Journal of Basic and Applied Engineering Research
Print ISSN: 2350-0077; Online ISSN: 2350-0255; Volume 1, Number 7; October, 2014 pp. 34-37

http://www.krishisanskriti.org/jbaer.html

Soft Biometrics: A Survey of Soft Computing for Biometrics

Prabha Sharma

[1]*CSE, Hoshiarpur*

Abstract: **Biometrics, the computer-based validation of a 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.**

Keywords: **Soft-computing, biometrics, soft-biometrics**

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 telecommunications or computer- -security, was comparable weak [3].

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 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. This paper's aim is to provide to give an overview on biometrics and introduction of soft-computing into biometric application.

2. BIOMETRICS

Biometric systems comprise the following components: data acquisition and pre-processing; feature extraction and coding; computation of reference data and validation. The systems compare an actual recorded characteristic of a person with a preregistered 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 he/she 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 and aging, 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 a resulting error rate cannot be easily assigned. However, adaptable 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 [5].

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 [6]. SC technologies are currently attracting a great deal of attention and have already found a number of practical applications ranging from industrial process control, fault diagnosis and to speech recognition, image processing and pattern recognition[2]. We are going to concentrate ourselves in the description of fuzzy logic, neural networks and evolutionary computing, because these are the SC technologies most used in biometric applications. In this perspective, the principal contribution of fuzzy logic is to provide algorithms for dealing with imprecision and approximate reasoning and computing with words, while neural network theory provides an effective methodology for learning from examples, and evolutionary computing a way to solve search and optimization problems. Fuzzy Logic (FL) corresponds to a mathematical approach for translating the fuzziness of linguistic concepts into a representation that computers can understand and manipulate. Because FL can transform linguistic variables into numerical ones without jettisoning partial truth along the way, it allows the construction of improved models of human reasoning and expert knowledge. FL and in general the fuzzy sets theory provides an approximate, effective and flexible means of describing the behavior of systems which are too complex or too ill-defined to admit precise mathematical analysis by classical methods and tools. Since the theory of fuzzy sets is a generalization of classical set theory, it has greater flexibility to capture faithfully the various aspects of incompleteness or ambiguity in information of a situation. In this way, more than to operate just with linguistic variables, modern fuzzy sets systems are designed to deal with any kind of information uncertainty. Artificial neural network (ANN) research takes its inspiration from biological neuronal systems. ANNs have some attributes as universal approximation, the ability to learn from and adapt to their environment, and the ability to invoke weak assumptions about the underlying physical phenomena responsible for the generation of the input data. ANNs are suitable to solve problems where no analytical model exists or where the analytical model is too complex to be applied. Basic units called artificial neurons that somehow model the working principles of their biological counterparts compose an ANN. Moreover, ANNs try not only to model the biological neurons but also their interconnection mechanisms and global functional properties. The mechanisms that drive natural evolution are reproduction, mutation and survival of the fittest. They allow the adaptation of life forms to particular changing environments over successive generation. From a computational point of view this can be seen as an optimization process. The application of evolution mechanisms by artificial/computational systems is called Evolutionary Computing (EC). From that we can say EC takes the power of natural selection to turn computers into automatic optimisation tools. EC algorithms are efficient, adaptive and robust search processes, producing near optimal solutions and have a large amount of implicit parallelism.

4. SOFT BIOMETRICS-SOFT COMPUTING AND BIOMETRICS

SC is increasingly being used in biometric systems whereas biometrics employing SC approaches are referred as soft-biometrics. SC, by its ability to consider variations and uncertainty is data, 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 inexibility and the loss of generalization ability. The general biometric system whose block-diagram 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 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 offline 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 [4], whereas, SC in pre-processing and feature study between different face recognition approaches was presented, which employ SC in FE/C-, RD/CG-, and AV-module. 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.

5. BIOMETRIC SYSTEM PERFORMANCE

The performance evaluation of a biometric system depends on two types of errors – matching errors and acquisition errors[18]. The matching errors consist of the following:

False Acceptance Rate (FAR)

Mistaking biometric measurements from two different be from the same person.

False Rejection Rate (FRR)

Mistaking biometric measurements from the same person to be from two different persons.

The acquisition errors consist of the following:

Failure to Capture Rate (FTC)

Proportion of attempts for which a biometric system is unable to capture a sample of sufficient quality.

Failure to Enroll Rate (FTE)

Proportion of the user population for which the biometric system is unable to generate reference templates of sufficient quality.

This includes those who, for physical or behavioral reasons, are unable to present the required biometric feature. All of the above are used to calculate the accuracy and performance of a biometric system.

Biometric systems like any authentication system are not completely foolproof. It has its own drawbacks. While a biometric is a unique identifier, it is not a secret and biometrics, once lost is lost forever (Lack of secrecy and non-replaceability).

5.1 Known Attacks on a Biometric System

Biometrics work well only if the verifier can verify two things:

- The biometric came from the genuine person at the time of verification.
- The biometric matches the master biometric on file .But a variety of problems hinder the ability to verify the above
- Noise in acquired data – Noisy biometric data caused by defective sensors, defective physical characteristics and unfavorable ambient conditions. This causes the data to be incorrectly matched or incorrectly rejected.
- Intra-class variations – The data acquired during authentication may be different from the data used to generate the template during enrollment, affecting the matching process.
- Distinctiveness – Every biometric trait has an upper bound in terms of its discrimination capabilities.
- Non-universality – A subset of the users not possessing a particular biometric.

The above-mentioned problems form the basis for many types of attacks against biometric systems.

There are 8 points in a generic biometric system which can be attacked.

Attacking the Sensor

In this type of attack a fake biometric such as a fake finger or image of the face is presented at the sensor.

Resubmitting Previously Stored Digitized Biometric Signals

In this mode of attack a recorded signal is replayed to the system bypassing to the sensor.

Overriding the Feature Extractor

The feature extractor is forced to produce feature sets chosen by the attacker, instead of the actual values generated from the data obtained from the sensor.

Tampering With the Biometric Feature Representation

The features extracted using the data obtained from the sensor is replaced with a different fraudulent feature set.

Corrupting the Matcher

The matcher component is attacked to produce pre-selected match scores regardless of the input feature set.

Tampering With the Stored Templates

Modifying one or more templates in the database, which could result either in authorizing a fraud or denying service to the person, associated with the corrupted template. A smart card

based system where the template is stored in the smart card is also vulnerable to this form of attack.

Attacking the Channel Between the Stored Template and the Matcher

Data traveling from the stored template to the matcher is intercepted and modified in this form of attack.

Overriding the Final Decision

Here the final match decision is overridden by the hacker disabling the entire authentication system.

6. CONCLUSION

Soft-Biometrics, the application of soft-computing in biometrics is motivated. SC approaches can be employed within all components of the biometric system, e.g. for data pre-processing itself or for designing of adapted pre-processing filters. Also, it can be applied for extracting significant features, for reference determination, as classifiers or as decision ruler. Along with that there is no security system that is completely foolproof. Every system is breakable with an appropriate amount of time and money. The techniques used to prevent the attacks help to increase the time, and cost of money.

REFERENCES

[1] Elsevier Advanced Technology. Biometrics technology today, 01/1997-02/2000.

[2] K. Franke and M. oppen. A computer-based system to support forensic studies on handwritten documents. International Journal on Document

[3] E. Newham, C. Bunney, and C.Mearns. Biometrics report, 1999.

[4] J. Schneider, K. Franke, and B. Nickolay. Konzeptstudie – Biometrics Authentication. Technical report, Fraunhofer IPK Berlin, 2000. (in German).

[5] X. Yang, T. Furuhashi, K. Obata, and Y. Uchikawa. Constructing a high performance signature verification system using a GA method. In Proc. 2nd International Two-Stream Conference on Artificial Neural Networks and Expert Systems, pp. 170-173, Dunedin, New Zealand, 1995.

[6] L.A. Zadeh. Some reections on soft computing, granular computing and their role in the conception, design and utilization of information/ intelligent systems. Soft Computing, 2:23-25, 1998.