ABSTRACT

Fingerprints are the most widely used biometric across all biometric systems in the world. Biometrics refers to the study of techniques for recognizing human beings uniquely on the basis of one or more of their physical (fingerprints, eye retinas and irises, facial patterns, hand measurements etc) or behavioral (signatures, gait, typing patterns etc)characteristics. Biometric based security applications work by matching the live biometric input from an individual to the stored biometric template about that individual. Among all the biometric techniques, fingerprint-based identification is the oldest and most successful method used in numerous applications as human beings are known to have unique, immutable fingerprints. Automatic fingerprint identification systems (AFIS), have been widely used in forensics for criminal identification and a large number of civilian and government applications for physical access control, computer log-in, welfare disbursement, international border crossing, national ID cards etc.

While biometric-based techniques have inherent advantages over other authentication techniques, ensuring the security and integrity of data (fingerprint images in our case) is a major concern. The tremendous growth in distribution of digital data through the internet has raised serious authentication issues. Biometrics datasets can be maliciously hacked by criminals who may tamper with them or use them to falsely incriminate individuals in a physical crime. Data hiding techniques are thus used in biometric systems for securing biometric data itself. Fingerprint images can thus be watermarked with some secret data to protect them against intentional and unintentional attacks and to transmit them securely from central databases to intelligent agencies in order to use them for identification and classification purposes.

The proposed work in this thesis aims at securing fingerprint images by watermarking them through computationally intelligent watermarking techniques. Computational Intelligence encompasses elements of learning, adaptation, heuristic and meta-heuristic optimization as well as any of their hybrids and hence their application
helped us to address major concerns in fingerprint image watermarking. The concerns addressed in the proposed work include i) watermarking the fingerprint should not affect its quality, ii) watermark should be robust i.e., it must be resilient to image processing attacks and iii) minutia features of the fingerprint should be preserved and it should be possible to reliably extract them from the watermarked fingerprint. However, the performance of a minutiae extraction algorithm relies heavily on the quality of the input fingerprint images. Hence, in the thesis, an input fingerprint image is first enhanced, then minutia are extracted and finally watermarking is done while preserving minutia features. The watermark embedded in the fingerprint image in this work is the face image of the same individual. Such a watermarking scheme with two levels of security not only protects the cover fingerprint but also provides a more secure system of personal recognition and authentication at the receiver’s end. The proposed work finds application in a number of security implementations based on multimodal biometric authentication.

This thesis presents fingerprint image enhancement based on type-2 fuzzy sets, followed by an efficient algorithm for extracting minutiae from a fingerprint image using the binary Hit or Miss Transform (HMT) of mathematical morphology. Finally, it presents watermarking techniques in the Spatial, Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) domain for hiding secret facial image data in the enhanced fingerprint image using Particle Swarm Optimization (PSO) and Neural Networks (NN).

Impulse noise removal and contrast enhancement algorithms have been proposed for fingerprint image enhancement in this thesis. The proposed impulse noise removal algorithm uses an S–shaped fuzzy membership function that is itself fuzzy, to detect the impulsiveness of a pixel. Further, the contrast of the fingerprint image is enhanced by using a contrast intensification operator based on type-2 fuzzy logic.

An algorithm to extract the minutiae present in the fingerprint image by using the binary Hit or Miss Transform (HMT) is proposed to be used after image enhancement. For this purpose, the structuring elements representing the different types of minutiae present in a fingerprint image have been developed and are used by the HMT. This is
done after preprocessing the fingerprint image with morphological operators for removal of any unwanted spurs, bridges, lakes and islands that may be present. This results in efficient minutiae detection, thereby saving a lot of effort in the post processing stage. In the post processing stage, the extracted minutiae are further validated to retain true ones and reject false ones.

Particle Swarm optimization has been used to find optimum pixel locations in the spatial domain and optimum transform coefficients in the transform domain for embedding secret data in fingerprint images. The objective function for PSO is chosen based on the Structural Similarity index (SSIM) between the original and the watermarked fingerprints and Orientation Certainty Level index (OCL) of the watermarked fingerprint image. This ensures that the watermarked fingerprint image is good in quality and its minutia features are completely preserved. The proposed work also presents an NN-PSO based hybrid approach for watermarking. The input image is first divided into blocks and then a Neural Network is used to determine the number of secret bits to be embedded in each block depending on its features. The output of the Neural Network is then used as input by the PSO module to find the locations of the best transform coefficients in that block where the secret facial image data can be embedded. The robustness of the all the proposed watermarking schemes have been tested against various image processing attacks. The performance of the presented algorithms has been compared with existing techniques in the literature and with each other as well. The proposed NN-PSO based hybrid approach has been found to exhibit better watermarked image quality and better robustness against possible attacks to the watermarked image. Moreover, as the presented watermarking schemes in this work retain the feature set of the original fingerprint, the extracted facial image and the cover fingerprint image can be correctly verified at the receiver’s end leading to a more secure and accurate biometric based personal authentication.