ABSTRACT

Techniques for establishing a person's identity are characterized by several shortcomings. Identification documents may be forged or altered, signatures are difficult to authenticate and verify, tokens or seals may be stolen or counterfeited, and physical descriptions are difficult to quantitatively assess. Establishing identity continues to be important for the purpose it has been for centuries in banking transactions, establishing legal presence, entering contracts, gaining entry to secured premises, identifying fugitives, etc. Recently biometrics, the science of recognizing an individual based on his physiological or behavioural traits has gained increasing acceptance as a legitimate method for these tasks. Currently, most deployed biometric systems are unimodal they rely on a single feature to identify a person. Although these features, such as face, iris, ear, fingerprint, signature, or voice, may be sufficiently unique, systems must still contend with a variety of problems such as noisy data, intra-class variations, restricted degrees of freedom, non-universality, spoof attacks, and unacceptable error rates. Some of these issues may be eliminated and system accuracy increased through a Multimodal Biometric Authentication System (MMBAS).

This dissertation formulate and investigate a method for processing multimodal biometric data collected from a single source to extract multiple biometric features from a sample and subsequently classify the identity of the sample using multiple biometric methods in such a way that some or all of the identity features may be selected. This work uses two biometric traits namely face image and finger knuckle print features. To implement this MMBAS the proposed method present face detection scheme which provides motivation for a feature recognition component. Face and Finger-Knuckle-Print (FKP) authentication system use feature detection and matching techniques in its hard core design. It works similar for almost every authentication system.

Scale Invariant Feature Transform (SIFT) is the most reliable feature extraction technique that is used in this proposed MMBAS. The feature descriptors detected by SIFT is capable to distinguish each and every image in the dataset from
one another with the cost involved in its operations. In SIFT based biometric system, the storage and computational cost will directly depend on the size of the feature descriptors used. Such a matching process will directly map these feature descriptors to find an exact match and the descriptors are directly stored in storage media as image templates. Hence there is a necessity for storing all feature descriptors of the enrolled original images for future references. The size of these feature descriptors data will be greater than the original image dataset and the performance of the system will rapidly decrease with respect to the increase in enrolment in the database.

The proposed method realized that the main cause of computation overhead is the representation of feature descriptors which consume much space even higher to that of original image. There are techniques for reducing the size of the feature descriptors by using some abstract representation of the same. The feature extraction techniques and dimensionality reduction techniques that can be used to reduce the size of the feature descriptors reduce the storage and computational cost during matching/authentication phase. The proposed MMBAS deals with the above issues using Scale Invariant Feature Transform (SIFT) for efficient computation and cost compared to the existing work and proven to be secure and tough resistant for authentication system. Further the concept of SIFT is also applied to face and finger knuckle detection mechanism for providing maximum space constraints for identifying the authentic face and finger knuckle process.

The proposed method transforms image data into scale-invariant coordinates relative to local features and performs better matching. It corrects the non-uniform brightness and improves the texture of the image. It is extremely acquiescent to hybridize the biometrics to authorize a person’s uniqueness. So far, researchers have made a lot of research on SIFT, including some improvements. The existing methods are used to calculate a coefficient matrix using all training samples to represent the test sample, and choose a certain number of neighbours to classify the test sample. These methods were effective on many face databases; however, it costs a large amount of time to calculate the coefficient matrix in practice. It is used to combine the facial features and finger knuckle for improving the performance of
security and decrease the size of data at a low computational cost by choosing some candidates as image templates. The Euclidean distance is used to choose a certain number of candidates, and apply SIFT features extracted from those candidates to classify the test sample. Large number of features can be extracted from typical images and increase the storage space with the proposed algorithm. Hence development of an efficient authentication system based on hybrid features become great demand in most of the real time authentication based applications.

The proposed method combines the process of face and finger knuckle recognition by staying different in using traditional finger print recognition. To that extent the proposed system has succeeded in achieving the closest result by making the missing object to zero score which means the match found exactly with the image that is compared. The phase I of face recognition and phase II of finger knuckle recognition combined together to provide unique solution for tracing the exact user using biometric operation. The extension of this work will be tried with different facial gesture and finger knuckle exposing technique as dealt with image and angle based result. Also proposed system can develop a hybrid classification model using statistical and machine learning techniques that can dramatically reduce the computational costs involved in the authentication phase as well as lead to more improved results in terms of Equal Error Rate (EER). The accuracy of the system, both as separate components and together, is evaluated on the Indian face database which obtained from Indian Institute of Technology, Kanpur (IITK) and Hong Kong PolyU FKP database, a long-range and high-quality face / FKP data set. The combination of face, finger print, palm print, iris recognition is readily available. The possible ratio of combining face and FKP is very less compared to other multimodal authentication system. Finally, the results were achieved using Scale Invariant Feature Transform (SIFT), and we discuss future work for flexible, targeted feature extraction.