Abstract

Biometrics is the science of recognizing the identity of a person based on the physical or behavioral attributes of the individual such as fingerprints, palmprint, face, voice, iris & gait. With the increasing need for robust human recognition techniques in sensitive applications such as secure access control, international border crossing and law enforcement, biometrics has emerged itself as a feasible technology that can be integrated into large-scale identity management systems. Biometric systems operate under the premise that many of the physical or behavioral characteristics of humans are distinctive to an individual, and that they can be reliably acquired via appropriately designed sensors and represented in a numerical format that lends itself to automatic decision making in the context of identity management. Thus, these systems may be viewed as pattern recognition engines that can be incorporated in diverse markets. Every part of human body is unique and if we can consistently capture the specified area or trait, efficient biometric authentication system can be built. With the advancement in technology sensors for variety of biometrics are available. We have fingerprint, handwritten signatures, palmprint, face, voice as conventional biometric traits, because of advance sensors we can have 3D face and hand geometry, finger-knuckle print, ear geometry, facial thermogram, gait, odor, DNA, retinal scan as emerging traits.

Biometric systems have to preprocess the captured data, extract the region of interest, extract the feature vectors to represent the biometric template numerically and finally perform matching based on this data. These steps are implemented by software and/or hardware blocks in the architecture of the systems. In this thesis the biometric recognition systems are explored in the context of digital signal & image processing techniques. Different image processing techniques based on transforms, filters, wavelets, vector quantization algorithms, mathematical & statistical measures are used to implement above mentions functional blocks of the biometric systems. Fingerprint, palmprint, finger-knuckle print, face, iris, handwritten signatures, keystroke dynamics and their multimodal combinations are studied and results are presented here.
Fingerprint, palmprint and finger-knuckle prints are biometric traits present on the hand. They are very rich in texture which is unique for each human being. Fingerprint capturing through scanner interface, preprocessing, core-point detection, segmentation methods are presented. Novel algorithm for orientation field estimation and automatic segmentation of fingerprint based on Gabor filter’s response is discussed. On the same lines segmentation and region of interest extraction methods are presented. Wavelet as well as transform domain analysis is used for feature extraction. Walsh, Hartley, Kekre’s transform, DCT, Kekre’s wavelets and Haar wavelets are used for feature extraction.

Face and iris consists of next set of biometrics that is studied here. Face requires least user cooperation level but permanence is less on the other hand iris requires higher degree of user cooperation but it has better uniqueness and permanence over time is more. Texture based features are extracted using directional Gabor filters and Kekre’s wavelets. The Gabor filter based approach is suitable for handheld devices. Iris recognition is performed using DCT, WHT, Vector Quantization as well as wavelets based feature vectors. The effect of iris normalization over the recognition rate is also studied and it is found that iris normalization improves the accuracy of recognition.

In another study, behavior based biometric traits such as handwritten signature and keystroke dynamics are explored. Dynamic signatures are more suitable in the context of authentication systems. Dynamic signature recognition based biometric implementations are tested and results are discussed here. Static signature recognition systems use morphological features available for recognition; in case of dynamic signature more information like pressure applied while signing, velocity, and acceleration of the pen tip is also available. Dynamic signature recognition systems based on Kekre’s vector quantization algorithms, transform domain analysis are discussed in this thesis. Keystrokes are captured from the keyboard and the timing information is used for evaluating matching between two password sequences, the accuracy of this system is further improved by combining this modality with face in a multimodal implementation.

Systems based on only one kind of biometric trait are generally called as unimodal biometric systems. The performance and scalability of a biometric system can be increased by combining
more than one biometric trait. Such systems are called as multimodal biometric systems. There are different variations in multimodal biometrics are possible, they are multi-algorithmic, multi-Sensorial, multi-instance implemented with one or more than one biometric traits. In this thesis multimodal, multi-algorithmic and multi-instance biometric systems implementations are discussed. Combination of face & keystroke dynamics is an example of multimodal biometric system. Iris recognition is implemented with the feature vectors for left and right iris as well as their combination; this is an example of multi-instance biometric systems. A new architecture called as hybrid multimodal system based on combination of multi-algorithmic and multi-instance systems is also proposed. Besides this an algorithm is proposed for making the biometric systems adaptive to ageing in human. This algorithm updates the biometric database automatically and securely in case of change in biometric trait such as face, voice.

Such systems are more reliable due to the presence of multiple & (fairly) independent pieces of evidence and they have given higher accuracy as compared to individual unimodal implementations. These systems are able to meet the stringent performance requirements imposed by various applications. They address the problem of non-universality, since multiple traits ensure sufficient population coverage. They also deter spoofing since it would be difficult for an impostor to spoof multiple biometric traits of a genuine user simultaneously.