ABSTRACT

Name of the Scholar:	**Farhana Javed Zareen**
Name of the Supervisor:	**Dr. Suraiya Jabin**
Department:	**Department of Computer Science**
Title:	**An Adaptive Signature Recognition System as a Biometric Technology Using Neural Networks**

Biometrics is being widely implemented in today's society to deal with the security requirement issues. A biometric system can either do identification or verification task. In identification, the biometric system can establish identity of a person whereas verification authenticates the person's claimed identity from the sample stored in the database. Biometric technology can be divided into two branches: physiological verification and behavioral verification.

In this thesis, a unique and novel preprocessing method is presented for biometric signature data which is multi-dimensional and non-uniform data with the aim of making it uniform and reduced in size without losing much of its value. The feature data set along with the structural data of biometric signature needs to be pre-processed in order to use it to train a machine learning based model for signature verification purposes. We demonstrate the success of the proposed data pre-processing method over other prevalent methods such as Principal Component Analysis (PCA), Singular Value Decomposition (SVD) and its variants etc. using experimental results for biometric signature data but the same can be implemented for any other data with similar properties of being multi-dimensional and with each dimension of varying size from a different domain.

An authentic mobile-biometric signature verification system is presented by comparing its performance on the two datasets one using the standard device that is used for

capturing biometric signatures and other one is a mobile biometric signature database captured using a smart phone. In this contribution, a comprehensive survey of mobile biometric signature verification systems, different devices and hardware needed to support mobile biometrics along with open issues and challenges are presented. The experiments presented establish that the performance of mobile devices is low as compared to normal biometric signature capturing devices and the major reason we found is the absence of pen-tilt angle information in the mobile device dataset.

These biometric systems are prone to spoof attacks. Spoofing attacks are one of the main threats to the security of biometric systems. They are carried out by submitting a counterfeited biometric (i.e., a replica of the client's biometric) to the sensor. For instance, a gummy finger can be used to fool a fingerprint recognition system. Spoofing attacks have a great practical relevance because they do not require advanced technical skills and, therefore, the potential number of attackers is very large. To deal with spoofing attacks, a novel liveness detection technique for signature biometric has been presented for tackling spoof attacks at stored template level. The database has been taken from ATVS labs. An error rate of 3.1 % has been reported which is good as no other liveness detection system has been proposed for signature biometric in the literature. The performance of the liveness detection system in other biometric has been reported. This liveness detection system can be combined with biometric signature authentication system to provide best results for user authentication. In this way, we present a novel Signature based Biometric system, which gives better accuracy rates and is immune to spoof attacks to a high level.