International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Voter Authentication System Using Feature Level Fusion of Iris,Face & Palmprint

V.LokeshRaju[1], V.Manitha[2], K.SuryaTeja[3], P.ManojKumar[4],T.JaiKrishna[5]

[1]Assistant Professor, Department of Electronics and Communication Engineering

[2, 3,4,5] Student, Department of Electronics and Communication Engineering Aditya Institute of Technology and Management, Tekkali, Srikakulam-AP

ABSTRACT

This paper presents fusion of three biometric traits, i.e., iris, face and palm print at matching score level architecture using weighted sum of score technique. The features are extracted from the pre-processed images of iris, face and palm print. 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.

IndexTerms-Iris, Face, Palmprint, Normalization, Secret key Analysis

1. INTRODUCTION

In this system, texture properties are extracted from the Palm print, face and iris images are stored as encrypted binary template in the server's database, to overcome the dictionary attacks mounted by the server. The image processing techniques are used to extract a biometric measurement from the palm print, finger print and iris. During login procedure the mutual authentication is done between the server and user and a symmetric key is generated on both sides, which could be used for further secure communication between them. Thus meet-in-the middle attack that happens between the user and the server can also be overcome. This system can be directly applied to strengthen existing password or biometric based systems without requiring additional computation.

2. LITERATURE SURVEY

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, then next step is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above considerations are taken into account for developing the proposed system

Most often associated with academic-oriented literature, such as a thesis, a literature review usually precedes a research proposal and results section. Its main goal is to situate the current study within the body of literature and to provide context for the particular reader.

1. Face Spoofing Detection from single images using Micro-Texture Analysis.
2.Fingerprint Liveness Detection based on Quality Measures.
3.Predicting IRIS Vulnerability to Direct Attacks based on Quality Related Features.
4.IRIS Recognition using Gabor Filters
5.IRIS Recognition using Gabor Filters and The Fractal Dimension
6.Contourlet Based Fingerprint Anti-Spoofing
7.Feature Selection:
Evalution,Application And Small Sample Performance
8.Generating Synthetic Iris By Feature Agglomeration
9.Awavelet Based Approach To Detecting Liveness In Fingerprint Scanners
10. Forensic Detection of Image Manipulation using Stastical Intrinisic Fingerprints

3. METHODOLOGY

3.1 INPUT IMAGE SELECTION

Digital images of melanoma and benign nevi were collected in JPEG format from different sources totaling 72, half melanoma and half benign. MATLAB's Wavelet Toolbox only supports indexed images with linear monotonic color maps so the RGB images were converted to grayscale images. The next step in the process was to segment the lesion from the surrounding skin. Since a clear color distinction existed between lesion and skin, thresholding was very suitable for this task. A black and white image was produced and its size increased by six pixels all around in order to include the entire border region in the segmented image.

An image can be defined as a two-dimensional signal (analog or digital), that contains intensity (grayscale), or color information arranged along an x and y spatial axis.

Also it is defined as collection of pixels.

Mathematically it defined in terms of Matrix (m x n)

Pixels – it is point that is having location(x, y) and value(I)

Two Coordinates – Spatial and Pixel Coordinates

An image is a picture that has been created or copied and stored in electronic form. An image can be described in terms of vector graphics or raster graphics. An image stored in raster form is sometimes called a bitmap.

Fig: input image

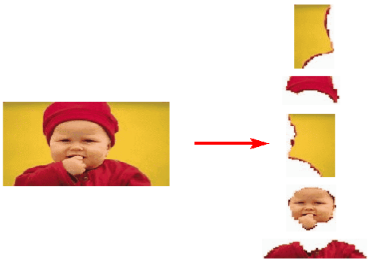
3.2 GRAYSCALE CONVERSION PROCESS

While displaying the different bands of a multispectral data set, images obtained in different bands are displayed in image planes (other than their own) the colour composite is regarded as False Colour Composite (FCC).

Fig : input image converted into gray colour image

3.3 DWT SEGMENTATION

DWT is a wavelet transform for which the wavelets are sampled at discrete intervals.DWT provides a simultaneous spatial and frequency domain information of the image. In DWT operation, an image can be analyzed by the combination of analysis filter bank and decimation operation. Segmentation procedures partition an image into its constituent parts or objects. In general, autonomous segmentation is one of the most difficult tasks in digital image processing. A rugged segmentation procedure brings the process a long way toward successful solution of imaging problems that require objects to be identified individually.



3.4 FUSION TECHNIQUE

In computer vision, Multisensor Image fusion is the process of combining relevant information from two or more images into a single image.The resulting image will be more informative than any of the input images.

In remote sensing applications,the increasing availability of space borne sensors gives a motivation for different image fusion algorithms. Several situations in image processing require high spatial and high spectral resolution in a single image. Most of the available equipment is not capable of providing such data convincingly. Image fusion techniques allow the integration of different information sources. The fused image can have complementary spatial and spectral resolution characteristics. However, the standard image fusion techniques can distort the spectral information of the multispectral data while merging.

In satellite imaging, two types of images are available. The panchromatic image acquired by satellites is transmitted with the maximum resolution available and the multispectral data are transmitted with coarser resolution. This will usually be two or four times lower. At the receiver station, the panchromatic image is merged with the multispectral data to convey more information.

Many methods exist to perform image fusion. The very basic one is the high pass filtering technique. Later techniques are based on Discrete Wavelet Transform, uniform rational filter bank, and Laplacian pyramid.

(First Input) (Second Input) (Fused Image)

Fig: fused image

3.5 FEATURE EXTRACTION TECHNIQUE

Feature extraction is a part of the dimensionality reduction process, in which, an initial set of the raw data is divided and reduced to more manageable groups. So when you want to process it will be easier. The most important characteristic of these large data sets is that they have a large number of variables. These variables require a lot of computing resources to process. So Feature extraction helps to get the best feature from those big data sets by selecting and combining variables into features, thus, effectively reducing the amount of data. These features are easy to process, but still able to describe the actual data set with accuracy and originality.

The technique of extracting the features is useful when you have a large data set and need to reduce the number of resources without losing any important or relevant information. Feature extraction helps to reduce the amount of redundant data from the data set

4. WORKING MODEL

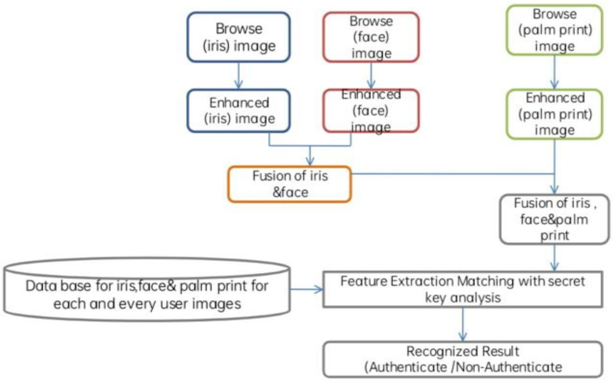
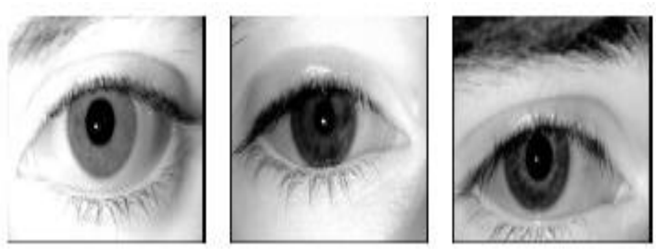

Browse (iris) image
Browse (face) image
Browse (palm print) image
Enhanced (iris) image
Enhanced (face) image
Enhanced (palm print) image
Fusion of iris &face
Fusion of iris , face&palm print
Data base for iris,face& palm print for each and every user images
Feature Extraction Matching with secret key analysis
Recognized Result (Authenticate /Non-Authenticate

Fig 4. Block Diagram

5.RESULTS

Results: Iris-Spoofing: The database used in this spoofing scenario is the ATVS-FIr DB which may be obtained from the Biometric Recognition Group-ATVS.1



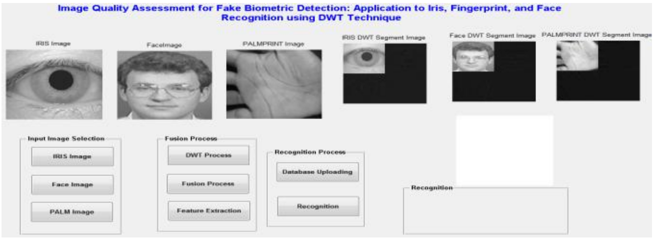
The database comprises real and fake iris images (real and fake samples was carried out using the LG IrisAccess EOU3000 sensor with infrared illumination which captures bmp grey-scale images of size 640 × 480 pixels. In Fig. 4 we show some typical real and fake iris images that may be found in the dataset. As mentioned above, for the experiments the database is divided into a: train set, comprising 400 real images and their corresponding fake samples of 50 eyes; and a test set with the remaining 400 real and fake samples coming from the other 50 eyes available in the dataset.

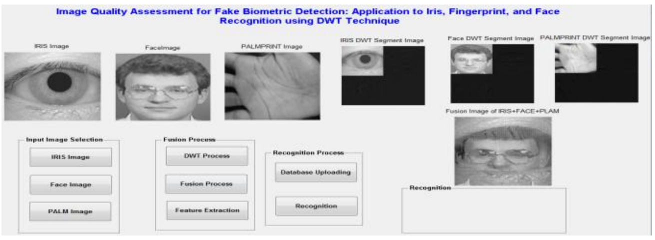
Results: Palmprints-Spoofing LivDet: The LivDet 2009 DB was captured in the framework of the 2009 palmprint Liveness Detection Competition and it is distributed through the site of the competition.4 It comprises three datasets of real and fake fingerprints captured each of them with a different flat optical sensor: i) Biometric FX2000(569 dpi),ii) CrossMatch Verifier 300CL (500 dpi), and iii) Identix DFR2100 (686dpi). The gummy palms were generated using three different materials: silicone, gelatin and playdoh, always following a consensual procedure (with the cooperation of the user). As a whole, the database contains over 18,000 samples coming from more than 100 different fingers

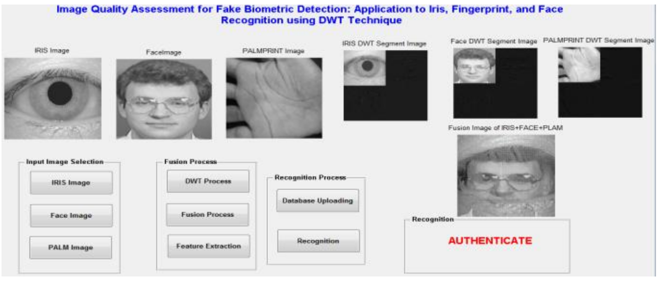
Results: - 2D Face

The performance of the IQA-based protection method has also been assessed on a face spoofing database: the REPLAY-ATTACK DB which is publicly available from the IDIAP Research Institute.5 The database contains short videos (around 10 seconds in mov format) of both real-access and spoofing attack attempts of 50 different subjects, acquired with a 320 × 240 resolution webcam of a 13-inch MacBook Laptop. The recordings were carried out under two different conditions: i) controlled, with a uniform background and artificial lighting; and ii) adverse, with natural illumination and non-uniform background. Three different types of attacks were considered: i) print, illegal access attempts are carried out with hard copies of high-resolution digital photographs of the genuine users; ii) mobile, the attacks are performed using photos and videos taken with the iPhone using the iPhone screen; iii) highdef, similar to the mobile subset but in this case the photos and videos are displayed using an iPad screen with resolution 1024 × 768.

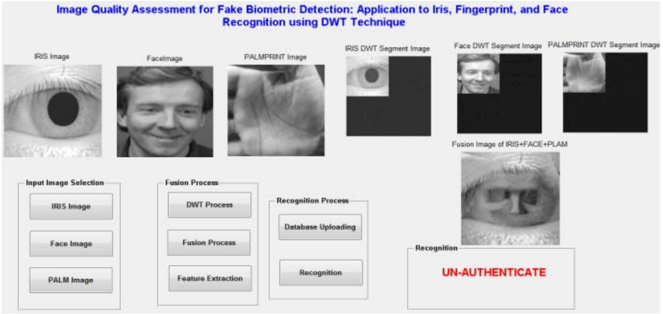
Such a variety of real and fake acquisition scenarios and conditions makes the REPLAY-ATTACK DB a unique benchmark for testing anti-spoofing techniques for face-based systems. As a consequence, the print subset was selected as the evaluation dataset in the 2011 Competition on Counter Measures to 2D Facial Spoofing Attacks. Some typical images (frames extracted from the videos) from real and fake (print, mobile and highdef) access attempts that may be found in the REPLAY-ATTACK DB are shown in Fig







AUTHENTICATE



UN-AUTHENTICATE

6. CONCLUSIONS

Several conclusions may be extracted from the evaluation results presented in the experimental sections:
i) The proposed method is able to consistently perform at a high level for different biometric traits (“multi-biometric”);
ii) The proposed method is able to adapt to different types of attacks providing for all of them a high level of protection (“multi-attack”);
iii) The proposed method is able to generalize well to different databases, acquisition conditions and attack scenarios;
iv) The error rates achieved by the proposed protection scheme are in many cases lower than those reported by other trait-specific state-of-the-art anti-spoofing systems which have been tested in the framework of different independent competitions; and
v) in addition to its very competitive performance, and to its “multi-biometric” and “multi-attack” characteristics, the proposed method presents some other very attractive features such as: it is simple, fast, non-intrusive, user-friendly and cheap, all of them very desirable properties in a practical protection system.

REFERENCES

[1] J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia, “On the vulnerability of face verification systems to hill-climbing attacks,” Pattern Recognize., vol. 43, no. 3, pp. 1027–1038, 2010.

[2] A. K. Jain, K. Nandakumar, and A. Nagar, “Biometric template security,” EURASIP J. Adv. Signal Process., vol. 2008, pp. 113–129, Jan. 2008.

[3] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, “A high performance fingerprint liveness detection method based on quality related features,” Future Generat. Comput. Syst., vol. 28, no. 1, pp. 311–321, 2012.

[4] ISO/IEC 19792:2009, Information Technology—Security Techniques— Security Evaluation of Biometrics, ISO/IEC

[5] K. Bowyer, T. Boult, A. Kumar, and P. Flynn, Proceedings of the IEEE Int. Joint Conf. on Biometrics. Piscataway, NJ, USA: IEEE Press, 2011.

[6] A. Anjos and S. Marcel, “Counter-measures to photo attacks in face recognition: A public database and a baseline,” in Proc. IEEE IJCB, Oct. 2011, pp. 1–7.

[7] (2012). BEAT: Biometrics Evaluation and Testing [Online]. Available: http://www.beat-eu.org/

[8] A. Hadid, M. Ghahramani, V. Kellokumpu, M. Pietikainen, J. Bustard, and M. Nixon, “Can gait biometrics be spoofed?” in Proc. IAPR ICPR, 2012, pp. 3280–3283.

[9] Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, “Evaluation of serial and parallel multibiometric systems under spoofing attacks,” in Proc.IEEE 5th Int. Conf. BTAS, Sep. 2012, pp. 283–288.

[`10] J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, “Iris liveness detection based on quality related features,” in Proc. 5th IAPR ICB, Mar./Apr. 2012, pp. 271–276.

BIOGRAPHIES

V.Lokesh Raju is an Associate Professor at Aditya Institute of Technology and Management (AITAM), Tekkali, Srikakulam, Andhra Pradesh, India .

V.Manitha B.Tech (ECE) Student form Aditya Institute of Technology and Management Tekkali, A.P**.**

K.SuryaTeja B.Tech (ECE) Student form Aditya Institute of Technology and Management Tekkali, A.P.

P.ManojKumar B.Tech (ECE) Student form Aditya Institute of Technology and Management Tekkali, A.P.

T.JaiKrishna B.Tech (ECE) Student form Aditya Institute of Technology and Management Tekkali, A.P.