Chapter 9
Chaotic Neural Networks and Multi-Modal Biometrics

ABSTRACT

Neural network is a collection of interconnected neurons with the ability to derive conclusion from imprecise data that can be used to both identify and learn patterns. This chapter presents the concept of neural network as an intelligent learning tool for biometric security systems. Neural networks have been extensively used in a variety of computational and optimization problems. In the first half of this chapter, focus is given to a specific topic—chaos in neural network. A detailed description of an on-demand chaotic noise injection method recently developed to deal with a common drawback of non-autonomous methods—their blind noise injecting strategy—is presented. The second part of the chapter discusses the issue of high-dimensionality in the context of a complex biometric security system. The amount of data and its complexity can be overwhelming, and one way of dealing with this issue is to use the dimensionality reduction techniques, which are typically based on clustering or transformations from one space to another. The reduced dimensionality vector can be then used in the energy model for an associative memory, which will learn the data patterns. The benefit is that this is a learner system that converges the given set of vectors to the stored pattern in a network, which can be later used for biometric recognition and also for identifying the most significant biometric patterns. At the end of this chapter, some examples are presented showing the feasibility of using such approach in biometric domain—both for single and multi-modal biometric.

DOI: 10.4018/978-1-4666-3646-0.ch009

1. INTRODUCTION

In the previous chapters, we exploited notion of multi-modal biometrics, specifically ranked-level fusion approach to design of highly reliable and accurate biometric system. We also looked at advantages which can be gained by utilizing additional information about a subject, such as height, age and gender, or so-called soft biometric patterns. We also looked at the new research domain combining behavioral and appearance-based characteristics one example of artificial entities, such as robots, avatars and intelligent software agents.

In this section, we look at learning approaches and try to bring benefits of utilizing and identifying most prominent/significant patterns in multitude of biometric data, which not necessary originates from the same biometric. Features from different biometric sources can be combined at either before-matching or after-matching stages and then most significant traits can be identified through dimensionality reduction or adaptive learning approaches.

The proposed methodology has a number of interesting features:

- There is no dependency on one strong biometric. Even if the sample is not available/ corrupted, accuracy of recognition and performance of security system will not be compromised;
- The combining of traits can be done on both pre-matching or post-matching levels, thus allowing choice for system design and implementation/integration in real applications;
- Computational complexity can be controlled through clever dimensionality reduction techniques, thus allowing for real-time performance;
- Utilizing learning approaches can lead to better recognition rates as training will take place on biometric database prior to matching.

In a practical biometric security system (i.e. a system that employs biometrics for personal recognition), there are a number of important issues that should be considered, including *performance* (achievable recognition accuracy and speed) and *circumvention* (system resistance to noise and to being fooled by fraudulent methods). In order for biometric system to meet the requirements on performance and circumvention, more than one type of biometric is required. Hence, the need arises for the use of multi-modal biometrics, which is a combination of different biometric recognition technologies, varying from physical biometrics (such as face, iris, and fingerprint recognition) to behavioral characteristics (i.e. signature, voice, and gate).

Having to deal with different biometrics characteristics and specifications usually leads to a number of issues that should be addressed in a multi-modal biometric system (Dalenol, Dellisanti, & Giannini, 2008; Ho, Hull, & Srihari, 1994; Johnson, 1991; Verlinde & Cholet, 1999). In such a system, one of the common problems is the high dimensionality of the data which negatively impacts the security system performance. Hence, dimensionality reduction methodologies need to be used. However, they have not been considered in recent multi-modal biometric systems due to gap between recently developed dimensionality reduction techniques in data mining and data analysis of biometric features. To correct this situation, a methodology for reducing the search space of all possible subspaces by utilizing axis-parallel subspaces and clustering can be used. This also helps in dealing with noisy data and makes the biometric system more error-proof.