Chapter 27
Biometric Identification System Using Neuro and Fuzzy Computational Approaches

Tripti Rani Borah
Gauhati University, India

Kandarpa Kumar Sarma
Gauhati University, India

Pranhari Talukdar
Gauhati University, India

ABSTRACT

In all authentication systems, biometric samples are regarded to be the most reliable one. Biometric samples like fingerprint, retina etc. is unique. Most commonly available biometric system prefers these samples as reliable inputs. In a biometric authentication system, the design of decision support system is critical and it determines success or failure. Here, we propose such a system based on neuro and fuzzy system. Neuro systems formulated using Artificial Neural Network learn from numeric data while fuzzy based approaches can track finite variations in the environment. Thus NFS systems formed using ANN and fuzzy system demonstrate adaptive, numeric and qualitative processing based learning. These attributes have motivated the formulation of an adaptive neuro fuzzy inference system which is used as a DSS of a biometric authenticable system. The experimental results show that the system is reliable and can be considered to be a part of an actual design.

INTRODUCTION

Of late biometric attributes have become important components of authentication systems. This is because biometric attributes are based on a physiological or behavioral characteristic which are unique to a person. Biometric aids are accepted as important components of highly secured identification and verification systems as solutions to security breaches, transaction frauds etc. in a diverse range of applications that have direct impact on the lives of the common man. This is more so with cases which are confidential in nature like that seen in financial transactions, restricted access zones, working with personal data

DOI: 10.4018/978-1-5225-0159-6.ch027

and privacy. Biometric authentication systems are also available in real time mode especially with applications including distributed computing resources where application logins, data protection, remote access, transaction security etc are linked to individual personal attributes. The primary benefit derived is security which re-enforces reliability and trust. In most case, biometric identification is found to be the most reliable method of trust-worthy transaction of any type.

Biometric authentication refers to the identification of humans by their characteristics or traits. Biometrics is used in human computer interaction (HCI) systems as a form of identification and access control. Biometric characteristics of a person are unique and remain unchanged over a lifetime. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals (Jain, Hong, & Pankanti, 2000).They are often categorized as physiological versus behavioral characteristics. A physiological biometric would identify a person by an iris scan, DNA or fingerprint etc. Behavioral biometrics is related to the behavior of a person, including but not limited to typing rhythm, gait and voice. Though behavioral biometrics is less expensive and less dangerous for the user, physiological characteristics offer highly exact identification of a person.

Fingerprint identification is a matured biometric technique used for criminal investigations. Major representations of the finger are based on the entire image, finger ridges or salient features derived from the ridges (minutiae). These characteristics are used to generate an orientation field of the fingerprint, which subsequently provides the discriminating details for authentication of persons. Fingerprint identification is a popular technique because of their easy access, low price of fingerprint sensors, non-intrusive scanning and relatively good performance. In recent years, significant performance improvements have been achieved in commercial automatic fingerprint recognition systems (FRS). The fingerprint of an individual is unique and remains unchanged over a lifetime (Jain, Hong, Pankanti, & Bolle, 1997).

Retina is another unique biometric pattern that can be used as a part of a verification system. Retina identification is an automatic method that provides true identification of the person by acquiring an internal body image which is difficult to counterfeit (Hill, 1978). Retina identification has found application in high security environments of all types.

In the most basic form, a biometric identification system has an acquisition stage, a pre-processing stage, feature extraction, a classifier and a decision making stage. Conventionally, the design solutions use a combination of a number of technologies some of which are also learning based. The primary benefit of a learning based system is that it can capture finer variations of the input, retain the knowledge and use it subsequently. Among the learning systems, Artificial Neural Networks (ANNs) have been the most preferred ones. These are non-parametric prediction tolls that generate non-linear computing and can make proper discrimination between closely varying patterns. One of the limitations of the ANN is that it cannot provide qualitative computing. It means it fails to make discrimination between minute variations within classes like, in case of illumination variation, it shall assume all changes of bright light to be same meaning that it shall provide a binary decision between bright and dark. To enable it make discrimination between subtle variations of light, structural modifications of the ANN type should be made. To deal with situations of subtle variations between two extreme cases like dark and bright, fuzzy systems are found be excellent choice. Fuzzy systems work best when it is combined with ANNs. These aspects are discussed in subsequent sections. One of the combinations of ANN and fuzzy system is the neuro-fuzzy system (NFS). The ANN is also configured with fuzzy attributes as a NFS for applications involving finer variation of inputs and also enabling it to deal with uncertainty. Such aspects are explored here in case of a framework for biometric authentication involving fingerprint and retina.