ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

Multimodal Biometric Recognition Security System

Anju.M.I, G.Sheeba, G.Sivakami, Monica.J, Savithri.M

Department of ECE, New Prince Shri Bhavani College of Engg. & Tech., Chennai, India

ABSTRACT: Security and the authentication of individuals is necessary for many different areas of our lives, with most people having to authenticate their identity on a daily basis; examples include ATMs, secure access to buildings, and international travel. Biometric identification provides a valid alternative to traditional authentication mechanisms such as ID cards and passwords, whilst overcoming many of the deficits of these methods; it is possible to identify an individual based on who they are rather than what they possess or what they remember. Iris/Fingerprint/palm vein/Face recognition are some of the biometric system that can be used to reliably identify a person by analysing the patterns. The objective of the proposed system is to improve the safety of biometric recognition mechanism, by adding liveness assessment in a fast, user-friendly, low cost, non-disturbing manner and performance through the use of image quality assessment. Thus we propose an secure authentication by combining the above four biometric systems to identify the fake / real users. Also we shall propose the best biometric system by comparing Iris/fingerprint/palm vein/face recognition techniques. Also focus on researching the system in accordance to the performance analyzing accuracy and time factors.

KEYWORDS: Biometrics, Iris, DWT based extraction, PCA based feature reduction and Finger- print.

I. INTRODUCTION

In recent years, the increasing interest in the evaluation of biometric systems security has led to the creation of numerous and very diverse initiatives focused on this major field of research: the publication of many research works disclosing and evaluating different biometric vulnerabilities lead to the proposed new protection methods. Recent research clearly highlight the importance given by all parties involved in the development of biometrics (i.e., researchers, developers and industry) to the improvement of the systems security to bring this rapidly emerging technology to put into practical service. Among the different threats examined, the so-called direct or spoofing attacks have motivated the biometric community to study the vulnerabilities against this type of fraudulent actions in modalities such as the iris, the fingerprint, the face, the vein and multimodal approaches. In these attacks, the invader uses some type of synthetically produced artifact (e.g., gummy finger, printed iris image or face mask), or tries to mimic the behavior of the genuine user (e.g., gait, signature), to fraudulently access the biometric system.

The two types of methods present certain advantages and drawbacks over the other and, in general, merging of both would be the most desirable protection approach to increase the security of biometric systems. In the current work we propose a novel software-based multi-biometric and multi-attack protection method which targets to overcome part of these limitations through the use of image quality assessment (IQA). An added advantage of the proposed technique is its speed and very low complexity, which makes it very well suited to work on real scenarios. As it does not deploy any trait-specific property (e.g., minutiae points, iris position or face detection), the computation load required for image processing purposes is reduced, using only general image quality measures quick to compute, combined with very simple classifiers.

II. BASE PAPER EXPLANATION

To prevent fraudulent access attempt by software based fake detection method. The enhancement through fast, user friendly , and non intrusive manner by the use of image quality assessment. Based on public available data sets of

10.15662/ijareeie.2015.0403069

finger print , iris , and 2D face and highly valuable information that may be very efficiently used to discriminate them from face traits.

III. PROPOSED METHODOLOGY AND DISCUSSION

In the digital world, it is very difficult to maintain our personal records and securing data from intruders. Today every person can easily access their information anytime and anyplace. At the same time with the help of modern technology and advanced techniques unauthorized access of other persons is also increased. To overcome these problems we propose a multimodal biometric authentication method that incorporates the features of iris/face/vein and fingerprint recognition which will be highly secure, user-friendly, privacy preserving and revocable. We also propose the best biometric system. The best biometric system will be compared with other algorithms in terms of accuracy, time for feature extraction. The system does not require user training, and is easy to use, fast to compute, combined with very simple classifiers.This fusion based approach is secure against various attacks. This method effectively reduces the processing time and increase the accuracy rate.

3.1 IRIS

ALGORITHM: K-NN

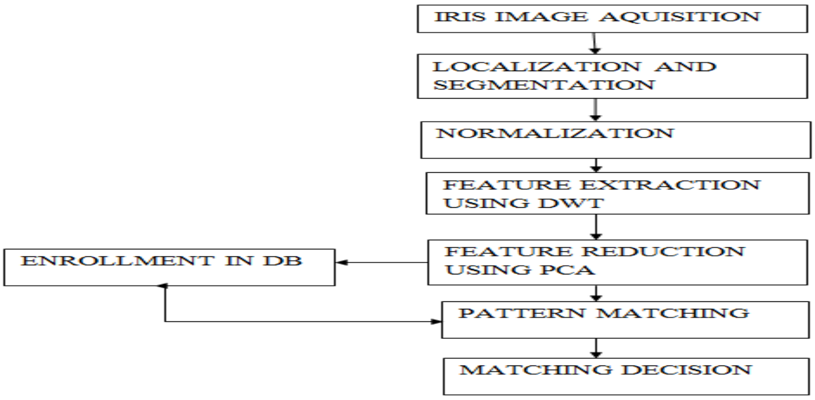

IRIS IMAGE AQUISITION
LOCALIZATION AND SEGMENTATION
NORMALIZATION
FEATURE EXTRACTION USING DWT
FEATURE REDUCTION USING PCA
ENROLLMENT IN DB
PATTERN MATCHING
MATCHING DECISION

Fig.3.1.1 Iris Recognition system

In image acquisition is to capture a sequence of iris images from the subject using a specifically designed sensor. In image localization and segmentation one detects the inner and outer boundaries of iris. In image normalization is required to convert the iris image to polar coordinates from Cartesian coordinates. In Feature extraction process the most important step in automatic iris recognition is the ability of extracting some unique attributes from iris, which help to create a specific code for each individual. In encoding stage, two level Discrete Wavelet Transformation (DWT) is applied on the above segmented and normalized iris region to get approximation. In feature reduction process based on a combined principle component analysis on the feature vectors that calculated from the wavelets limiting the feature vectors to the component selected by the PCA. After this process, an iris image is represented as a feature vector of a small length. Therefore, our final task is to classify(match) the image. In pattern recognition, the k-nearest neighbor algorithm k-NN is a method for classifying objects based on closest training examples in the feature space.

3.2 FINGER

ALGORITHM: MINUTIAE MAP

The location where a ridge comes to an end is called termination. The location where a ridge divides into two separate ridges called bifurcation. The process of converting the original gray scale image to a black-and white image called binarization. The process of minimizing the width of each ridge to one pixel is called thinning. The angle between the horizontal and the direction of the ridge is called termination angle. After minutiae extraction, the minutiae location and the minutiae angles are derived. The terminations which lie at the outer boundaries are not considered as minutiae points and Crossing Number is used to place the minutiae points in fingerprint image. For implementation the entire system has been divided into the following modules such as finger print identification, data hiding technique, finger print extraction and finger print comparison.

3.3 VEIN

ALGORITHM: ORIENTATION MAP Palm vein authentication has high level of authentication accuracy due to the uniqueness of vein patterns of the palm. It is difficult to forge the palm vein pattern because it is internal in the body. Palm vein system is more robust than other biometric authentication such as face, iris and retinal. Palm vein authentication done by comparing the pattern of veins in the palm (which appear as blue lines) of a person being authenticated with a pattern stored in a database.

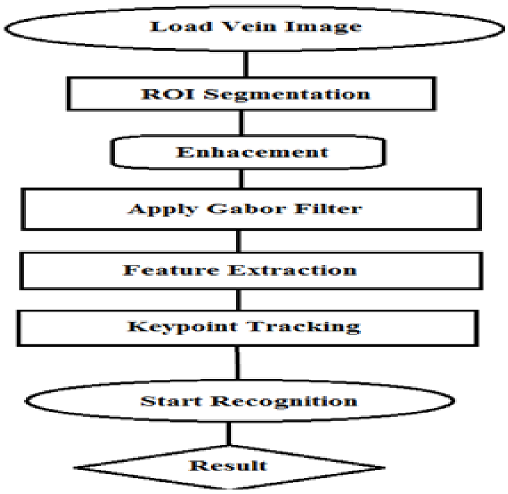


Fig.3.3.1 Vein Recognition Method

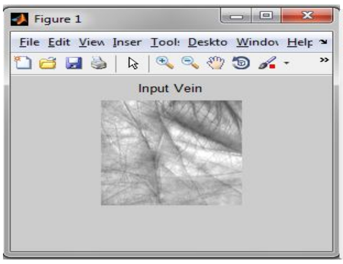
3.4 FACE RECOGNITION

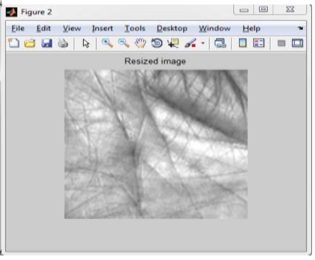
ALGORITHM: HISTOGRAM METHOD

Face recognition is a task humans perform remarkably easily and successfully. It has the accuracy of a physiological approach without being intrusive. We propose Eigen value along with histogram equalization. The efficiency of the system is far better than present systems. Histogram or Frequency Histogram is a bar graph. The horizontal axis depicts the range and scale of observations involved and vertical axis shows the number of data points in various intervals.Initially the image is taken and if the image is RGB image then it is converted into gray scale image and size normalization is performed as pre-processing. The frequency of every gray-level is computed. These frequencies act as Eigen value for the face images. Eigen value represent the variation in the data set. These Eigen values are then stored in vectors. Mean of consecutive nine frequencies from the stored vectors is calculated and are stored in another vectors for later use in testing phase. This mean vector is used for calculating the absolute differences among the mean of trained images and the test image. Finally the minimum difference found identifies the matched class with test image.

IV. EXPERIMENTAL RESULT

STEP 1- SELECT THE TEST VIEN IMAGE





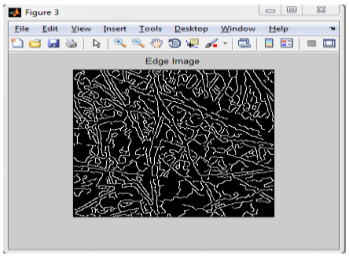
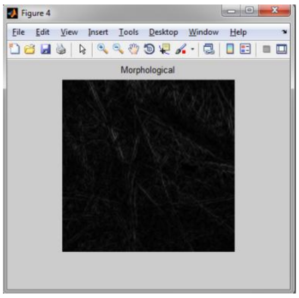


Fig.4.1 Input Vein Image Fig.4.2 Resized Image Fig.4.3 Edge Image



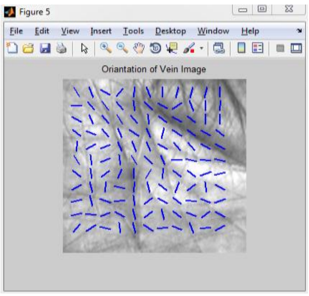


Figure 5
File Edit View Insert Tools Desktop Window Help
Oriantation of Vein Image

Fig.4.4 Morphological Image Fig.4.5 Orientation Of Vein Image

STEP 2-SELECT THE RECOGNIZED VEIN IMAGE

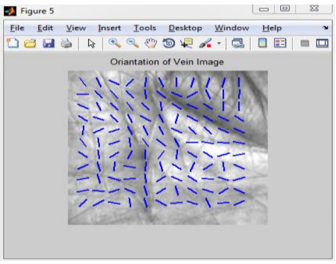
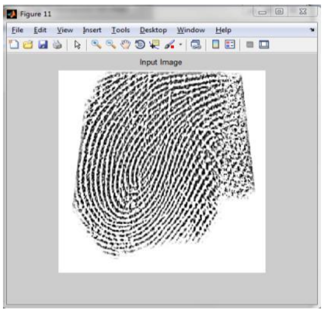
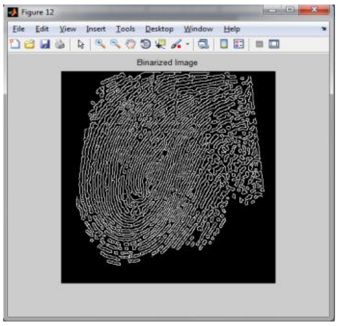


Figure 5
File Edit View Insert Tools Desktop Window Help
Oriantation of Vein Image

Fig.4.6 Orientation Of Recognized Vein Image

STEP 3- SELECT THE TEST FINGER IMAGE





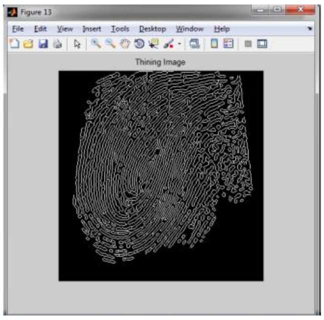


Fig.4.7 Input Finger Image Fig.4.8 Binarized Image Fig.4.9 Thinning Image

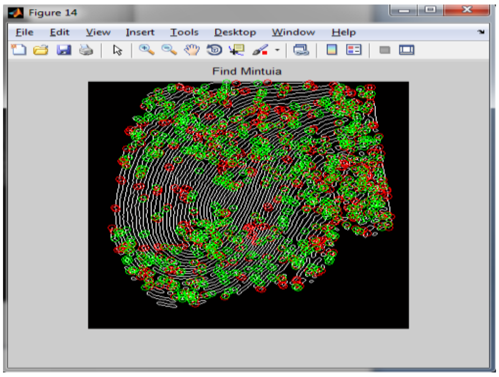


Fig.4.10 Finding Of Minutiae Image

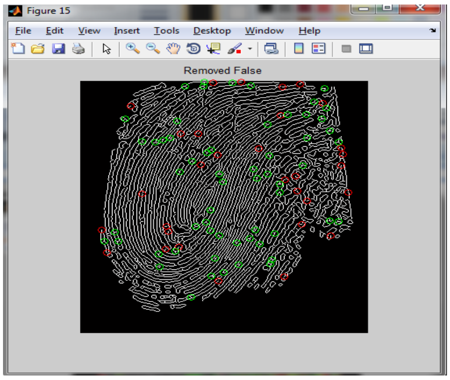


Fig.4.11 Removed False Image

STEP 4- SELECT THE RECOGNIZED FINGER IMAGE

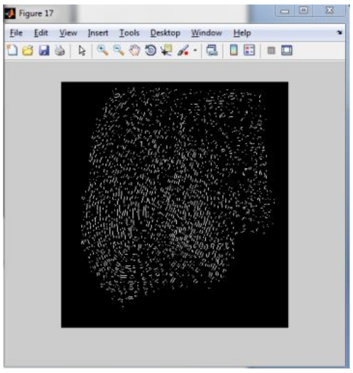


Fig.4.12 Recognized Finger Image

STEP 5-SELECT THE TEST IRIS IMAGE

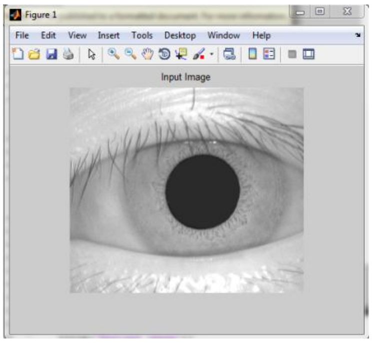


Fig.4.13 Input Iris Image

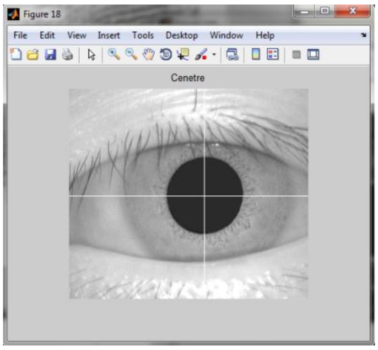


Fig4.14 Iris Cenetre Image

STEP 6-SELECT THE RECOGNIZED IRIS IMAGE

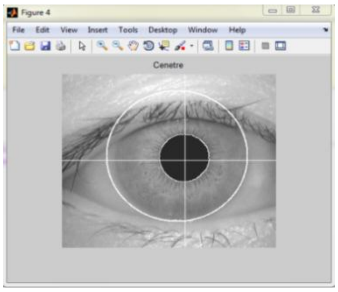
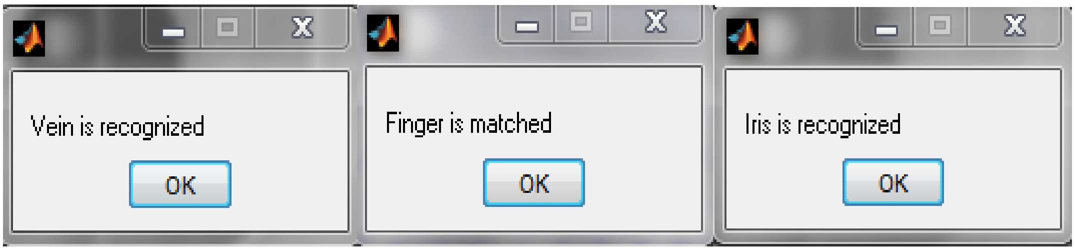


Fig.4.15 Recognized Iris Image

RECOGNITION

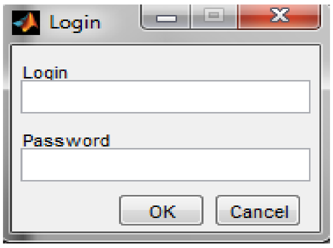


Vein is recognized

Finger is matched

Iris is recognized

LOGIN

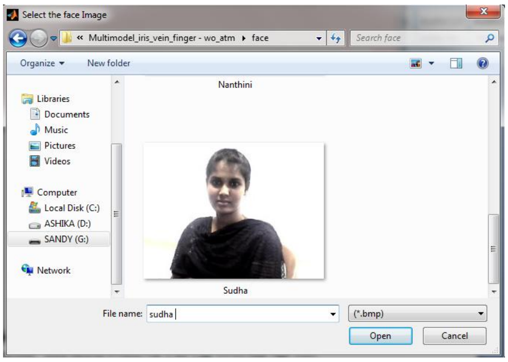


Login

Login

Password

FACE RECOGNITION



Select the face Image

« Multimodel_iris_vein_finger - wo_atm ▸ face

File name: sudha

(*.bmp)

Fig.4.16 Recognized Face Image

After the completion of face recognition it automatically login to application

V. CONCLUSION

To improve the safety of biometric recognition mechanism, by adding liveness assessment in a fast, user-friendly, low cost, and performance through the use of image quality assessment. Thus we propose an secure authentication by combining the four biometric systems to perform at a high level for different biometric traits and adapt to different types of attack providing for all of them a high level of protection. The future enhancement can be implementing the high fusion security in e-commerce/m-commerce applications. Thus focusing on developing an efficient algorithm for feature extraction in terms of accuracy / time for the best biometric system.

REFERENCES

[1] 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.

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

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

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

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

[6] K. A. Nixon, V. Aimale, and R. K. Rowe, “Spoof detection schemes,” Handbook of Biometrics. New York, NY, USA: Springer-Verlag, 2008, pp. 403–423.

[7] S. Prabhakar, S. Pankanti, and A. K. Jain, “Biometric recognition: Security and privacy concerns,” IEEE Security Privacy, vol. 1, no. 2,pp. 33–42, Mar./Apr. 2003.

[8] T. Matsumoto, “Artificial irises: Importance of vulnerability analysis,” in Proc. AWB, 2004.