption is that each individual presents a unique typing pattern when using the keyboard to enter words that the user is familiar with, for example, passwords and user or account names. The keystroke patterns may come in the form of the timing delays between successive key pairs, duration while pressing a key, or even the pressure exerted on individual keys on the keyboard.

In most real-world situations the number of typing patterns from intruders is basically infinite and it is hard to collect intruders' samples when the system is first implemented. Therefore it may not be feasible to train a typing biometric system on all possible data classes that the system is likely to encounter. Given the fact that keystroke patterns from intruders are not known at the time of training the model, only single class information from legitimate user is available for the learning process. Therefore, typical discrimination-based or binary classifiers that require training samples from positive and negative classes might not be suitable for typing biometric systems. In this paper, ARTMAP-FD (FD: Familiarity Discrimination) neural network [1] is employed for keystroke pattern classification because it only requires samples from a legitimate user to build an accurate model. ARTMAP-FD denotes typing patterns of a valid user as normal patterns, whereas an intruder's typing patterns are denoted as novel patterns. Similar to other novelty detectors, the main function of ARTMAP-FD is to define closed boundaries for normal patterns and yet, be able to detect novel patterns that are outside the boundaries.

ARTMAP-FD is an extension of the Fuzzy ARTMAP (FAM) neural network [2] with improvement in detecting patterns from unfamiliar classes. It also inherits the advantages from FAM, such as fast convergence and on-line learning capability. The method has been tested on simulated radar range profile data with fairly good results [1]. In this study, the applicability of ARTMAP-FD to keystroke patterns classification is examined by using keystroke data collected from one hundred participants. The results obtained are then compared with a statistical method proposed by Joyce and Gupta (JG) [3], Gaussion density estimator, Parzen window density estimator, *K*-Nearest Neighbour (KNN), Support Vector Domain Description (SVDD) [4], one-class Support Vector Machine (1-SVM) [5] and the original FAM network. Apart from that, the paper also investigates the use of combined keystroke pressure and keystroke latency for the verification process, and compares the performance with those from conventional timing-based techniques.

The organisation of this paper is as follows. A review of previous work is given in Part 2. Details of the experimental procedure are provided in Part 3. Part 4 summarises the dynamics of ARTMAP-FD for novelty detection. The results are reported and discussed in Part 5. Finally, the paper concludes with some suggestions for further investigation in Part 6.

## 2. Previous Work

This section highlights some methods that have been proposed in the past. There are two metrics that are commonly used to assess the reliability of a biometric system, namely False Acceptance Rate (FAR) and False Rejection Rate (FRR). Since different values of the operating threshold may result in different values of FRR and FAR, in order to ensure comparability across different systems, another metric that is commonly used is Equal Error Rate (EER), the point at which both FAR and FRR are equal. Some researchers have also used accuracy and error rate to measure the performance of their methods.

A number of learning strategies have been proposed for typing patterns classification, which can be generally grouped as statistical methods [3][6] and neural network methods [7][8]. Some neural network approaches proposed for keystroke pattern classification include discrimination-based, i.e., the classifiers require both intruders' and legitimate users' keystroke patterns in the learning phase. These approaches might be impractical as pointed out in the previous section. An example is as follows.

In [8], Obaidat and Sadoun carried out a comprehensive study of different statistical-based and neural network-based classification methods that can be used with keystroke dynamics. They concluded that neural network-based methods gave better results as compared with statistical methods in keystroke patterns classification. Encouraging results were reported as neural network-based methods are able to achieve zero FAR and zero FRR when both latency and duration were combined as features. However, there is concern that the results obtained may be over optimistic. Besides using the legitimate users' samples for training, Obaidat and Sadoun also divided the same set of intruders' samples for learning and testing purposes. In other words, the neural networks were trained in advance not only by using legitimate users' sample, but also intruders' samples. Hence, the classifier is expected to produce better results with low FAR as the classifier now has prior knowledge of the intruders' patterns.

On the other hand, some statistical methods require only the legitimate user's patterns for learning. For instance, the statistical method proposed by Joyce and Gupta [3] constructs a mean reference signature based on eight latency vectors provided by a legitimate user. During verification, an unknown typing pattern is compared with the mean reference signature to determine the similarity between the two profiles. A user would login successfully if the magnitude of difference is less than the declared threshold. Note that the learning process used here does not involve any typing patterns from the imposter.

Apart from that, there are other novelty detection methods introduced for keystroke dynamics-based system, such as Auto-Associative neural network (ASNN) [9], Support Vector Data Description (SVDD) [10], and one-class Learning Vector Quantization (1-LVQ) [11]. These approaches employed only the keystroke information from the legitimate users in the training stage.

## 3. Experimental Procedure

In order to capture the typing pressure patterns, a normal keyboard was modified into a pressure sensitive keyboard by adhering pressure piezoresistive force sensors underneath the keyboard matrix. A pressure sensor is analogous to a variable resistor in which its resistance changes in accordance with the amount of force exerted on its sensing surface. A force-to-voltage circuit was used to convert the resistance into discrete voltage signals ranging from 0 to 10 volts. Next, the voltage signals were acquired into the processing unit by using a data acquisition card for subsequent analysis such as pre-processing and feature extraction.

Ideally, a keystroke pressure pattern should rest on the horizontal line $y = 0$ when the keys are not pressed. However, due to unwanted forces exerted by the base plate and face plate of the keyboard, the raw pressure signals present an elevated and non-constant baseline. In order to ensure the comparability between different samples, the baseline must be subtracted from each raw pressure signal. Firstly, spurious peaks were removed from the pressure patterns using moving averages of $k_s$ nearest neighbours. The value of $k_s$ is presently set at 20. The removal of baseline was achieved by subtracting from a pressure signal, an estimate of its varying minimum values. In this study, the robust local regression method reported in [12] was applied to estimate the varying minimum values of the pressure pattern. This was achieved by fitting a local regression to the local minima. First, for each pressure pattern, the local minima were found by using a moving window. Next, a local regression to data below the local quantiles was fitted for each pressure pattern. Finally, the estimated baseline was subtracted from each pressure signal.

After baseline subtraction, a Fast Fourier Transform (FFT) was deployed to transform the pressure discrete time signals into frequency domain signals. The resulting outputs contained both the magnitude and phase information, but only the magnitude information was used for subsequent feature extraction. After careful examination, a total of nine features were extracted from the frequency domain signal, as shown in Table 1.

**Table 1.** Features extracted from keystroke pressure

| No. | Name of Feature | No. | Name of Feature |
|---|---|---|---|
| 1 | Arithmetic mean | 6 | Fundamental frequency |
| 2 | Root mean square | 7 | Energy |
| 3 | Peak | 8 | Kurtosis |
| 4 | Signal in noise & distortion | 9 | Skewness |
| 5 | Total harmonic distortion | | |

During the data collection session, a program was developed to collect keystroke latency and keystroke pressure from a total of one hundred computer users. Keystroke latency data samples were captured at an accuracy of milliseconds (ms). There was no specific range for the latency as it relies on the speed of typing. The participants were requested to familiarise themselves with the password "*try4-mbs*" prior to the actual data collection session. The use of a common password among all participants is to ensure the comparability of typing patterns of the same password from different individuals. A total of ten timing vectors and ten pressure vectors were collected from each participant.

## 4. Keystroke Patterns Classification

This section provides description on ARTMAP-FD with emphasis on its familiarity discrimination mechanism. Since ARTMAP-FD and FAM share a number of common features, this section will commence with the explanation on FAM and followed by the enhancements introduced in ARTMAP-FD.

FAM is a supervised neural network that comprises of two fuzzy Adaptive Resonance Theory (ART) modules designated as $ART_a$ and $ART_b$, which create stable

recognition categories in response to arbitrary sequences of input patterns. Both ART modules are linked together by a map field module, $F^{ab}$, an associative learning network to establish an association between input patterns and target classes $C$. The following is a brief explanation on the typical operation in $ART_a$, which also occurs in $ART_b$. In the training stage, the original $M$-dimensional input vector $\boldsymbol{a}$ is complement-coded into a $2M$-dimensional vector $\boldsymbol{A}$:

$$\boldsymbol{A} = \left(\boldsymbol{a}, \boldsymbol{a}^c\right) \equiv \left(\boldsymbol{a}^1,...,\boldsymbol{a}^M, 1-\boldsymbol{a}^1,...,1-\boldsymbol{a}^M\right) \quad (1)$$

$\boldsymbol{A}$ is propagated from the input layer $F_1^a$ to the dynamic output layer $F_2^a$ through a set of adaptive weights $\boldsymbol{w}_j$. Activation of the $j^{\text{th}}$ $F_2^a$ node is determined by the choice function $T_j(\boldsymbol{A})$ as defined in Equation (2), with $\boldsymbol{w}_j^a$ denoting the weight vector of the $j^{\text{th}}$ $F_2^a$ node.

$$T_j(\boldsymbol{A}) = \frac{|\boldsymbol{A} \wedge \mathbf{w}_j^a|}{\alpha_a + |\mathbf{w}_j^a|} \quad (2)$$

According to the winner-take-all strategy, the node with the highest response value, denoted as node $J$, is selected as the winning node, while all other nodes $j \neq J$ are deactivated. The winning node $J$ remains active if the match function of the chosen category meets the vigilance criterion:

$$\frac{\left|\boldsymbol{A} \wedge \boldsymbol{w}_J^a\right|}{|\boldsymbol{A}|} \geq \rho_a, \quad (3)$$

where $\bar{\rho}_a \in [0,1]$ is the baseline vigilance parameter of $ART_a$

If the vigilance test is satisfied, the network will proceed to the map field association. However, if the existing winning node fails to predict the output class, i.e., $c(J) \neq C$, a match tracking process is triggered until the best winning node that satisfies both the $ART_a$ and map field vigilance test is found. Subsequently, learning takes place by updating the weight vector of the winning node $J$ in $ART_a$. The learning mode of the network is determined by the learning parameter, $\beta_a$. There are two learning modes: fast learning ($\beta_a = 1$ for all times) and fast-commit slow recode learning ($\beta_a = 1$ for an uncommitted node and $\beta_a < 1$ for a committed node).

In the testing stage, an input pattern that activates node $J$ is assigned to class $C = c(J)$. In fact, FAM may be used for novelty detection by checking the vigilance criterion as defined in Equation (3). It can be re-written as a familiarity function, $\phi(\boldsymbol{A})$ as shown in Equation (4). In this context, the baseline vigilance parameter of $ART_a$, $\bar{\rho}_a$ is equivalent to the decision threshold $\gamma$. An input pattern is categorised as "*familiar*" if $\phi(\boldsymbol{A})$ is greater than $\gamma$.

$$\phi(\boldsymbol{A}) = \frac{\left|\boldsymbol{A} \wedge \boldsymbol{w}_J^a\right|}{|\boldsymbol{A}|} \quad (4)$$

Given an input $\boldsymbol{a} \in R_J$, where $R_J$ is the hyperbox that encloses all the vectors $\boldsymbol{a}$ that chosen category $J$ during training, the function defined by Equation (4) sets $\phi(\boldsymbol{A}) = |\boldsymbol{w}_J^a| / |\boldsymbol{A}|$. The result may not be accurate because the value of $\phi(\boldsymbol{A})$ may be large or small depending on the value of $|\boldsymbol{A}|$ [1]. In addition, accurate novel detection using FAM requires $\bar{\rho}_a$ to be very close to unity, which causes category proliferation during training [1]. These problems lead to the proposed improvements to the FAM algorithm. The training phase of ARTMAP-FD remains identical to FAM. The only difference is the computation of familiarity function, $\phi(\boldsymbol{A})$ as given in Equation (5). It is computed based on the choice function after a winner node $J$ is selected and a class prediction $C = c(J)$ is made. In contrast to Equation (4), any input that chooses category $J$ during testing is assigned the maximum familiarity value 1 if and only if it lies within $R_J$. As a result of this modification, better familiarity discrimination can now be estimated. In ARTMAP-FD, an input is predicted as class $C$ if and only if $\phi(\boldsymbol{A})$ is larger then the threshold $\gamma$. Otherwise, the input is categorised as an unfamiliar pattern and no prediction is made. Note that the threshold $\gamma$ is a user-defined parameter that is independent of the existing FAM's parameters.

$$\phi(\boldsymbol{A}) = \frac{T_J}{T_J^{MAX}} = \frac{\left|\boldsymbol{A} \wedge \boldsymbol{w}_J^a\right|}{\left|\boldsymbol{w}_J^a\right|} \quad (5)$$

## 5. Results and Discussion

Two experiments were carried out in this study. The objective of the first experiment is to compare the performances of ARTMAP-FD with some of its counterparts. The second experiment investigates the suitability of keystroke pressure for identity verification. Leave-one-out cross validation (LOOCV) was employed in both experiments. Here the legitimate user's keystroke data set was separated into two partitions, whereby nine samples (from a total of ten samples) were used as training data and the remaining sample was retained to form a complete testing data set with typing patterns from intruders. The cross-validation process is then repeated ten times with each of the ten legitimate user's samples used exactly once as part of the testing data set. Following these partitions, the above steps were repeated one hundred times with each of the participants selected exactly once as the legitimate user. The results from the cross validation were averaged to produce a single estimated FRR and FAR. Furthermore, in order to investigate the performance of each novelty detector at different operating thresholds, experiments were conducted across different values of trade-off parameter ranging from 0 to 1. Neither the intruders' samples nor other testing samples were involved in the prediction model building process in order to avoid biased results.

The results of the first experiment were summarised in Table 2. The Gaussian density estimator, Parzen window density estimator, KNN, and SVDD were implemented by using the Data Description Toolbox [13]. The best FRR and FAR were reported instead when the EER cannot be found within the range of the operating threshold. As shown in Table 2, both the Gaussian method and Parzen method exhibited extremely high FRR across different operating thresholds. On the contrary, SVDD and 1-SVM gave lower FRR but with a considerably higher FAR. The high FAR of SVDD and 1-SVM might due to the large space enclosed by the decision boundaries. Although JG is a simple statistical method, it gave noticeably good results among the various methods studied here. The performance of KNN was slightly

inferior when compared with that of JG. Experiments on FAM were conducted using two different settings, i.e., fast learning and fast-commit slow-recode learning. Both settings of FAM performed better than KNN, but performed poorer than JG. Four different settings of ARTMAP-FD were tested. The best performance was obtained with $\overline{\rho}_a = 0$ in the fast learning mode.

In the second experiment, keystroke pressure, keystroke latency, and the combination of both features were used as the inputs to ARTMAP-FD, respectively. The main goal is to examine the differences of the classifier's performance while using different sets of the aforementioned input features. As shown in Table 3, even though the keystroke pressure performed slightly poorer than keystroke latency, the combination of both features improved the overall performance with EER of 11.78%.

**Table 2.** Comparison of Equal Error Rate (EER)

| Method | Model Setting | FAR (%) | FRR (%) |
|---|---|---|---|
| Gaussian | – | 0.44 | 85.90 |
| Parzen | – | 2.20 | 77.10 |
| SVDD | RBF[a] kernel | 12.10 | 33.30 |
| 1-SVM | RBF kernel | 11.83 | 37.00 |
| JG | – | 17.53 | |
| KNN | $K = 5$ [b] | 23.61 | |
| FAM | $\beta_a = 1.00$ | 20.44 | |
| | $\beta_a = 0.01$ | 19.17 | |
| ARTMAP-FD | $\beta_a = 1.00, \rho_a = 0.00$ | **14.94** | |
| | $\beta_a = 1.00, \rho_a = 0.99$ | 19.35 | |
| | $\beta_a = 0.01, \rho_a = 0.00$ | 25.18 | |
| | $\beta_a = 0.01, \rho_a = 0.99$ | 19.38 | |

a. RBF = Radial Basis Function, b. $K$ = number of neighbours

**Table 3.** Performance using keystroke pressure features and latency features

| Features | EER (%) |
|---|---|
| Pressure | 16.50 |
| Latency | 14.94 |
| Pressure + Latency | **11.78** |

## 6. Conclusions and Further Works

The work presented in this paper investigates the use of ARTMAP-FD as a novelty detection method for keystroke patterns. A series of experiments were systematically carried out to compare the performance of ARTMAP-FD with other widely used novelty detectors. The performance of ARTMAP-FD and other methods were tested against a data set comprising keystroke pressure patterns and keystroke latencies from one hundred participants. The experimental results showed that ARTMAP-FD outperformed other novelty detectors in keystroke patterns classification.

Applicability of individual's typing pressure to determining the identity of a user has also been examined. The explanation of the development of pressure-sensitive keyboard has been given. The experimental results showed that the use of keystroke pressure patterns could improve the overall EER by fusing the conventional timing-based typing characteristics and pressure features in the frequency domain.

Future work will focus on investigating the use of intruders' samples to improve the performance of ARTMAP-FD. Although the number of intruders' samples is not sufficient to train the novelty detector, they may be useful to refine the boundaries of the normal class patterns. Another interesting direction is to explore the use of artificial intruders' samples in training the classifier. The artificial intruders' typing patterns are computed in such a way so that they are located very near to the closed boundaries in the normal class data space. The main purpose of generating intruder samples is to form an attraction region outside the closed boundaries so that novel patterns, which do not belong to the known class, will be "attracted" to fall in this rejection region.

## References


[1] Carpenter, G.A., Rubin, M.A., Streilein, W.W.: ARTMAP-FD: Familiarity Discrimination Applied to Radar Target Recognition. Proc. of the Int. Conf. on Neural Networks (1997) 1459–1464

[2] Carpenter, G.A., Grossberg, S., Markuzon, N., Reynolds, J.H., Rosen, D.B.: Fuzzy ARTMAP: A Neural Network Architecture for Incremental Supervised Learning of Analogue Multidimensional Maps. IEEE Trans. on Neural Networks 3(5) (1992) 698–713

[3] Joyce, R., Gupta, G.: Identity Authentication Based on Keystroke Latencies. Comm. ACM 33(2) (1990) 168–176

[4] Tax, D.M.J., Duin R.P.W.: Support Vector Domain Description. Pattern Recognition Letter 20 (1999) 1191–1199

[5] Schlökopf, B., Williamson, R.C., Smola, A.J., Shawe-Taylor, J., Platt, J.: Support Vector Method for Novelty Detection. Advances in Neural Information Processing Systems 12 (2000)582–588

[6] Monrose, F., Rubin, A.D.: Keystroke Dynamics as a Biometric for Authentication. Future Generation Computer System 16(4) (2000) 351–359

[7] Obaidat, M.S., Macchairolo, D.T.: A Multilayer Neural System for Computer Access Security", IEEE Trans. on Systems, Man, and Cybernetics, 24(5) (1994) 803–816

[8] Obaidat, M.S., Sadoun, B.: Verification of Computer Users using Keystroke Dynamics. IEEE Trans. on Systems, Man, and Cybernetics, Part B: Cybernetics 27(2) (1997) 261–269

[9] Cho, S., Han, C., Han, D., Kim, H.: Web Based Keystroke Dynamics Identity Verification using Neural Networks. Journal of Organizational Computing and Electronic Commerce 10(4) (2000) 295–307

[10] Yu, E., Cho, S.: Keystroke Dynamics Identity Verification - Its Problems and Practical Solutions. Computer and Security 23(5) (2004) 428–440

[11] Cho, S., Lee, H.: Retraining a Novelty Detector with Impostor Patterns for Keystroke Dynamics-based Authentication. Proc. of the Int. Conf. on Biometrics (2006) 633–639

[12] Ruckstuhl, A..F., Jacobson, M.P., Field, R.W., Dodd, J.A.: Baseline Subtraction using Robust Local Regression Estimation. Journal of Quantitative Spectroscopy and Radiative Transfer 68(2) (2001) 179–193

[13] Tax, D.M.J.: DDtools, the Data Description Toolbox for Matlab. (2007)