Soft-Biometrics: Soft-Computing Technologies for Biometric-Applications

Katrin Franke[1] and Javier Ruiz-del-Solar[2]

[1] Dept. of Pattern Recognition, Fraunhofer IPK, Berlin, Germany,
E-mail: katrin.franke@ipk.fhg.de
[2] Dept. of Electrical Engeneering, Universidad de Chile, Santigo, Chile,
E-mail: jruizd@cec.uchile.cl

Abstract. Biometrics, the computer-based validation of persons' identity, is becoming more and more essential due to the increasing demand for high-security systems. A biometric system testifies the authenticity of a specific physiological or behavioral characteristic possessed by a user. New requirements over actual biometric systems as robustness, higher recognition rates, tolerance for imprecision and uncertainty, and flexibility call for the use of new computing technologies. In this context soft-computing is increasingly being used in the development of biometric applications. Soft-Biometrics correspond to a new emerging paradigm that consists in the use of soft-computing technologies for the development of biometric applications. The aim of this paper is to motivate discussions on application of soft-computing approaches in specific biometric measurements. The feasibility of soft-computing as a tool-set for biometric applications should be investigated.

1 Introduction

Biometrics offers new perspectives in high-security applications while supporting natural, user-friendly and fast authentication. Biometric identification considers individual physiological characteristics and/or typical behavioral patterns of a person to validate their authenticity. Compared to established methods of person identification, employing PIN-codes, passwords, magnet- or smart cards, biometric characteristics offer the following advantages:

- They are significant for each individual,
- They are always available,
- They cannot be transferred to another person,
- They cannot be forgotten or stolen,
- They always vary [1].

Although, there was a strong growth in biometric technologies during the past years [1], the introduction of biometrics into mass market applications, like telecommunication or computer-security, was comparable weak [9].

[1] Rem.: The presentation of two 100% identical feature sets indicates fraud.

From our point of view there are three main aspects responsible for the current situation. First, soft- as well as hardware (sensor) technologies are still under development and testing, although, black sheep promising 100 percent recognition rates. Second, there is a lack of standardization and interchange of biometric systems; basically, such systems are proprietary. And third, there are only few large-scale reference projects that gave evidence of the usability and acceptance of biometrics into real worlds applications.

The work presented in this paper will contribute to the first aspect by employing soft-computing approaches to improve algorithms of biometric analysis. The aim is to provide tool-sets that are able to handle natural variations being sticking in biometrics. Also, the tool-sets should be tractable, robust and of low costs. So, the authors studied soft-computing approaches and their feasibility into biometric measurements.

Section 2 gives a short overview on biometrics where section 3 introduces soft-computing. Section 4 deals with the introduction of soft-computing into biometric application and claims the paradigm of soft-biometrics. A realized application examples, in particular for signature verification, will be described in section 5. Finally, section 6 concludes the presented work and provides some practical hints.

2 Biometrics

Biometric systems comprise the following components: data acquisition and preprocessing; feature extraction and coding; computation of reference data and validation. The systems compare an actual recorded characteristic of a person with a pre-registered characteristic of the same or another person. Thereby, it has to be decided between *identification* (1 to many comparison) and *verification* (1 to 1 comparison). Then, the matching rate of the both characteristics is used to validate, whether the person is what they claim to be. The procedures seem to be equivalently to the traditional methods using PIN or ID-number. However, the main difference is founded by the fact that in biometrics an absolute statement *identical / not identical* cannot be given. For instance a credit card has exact that number "1234 5678 9101" or not, contrary, a biometric feature varies naturally at any acquisition.

Biometric technologies will be divided into approaches utilizing *physiological* characteristics, also referred as *passive* features, and approaches using *behavioral* characteristics that are *active* features. Behavioral characteristics, used e.g. in speaker recognition, signature verification or key-stroke analysis are always variable. On the other hand physiological characteristics employed e.g. in hand, fingerprint, face, retina or iris recognition, are more or less stabile. Variations may be caused by injuries, illness as well as variations during acquisition.

Each biometric system has to be able to handle diverse variation by using "tolerance-mechanisms". Also, it should be possible to adjust a statement about a person's identity gradually with a certain probability, and, it should allow

for tuning a system not to reject a person falsely or to accept another person without permission.

Due to the variability of the biometric characteristics, a resulting error rate cannot be easily assigned. However, adapted algorithms that are able to handle inaccuracies and uncertainty might slow down resulting error rates.

Biometric approaches have to solve the two-class problem *person accepted* or *person rejected*. So, the performance of biometric systems is measured with two basic rates: False acceptation rate (FAR) is the number of falsely accepted individuals; False rejection rate (FRR) is the number of falsely rejected individuals [11].

3 Soft-computing

Since the early days of Artificial Intelligence scientists and engineers have been searching for new computational paradigms capable of solving real-world problems efficiently. Soft-Computing (SC) is one of such paradigms that has emerged in the recent past as a collection of several models of computation, which work synergistically and provide the capability of flexible information processing. The principal constituents of SC are fuzzy logic, neural networks, evolutionary computing, probabilistic reasoning, chaotic theory and parts of machine learning theory. SC is more than a melange of these disciplines, it is a partnership, in which each of the partners contributes a distinct methodology for addressing problems in its domain. In this perspective, these disciplines are complementary more than competitive.

4 Soft-Biometrics: Soft-computing and Biometrics

SC being able to consider variations and uncertainty is suitable for biometric measurements due to the following reasons:

- Biometric features do not have an absolute "ground truth" and they will hardly reach this. Biometric features always vary!
- Derivations from the "ideal" biometric characteristic are difficult or even unable to describe analytically.
- High accuracy within the measurement may cause inflexibility and the loss of generalization ability.

SC is increasingly being used in biometric systems whereas biometrics employing SC approaches are referred as *soft-biometrics*.

The general biometric system whose block-diagram is shown in figure 1 is made of a pre-processing module (PP); a feature extraction and coding module (FE/C); a reference determination and/or classifier generator module (RD/CG); an analysis and validation module (AV) and a result fusion module (RF). The PP-module comprises diverse methods that treat recorded data in such a way that significant features can be extracted easily. The FE/C-module includes

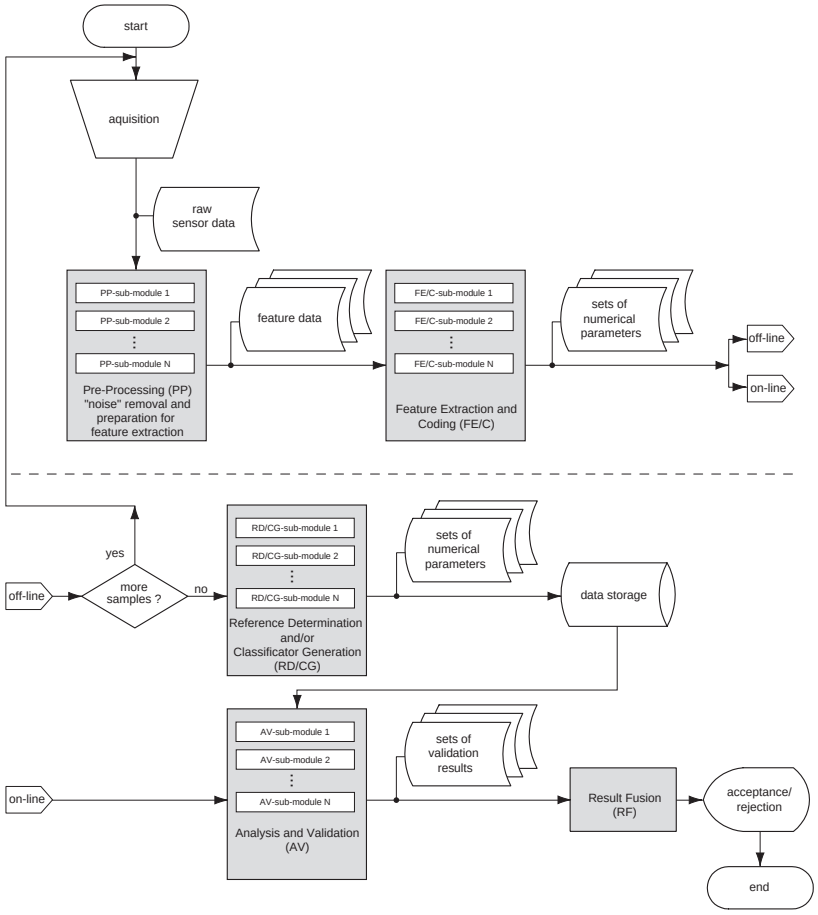

Fig. 1. Block-diagram of a biometric system in general

methods that convert treated input data into numerical parameters, which represent specific aspects of a biometric characteristic. Within the RD/CG-module the numerical parameters are used to determine reference/template-data or to generate classifiers. It is only employed in the off-line phase during enrollment/training. The AV-module is activated during the on-line phase to analyze and to validate the numerical parameters of a questioned (also called sample) characteristic. Last but not least the RF-module combines different outputs, in case there is more than one AV-module, to decide whether a person is what they claim to be.

SC can be introduced into any component/module of a biometric system. The application of SC as classifiers or decision-ruler is widely spread [10], whereas, SC in pre-processing and feature extraction is sparsely used. From our point of view the application of SC in biometrics has to be decided individually. Since SC

is always data-driven, the available data has to be analyzed to decide in detail whether it is useful to employ SC or not.

To give an example. In fingerprint identification for the matching of e.g. 14 minutia the application of SC is overpowered, contrary in static signature verification, here, e.g. the number and shape of signature strokes varies. (Rem.: In case there are two almost identical sets of strokes it indicates fraud.) Consequently, SC approaches might be employed if the biometric features are of high complexity, less accurate and an analytical description is time consuming or almost impossible (see figure 2).

On the other hand it does not make sense to feed SC approaches with any available detail of a biometric characteristic. As in the traditional approach features that are considered during validation have to be significant. Here, SC can support the selection of typical details of a biometric characteristic.

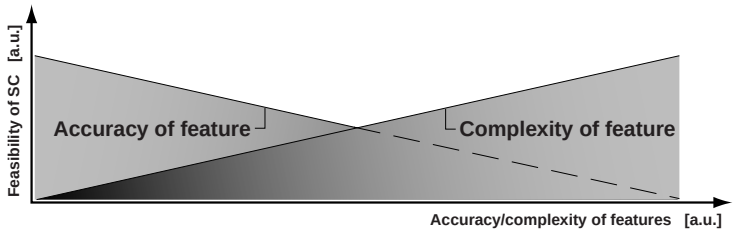

Fig. 2. Feasibility of soft-computing depending on complexity and accuracy of the biometric features

5 Application Example: Signature Verification

In signature verification artificial neuronal networks (ANN) were mainly employed as trainable classifiers [8],[10]. Until now there are only few approaches that use other SC approaches (e.g. fuzzy logic (FL) and/or evolutionary computation (EC)), too [12].

During the past years we have developed the *SIC Natura* system [4], [3] for signature verification that includes SC methods in the document-PP-module, in the RD/CG-module and within the AV-module.

For pre-processing, in particular for the elimination of textured backgrounds on paper documents, EC was considered [2], [3]. During a preparation phase a probe and a goal image has to be presented to the *LUCIFER* system, which generates morphological images-processing-filters for further usage (see figure 3).

To derive fuzzy matching rules a neuro fuzzy approach proposed by Kosko [7] is employed within the RD/CG module [5]. Thereby, questioned and reference signatures are threaded morphologically to derive such called regions. Then, human labeled region-training-sets are used to select and to adapt fuzzy rules for upcoming region matching within the AV-module.

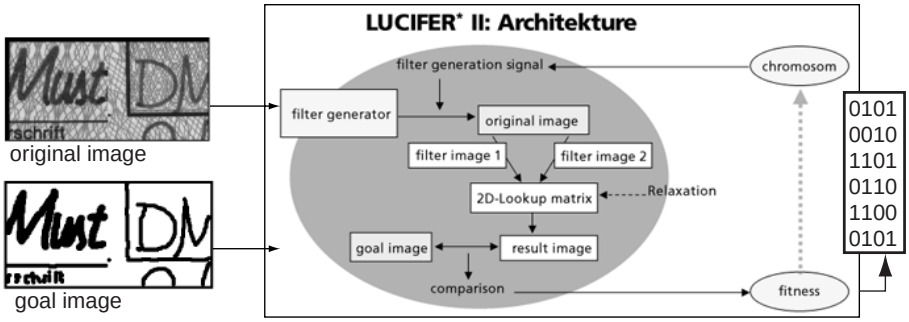

Fig. 3. LUCIFER-module for background filter generation

Here, soft-computing technologies are employed to derive a sophisticated schema for the region approach validating the spatial organization of signatures. A comparative study with the first empirically determined rules as well as the increasing of the achievable matching rate by 20% for the manual designed rules up to 98% for the automatically approximated rules punctuate the performance of soft-computing technologies in real-life applications. As it can be seen in table 1, the studied SOM-net providing 35 rules is mostly effective, compared to the 45 rules the applied 35 rules provide the same error of 1.98% (117 falsely classified region pairs out of 5914 region pairs).

Net nodes	Number of rules	MSE 1. stage	MSE 2. stage	Err. train. data	Err. all data
3×8	19	0.0327	0.0286	129	255
3×12	29	0.0281	0.0217	98	202
3×16	35	0.0216	0.0171	55	117
3×24	54	0.0180	0.0131	45	117

Table 1. Result for SOM-architectures providing different numbers of adapted fuzzy rules. The total number of samples was 2929 for training and 5914 for testing.

Since there is a bundle of feature extraction and validation methods within the *SIC Natura* system further work will be devoted to the fusion of sub-module-results by using fuzzy fusion (e.g. Fuzzy Integral [6]).

6 Conclusions

SC approaches can be employed within all components of the biometric system, like for data pre-processing itself or for designing of adapted pre-processing filters, also, for the extraction of significant features, for reference determination, as classifiers or as decision-ruler as well as for result fusion. SC has to be used with care in biometric applications. Take a look at the kind of biometric data that are available to make your final decision.

Acknowledgement

The authors would like to thanks Mario Köppen, Aureli Soria-Frisch, Jan Schneider and Anita Stellmacher for inspiring discussions about soft-computing and biometrics.

References

1. Elsevier Advanced Technology, *Biometrics technology today*, 01/1997-02/2000.
2. K. Franke and M. Köppen, *Towards an universal approach to background removal in images of bankchecks*, in Proceedings 6th International Workshop on Frontiers in Handwriting Recognition (IWFHR), Tajon, Korea, 1998.
3. ———, *A computer-based system to support forensic studies on handwritten documents*, International Journal on Document Analysis and Recognition, 3 (2001), pp. 218–231.
4. K. Franke, M. Köppen, B. Nickolay, and S. Unger, *Machbarkeits- und Konzeptstudie Automaisches System zur Unterschriftenverifikation*, tech. rep., Fraunhofer IPK Berlin, 1996.
5. K. Franke, Y.-N. Zhang, and M. Köppen, *Static signature verification employing a kosko-neuro-fuzzy approach*. submitted to the International Conference on Fuzzy Systems (AFSS) 2002.
6. M. Grabisch and J.-M. Nicolas, *Classification by fuzzy integral: Performance and tests*, Fuzzy Sets and Systems, 65 (1994), pp. 255–271.
7. B. Kosko, *Fuzzy Engineering*, Prentice Hall Internationall, Inc., 1997.
8. F. Leclerc and R. Plamondon, *Automatic signature verification: the state of the art-1989-1993*, International Journal of Pattern Recognition and Artificial Intelligence, 8 (1994), pp. 643–660.
9. E. Newham, C. Bunney, and C.Mearns, *Biometrics report*, 1999.
10. J. Schneider, K. Franke, and B. Nickolay, *Konzeptstudie - Biometrische Authentifikation*, tech. rep., Fraunhofer IPK Berlin, 2000.
11. Tele Trust - AG 6, *Biometrische Identifikation - Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren*, 1998.
12. X. Yang, T. Furuhashi, K. Obata, and Y. Uchikawa, *Constructing a high performance signature verification system using a GA method*, in Proceedings 2nd New Zealand International Two-Stream Conference on Artificial Neural Networks and Expert Systems, Dunedin, New Zealand, 1995, pp. 170–173.