We are IntechOpen,
the world's leading publisher of
Open Access books
Built by scientists, for scientists

4,800
Open access books available

122,000
International authors and editors

135M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

CLARIVATE ANALYTICS
BOOK CITATION INDEX
INDEXED

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

Application of Self Organizing Maps to Multi Modal Adaptive Authentication System Using Behavior Biometrics

Hiroshi Dozono

Additional information is available at the end of the chapter

1. Introduction

Password mechanisms are widely used for the authentication method. However, Password mechanism has many issues. For examples, Password can be stolen easily, Password may be guessed from personal information, such as birthday, families name or telephone number. Some users set unique password to different systems. If one system is hacked, all of the systems can be accessed. Some users feel troublesome to memorize the password. For these problems, biometric authentication is one of the solutions.

Biometric authentication [1] is classified into two types. The first one is the biometric authentication with biological characteristics, such as fingerprint, Vein patterns and Iris patterns. To measure these characteristics, the additional hardware is necessary, and it costs up the computer system. And, some users may feel mentally uncomfortable to register their fingerprint to the computer system. Furthermore, static information about biological characteristics may be imitated by dummy. For example, the fingerprint authentication is easily hacked in the TV show.

The second type is biometric authentications with behavior characteristics, such as keystroke timings [2], Signature [3], hand written pattern and mouse moving pattern. For these methods, the standard input equipments of computer are available. The dynamic information about behavior characteristics is hard to imitate even if it is looked by illegal one. However, the accuracy of authentication is worse compared with that of biological characteristics. For use behavior characteristics, it is necessary to select the pattern of behavior and the features used for authentication. For this selection, Self Organizingmap(SOM)s are used for the analysis in our research.

SOM [4] is the architecture of neural networks, which is feedforward type and single layer network. SOM organizes the map which reflects the similarities of input vectors; thus SOM can visualize the relations among the input vector on the lower dimensional, usually 2-dimensional map. SOM is often used for the visualization of the multidimensional data. SOM is also applied to the authentication with biological characteristics, such as facial recognition system.

At first, SOM is applied to the authentication systems of behavior biometrics of pen calligraphies [5] [6] and keystroke timing [7] in this research. SOM is used for the analysis of input data to select the appropriatepattern of behavior and featureswith visualizing the input data on the map, and also for constructing an authentication system.

However, the accuracy of single behavior biometrics is not enough. For this problem, Pareto learning SOM(P-SOM) and Supervised Pareto learning SOM(SP-SOM), which can integrate multi-modal behavior biometrics [8], is proposed, and applied to the authentication system using keystroke timing and pen calligraphy [9] [10].

Furthermore, the multi-modal authentication system using keystroke timing and key typing sound, which can be obtained at the same time, is proposed [11]. Additionally, the incremental learning of the biometric data during the authentication is applied to implement the adaptive authentication system which can follow the changes of the biometrics of time [12] [13].

SP-SOM shows satisfactory performance as authentication system. However, SP-SOM needs to learn data of some users. For mobile devices, the number of users is usually one; thus the system may need dummy data. For this problem, Concurrent Full Pareto learning SOM(CFP-SOM), which uses a small map for each user, is applied. CFP-SOM can detect the unregistered user using the size of the Pareto set as index, and shows better performance than the SP-SOM [14].

In this chapter, SOM and its application to biometric authentication system are mentioned in section 2 and 3,4 respectively. In section 5 and 6, application of the SP-SOM to multi-modal authentication system and its extension to adaptive authentication system are mentioned respectively. In section 7, application of CFP-SOM to the multi-modal authentication system is mentioned.

2. Self Organizing Map (SOM)

SOM [4] is a kind of neural network, which was proposed by Kohonen, and SOM can extract the feature on the multidimensional input vectors and can visualize the relations among them by unsupervised learning. SOM can integrate multi-modal input vectors and can extract relations among them in 2-dimensional plane. SOM can be used for clustering of unlabeled data or classification of labeled data with labeling the output units after learning.

Figure 1 shows the basic learning algorithm of SOM. For each input vector, the neuron, which is closest to the input vector, is searched from the neurons which are arranged on the 2 dimen-

sional map. The closest neuron is called as winner neuron. The winner neuron and the neurons in the region of the neighborhood are updated as to decrease the difference to the input vector depending on the learning rate and neighboring functions. These steps are iterated for each input vector with decreasing the region of the neighborhood and learning rate.
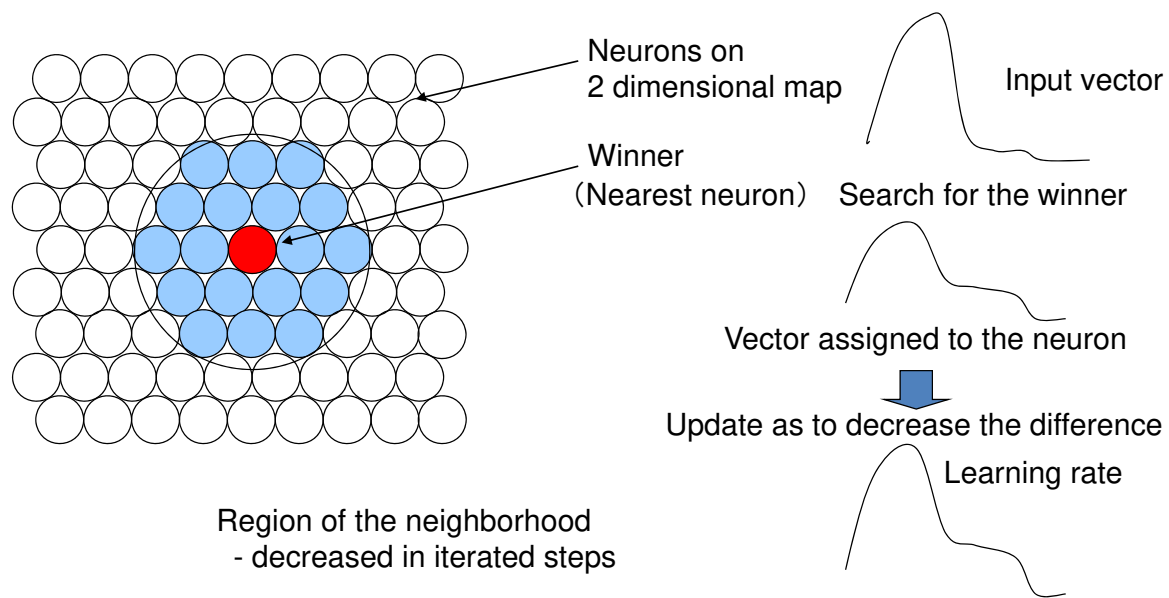
Neurons on
2 dimensional map

Input vector

Winner
(Nearest neuron)   Search for the winner

Vector assigned to the neuron

Update as to decrease the difference

Learning rate

Region of the neighborhood
- decreased in iterated steps

Figure 1. Schematic description of SOM algorithm

3. Application of SOM to the authentication system using handwritten patterns

Recently, many mobile devices, such as Smartphones, tablet devices and small computers, are equipped with touch screen. As the authentication method for touch screen devices, the password authentication is often used. But, on touch screen devices, password can be looked while typing on the screen. It is troublesome to enter the password using handwritten character recognition or screen keyboard. For the touch screen devices, handwritten signature authentication is often applied, because the touch screen is considered to be useful for signature input. However, the shape of the signature may be copied, and it is difficult to write the exact signature on slippery screen, especially for people who do not usually write signatures.

For this problem, we propose a user authentication method using the identical symbol for all users. Using this method, the symbol which is used for authentication is displayed on the touch screen and users simply trace it. However, the pen stroke data may not be enough for user authentications. We used the pen pressure data which may have enough information for user authentication. For this purpose, We analyzed the pen stroke data and pen pressure data using Self Organizing Map [5] [6].
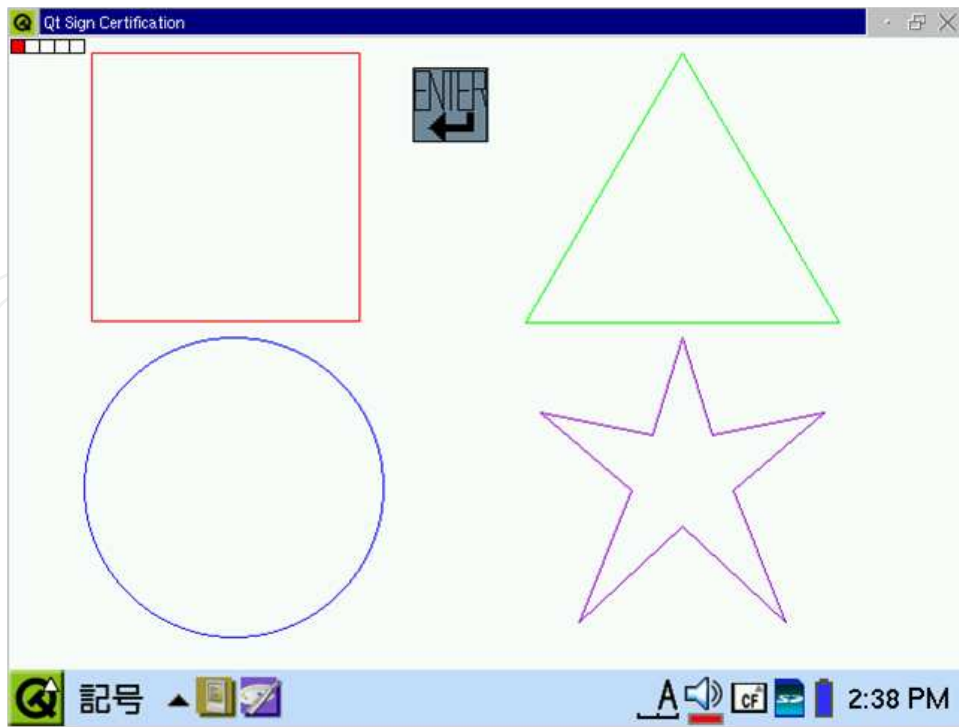
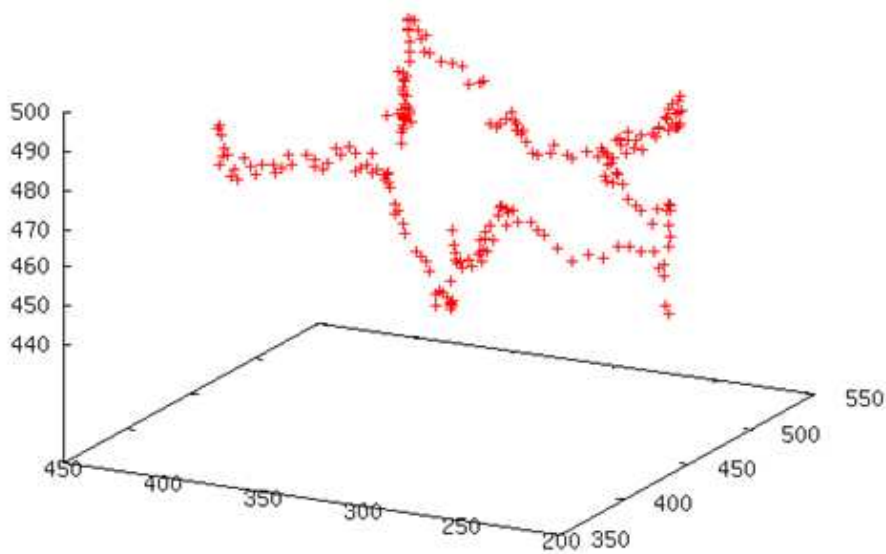**Figure 2.** Test input screen

Figure 3. Pen input of symbol star

Figure 2 shows the screen of the application which measures the pen stroke data and pen pressure data of symbols square, circle triangle and star. Each symbol is written in a single stroke, and starting point is specified for all users. 5 samples are taken from each of 12 users. Figure 3 shows an example of symbol star taken from a user. This sample contains 232 points of x-axis, y-axis and pen pressure data in z-axis.
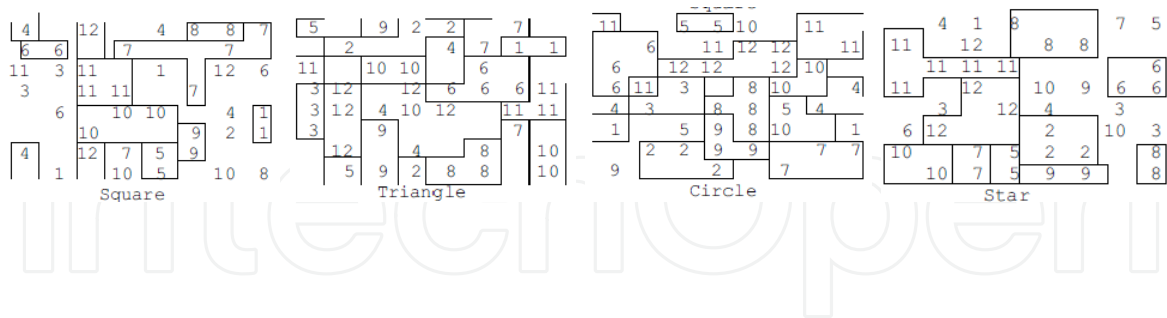
Figure 4. Organizied map for simple symbols

Figure 4 shows the maps of each symbol. The numbers in these figures denote the used-id. With these figures, the symbols of circle and star show better separations compared with others. We consider that the symbols comprised of oval lines or acute angle have more specific features of each user. The symbols of spiral and complex star are selected for next experiments.
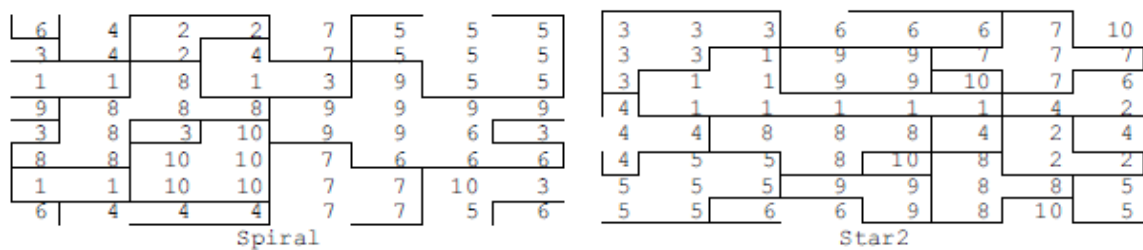

Figure 5. Organized map for symbols spiral and complex star

Figure 5 shows the maps of the symbols spiral and complex star. We use the torus map for this analysis, so the upper side of the map is connected to the lower side, and the right side is connected to the left side. Both of the symbols star and spiral show better separations compared with the simple symbols. It will be possible to authenticate the user using pen pressure data and pen speed data.

The authentication experiments using these symbols are conducted. As the authentication system, we used SOM. The settings of the experiments are as follows. 10 samples of spiral and complex star were taken from each of 10 users.

7 samples of each person were used for training SOM map, and 3 samples were used as test data. The maps were retrained by LVQ3 algorithm.

Spiral learned data			
	authenticated	false rejection	false acceptance
user-1	1.000	0.000	0.000
user-2	0.714	0.286	0.000
user-3	0.857	0.143	0.000
user-4	1.000	0.000	0.016
user-5	1.000	0.000	0.016
user-6	0.714	0.286	0.032
user-7	0.857	0.143	0.032
user-8	1.000	0.000	0.000
user-9	0.857	0.143	0.016
user-10	0.857	0.143	0.016
total	0.886	0.114	0.012
Spiral test data			
	authenticated	false rejection	false acceptance
user-1	0.667	0.333	0.000
user-2	1.000	0.000	0.000
user-3	1.000	0.000	0.037
user-4	1.000	0.000	0.037
user-5	0.667	0.333	0.037
user-6	0.000	1.000	0.037
user-7	1.000	0.000	0.074
user-8	1.000	0.000	0.074
user-9	0.333	0.667	0.000
user-10	0.333	0.667	0.037
total	0.700	0.300	0.033

Star-2 learned data			
	authenticated	false rejection	false acceptance
user-1	1.000	0.000	0.048
user-2	1.000	0.000	0.000
user-3	1.000	0.000	0.000
user-4	1.000	0.000	0.032
user-5	1.000	0.000	0.000
user-6	0.571	0.429	0.000
user-7	1.000	0.000	0.000
user-8	0.857	0.143	0.000
user-9	0.857	0.143	0.016
user-10	0.714	0.286	0.016
total	0.900	0.100	0.011
Star-2 test data			
	authenticated	false rejection	false acceptance
user-1	1.000	0.000	0.074
user-2	1.000	0.000	0.037
user-3	1.000	0.000	0.037
user-4	1.000	0.000	0.074
user-5	1.000	0.000	0.000
user-6	0.000	1.000	0.000
user-7	1.000	0.000	0.000
user-8	0.667	0.333	0.037
user-9	0.000	1.000	0.037
user-10	0.000	1.000	0.074
total	0.667	0.333	0.037

Table 1. Results of authentication experiments

Table 1 shows the result. For the learned data both of the spiral and complex star show high rate of authentication and low rate of false acceptance, but for the test data, rate of successful authentication was about 70%. From the table of spiral test data, users 6,9,10 show low rate of successful authentication, and from the table of star, same users are not authenticated at all. Both of the symbols can authenticate 7 users from 10 users. It depends of the characters of the users. The careful users tend to be authenticated better and careless users tend to be rejected falsely.

4. Application of SOMto the authentication method using keystroke timings

It is well known that keystroke timing is usable for user authentication. We propose an authentication method which uses the keystroke timings of identical phrase for all users. Users do not need to memorize phrases. For this purpose, the phrase, which is suitable for authentication, is selected by the analysis using SOM [7].

Figure 6. Keystroke timings

The method for taking keystroke timing is dependent on the Operating System(OS)s. The keystroke timing is the vector of intervals between pushing and releasing keys. We use this sequence as the vector of keystroke timing. The length of the vector is 2L-1, where the length of the phrase is L

The experiments are conducted using Romaji Phrases because the examinees are always typing Japanese using Romaji. As samples of phrases, „arigato"(Thank you in English), „kira-kira"(Twinkle Twinkle), „denatsu"(Voltage), „sagadai"(name of our university) and „kousatsu"(prospect) are used. The number of examinees is 10, and each examinee types each phrase in 8 times.
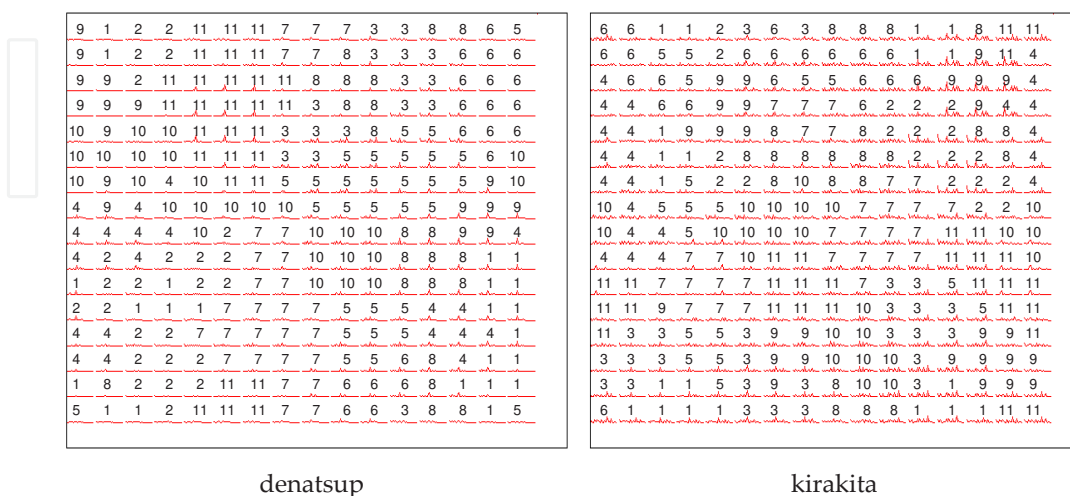

denatsup   kirakita

Figure 7. Organized maps for keystroke timings „denatsu" and „kirakita"

Figure 7 shows the maps of the phrases "denatsu" and "kirakira". Comparing these 2 maps, the map of "kirakira" shows better clustering results of user-id. The simple phrase "kirakira" is considered to be suitable for authentication because users can type unconsciously.

Next, we conducted authentication experiments using the map organized by SOM. The half of the keystroke timing data is used for learning, and the remained half is used for authentication experiments.As the indexes for evaluation, FRR which is the rate of rejection of the regular user falsely and FAR which is the rate of acceptance of the irregular user falsely, are used.

<div align="center">denatsu</div> <div align="center">kirakira</div>

	Success	FRR	FAR		Success	FRR	FAR
User 1	1.00	0.000	0.000	User 1	0.500	0.500	0.000
User 2	0.500	0.500	0.048	User 2	1.000	0.000	0.048
User 3	0.000	1.000	0.190	User 3	0.250	0.750	0.238
User 4	0.500	0.500	0.095	User 4	1.000	0.000	0.000
User 5	0.750	0.250	0.048	User 5	0.000	1.000	0.000
User 6	0.000	1.000	0.286	User 6	0.750	0.250	0.095
User 7	0.500	0.500	0.048	User 7	0.750	0.250	0.095
User 8	0.500	0.500	0.095	User 8	0.750	0.250	0.048
User 9	0.500	0.500	0.143	User 9	1.000	0.000	0.000
User 10	0.000	1.000	0.143	User 10	0.750	0.250	0.000
Average	0.425	0.575	0.081	Average	0.675	0.325	0.052

Table 2. Results of authentication experiments using keystroke timings

Table 2 shows the results of authentication experiments using the phrases of "denatsu" and "kirakira". As expected from the map, the phase "kirakira" shows the better result. On average, rate of false rejections about 32%. Some users show a remarkably high rate of false rejection. It depends on the skill of typing.

5. Integration of muti-modal biometrics using pareto learning SOM

As shown before, accuracy of authentication using behavior characteristics is worse compared with biological characteristics. It is due to the variation of the behavior characteristics and noise. We consider that Integration of some behavior characteristics will improve the accuracy.

We proposed the authentication methods using the integrated information of multi-modal behavior characteristics to improve the accuracy. For example, keystroke timing and hand-

written symbol at login time, keystroke timing and key typing sound at login and keystroke timings and mouse moving patterns during the operating time. For the integration of multi-modal biometrics, we propose the Pareto learning SOM(P-SOM). Furthermore, we propose the Supervised P-SOM(SP-SOM) which can improve the accuracy of the authentication.

5.1. Pareto leatning SOM [15]

Generally speaking, the multi modal vector is the vector composed of multi-kind of vectors or attributes. For examples, in the authentication problem using key typing features, the keystroke timing vector and key typing intensity vector are composed. For face image classi-fication, the image vector, age, gender, jobs and other features are composed. In multi-mo-dal vector, each element of the vector and the attribute is described in a different unit and scale. Accuracy of each element may differ.

Conventional SOM can be applied for integrating multi-modal vectors. For example, the simple concatenated vector $(x_1, x_2, …, x_m)$ can be used as the input vector.

Then, the quantization error is calculated in (1).

$$\sum_n \left| x_n - m_n^{ij} \right|^2 \tag{1}$$

The map is organized based on the value of the error. So, the resulting map is dominated by the largely scaled vectors and easily affected by inaccurate vector. For this problem, the con-catenated vector $(w_1 x_1, w_2 x_2, …, w_m x_m)$ with weight values is often used. Then the quantiza-tion error is calculated in (2).

$$\sum_n \left| w_n x_n - m_n^{ij} \right|^2 \tag{2}$$

So, the resulting map heavily depends on the weight values. It is difficult to select the opti-mal value of the weights.

Same situations occur in multi-objective optimization problem. Consider the problem, Sub-ject to $x \in S$, minimize multiple objective functions Fi(x). To solve this problem as a single objective optimization problem, the weighted sum of multi objective functions.

$$F(x) = \sum_n w_n F_n(x) \tag{3}$$

is minimized. However, the quality of the solution depends on the setting of weight values.

For this problem, the concept of Pareto optimal is proposed in multi-objective optimiza-tion problem.
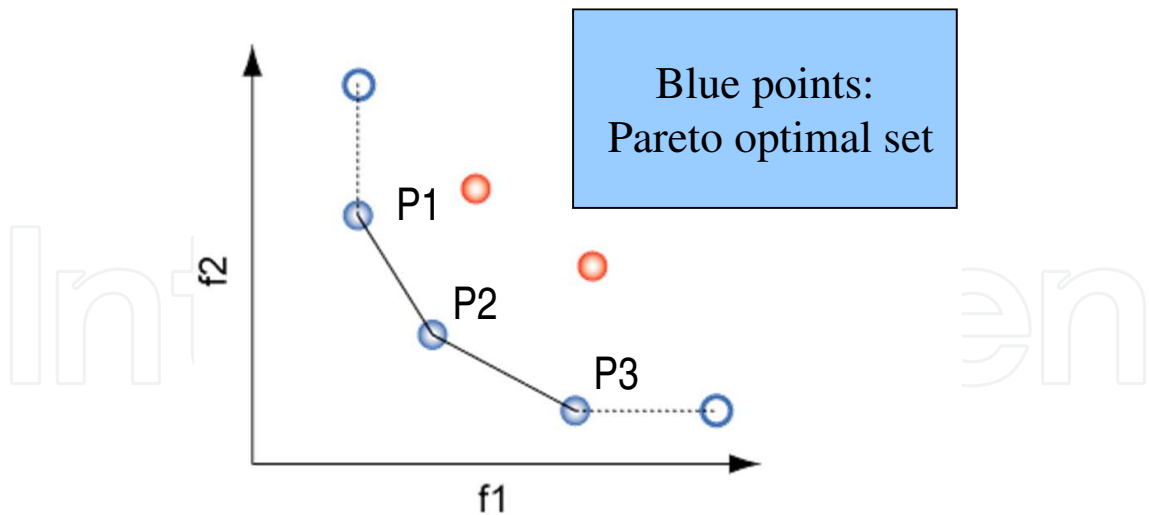
Figure 8. Pareto Optimality

Suppose that the objective function f1 and f2 should be minimized under the condition f1 and f2 should be the upper right side of this line. For this problem, P1 is better than P2 concerning f1, but P2 is better than P1 concerning f2. If no priority is given to f1 and f2, these 3 points P1, P2, P3 are not inferior to others among them. These points are named as Pareto optimal set, and they are the candidates of optimal solutions.

Pareto Learning Self Organizing Map(P-SOM) uses the concept of Pareo optimality for finding winner units. The error of each element of multi-modal vector is considered as the objective functions $f_n(x,U^{ij})=|x_n-m^{ij}_n|$, where $x=(\{x_1\},\{x_2\},\dots,\{x_m\})$ is the input vector and $m^{ij}=(\{m^{ij}_1\},\{m^{ij}_2\},\dots,\{m^{ij}_m\})$ is the reference vector associated to the unit U^{ij}. Pareto optimal set $P(x)$ is the set of units U^{ij} which are pareto optimal for the objective functions $f_n(x,U^{ij})$. So, the Pareto SOM is multi-winner SOM and all winner units and their neighbors are updated simultaneously.

$$U^{ij}_w = \arg\min_{i,j}\left|\mathbf{X}-\mathbf{m}_{ij}\right|$$

Conventional SOM

$$P(x) = \left\{U^{ij}_p\middle|^{\exists}h, e^{ij}_h \le e^{kl}_h, U^{kl} \in P - U^{ij}_p\right\}$$
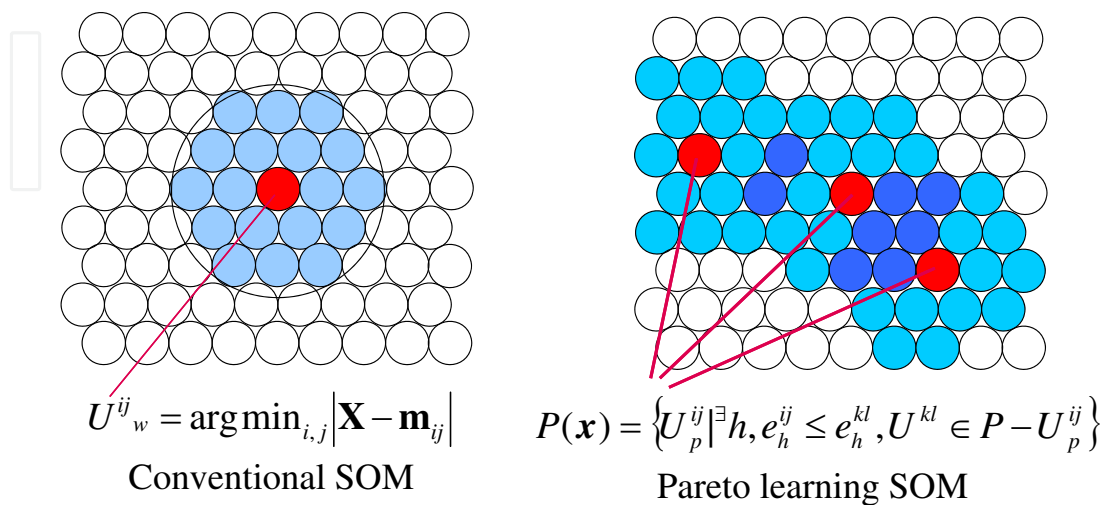
Pareto learning SOM

Figure 9. Difference betwen convential SOM and Pareto learning SOM

Figure 9 shows the learning process of SOM and Pareto learning SOM. As for SOM, only one winner is selected and the winner and its neighbors are updated. As for pareto learning SOM, pareto winner set are selected, and they are updated simultaneously. For Pareto learning SOM, overlapped neighbors are updated more strongly, and it play an important role for integration of muti-modal vectors. In other word, conventional SOM integrates the multi-modal vector in a unit and P-SOM integrates the multi-modal vector in the region of Pareto optimal set. Algorithm of P-SOM is as follows.

P-SOM Algorithm

1. Initialization of the map: Initialize the vector $\mathbf{m}^{ij}$ which are assigned to unit U^{ij} on the map using the 1st and 2nd principal components as base vectors of 2-dimensional map.

2. Batch learning phase:

    • Clear all learning buffer of units U^{ij}.

    • For each vector xi, search for the pareto optimal set of the units $P = \{U^{ab}_p\}$. $U^{ab}p$ is an element of pareto optimal set P, if for all units $U^{kl} \in P - U^{ab}_p$ existing h such that $e^{ab}_h \leq e^{kl}_h$ where $e^{kl}_h = |\, \mathbf{x}^i_h - \mathbf{m}^{kl}_h \,|$.

    • Add $\mathbf{x}^i$ to the learning buffer of all units $U^{ab}_p \in P$.

3. Batch update phase: For each unit U^{ij} update the associated vector $\mathbf{m}^{ij}$ using the weighted average of the vectors recorded in the buffer of U^{ij} and its neighboring units as follows.

• For all vectors $\mathbf{x}$ recorded in the buffer of U^{ij} and its neighboring units in distance $d \leq Sn$, calculate weighted sum $\mathbf{S}$ of the updates and the sum of weight values W.

$$S = S + \eta fn(d)\left(x - m^{i'j'}\right)$$

$$W = W + fn(d)$$

where $U^{i'j'}$'s are neighbors of U^{ij} including U^{ij} itself, η is learning rate, fn(d) is the neighborhood function which becomes 1 for d=0 and decrease with increment of d.

• Set the vector $\mathbf{m}^{ij} = \mathbf{m}^{ij} + \mathbf{S}/\mathbf{W}$.

Repeat 2. and 3. with decreasing the size of neighbors Sn for pre-defined iterations.

As shown in step 2 of this algorithm, Pareto winner set for the integrated input vector $\mathbf{x}$ are searched for based on the concept of Pareto Optimality using the distance as the objective function $f_h(\mathbf{x})$ for each element x_h in $\mathbf{x}$. Thus, the multiple units become winners. The winners and their neighboring units are modified in the update process in step 3. Overlapped neighbors are updated multiply, and the overlapped region will contribute to generalization ability and integration ability of P-SOM.

5.2. Supervised paretolearning SOM (SP-SOM)

Because Pareto learning SOM can integrate any type of vectors, the category element can be introduced as an independent vector to each input vector x_i as follows.

$$x_i^s = (x_i, c_i)$$

where

$$c_i = \begin{cases} 1 & x_{i'} \in C_i \\ 0 & x_i \notin C_i \end{cases}$$

With introducing category element, it attracts the input vectors in the same category closely on the map corporately with other input vectors in the learning phase. In this meaning, P-SOM learning algorithm becomes supervised. In the recalling process, category of test vector $\mathbf{x}_t$ is determined by the following equation.

$$\arg\max_k \left\{ \sum_{U^{ij} \in P(x_t)} c_k^{ij} \right\}$$

where $P(\mathbf{x}_t)$ is the Pareto optimal set of units for $\mathbf{x}_t$

Considering the Further extension of Pareto learning SOM, anything which has its own metrics can be element of multi-modal input vector for P-SOM. Structured data and vectors can be integrated as input data. For example, in bioinformatics amino acid sequence data comprised of Hidden Markov Model(HMM) of the data, HMM of the structures and other features can be integrated. Furthermore, the map can be organized using the partial vectors which lack some attributes in the vectors.

5.3. Experiment of authentication system using multi-modal behavior biometrics

The experimental results of the authentication system using handwritten patterns and keystroke timings were shown in the previous section. Another experiments using both of handwritten patterns and keystroke timings were conducted [9] [10]. The experimental settings are as follows. 6 samples are taken from each of 11 examinees. Each sample is comprised of the keystroke timings and pen calligraphy data which is inputted alternately. For these experiments, tablet PC, which is equipped with keyboard and touch panel, is used.

The phrase "kirakira" which marked the best results in the previous experiments is used. The symbol Spiral is used as the handwritten symbol. SP-SOM is used for the analysis and authentication.

Figure 10 shows the map of SP-SOM using behavior biometrics data, key stroke timing, pen speed and pen pressure. Using keystroke timing, the users are clustered well except small fragmentations. Using pen speed and pen pressure, thefragmentations are increased compared with those of keystroke timings. Using the integrated biometrics of key stroke timing, pen speed and pen pressure, the fragmentations decreased compared with that of keystroke timings without affected by pen data.

The Authentication experiments are conducted using the map organized by SOM, P-SOM and SP-SOM for the comparisons. 4 of the 6 samples of each user are used to organize the map and 2 remainders are used for the test data. All of the combinations of training data and test data are examined. 6C2 x 10x2 =300 input vectors are tested.
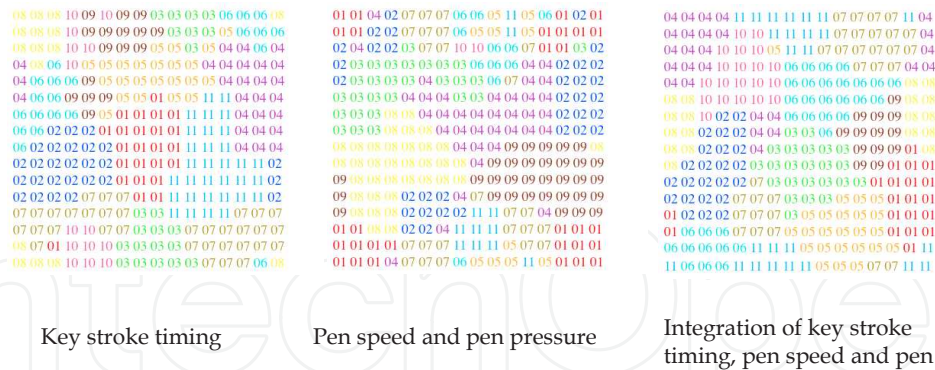
Key stroke timing   Pen speed and pen pressure   Integration of key stroke timing, pen speed and pen

Figure 10. Organized map of SP-SOM with behavior biometrics data

	key		pen speed		pen pressure	
	FRR	FAR	FRR	FAR	FRR	FAR
User 1	0.167	0.0000	0.400	0.0000	0.467	0.0000
User 2	0.000	0.0000	0.133	0.0767	0.467	0.0083
User 3	0.000	0.0000	0.700	0.0000	0.100	0.0017
User 4	0.033	0.0000	0.000	0.0317	0.333	0.0200
User 5	0.033	0.0083	0.667	0.0100	0.700	0.0217
User 6	0.233	0.0083	0.567	0.0000	0.667	0.0333
User 7	0.167	0.0017	0.367	0.0100	0.200	0.0383
User 8	0.000	0.0000	0.167	0.0433	0.200	0.0167
User 9	0.167	0.0033	1.000	0.0217	0.000	0.0150
User 10	0.033	0.0033	0.200	0.0000	0.400	0.0067
User 11	0.000	0.0000	0.600	0.0283	0.600	0.0283
Average	0.076	0.0022	0.436	0.0202	0.376	0.0173

Table 3. Result of Authentication experiment using each of behavior biometrics

Table 3 shows the result of authentication using each data independently. In this experiment, FRR of keystroke timings is much better than that of the previous experiment because the typing skill of each user becomes much better. FRR of pen speed data and pen pressure data are much worse than that of keystroke timing.

Table 4 shows the results of authentication experiments using integrated vectors of keystroke timing, pen speed and pen pressure. The weight values for pen speed data and pen pressure data are studiously selected from many iterations of try and error for SOM. SP-SOM can achieve almost same authentication performance without tunings of parameters.

	SOM		P-SOM		SP-SOM	
	FRR	FAR	FRR	FAR	FRR	FAR
User 1	0.333	0.0000	0.467	0.0000	0.200	0.0000
User 2	0.000	0.0000	0.100	0.0083	0.000	0.0000
User 3	0.000	0.0000	0.333	0.0000	0.000	0.0000
User 4	0.000	0.0000	0.067	0.0033	0.000	0.0000
User 5	0.000	0.0000	0.033	0.0067	0.000	0.0167
User 6	0.000	0.0083	0.167	0.0033	0.133	0.0000
User 7	0.167	0.0000	0.033	0.0150	0.000	0.0083
User 8	0.000	0.0000	0.100	0.0267	0.000	0.0117
User 9	0.000	0.0000	0.333	0.0083	0.100	0.0000
User 10	0.000	0.0000	0.033	0.0050	0.033	0.0000
User 11	0.000	0.0000	0.200	0.0117	0.033	0.0000
Average	0.045	0.0008	0.170	0.0080	0.045	0.0020

Table 4. Result of authentication experiment using integrated biometrics

6. Adaptive authentication system using integrated biometrics of keystroke timing and key typing sound

In this section, the experiments on the Integration of Keystroke timings and Key Typing Sound, and adaptive authentication system is mentioned [11]. Key typing sound is used as the intensities of key typing. 10 samples are taken from each of 10 examinee. The phrase "kirakira" is used for sampling keystroke timings and typing sounds. Sampling rate of the sound is 44Khz, and the maximum amplitude for each key is used as a feature vector.

The setting of the authentication experiments is as follows. 5 of the 10 samples of each user are used to organize the map and 5 remainders are used for the test data. All of the combinations of training data and test data are examined. The results of the authentication using keystroke timing, using key typing sounds and using the integrated vector are examined.
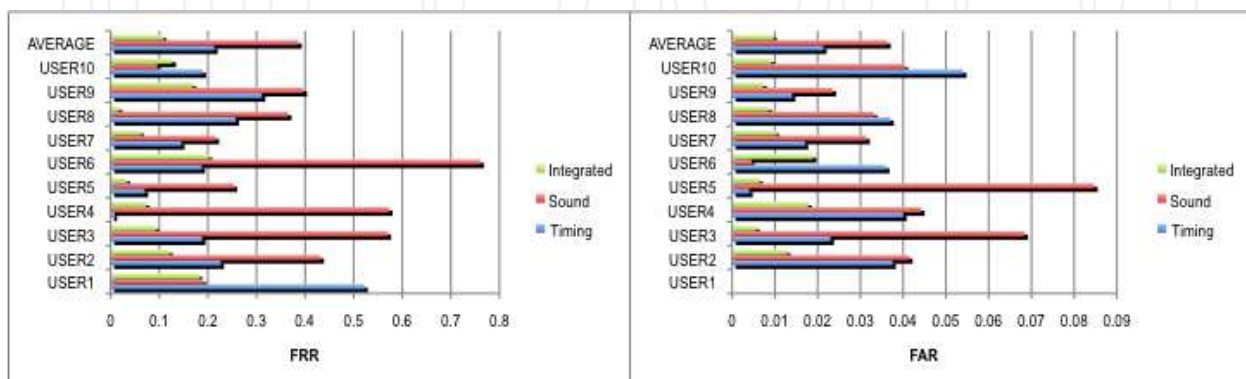

Figure 11. Result of authentication experiments using keystroke timing and key typing sound

Figure 11 shows the FRR and FAR of all user and their averages. In this experiments, average of FRR of keystroke timing is about 0.2. With integrating the typing sound, average of FRR is improved as about 0.1. For almost users, FRR and FAR is improved by integration.

As to adapt the changes of biometrics, incremental learning is introduced [15] [13]. At first, incremental learning of SP-SOM is examined using the test data. Incremental leaning is performed by updating the map after recalling process using the updating method of conventional SOM by the following equation.

$$m'_{ij} = m'_{ij} + \eta' (x' - m'_{ij})$$

where m'_{ij} is the vector assigned to and P isPareto winner set for input vector x. Two types of incremental learning, which are supervised learning using the input vector with category element and unsupervised learning without category element, are examined.
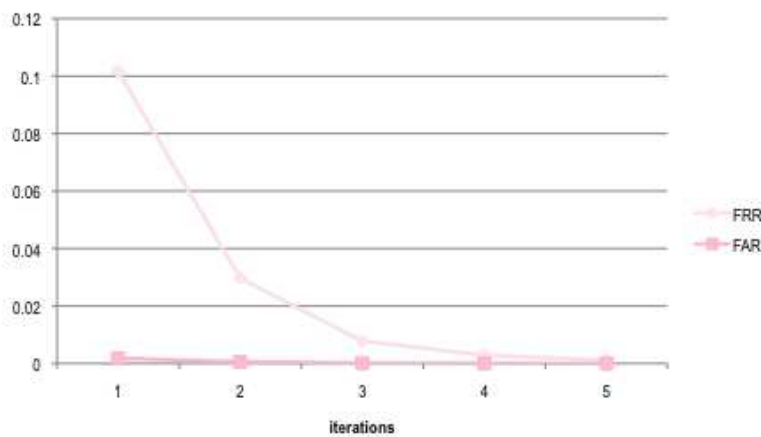
Figure 12. Result of iterated authentication with incremental learning

At first, test data is incrementally learned during the iterations of authentication. Figure 12 shows the result. Both of the FRR and FAR are improved by repeating incremental learning.

Changes of behavior biometrics by time, variation of the behavior biometrics and noise affect the accuracy of authentication. The authentication system will be able to adapt changes of behavior characteristics by the time with incremental learning of the input data for authentication. However, Incremental learning of the input data with variations or noises may affect the authentication system.

Next, we conducted experiments for changes of biometrics by the time of authentication input. It will take very long time to obtain the data which changes by the time from examinees. So, simulated data is made with changing the observed data at each authentication gradually. The experimental settings are as follows. Before authentication experiments, all data are learned by SP-SOM. For each authentication, 4 elements of the keystroke timing vector are selected randomly and multiplied by 0.8 and replaced with the new values. This case is very extreme case of changing the biometric input by the time. The results of supervised learning with used-id and unsupervised learning without user-id are examined.
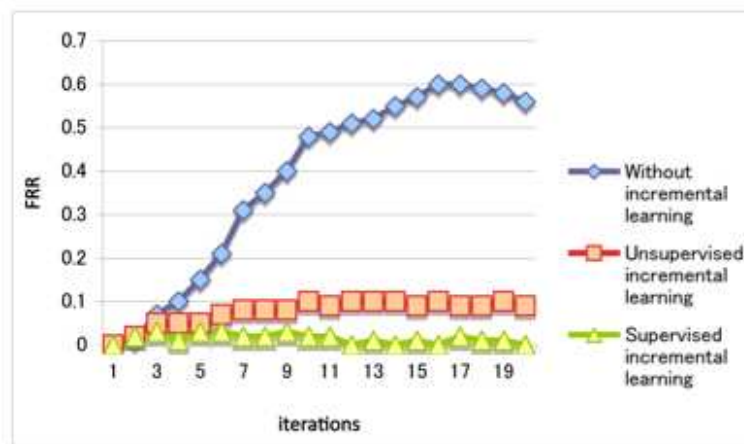
Figure 13. Result of authentication experiment of adaptive authentication system with changing the keystroke timing by time

Figure 13 shows the result. Average of the FRR becomes worse with iterations without incremental learning because the input for biometrics changing. Average of FRR is kept almost 0 with supervised incremental learning. Average of FRR becomes about 0.1 with unsupervised incremental learning. From this result, supervised incremental learning can adapt the changes by time almost perfectly.

Next, we conducted experiments for examining robustness to the noises and variations. Incremental learning may affect worse using the data with noise and variations because the noisy data is added to the map. The authentication data with noises is made artificially by adding the noise to the input vector. The experimental settings are as follows. For each authentication, 5 elements of the typing sound vector are selected, and 50% random noise is added at each authentication.
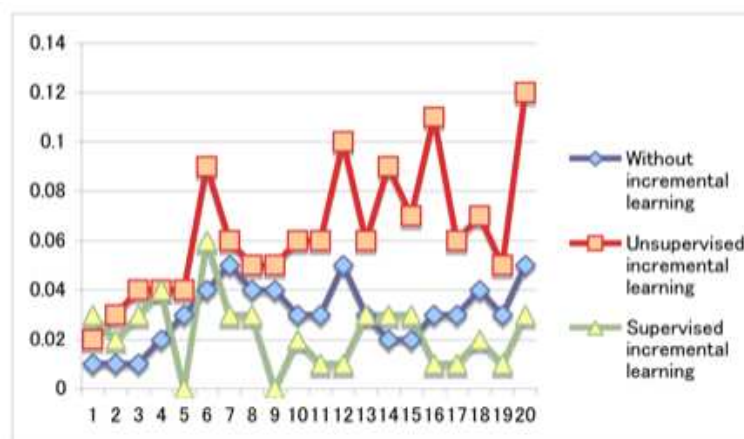
Figure 14. Result of authentication experiment with adding the noises to key typing sounds

The result for unsupervised incremental learning becomes worse by iterations. In contrast, supervised incremental learning is not affected by noises rather it becomes better than without incremental learning.

Next we conducted the experiment with changes of keystroke timings by time and adding the noises to key typing sounds simultaneously.

FRR for without incremental learning and unsupervised incremental learning becomes worse with iterations. FRR for supervised incremental learning is kept less than 0.1. In spite of the noises, supervised incremental learning can adapt to changes by time.

As the authentication system, unregistered user must be detected. Simple SP-SOM algorithm can classify the input vector to one of learned category, and cannot detect unlearned vector. For this problem, threshold values are introduced. As the features of SP-SOM, the size of Pareto set becomes large for unregistered user(unlearned data), and the magnitude of the category value becomes small for unregistered data. Thus, unregistered users can be identified with setting the threshold values to these values.

Figure 16 shows the result of authentication experiment with setting the threshold for size of Pareto set and category value as 10 and 0.5 respectively. Both of the FRR and FAR of registered users are remarkably small, and FAR of unregistered user is also small.

Figure 17 shows the result with adding changes by the time and noises. In this experiment, the authentication system can also adapt to the changes by time with incremental learning.
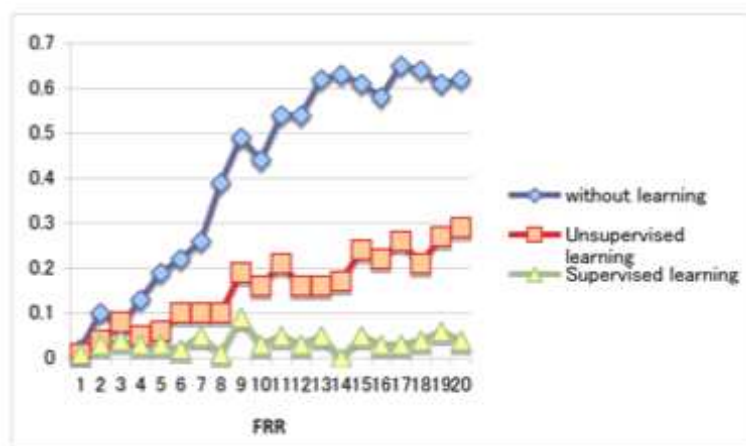

Figure 15. Result of authentication experiment with changing keystroke timing by time and adding noises to key typing sounds (x-axis: iterations, y-axis: FRR)
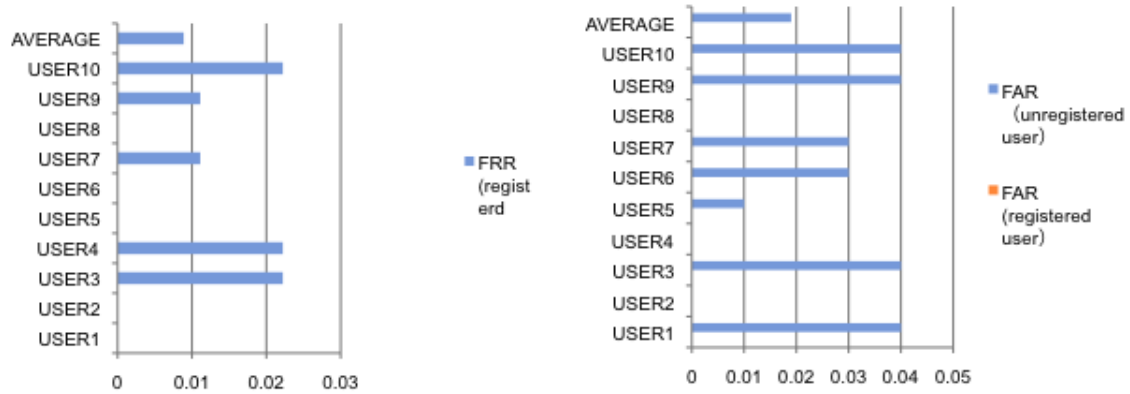
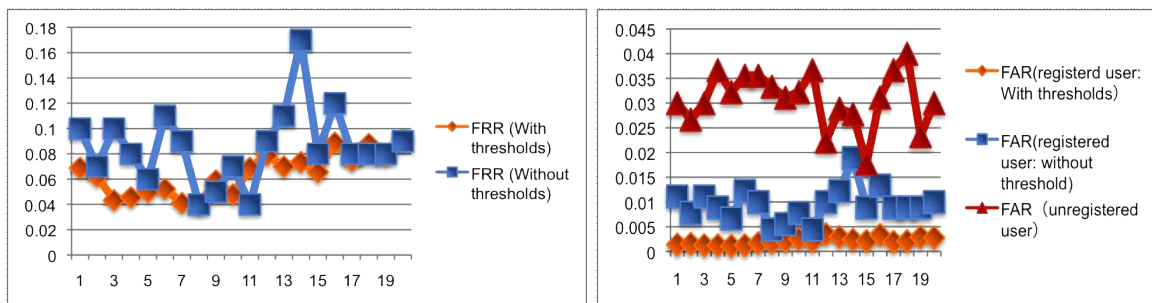**Figure 16.** Result of authentication experiment with rejecting unregistered user

Figure 17. Result of authentication experiment with adding changes by time and noises using the threshold for rejecting unregistered user (x-axis: iterations, y-axis: FRR and FAR)

7. Concurrent paretolearning SOM and its application to the authentication system using multi-modal behavior biometrics

As mentioned in the previous section, we have proposed the authentication system using Supervised Pareto learning SOM(SP-SOM). However, SP-SOM needs the training data of multiple users for learning. For the device of single user, the authentication system, which requires the data of single user, is recommended. For this problem, Concurrent Pareto learning SOM (CP-SOM) is introduced [14]. CP-SOM is P-SOM which uses the small map for each user.
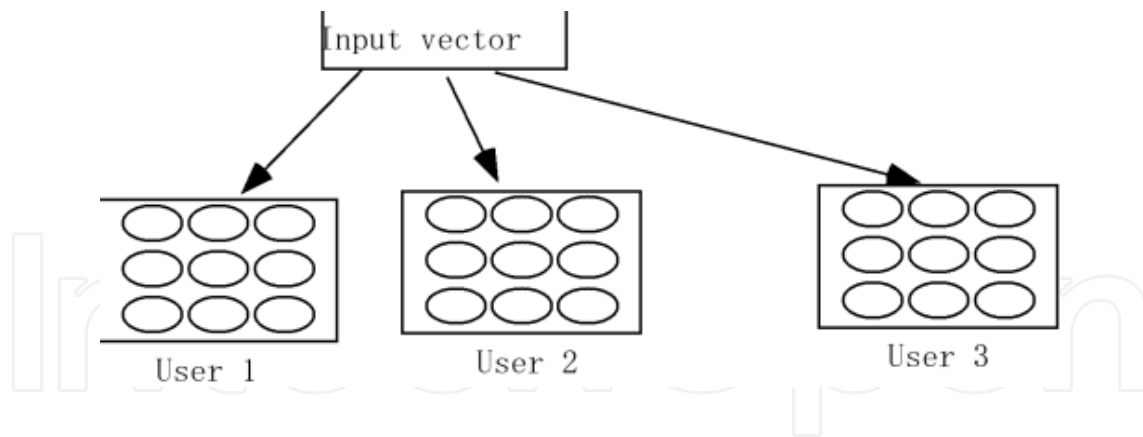
Figure 18. Concurrent P-SOM

Conventional concurrent SOM [16] uses threshold value of quantization error for classifying the learned data and unlearned data. Concurrent P-SOM uses the size of Pareto Optimal Set for detecting unregistered user.The threshold value of the size is set to TH_T*P_LAST, where P_LAST is the average size of Pareto optimal set in the last phase of learning.

The authentication experiment is conducted using the keystroke timing and key typing sound data used in the previous section. Each user data is learned as the registered user on the distinct map, and the data of other users is used as the test data of unregistered users. The experiments are conducted with changing map sizes and threshold values, TH_P. The size of Pareto sets are adaptively tuned as 1/4 and 1/2 of all units in initial learning step and last learning step respectively. The difference between registered user and unregistered users becomes larger using larger size of Pareto set in the last step.
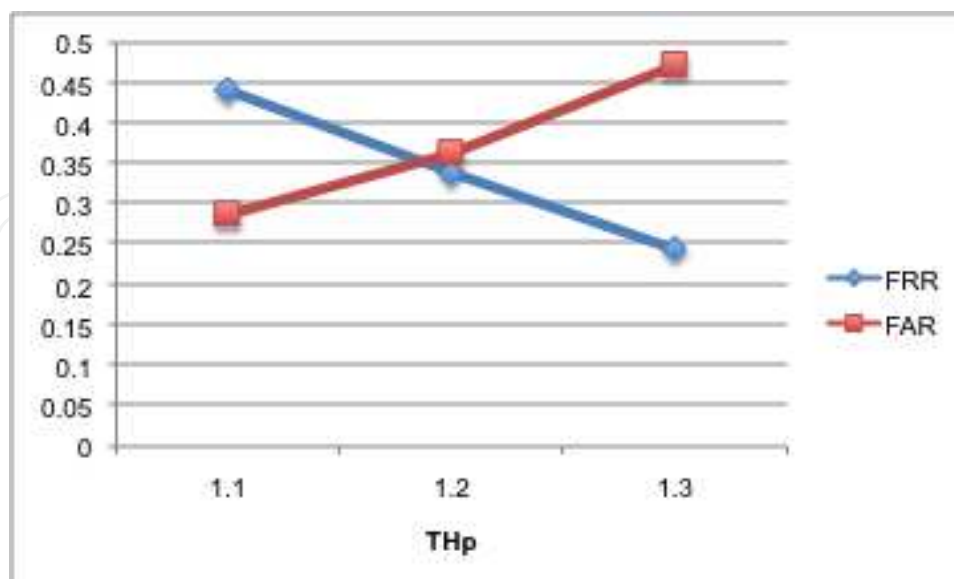

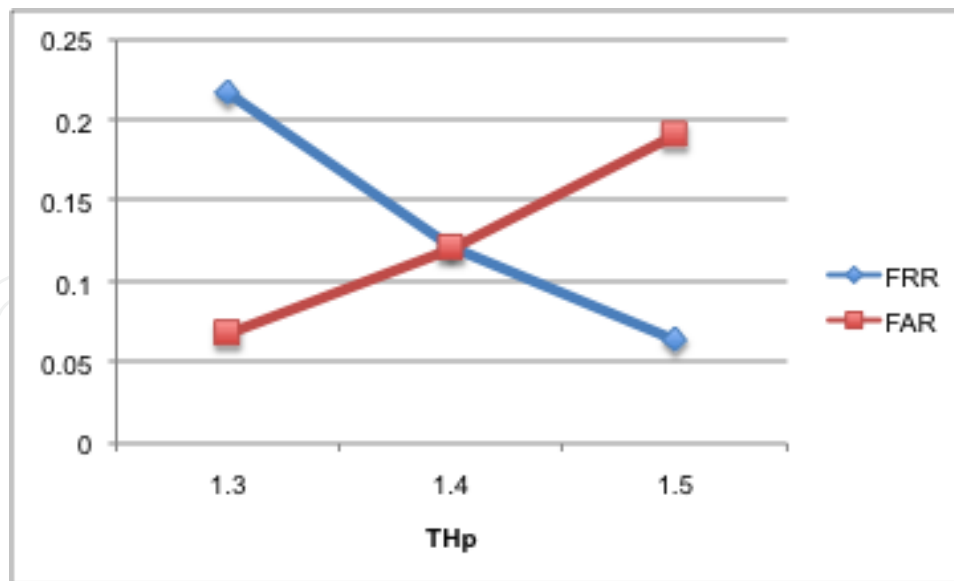**Figure 19.** Experimental result of CP-SOM

Figure 20. Experimental result of CFP-SOM

Figure 19 shows the experimental result of CP-SOM using the multi-modal vector composed of the 2 vectors, which are key stroke timing vector and key typing sound vector, with changing the threshold THp. The size of the map is 6x6. For typical tuning of authentication system, the threshold value is set to cross point of FRR and FAR. In this experiment, THp=1.2 and FRR=FAR=0.35 at the cross point, and this result is not adequate for authentication system. It is because of the small difference of the size of Pareto set between registered user and unregistered user, which are 6.22 and 7.77 respectively.

To enlarge the difference of the size of Pareto set, the number of integrated vectors should be increased. For this purpose, Full Pareto learning SOM(FP-SOM) is applied. FP-SOM is P-SOM which uses each element in the vector as independent 1-dimensional vector. Concurrent Full Pareto learning SOM(CFP-SOM) using multi-modal vector composed of 23 elements(15 keystroke timing and 8 typing sound) is applied to authentication system. Figure 20 shows the result. At the cross point, FRR=FAR=0.121, and the average size of the Pareto set for registered user and unregistered user are 17.95 and 27.95 respectively. FRR and FAR are much improved compared with the previous experiment because the difference of the size of Pareto set becomes larger.

Figure 20 shows the FRR and FAR of each user for experimental result of CFP-SOM. With checking each user, FARs of user 9 and user 6 are too large. Such users are called as "SHEEP" and are not adequate for this authentication method. Excluding user 6 and 9, average of FRR=0.112, FAR=0.070, and they are better than that of SP-SOM(FRR=0.187, FAR=0.065) which are conducted in the same setting of the experiment using CFP-SOM.

Figure 21 shows the experimental result with changing map size. TH_p is fixed to 1.4. With changing map size, FAR is not improved, however FRR is improved by enlarging map size. For map size 9x9, average of FAR=0.095, FAR=0.123, and FRR =0.090m FAR=0.061 excluding user 6 and 9.
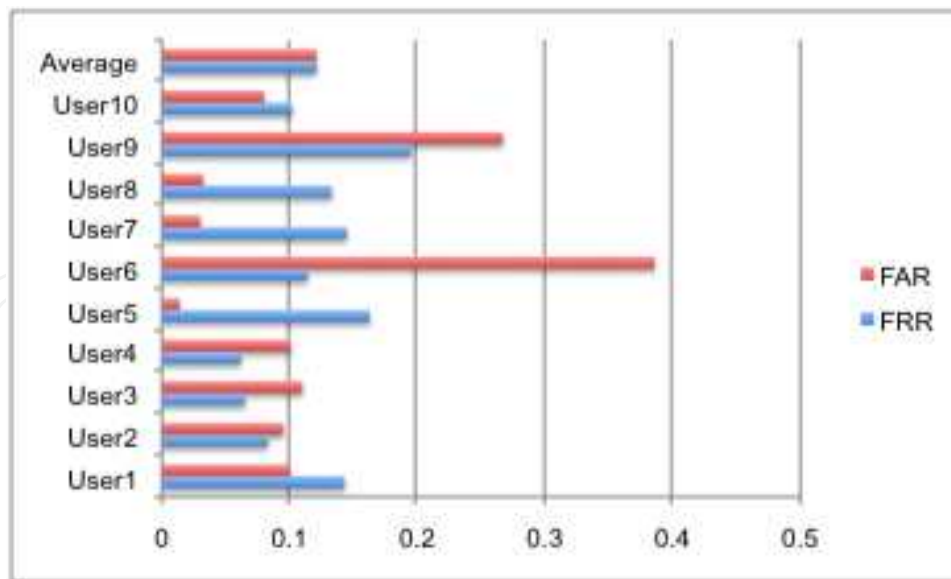
Figure 21. FRR and FAR of each user for experimental result of CFP-SOM
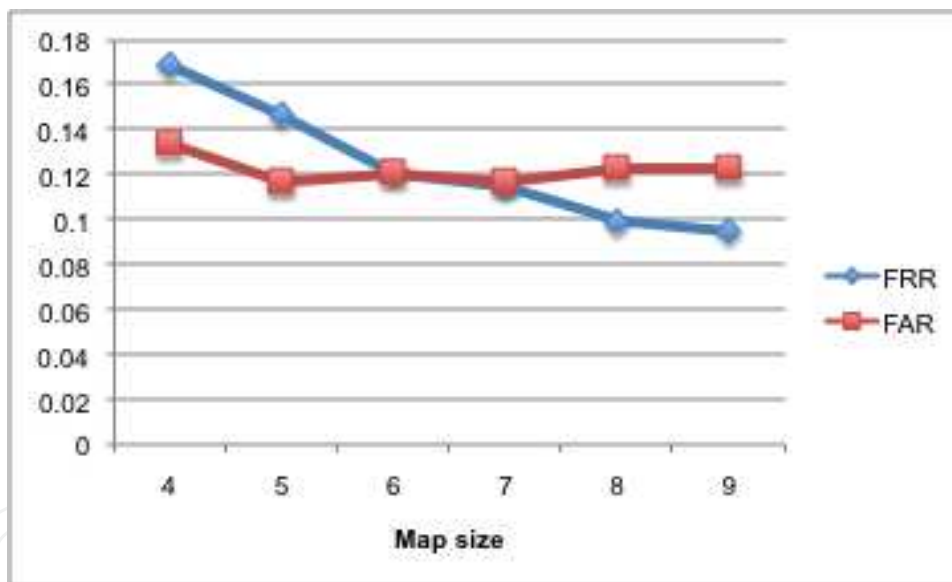

Figure 22. Experimental result with changing map size

8. Conclusions

In this chapter, application of Self Organizing Map(SOM)s to the authentication system using behavior biometrics is mentioned.

In section 3 and section 4, the application of SOM to the authentication systems using pen calligraphy and keystroke timing are mentioned respectively. SOM is used to visualize the

relations among the biometrics data of users, and is used to select the appropriate feature, and to select the appropriate patterns of behavior for authentication. For the authentication system using pen calligraphy, the pen speed data and pen pressure data is selected as the features, and drawing spiral or star on the screen are selected as the patterns of behavior. For the authentication system using keystroke timing, keystroke timing data typing "kira-kira" is selected as the behavior. These systems show superior performance considering the simplicity of these methods. However, using single behavior biometrics, enough accuracy is hard to be accomplished.

In section 5, the application of SOM to the authentication system using multi-modal behavior biometrics is mentioned. As the multi-modal behavior biometrics, pen calligraphy drawing the symbols and keystroke timing which are measured on tablet PC are used. Supervised Pareto learning SOM(SP-SOM), which can integrate multi-modal vector naively with supervised learning, is proposed, and applied to the analysis of multi-modal biometric features and to the authentication system. The accuracy of authentication is improved compared with that of single behavior biometrics without disturbance from unreliable features.

In section 6, the application of SP-SOM to the authentication system using multi-modal behavior biometrics of keystroke timing and key typing sound is mentioned. These features can be measured simultaneously during typing a phrase. Additionally, the adaptive authentication system, which can follow the changes of biometrics by the time, is examined. The authentication system shows superior accuracy with following changes of keystroke timing by the time without disturbed by noises. As the practical authentication system, the unregistered users are detected using the size of the Pareto set and category magnitude of the user inputs.

In section 7, Concurrent Full P-SOM(CFP-SOM), which uses small map for each user, is applied to the authentication system using multi-modal behavior biometrics. CFP-SOM is suitable for mobile system because it only needs the learning data of single user, in contrast, SP-SOM needs the learning data of some users. CFP-SOM classifies the registered user from unregistered users using the size of Pareto set. With adjusting the threshold of size of Pareto set, the accuracy becomes almost same or better compared with that of SP-SOM.

As the future work, the adaptive algorithm for CFP-SOM should be developed. CFP-SOM needs the adjustment of threshold to apply to authentication system, thus adaptive scheme for the threshold is required. Furthermore, P-SOM and SP-SOM is a generic extension of SOM, and it can be applied to many applications, which need both of visualization and classification by supervised learning. P-SOM and SP-SOM can be used to integrate the multiple objects for which distance metric is defined. The novel application from this point of view should be explored.

Author details

Hiroshi Dozono

Faculty of Science and Engineering Saga University, Honjyo Saga, Japan

References

[1] Bolle R., Connell J., Pankanti S., Ratha N., Senior A.Guide to Biometrics, Springer; 2004

[2] Monrose F., Rubin A.D., Keystroke Dynamics as a Biometric for Authentication. Future Generation Computer Systems: March;2000

[3] Brault J.J., Plamondon R. A Complexity Measure of Handwritten Curves: Modelling of Dynamic Signature Forgery. IEEE Trans. Systems, Man and Cybernetics. 1993; 23 400-3

[4] Kohonen T. Self Organizing Maps, Springer;ISBN 3-540-67921-9

[5] Dozono H., Nakakuni M., et al. The Analysis of Pen Pressures of Handwritten Symbols on PDA Touch Panel using Self Organizing Maps. Proceedings of the International Conference on Security and Management; 2005: 440-5.

[6] Dozono H., Nakakuni M., et al. The Analysis of pen Inputs of Handwritten Symbols using Self Organizing Maps and its Application to User Authentication. Proceedings of 2006 International Joint Conference on Neural Networks: 2006; 4884-9.

[7] Dozono H., Nakakuni M., et al. The Analysis of Key Stroke Timings using Self Organizing Maps and its Application to Authentication. Proceedings of the International Conference on Security and Management; 2006: 100-5

[8] Dokic S., Kulesh A., et al. An Overview of Multi-modal Biometrics for Authentication. Proceedings of the International Conference on Security and Management; 2007: 39-44

[9] Nakakuni M., Dozono H., et al. Application of Self Organizing Maps for the Integrated Authentication using Keystroke Timings and Handwritten Symbols. WSEAS TRANSACTIONS on INFORMATION SCIENCE & APPLICATIONS. 2006; 2-4 413-420

[10] Dozono H., Nakakuni M., et al. Application of Self Organizing Maps to User Authentication Using Combination of Key Stroke Timings and Pen Calligraphy. Proceedings of the 5th WSEAS Int. Conf. on COMPUTATIONAL INTELLIGENCE; 2006: 105-10

[11] Dozono H., Nakakuni M., et al. Application of the Supervised Pareto Learning Self Organizing Maps to Multi-modal Biometric Authentication. Journal of Information Processing Society of Japan. 2008 49(9) 3028-37

[12] Dozono H., Nakakuni M., et al. Comparison of the Adaptive Authentication Systems for Behavior Biometrics using the Variations of Self Organizing Maps

[13] Dozono H., Nakakuni M., et al. The Adaptive Authentication System for Behavior Biometrics Using Pareto Learning Self Organizing Maps. Neural Information Processing Models and Applications ICONIP 2010. Springer; 2010 LNCS6444 383-90

[14] Dozono H., Nakakuni M., et al. The Authentication System for Multi-modal Behavior Biometrics Using Concurrent Pareto Learning SOM, Artificial Neural Networks and Machine Learning- ICANN 2011. Springer; 2011 LNCS6792 197-204

[15] Dozono H., Nakakuni M., et al. Application of Supervised Pareto Learning Self Organizing Maps and Its Incremental Learning. Advances in Self Organizing Maps WSOM 2009. Springer; 2009 LNCS 5629 54-62

[16] Neagoe, V., E., Ropot, A., D. Concurrent Self-Organizing Maps for Pattern Classification, Proceeding ICCI '02 Proceedings of the 1st IEEE International Conference on Cognitive Informatics; 2002: 304-12