3. RESEARCH METHODOLOGY

3.1. Introduction

Biometric recognition applications become more and more popular. Biometric authentication systems can resolve most of security issues of traditional token based or knowledge-based authentication systems, since a biometric feature belongs only to one person and cannot be lost or forgotten. But eventually, biometric features can be stolen or adopted and there exist various other ways to circumvent the integrity of a biometric authentication system.

Recent work systematically identifies security threats against biometric systems and possible countermeasures. Biometrics can be subdivided into behavioral and physiological approaches. Behavioral biometric include signature recognition, voice recognition, keystroke dynamics, and gait analysis. Physiological biometric include fingerprints, iris, retina scans, hand, finger, face, ear geometry, hand vein, nail bed recognition, DNA and palm prints. As biometrics can't be borrowed, stolen, forgotten, and forging is practically impossible, it is a natural identity tool that offers more security than conventional methods of personal recognition. Biometric system is a technology with the capability to minimize fraudulence, and enhance user convenience by ensuring verification, identification, screening and enrolment.
Biometric authentication employs unique combinations of measurable physical characteristics--fingerprint, facial features, iris of the eye, voice print, hand geometry, vein patterns, and so on--that cannot be readily imitated or forged by others. Uni-modal biometric systems have variety of problems such as noisy data, intra-class variations, restricted degree of freedom, non-universality, spoof attacks, and unacceptable error rates. Multimodal biometrics refers the combination of two or more biometric modalities in a single identification system. This work discusses the various scenarios that are possible to improve the performance of multimodal biometric systems in order to increase the overall system performance.

3.2. Research Design

This research mainly focuses on approaches for network security using novel techniques for personal authentication, where the biometric features used for authentication are fingerprint, iris and retina. In this research, three approaches are used for personal authentication. They are:

1. A New Biometrics-based Key Exchange and Lipmaa’s PIR Authentication Protocol
2. Iris and Retinal Biometrics-based Authentication and Key Exchange System
3. Multimodal Biometrics- based Authentication and Key Exchange System
Figure 3.1 shows the overall research flow of the present research work. In the first proposed approach, fingerprint biometric features and deniable authentication protocol are used for network security. The various phases included in this approach are user registration, fingerprint enhancement, minutiae point extraction, mapping function, fingerprint hardening protocol and fingerprint authentication protocol based on Lipmaa’s PIR.
An New Biometrics based Key Exchange and Lipmaa’s PIR Authentication Protocol

PHASE I

A. User Registration
B. Fingerprint Enhancement
C. Minutiae Feature Extraction
D. Mapping Function
E. The Finger Print Hardening Protocol
F. The Finger Authentication Protocol (Lipmaa’s PIR)

Iris and Retinal Biometrics based Authentication and Key Exchange System

PHASE II

Iris Based Authentication and Key Exchange System
A. Extraction of Minutiae Feature
B. Generation of Secret Key
C. Extraction of Lock/Unlock data
D. Implementation Stage
• Transformation
• Encoding
• Decoding
• Iris Authentication Protocol
Retina Based Authentication and Key Exchange System
A. Extraction of Feature point from Retina and Generation of Secret Key
B. Encoding
C. Decoding
D. Retinal Authentication Protocol

Multimodal Biometrics based Authentication and Key Exchange System

PHASE III

A. Feature level fusion
B. Mapping Function
C. Hardening Protocol
D. Authentication Protocol
In the second phase of the present research work, Iris and Retinal biometric features are used for the network security. The phases incorporated in this iris based approach are User registration, Extraction of retinal minutiae points, Extraction of Minutiae Feature, Generation of Secret Key, Extraction of Lock/Unlock data. The implementation stage of the proposed approach comprises of four steps namely Transformation, Encoding, Decoding and Iris Authentication Protocol. This approach also explains some of the Iris localization and Normalization techniques to make the biometric template noise free. The second proposed approach also uses an efficient retinal biometric technique for providing network security where the biometric feature used for authentication is the retinal vessel tree. The configuration of the retinal vessels is unique for each individual and that it does not vary forever, so it can be used for the authentication. The various phases included in this proposed approach are User registration, Extraction of retinal features, Encoding, Decoding and Retinal Authentication protocol.

The third phase of the present research work concentrates on the multimodal biometric techniques for providing better and effective network security. In this approach, the biometric features such as fingerprint, iris and retina are combined using multi-modal biometric techniques and are used for authentication purposes. Feature level fusion is used in this approach which refers to combine different feature sets that are extracted from multiple biometric sources.
The experiment is conducted on the fingerprint, iris and retina datasets. Digital Retinal Images for Vessel Extraction (DRIVE) dataset is used for retina [98]. Iris datasets used in this approach are Chinese University of Hong Kong (CUHK) [99] and the Institute of Automation, Chinese Academy of Sciences (CASIA) [100] data sets. Second International Fingerprint Verification Competition (FVC2002 DB2) database [101] is used for fingerprint processing. The iris and the retina biometric template are altered for three different user passwords namely ‘location’, ‘template’ and ‘pictures’ to check for revocability.

3.3 Summary

This chapter introduced the general methodology used by the present research work. The working process of the proposed approaches for the network security was explained. Moreover, the three phases involved in the research methodology of biometric identification such as Fingerprint biometric features, Iris and Retina biometric feature, Multimodal Biometric Techniques were also discussed in this chapter. The techniques and algorithms used in the proposed approaches for the network security were tabulated.