Application of Adaptive Neuro-Fuzzy Inference System in Multimodal Biometrical Identification

Gabor Werner*, Arnold Őszi*, László Hanka Ph.D.**
* Applied Biometric Institute, Óbuda University, Budapest, Hungary
** Institute of Mechatronics and Vehicle Engineering, Óbuda University, Budapest, Hungary
wga.bme@gmail.com
hanka.laszlo@bgk.uni-obuda.hu

***Abstract*—In the modern society, the rights and the limitations became a crucial part of the everyday life. While more and more PIN code, password and RFID tag spreads, the growth of the biometrical authentication is less pronounced. Certainly, the background of this phenomenon is complex, but the efficiency and robustness are significant determinants. The multimodal identification brings biometrics closer into the everyday life. Nevertheless, to break the limits an effective and adaptive controller algorithm is necessary. In this study, the adaptive neuro-fuzzy inference system has been revealed as a possible controller algorithm in a complex biometrical identification system, which simultaneously accomplishes fuzzy and neural attributions.**

I. INTRODUCTION

Among the different identification methods, biometrics represents a desirable mixture of the required attributions. It can be selective, unique, hardly be stolen[1] and universal, but it has some limitations too, which is the consequence of the natural background [1] [5].

Humans, as part of nature, are constantly changing. Tough these changes are small, they can have a significant effect in total, which can even deteriorate the outcome of an identification procedure.

Either the environment or the user itself can be the source of the negative effects [2], which compared to the inner distortion (e.g. scanner error) cannot be treated with simple error correction. The system has to be prepared to change the algorithm.

A. Flexibility and accuracy

Through the conventional biometrical identification procedure, the extracted sample is compared to the stored templates. If the recognized individual identification marks (IIM) are matching, the authentication is successful. The matching inspection basically determines the whole process, because if the chosen the number of the matching IIM's limit is low, then the False Acceptance Rate (FAR) grows, in other cases the False Rejection Rate (FRR) increases [3].

Depending on the nature of the authentication is verification (one-to-one) or identification (one-to-many) and the analysis of the risks, the desired number of the matching IIMs are different. According to the correlation of the FAR and FRR (Fig. 1), the matching number cannot be changed to improve both simultaneously [4].

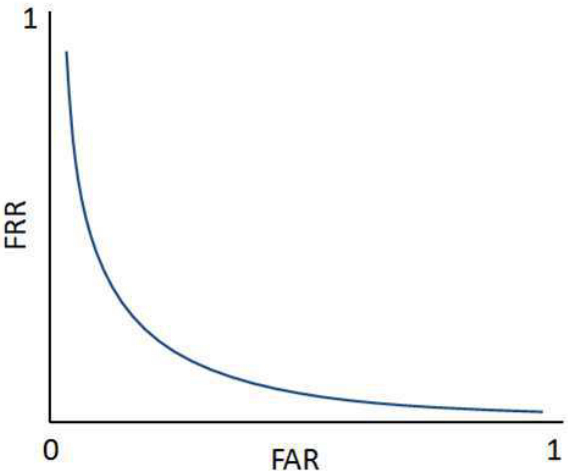


Figure 1. Correlation among FAR and FRR (source:[5])

To achieve a better operation, the Receiver Operation Characteristics (ROC) curve has to move upwards, which can be implemented with a developed extracting and matching algorithm [4] or, as the authors revealed in a former study, it can be changed by the different selection of error sources. The failure distribution can be approximated by beta-binomial distribution, due to this, if its parameters are changed, then the combined probability of error rates can be reduced. The distinct biometrical methods have different beta parameters, independently from other circumstances. As long as these biometrical method proportions are chosen well, the desired ROC will improve [6].

Thus the distinct authentication methods, i.e. multi-modal biometrics, are able to simultaneously improve the failure rates. According to the security sciences, the multistep authentication is becoming widespread, but it has to be stated that the multi-factor authentication is not equal to multi-modal biometrical identification. The multi-factor (Fig. 2) literally means different forms of information (knowledge - password; possession - RFID tag; inherence - fingerprint), while the multi-modal biometrical identification is a more complex implementation of the third factor (inherence).

Due to this fact, the possession and knowledge based information is less mutable, the matching rate is 100% or 0%, so far the result of these factors is bivalent. Meanwhile,

[1] depends on the usage and types

the natural background of biometrics limits this rate and leads us to conduct a deeper investigation.

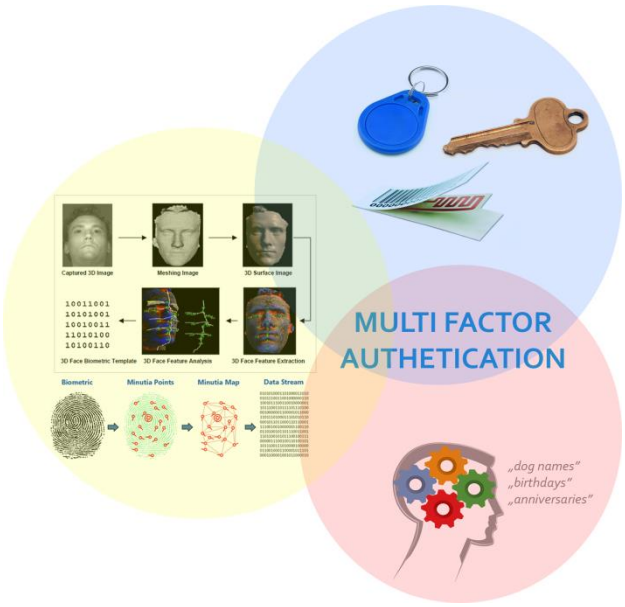


Figure 2. Multi Factor Authentication

II. MATHEMATICAL BACKGROUND

As the biometrical identification's nature is less discrete, it is favorable to use a mathematical method which is adaptable to these inaccuracies and changes.

The Soft Computing (SC) methods not only implement a flexible environment but also represent an accurate analysis for complex systems with nonlinear problems. Among the SC methods (Fuzzy Logic- FL; Genetic Algorithms - GA; Artificial Neural Networks - ANN) there are some combined techniques, like the Adaptive Neuro-Fuzzy Inference System (ANFIS), or the extended variant the Multi Adaptive Neuro-Fuzzy Inference System (MANFIS).

A. Fuzziness attributions

The fuzziness in MANFIS algorithm helps to implement linguistic uncertainty. This means that the used biometric templates will be judged by a non-conventional logic. The FL is well adoptable in risk assessment problems like biometric identification, due to it being able to handle uncertainty, imprecision and subjectivity [7].

The fuzzy set theory originates from the conventional set theory, but the sets contain the members by a membership function [8]. In this study, besides that the input variables are over the fuzzification, the process is becoming a bit more complex than a regular fuzzy logic controller algorithm, because the fuzzy parameters are optimized by an ANN.

B. Neural networks in optimization

In this presented approach the fuzzy logic is hidden in an artificial neural network which is structured to learn the optimal setting of fuzzy inference.

The ANNs are based on the biological background of the human brain, which means there are points (neurons) and linkages (synapses) among them. These linkages have a weight number which represents the strength of the connection between two neurons [9]. In the presented algorithm these weight numbers will represent the fuzzy parameters.

C. Structure of the ANFIS

According to the multiple advances of the fuzzy and neural systems, the mixed implementation worth the effort. One of the possible combinations is the Adaptive Neuro-Fuzzy Inference System (ANFIS) or the multiple outcome type of this, the MANFIS. The role of this module in the detection phase is to set up the reliability index of the different sensors. The fuzzy attributions are the unknown premise and consequent parameters, which have to be set during the learning phase [8]. Figure 3 shows the structure of the implemented ANFIS.

Premise parameters:

$$\mu_{A_i}(x) = \frac{1}{1 + \left|\frac{x - c_i}{a_i}\right|^{2b_i}} \tag{2.1.}$$

where A determines the input set (A;B;C) and i represents the degree of the granulation in the fuzzy sets (i=2, in the implemented algorithm)

Consequent parameters:

$$f_{ijk} = p_{ijk}x + q_{ijk}y + r_{ijk}z + s_{ijk} \tag{2.2.}$$

where i,j,k represents the degree of the granulation in the fuzzy sets (i,j,k=2)

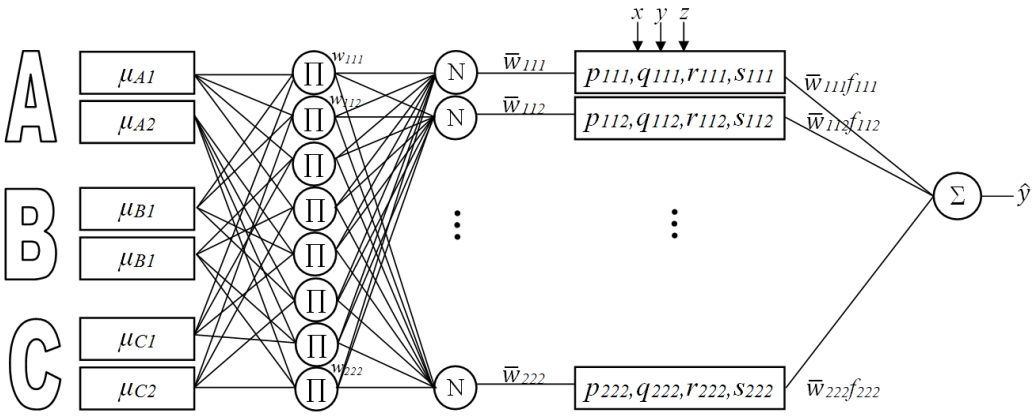


Figure 3. The structure of the implemented ANFIS algorithm

The shape of the membership functions in the first layer is a Gaussian Function, which curving is determined by a_{ijk}, b_{ijk}, c_{ijk} adaptive *premise parameters*. In the second layer $\prod$ as a fix, recapitulative operator stands. The outcome of the second layer (w_{ijk}) is the computed strength of the incoming firing membership functions:

$$w_{ijk} = \mu_{A_i}(x) \cdot \mu_{B_i}(y) \tag{2.3.}$$

In the third layer the fix neurons are normalizing the incoming values: ($\bar{w}_{ijk}$):

$$\bar{w}_{ijk} = \frac{w_{ijk}}{\sum_1^{ijk} w_{ijk}} \tag{2.4.}$$

In the fourth layer the Sugeno type implications (which uses the original input variables) are multiplied by the normalized firing strength of the membership functions, where p_{ijk}, q_{ijk}, r_{ijk} and s_{ijk} represent the linear combination's parameters (*consequents parameters*) of the incoming variables, as it has found by Sugeno [10]. The outcome of the fourth layer is:

$$\bar{w}_{ijk} f_{ijk} = \bar{w}_i (p_{ijk} x + q_{ijk} y + r_{ijk} z + z_{ijk}) \tag{2.5.}$$

In the last layer there is only one neuron. Its task the summarizing of the previous values.

$$o_{ANFIS} = \sum_1^{ijk} \bar{w}_{ijk} f_{ijk} \tag{2.6.}$$

III. Applied MANFIS Algortihm for Multibiometric Indentification

The implemented algorithm in this study has three possible inputs, which means that, there can be three investigated vectors as an incoming data. The author's former study investigated a two input structure, consequently it seemed worthwhile to develop.

Though the possible number of the inputs is three, it doesn't mean that there must be three different kinds of biometrical traits. Multimodality related to the possible sets of error sources, so it even works with only one biometrical trait, but with multiple sampling (Fig. 4).

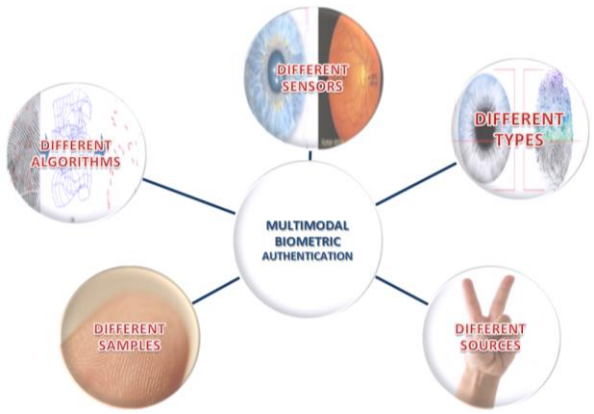


Figure 4. Possible multimodality

Through the fuzzification, the degradation of the fuzzy sets is only two, with three parameters for each like a_{ijk}, b_{ijk}, c_{ijk}, where i,j,k=2 (like in (2.1). According to Wang and Elhang it is inappropriate to choose three or more Membership Functions (MFs) for each input because in that case, the parameters needed to be taught with a greater number of training samples [11]. These 18 variables will be the premise matrix ('`premise`').

According to the Sugeno type inference, there will be p_{ijk}, q_{ijk}, r_{ijk}, *and* s_{ijk} parameters, where i,j,k=2, these 32 parameters are the consequent matrix's components ('`consequent`') (like 2.2). These two matrices have to be optimized during the learning phase, which can be implemented in various ways. According to Jang [12] it is possible to train in a forward pass and a backward pass. In this approach the backward pass has been chosen with a gradient descent method, that is precisely a special back propagation, the Resilient Back Propagation (Rprop) learning rule (3.1) [13].

$$\Delta w_{ijk}^{(t)} = \begin{cases} -\Delta_{ijk}^{(t)}, \ if \ \frac{\partial E^{(t)}}{\partial w_{ijk}} > 0, \\ +\Delta_{ijk}^{(t)}, \ if \ \frac{\partial E^{(t)}}{\partial w_{ijk}} < 0 \\ 0, otherwise \end{cases} \tag{3.1.}$$

$\Delta w_{ijk}^{(t)}$: direction of weight update
$\partial E^{(t)} / \partial w_{ijk}$: summed gradient of the error partial derivates (Error is the different of target and the current output)

In this kind of back propagation, instead of the value of the partial derivative, only the sign of the derivative is important, which determines the direction of the weight step ($\Delta w_{ijk}^{(t)}$). Certainly, it is necessary to find a way to determine the size of the correction steps, which is the following. The update-value ($\Delta_{ijk}^{(t)}$) based on a sign dependent adaptation process (3.2.) [13].

$$\Delta_{ijk}^{(t)} = \begin{cases} \eta^+ \Delta_{ijk}^{(t-1)}, & if \ \frac{\partial E^{(t-1)}}{\partial w_{ijk}} \cdot \frac{\partial E^{(t)}}{\partial w_{ijk}} > 0 \\ \eta^- \Delta_{ijk}^{(t-1)}, & if \ \frac{\partial E^{(t-1)}}{\partial w_{ijk}} \cdot \frac{\partial E^{(t)}}{\partial w_{ijk}} < 0 \\ \Delta_{ijk}^{(t-1)}, & otherwise \end{cases} \tag{3.2.}$$

The η^- and η^+ factors are proposed to be 0.5 and 1.2, according to the author of this Rprop.

A. How to use the MANFIS

The table below lists a sort of biometrical methods which vectors result from the outcome of the transformation of the biometric traits. The vectors are used during the biometrical identification, but at this point, an index number about the goodness of the extractable information is necessary.

This value, like a benchmark index, is correlated to the size of vector's component because this qualifies the biometrical sample's conformity. The bigger the identifiable IIM's amount, the better the fitting of the given biometric modality.

Table 1. List of different template transformation techniques available in literature and their characteristics.

Technique	Trait	Features	Transformation	Final representation
Biohashing PalmHash	Face, Palmprint, Fingerprint	Vector (Fisher Discriminant Features)	Random matrix multiplication	Vector
BioPhasor	Fingerprint	Vector (FingerCode)	Non-linear	Vector
Cancelable Face	Face	Vector (Face image)	Random matrix convolution	Vector
Robust Hash	Face	Vector (Singular Values of face image matrix)	Smooth multimodal function evaluation	Vector
Class Distribution Preserving Transformation	Face	Vector (Fisherface features)	Evaluation of distance of the feature vector from a set of points	Vector
Cancelable Iris	Iris	Vector (Log-Gabor response)	Circular shift and combination, adding new pattern	Vector
Histogram of minutiae triangle	Fingerprint	Interest point	Hashing the histogram of minutiae triangle features	Vector
Symmetric Hash	Fingerprint	Interest point (Minutiae as complex numbers)	Set of order invariant functions of minutiae	Minutiae map
Cancelable Finger Prints	Fingerprint	Interest point (Minutiae map)	Image folding	Minutiae map
Alignment free cancelable fingerprint	Fingerprint	Interest point (minutiae map, orientation field)	Transform minutiae according to surrounding orientation field	Minutiae map
Cuboid based Minutiae Aggregates	Fingerprint	Interest point (Minutiae map)	Minutiae aggregate feature selection from random local regions	Vector

According to Kryszczuk and Drygajlo there are more possibilities to get an index number for classification. In a conventional biometric classification system with quality measurement has two sources of complementary information: the baseline scores and the quality measures. The baseline scores are obtained from biometric classifiers operating on feature sets derived from class-selective raw biometric data and can be viewed as a compressed representation of this data. The quality measures convey information about the conditions of data acquisition and the extent of extraneous noise that shapes the raw data and therefore are class-independent. In order to make use of the quality information, many algorithms have been proposed - for single classifier systems they were often referred to as adaptive model/threshold selection, while for multiple classifier systems they are frequently referred to as quality-dependent fusion [14].

There are several methods of how to be classified by the quality indexes like an Additive Noise Model or Multiplicative Noise Model with different classifier types; Linear Discriminant Analysis - based analysis (LDA), Quadratic Discriminant Analysis - based classifier: QDA, a Bayes classifier using Gaussian Mixture Model - based distribution representation: Bayes, and a Support Vector Machines - based classifier using RBF kernel: SVM. [15] [16].

The authors also investigated the research of M. Abreu and M. Fairhurst, who compared the individual machine learning techniques in signature and fingerprint classification. However, there were more classifier techniques which are based on ANN, the best result was achieved by the fuzzy Multi-Layer-Perceptron [16].

According to this and the empirical results the fuzzy-neuro hybrid models, the MANFIS is fitting into the nature of these analyzed problems [17].

In the implemented algorithm three different inputs have been set, representing three biometric modalities to each ANFIS. One ANFIS block is dedicated to representing the relative quality of one modality to the others. The analogy is the following: each incoming dataset has to be compared to the other modalities by benchmark index, which is correlated to the quality of dataset. For instance, the quality of a fingerprint sample has to be compared to the face and palmprint modal's quality. Following the comparison, the result of the ANFIS can determine the severity of the matching or the final decision which is done by the summing decision block (Fig. 5).

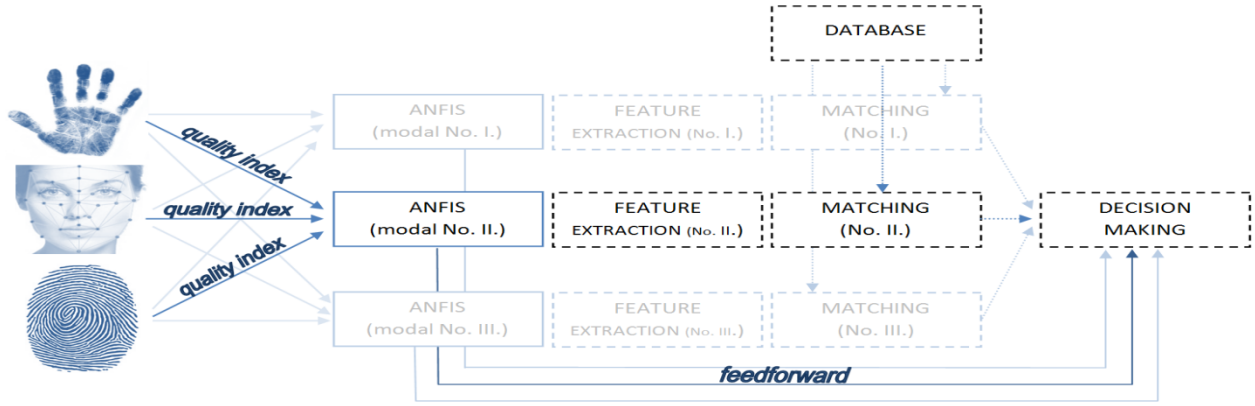


Figure 5. MANFIS block diagram in biometric identification

IV. RESULTS

The constructed algorithm has been designed in MATLAB, and the η^- and η^+ factors were chosen to be 0.5 and 1.2, according to resilient back propagation's studies. Finally, as a multimodal input, three different fingerprint readers were chosen (BioEntry+, iEVO, Bioscrypt).

The quality index was the elapsed time of identification process (*the maximum elapsed time was limited to 15 seconds*), meanwhile, the target (4.1) was determined by the particular ratio of (1-FRR).

$$target_A = \frac{1 - FRR_A}{(1 - FRR_A) + (1 - FRR_B) + (1 - FRR_C)}$$

$$target_B = \frac{1 - FRR_B}{(1 - FRR_A) + (1 - FRR_B) + (1 - FRR_C)}$$

$$target_C = \frac{1 - FRR_C}{(1 - FRR_A) + (1 - FRR_B) + (1 - FRR_C)} \quad (4.1)$$

The elapsed time and the FRR pairs were calculated as an average amount of ten attempts blocks. According to this, the distribution is quite discrete, so the target function is peaked. The database contains 200 time-FRR pairs for each fingerprint reader, which means 6000 attempts in total. The algorithm has been trained and tested with two tables, which contain 100-100 blocks of multimodal biometric data. The results have been shown in the following figures (Fig. 6).

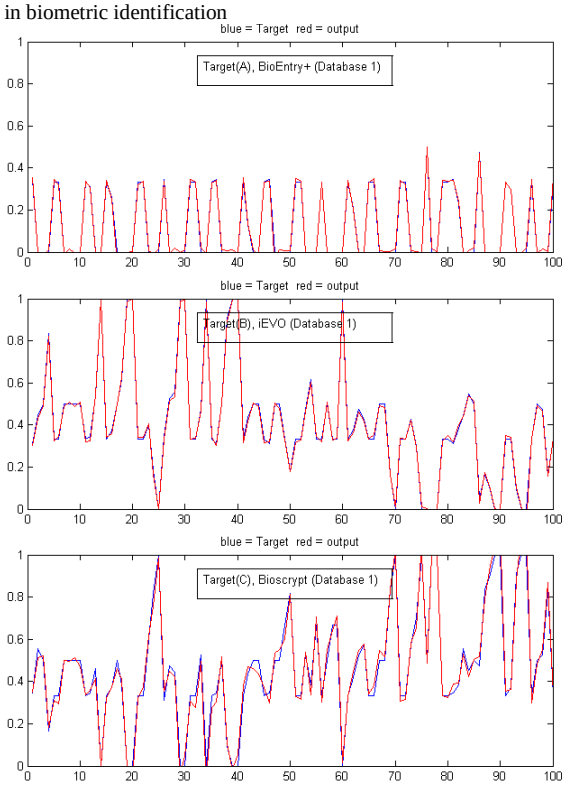
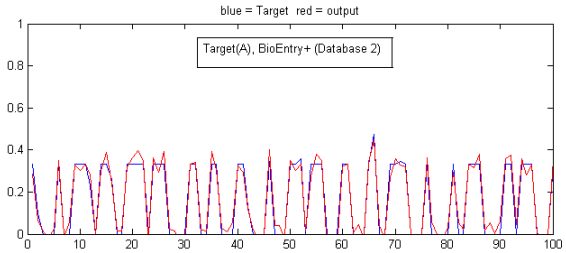


Figure 6./A Desired and target output of different modals (database 1)



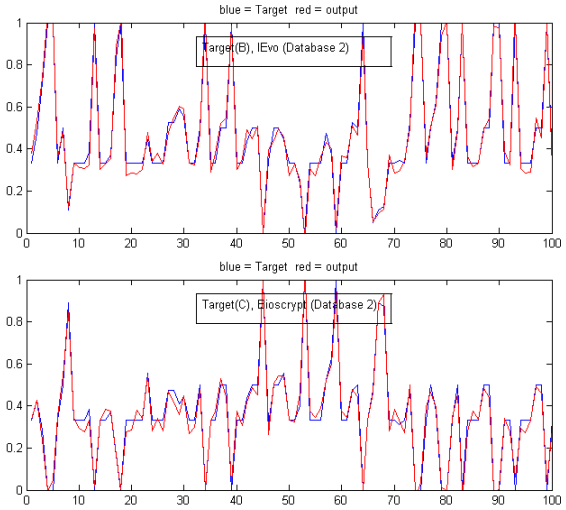


Figure 6./B Desired and target output of different modals (database 2)

CONCLUSIONS

As it was shown, the presented method and algorithm are able to be adaptive, thus the multimodal identification can be more flexible. A multiple adaptive neuro-fuzzy inference system (MANFIS) can be trained with a database to recognize the quality of the input information, which helps to optimize the pattern analysis and the decision process through the biometrical authentication.

REFERENCES

[1] A. Jain, L. Hong, and S. Pankanti, "*Biometric Identification*," in Communications of the ACM, Vol. 43. No. 2, February 2000 0002-0782/00/0200

[2] S. J. Elliott, E. P. Kukula, N. C. Sickler, The Challanges of the Environment and the Human / Biometric Device Interaction on Biometric System Performence, Biometric Standards, Performence, and Assurance Laboratory, Department if Industrial Technology, Purdue University, West Lafayette, US

[3] T. Kovács, I. Milák, Cs. Otti, Biometrical Aspects of Security Sciences, Pécs: Pécsi Határőr Tudományos Közlemények, XIII. kötet, HU ISSN 1589-1674, 2012.

[4] S. A. Sudiro, R. T. Yuwono, Adaptable Fingerprint Minutiae Extraction Algorithm Based-on Crossing Number Method for Hardware Implementaion using FPGA Device, Gunadarma University, Jl. Margonda Raya 100, Depok, Indonesia, DOI: 10.5121/ijcseit.2012.2301

[5] M. El-Abed, C. Charrier, Evaluation of Biometric Systems, InTech, DOI:10.5772/52084, 2012

[6] Werner, G., Hanka, L. (2015). Using the Beta-Binomial Distribution for the Analysis of Biometric Identification, *SISY 2015 IEEE 13th International Symposium on Intelligent Systems and Informatics*, p. 209-215. ISBN 978-1-4673-9388-1.

[7] E. Tóth-Laufer, A Flexible Fuzzy Logic-based Risk Assessment Framework, Óbuda University e-Bulletin, Vol. 6. No. 1. pp. 3-8, 2016

[8] Sang-hyun, L., Jeong-gi L., Kyung-il, M. (2013, May); Smart Home Security System Using Multiple ANFIS, *International Journal of Smart Home* , Vol. 7., No. 3, p. 121-132.ű

[9] Hajek, M. (2005) Neural Networks, University of KwaZulu-Natal (South Africa)

[10] Kóczy, T. L., Tikk, D. (2007), Intelligent systems (Intelligens rendszerek), *Értékünk az Ember*, Szeged (Hungary)

[11] Wang, Y. M. and Elhag, T. (2008) An Adaptive Neuro-fuzzy Inference System for Bridge Risk Assessment. *Expert Systems with Applications*, Vol. 34, Issue 4., p. 3099-3106.

[12] Jang, J.-S. R., Sun, C.-T., and Mizutani, E. (1997), Neuro-Fuzzy and Soft Computing; A Computational Approach to Learning and Machine Intelligence, Prentice Hall, Upper Saddle River

[13] Weeraprajak, I., Chacko, E. (2007); New Learning Algorithm for Adaptive Network Based Fuzzy Inference System in Application of Forecasting Chaotic Time Series, University of Canterbury, Christchurch, New Zealand

[14] K. Kryszczuk, A. drygajlo, On quality of quality measures for classification; Swiss Federal Intitute of Technology Lausanne, in Biometrics and Identity Management, 2008, pp. 21-30. ISSN 0109-9779

[15] K. Kryszczuk, A. Drygajlo. Q – stack: Uni- and Multimodal Classifier Stacking with Quality Measures. In Michal Haindl, Josef Kittler, and Fabio Roli, editors, 7th International Workshop on Multiple Classifier Systems, volume 4472 of LNCS, pages 367 – 376, 2007.

[16] M. Abreu, M. Fairhurst, An Empirical Comparison of Individual Machine Learning Techniques in Signature and Fingerprint Classification, Department of Electronics, University of Kent, in Biometrics and Identity Management pp. 133-143., 2008, ISSN 0109-9779

[17] C. Cenol, T. Yildrim, Thyroid and Breast Cancer Disease Diagnosis using Fuzzy-Neural Networks, International Conference on Electrical and Electronics Engineering, 2009. DOI: 10.1109/ELECO.2009.5355297