CHAPTER 6

CONCLUSIONS AND FUTURE WORK

This chapter presents the findings of research work and describes potential future orientation for multimodal biometric device analysis.

6.1 CONCLUSIONS

Today security is major concern in computer technology as well as various applications such as banking, e-commerce, military, health application, etc., Traditional knowledge based techniques such as using pincode, passwords, cards are not feasible because they can be stolen, forgot or forged by third party. Biometric authentication is an alternative solution for person identification as they are unique and their features are unchanged throughout person lifespan. Existing biometric system are facing some challenges such as noisy input samples, occlusion and truncation, pose and orientation and changing luminance conditions, etc. Because of these issues, the biometric systems are vulnerable against security attacks. A better performance of biometric system can be achieved by overcoming some of these listed drawbacks by integrating multiple cues such as iris-fingerprint, iris-face, iris-voice, etc. There have been substantial studies to evaluate better ways of integrating multiple cues from different modalities.

Fusion taken place at decision level is commonly preferred because it is simple as the minimal knowledge content accessible at this level. Therefore, researchers normally choose the corresponding score to merge, which would make the best compromises between the quality of knowledge and fusion simpler. One of the key issues with the score level fusion is the not often comparable values produced by various biometric matches. Characteristics and representation of these match score may be different. Therefore, there is need to normalize score value using slandered methodology.

Another drawback of existing biometric modality fusion techniques is that they are not able to secure data's in the database, especially in the area where high level security is needed for authentication. There are several issues while providing security through biometric in multimodal eye recognition system. Our research work emphasis on the accurate matching of authenticated person with multi-modal biometrics system.

The quality measure only works on counting features that are extracted and the occlusion cases, which may or may not measure the image quality. Fusion of features works on the combined feature vectors providing more data points for comparing the matching score. The performance of unimodal biometric system varies with change in environmental surroundings conditions and unconstrained scenario without user cooperation. The sensitivity, durability and data quality of the sensor are also important. Apart from them iris occlusion, posture, age, expression, diseases and some other factors are also responsible for degraded performance of biometric systems.

To overcome the limitations of unimodal biometric system, fusion of multiple biometric modalities is recommended and also checked with several traits. Multimodal frameworks are harder to be undermined and highly accurate. They are less vulnerable to spoofing and can accommodate lost data as well. Fusion itself greatly enhances device efficiency. Therefore, it is not appropriate to tune person unimodal results. Fusion also makes the biometric system flexible and scalable. Hence, without any degradation in performance, multimodal systems can accommodate more and more matches. In this thesis, we have extensively addressed these significant issues in systematic manner.

In this research study, we explored an ability to distinguish iris, sclera and pupil regions with entropy based CNN clustering methodology for visual wavelength eye images acquired in uncontrolled environment. Initially, input eye images are pre-processed and enhanced using min-max normalization followed bilateral filtering. At that point we extract the brightness, color and texture (which are contour based features) from the pre-processed images and then entropy is measured on these selected features.

CNN clusters the pupil, iris and sclera regions efficiently centred on entropy values. The experimental results exhibits that in terms of performance metrics, such as FPR, FDR, FNR, PPV, NPV, sensitivity, specificity, MCC, F-measure and accuracy, Our entropy based convolutional neural network(E-CNN) provides better results for segmentation in comparison with present KNN and SVM methods. Further to improve its performance we have analysed an effective multimodal biometric system using Support value based matching process.

Here, at first the iris, sclera regions are adequately segmented utilizing entropy-based CNN clustering. After that, the effective features are extricated for all the iris, sclera, pupil segments and dependent on the extracted features support value is estimated.

Matching score is at last determined to decide the data is recognized or Non-recognized. Using this multimodal biometric method then results in the accurate matching and authentication of the person. By utilizing feature level fusion, we combine the feature vectors, which in turn provide more data points for comparing the matching score.

The multimodal biometrics could be applied resulting in improved security. The high accuracy is achieved by using the research methodology and the exploratory results shows that our multimodal eye biometric system for visible wavelength images outperforms in uncontrolled environment in terms of FAR, FRR, PPV, NPV, accuracy, sensitivity, F-measure, MCC, specificity and GAR.

We have carried out a detailed evaluation of the various existing classification techniques for iris, sclera and multimodal eye biometrics such as K-Nearest Neighbors (K-NN), Adaptive neuro fuzzy inference system (ANFIS) and various other existing classification techniques such as Mixed Convolutional and Residual Network (Mi Co Re-Net), CNN, SVM that has been mentioned in the literature in terms of their efficiency and robustness. First, we studied the impact of individual modalities iris, sclera and pupil on the performance of the multimodal biometric system. Our analysis would show that improvement in accuracy and GAR while reduction of FRR and FAR, providing a good recognition performance for noisy relaxed color images. Although a high level of security is achieved by proposed research methodologies.

6.2 FUTURE WORK

Future research for this paper will be in a direction to develop a real time application. For designing a reliable and effective biometric security application a real multimodal database is useful. The variations in context and lighting are different due to the form of sample data gathered. For more performance measurement, real multimodal database with the same requirements may be used. In certain situations, in real time mode, biometric protection systems must run. The framework suggested may be generalized to function in real time registration and authentication.