ENHANCING SECURITY USING MULTIMODAL BIOMETRICS

1.) S.BALAJI Professor, ECE DEPARTMENT
CMR GROUP OF INSTITUTIONS

2).Dr. HABIBULLAH KHAN DEAN,
(SW),KL UNIVERSITY

3).V.SAI KRISHNA,ECE DEPARTMENT
CMR GROUP OF INSTITUTIONS

ABSTRACT

Thispaper presents fusion of three biometric traits, i.e., iris, faceand fingerprint, at matching score level architecture using weighted sum of score technique. The features are extracted from the pre-processed images of iris, face and fingerprint. These features of a query image are compared with those of a database image to obtain matching scores. The individual scores generated after matching are passed to the fusion module. This module consists of three major steps i.e., normalization, generation of similarity score and fusion of weighted scores. The final score is then used to declare the person as Authenticate or Un-Authenticate with Secret Key Analysis.

Introduction

Biometrics, as an integral component in identification science, is being utilized in large -scale biometrics deployments such as the US Visitor and Immigration Status Indicator Technology (VISIT), UK Iris Recognition Immigration System (IRIS) project, UAE iris-based airport security system, and India's Aadhaar project. These far-reaching and inclusive delivery systems not only provide a platform to assist and enhance civilization but also offer new research directions. An important research challenge among them is the measurement of quality of a biometric sample. For instance, as shown in Figure 1, an input biometric sample may possess a wide range of *quality(fig 1.).*

Quality assessment (QA) of an *image* measures its degradation during acquisition, compression, transmission, processing, and reproduction. Several QA algorithms exist in image processing literature, which pursue different philosophies, performance, and applications. A majority of these methods are motivated towards accurate *perceptual* image quality It is well established that environmental distortions such as noise, blur, and adverse illumination, affect the performance of state-of-the-art recognition algorithms. However, existing image quality metrics that measure such degradations encode only a part of the information that can measure the overall quality of a biometric sample. Hence, a clear distinction must be made between perceptual image quality assessment (PIQA) and biometric quality assessment (BQA). PIQA research attempts to understand why human subjects prefer some images to others. The task is complex and involves multiple disciplines, including an understanding of the HVS. On the other hand,

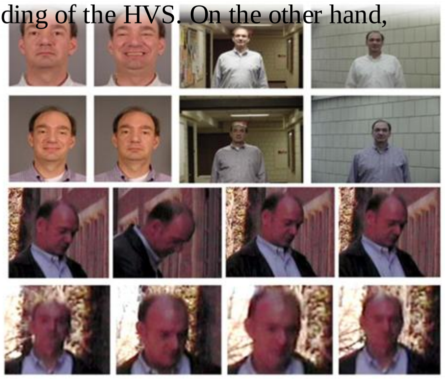

Fig 1. Different types of images for assessment.

BQA provides an initial estimate of the ability of a sample to function as a biometric. i.e., quality as perceived by the sophisticated human visual system (HVS) . These approaches require an in depth understanding of the anatomy and psychophysical functioning of the human cognitive system. Several perceptual quality metrics are surveyed by Wang and Bovik and Lin and Kuo . On the other hand, the quality of a biometric sample is interpreted differently throughout literature. A summary of these interpretations is provided in Table 1. In general, biometric quality is defined as an indicator of the *usefulness* of the biometric sample for recognition.

LITERATURE REVIEW

In literature, quality assessment metrics are widely used in the formulation of biometric techniques. As illustrated in Figure 3, quality metrics can be used at various stages of the recognition pipeline to improve performance and usability of biometrics in challenging conditions. The application of quality metrics can be during both enrolment and recognition phases. Since enrolment phase is the best opportunity to re-capture a sample to maintain the overall quality of the gallery set, the quality of input sample is an important consideration. On the other hand, the quality of a probe sample during recognition phase is utilized in different methodologies to improve the recognition performance. Some important applications and evaluation metrics of quality assessment techniques in biometric systems are described here.

Quality assessment during enrolment :

Quality feedback during enrolment is critical in collecting high-quality gallery data. It is common, especially in large- scale biometric systems, to have a supervised enrolment process as in the case of the India's Aadhaar project. An active quality feedback enables the collection officer to evaluate and maintain quality standards during the enrolment process [15]. It can also be a performance measure for the collection apparatus and procedure employed for data capture . Aggregated quality may also be used to create timeline along with historical or geographical meta-data for other analysis.

Quality assessment during recognition:

Quality assessment and feedback during verification can help mitigate false alarms. A verification system can choose not to perform matching if the quality score is below a threshold, depending on the computation time of matching and the overhead of re-acquisition of data. Most modern fingerprint and iris sensors are now bundled with active quality-control mechanisms. Identification is inherently a computationally expensive process, hence, it is a good idea to use quality assessment (computationally less expensive) to improve system usability. For example, quality can be used in negative identification, where it is in the interest of the subject to provide a poor quality sample.

. Quality-assessment-based selection of parameters for image enhancement shows marked improvement in the recognition performance of the resultant biometric sample, when compared to using generic parameters. Also, biometric images obtained from different uncorrelated or orthogonal bands of the spectrum can provide different amounts of information, as demonstrated with the face and iris .

REVIEW ON BIOMETRIC SYSTEM

In this section we will be relating the various approaches that were used in person identification by using biometric systems. A biometric system is the specific physiological or behavioral features haunted by the user for identification and these features are distinctive, general and persistent. These Biometric systems include face recognition, fingerprint technology, iris recognition, hand geometry, and signature and speech recognition. We are mainly focusing and surveying on face recognition, fingerprint and iris technology in this paper.

a.Finger print technology :

A fingerprint is the made of ridges and valleys on the surface of a fingertip. The fingerprints are highly stable and unique. The uniqueness of fingerprint is determined by the prototype like valleys and ridges, as well as minutiae points which are local ridge characteristics that occurs at either a ridge bifurcation or ridge endings The recent studies shows that probability of two individuals fingerprint, having the same fingerprint is less than one in a billion. There are several fingerprint matching algorithms like minutiae based matching, correlation based matching, genetic algorithms based matching Among these algorithm, minutiae based matching is the best one. In minutiae based matching the similarity of two fingerprints is determined by computing the total number of matching minutiae i.e. ridges and valleys from these two scanned fingerprints (fig 2.). Extraction of minutiae features before matching fingerprint requires a series of processes containing position calculation, image segmentation, image enhancement, and ridge extraction and shinning, minutiae. Extraction and filtering. Correlation based matching uses 1:1 correlation between fingerprints.

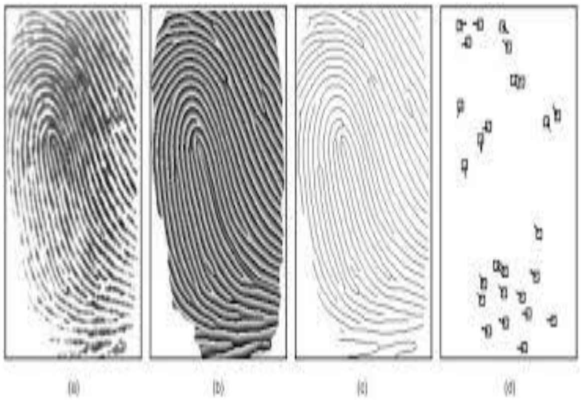

Fig 2. Finger print recognition

b. Iris recognition

Iris recognition systems make use of the uniqueness of the iris patterns to identify a person. This system uses high quality camera to capture a black-and-white image, high resolution image of the iris. In image acquisition step the systems takes a high-quality image of the iris, Iris localization takes place to detect the edge of the iris as well as that of the pupil; thus extracting the iris region, Normalization is used to transform the iris region to have fixed dimensions, and hence removing the dimensional inconsistencies between eye images, other inconsistencies include varying image distance, camera rotation, eye rotation within eye socket, tilting of the head, the normalized iris region is unwrapped into a rectangular region. The feature encoding is used to extract the most discriminating feature in the iris pattern so that a comparison between templates can be done. Finally a decision can be made in the matching step, for matching, the Hamming distance was chosen as a metric for recognition .

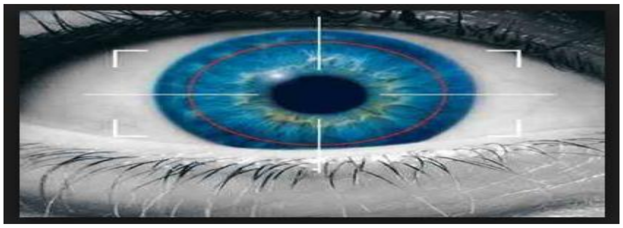

Fig 3.iris recognition

c.Palm-print Recognition : There are various ways to capture palm print image. Researchers utilize CCD-based scanners, digital scanners, video camera and tripod to collect palmprint images. Fig.2 shows a CCD-based scanner developed by Hong Kong Polytechnic University. A CCD-based scanner captures high resolution images and aligns palms accurately because it has pegs for guiding the placement of hand. Digital scanners produces low quality image and requires large time for scanning, therefore it cannot be used for real time applications. Digital and video cameras can also captured palm images but can cause recognition problems. Fig. 2 CCD Based Scanner The proposed palmprint recognition system has been depicted in figure 4 which is a flowchart of the palmprint recognition system. Each step is further described below in detail. Pre-processing is used to correct distortions, align different palm prints, and to crop the region of interest for feature extraction. Research on pre-processing commonly focuses on five steps 1.Binarizing the palm images 2.Boundary tracking 3.Identification of key points 4.Establishing a coordination system and 5.Extracting the central part. The third step can be accomplished by two approaches, tangent based and finger based. The tangent based approach is preferred..

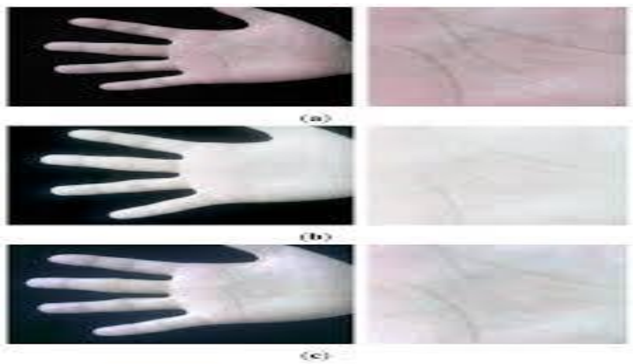

Fig 4 Palm print recognition

CHAPTER 4

FUSION TECHNIQUE

The important issue to designing multi biometric system is to determine the sources of information and combination strategies. Depending on the type of information to be fused, the fusion scheme can be classified into different levels. According to Sanderson and Paliwal , the level of fusion can be classified into two categories, fusion before matching (pre classification) and fusion after matching (post classification) as shown in 2 Level of fusion For fusion before matching, the integration of information from multi biometric sources in this scheme includes fusion at the sensor level and fusion at the feature level. Meanwhile, fusion after matching can be divided into two categories which are fusion at the match score level and fusion at the decision level.

A. Fusion Before Matching

Sensor Level Fusion: In this level, the raw data from the sensor are combined together as shown in Fig. 3. However, the source of information is expected to be contaminated by noise such as non-uniform illumination, background clutter and other .Sensor level fusion can be performed in two conditions i.e. data of the same biometric trait is obtained using multiple sensors; or data from multiple snapshot of the same biometric traits using a single sensor

Feature level fusion :In feature level fusion, different feature vectors extracted from multiple biometric sources are combined together into a single feature vector as depicted in Fig. 4. This process undergoes two stages which are feature normalization and feature selection. The feature normalization is used to modify the location and scale of feature values via a transformation function and this modification can be done by using appropriate normalization schemes There are several feature selection algorithms have been applied in the literature for instances Sequential Forward Selection (SFS), Sequential Backward Selection (SBS) and Partition About Medoids .The advantage of the feature level fusion is the detection of correlated feature values generated by different biometric algorithms, and, in the process, identifying a salient set of features that can improve recognition accuracy. Hence, only few researchers have focused on the feature level scheme compared to the other levels of fusions such as score level and decision level.

B. Fusion After Matching

Score level fusion : In score level fusion, the match outputs from multiple biometrics are combined together to improve the matching performance in order to verify or identify individual as shown in Fig. 5 [32]. The fusion of this level is the most popular approach in the biometric literature due to its simple process of score collection and it is also practical to be applied in multi biometric system. Moreover, the matching scores contain sufficient information to make authentic and imposter case distinguishable. However, there are some factors that can affect the combination process hence degrades the biometric performance. The density-based scheme is based on score distribution estimation and has been applied in well-known density estimation models such as Naive Bayesian and Gaussian Mixture Model (GMM) . This scheme usually achieves optimal performance at any desired operation point and estimate the score density function accurately. However, this scheme requires a large number of training samples in order to perfectly approximate the density functions. Moreover, it requires more time and effort for the operational setting compared to the other schemes.

. This scheme can be applied using various techniques such as sum rule, product rule, min rule and max rule techniques . In the classifier-based scheme, the scores from multiple matchers are treated as a feature vector and a classifier is constructed to discriminate authentic and imposter score. From the literatures, various types of classifiers such as SVM, neural network and multi-layer perceptron (MLP) have been implemented to classify the match vector in this scheme. However, this scheme has some drawbacks such as unbalanced training set and misclassification problems

CONCLUSION

Multi biometric systems are expected to alleviate many limitations of biometric systems by combining the evidence obtained from different sources using an effective fusion scheme. In this paper, the sources of biometric information were presented. The description regarding the level of fusions was also presented in this paper. From the study, it reveals that, performance of multi biometric systems can be further improved if an appropriate fusion strategy is used especially for the system which executed in uncontrolled environment. Hence, a different weighting in fusion is applied to maximize the performance of multi biometric system. Based on the review, the most promising recent research that can be implemented is fusion at the score level involving adaptive weighting. This approach have great potential to get rid the uncertain problem such as noise in sensed data, non-universality, upper bound on identification accuracy and spoof attacks.

REFERENCES

[1] Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition. Javier Galbally, Sébastien Marcel, *Member, IEEE*, and Julian Fierrez vol. 23, no. 2, February 2014

[2] International Journal of Computer Applications Technology andResearch Volume 2– Issue 3, 250 - 254, 2013 www.ijcat.com 250Visual Image Quality Assessment Technique using FSIM RohitKumarCsvtubhilaiSscetbhilai India, Vishal MoyalCsvtu bhilaiSscetbhilai India.

[3] G. L. Marcialis, A. Lewicke, B. Tan, P. Coli, D. Grimberg, A. Congiu, *et al.*, “First international fingerprint liveness detection competition— LivDet 2009,” in *Proc. IAPR ICIAP*, Springer LNCS-5716. 2009, pp. 12–23.

[4] Fingerprint Spoof Detection Using Near Infrared Optical AnalysisShoude Chang1, Kirill V. Larin2, Youxin Mao1, Costel Flueraru1 and Wahab Almuhtadi3 *1Institute for Microstructural Sciences, National Research Council Canada, Ottawa 2Department of Biomedical Engineering, University of Houston, Houston 3Algonquin College, Ottawa 1,3Canada 2USA*

[5] Direct Attacks Using Fake Images in Iris Verification Virginia Ruiz-Albacete, Pedro Tome-Gonzalez, Fernando Alonso-Fernandez,JavierGalbally, Julian Fierrez, and Javier Ortega-GarciaBiometric Recognition Group – ATVS EscuelaPolitecnica Superior- Universidad Autonoma de Madrid Avda. Francisco Tomas y

6] International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.2, No.1, February 2012 DOI : 10.5121/ijcseit.2012.2106 57 biometrics authentication technique for intrusion detection systems using fingerprint recognition. Smita S. Mudholkar 1, Pradnya M. Shende 2, Milind V. Sarode 3 1, 2& 3 Department of Computer Science & Engineering, Amravati University, India.