International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 14 Issue 1 –APRIL 2015.

SECURITY-ENHANCING TECHNOLOGIES FOR BIOMETRIC SYSTEMS

HANIMOL T M

M E. Computer Science and Engineering, Gnanamani College of Technology, Namakkal.

hanikutty.18@gmail.com

SVIDHUSHAVARSHINI, *Assistant Professor,*

Department of Computer Science and Engineering, Gnanamani College of Technology, Namakkal.

vidhushasuresh@gmail.com

ABSTRACT:

Many organizations are using different kinds of automated person's identifications systems which improve the user's needs, satisfaction, and efficiency to secure critical resource. In this paper we are giving the information on the recent developments in person's identification using Biometric technology method. By using this technology we are to ensure to identify a person whether he/she is real person or a fake person. The objective is to increase the security of biometric recognition frameworks, in a fast, user-friendly, and non-intrusive manner by adding liveness assessment. In this paper we are giving information about different modalities such as fingerprint, face recognition, and iris to study against the different types of vulnerabilities attacks. The proposed advance presents a very low level of convolution, using 25 general image quality features extract from one image to differentiate between real and impostor samples, which makes it suitable for real-time applications. The ANN classifier approach makes the proposed method highly competitive as compared with other classification methods, based on the available data sets of finger print, iris, and 2D face. The analysis of the image quality of real biometric samples gives important information that helps to discriminate the samples from fake traits.

1. INTRODUCTION:

In Recent years, automated person identification is highly researched because for protected access to computer, buildings, mobile phones, ATM'S and video surveillance. Person identification is the process of associating an identity to an individual. Person identification techniques are broadly classified into three types such as knowledge based approach, token based approach, and biometric based approach. A knowledge-based approach depends on something an individual knows to make a personal identification, like a password or a personal identification number (PIN).

Token-based approaches are based on something an individual have to make a personal identification like a passport, driver's license, ID card, credit card, or keys. Biometric based systems use physiological or behavioral features of an individual for identification. Knowledge based and Token based approaches have several disadvantages like password forgotten, or password was stolen by hackers or unauthorized person, Tokens may be forgotten, lost, stolen, or misplaced. Whereas, in Biometric based systems it cannot be forged or stolen [1]. You don't want to replace password based access control to avoid having to reset forgotten password and be bothered about the integrity of your system? You don't want to like to rest secure in comfort that your healthcare system does not merely on your social security number as proof of your identity for granting access to your medical records? Using the proper PIN gains access, but the user of the PIN is not verified. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Although warning, many people continue to choose easily guessed PIN's and passwords: birthdays, phone numbers and social security numbers. Recent cases of identity theft have enhance the need for methods to prove that someone is truly who he/she claims to be.

The short comings of current protection methods is the lack of generality and is based on the certain specific properties of the give trait which results in a very reduced interoperability. In order to

overcome the drawbacks of the present method we propose a new software based multi-biometric and multi-attack protection method through the use of image quality assessment. It operates with a very good performance and provides a high level protection against certain multi attacks. The new method is fast and it needs only one image to detect whether it is real or fake. Here 25 image quality features are extracted from one single image and based on these 25 quality features, the technology detect whether it is real or fake image. The new method is non-intrusive, user-friendly, cheap and easy to embed in the existing function systems. It offers high speed and very low complexity which helps in the implementation in the real time systems.

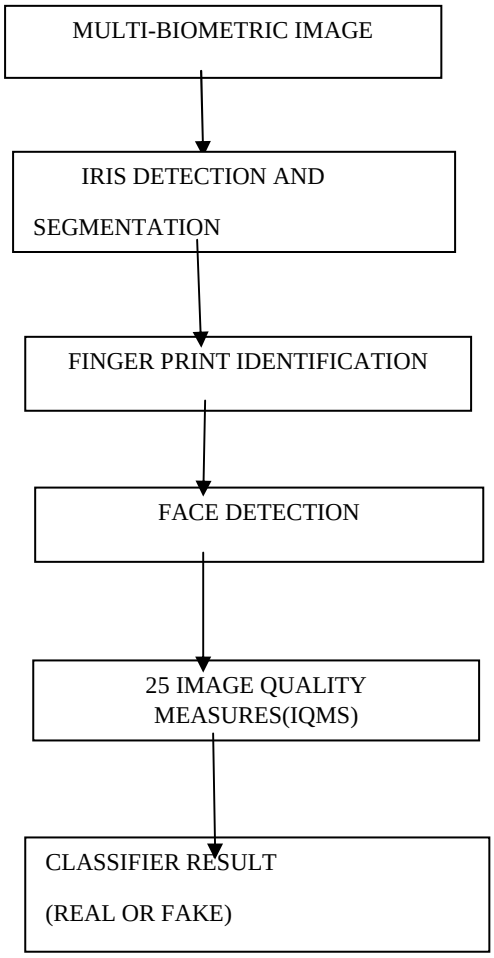


Fig 1: Early Detection Method.

2. PROPOSED SYSTEM:

The methodology carried out in the proposed work is artificial neural network technique. We used feed forwardA single stage feed forward neural network classifier containing one input, one hidden and one output layer waspredominantly used for the classification.The fake biometric detection method is a two-class classification problem, where the sample can be classified as real or fake. In this method a set of discriminant features extracted from a single image helps to determine the quality of the image. In the present work we propose a new parameterization using 25 general image quality measures.

The system needs only one input sample i.e. the biometric sample to determine the fake image. The method works on the whole image without searching for the specific properties of the image and does not need the different pre-processing steps like finger print segmentation, iris detection or face extraction. The method requires only the computation of different IQ measures. Thus the new protection method minimize the computational loads and it brings simplicity and generality for the efficient use. In order to classify the image we propose a classifier method called ANN classifier to determine whether the image is real or fake. In the existing methods standard implementations in Matlab of the Linear Discriminant Analysis (LDA) and Quadratic Discriminant Analysis (QDA) classifier are used [1]. For our experiments we have considered standard implementations in Matlab of Artifical Neural Network. These classifiers are attractive because they have closed-form solutions that can be easily computed, are inherently multiclass, and have proven to work well in practice. Also there are no parameters to tune for these algorithms.

The method has been tested on the publicly available database of iris [3], finger print [5] and 2D face [4] and classify the image by using the classifier method called ANN classifier

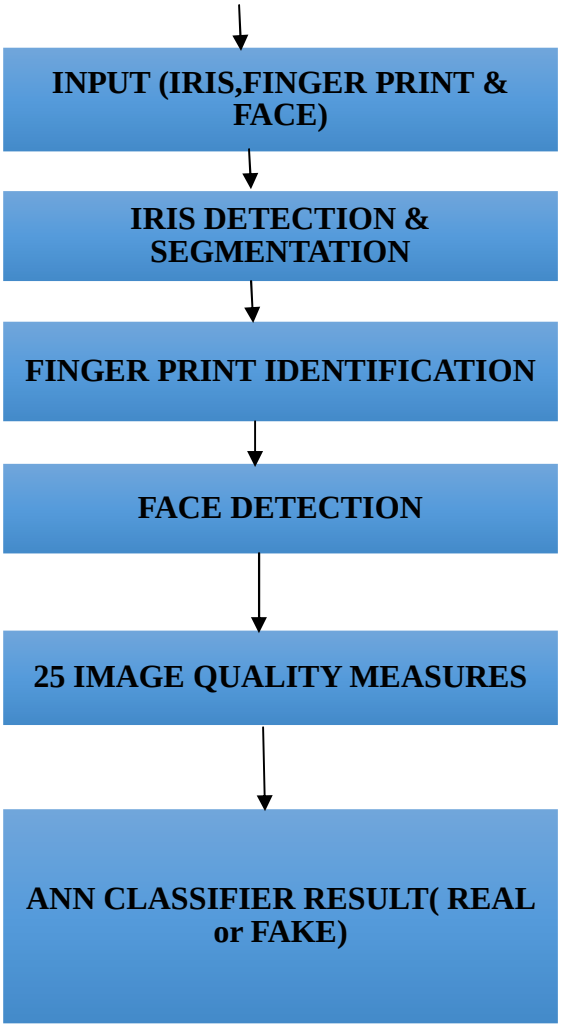


Fig 2: Proposed System

3. THE25 IQA FEATURES:

In the proposed method we use a set of 25 image quality features both blind and reference. Based on the availability of the image, image quality assessment algorithms are classified into full reference and no reference. Among the 25 features, 21 are full reference IQ measures and 4 are no reference IQ measures. The 25 IQMs are carried out using the 3 selection criteria. They are speed, complexity and performance.

3.1Full-Reference IQ Measures.

In full reference method a complete distortion free image is available for the comparison. Full reference algorithms normally adopt a two stage structure including local quality measurement and pooling to get the quality value. The different full reference IQ measures are Error Sensitivity Measures, Structural Similarity Measures and Information Theoretic Measures.

3.2 No-Reference IQ Measures.

NR-IQA measures handle the visual quality of images in the absence of a reference.NR-IQA methods estimate the quality of the image based on the some pre-trained statistical models. Different NR-IQAs are Distortion-specific approaches, Training-based approaches and Natural scene statistic approaches.

The different image features category are:

1.FULL REFERENCE

1.1 Error Sensitivity Measures

- Difference Based
  - Mean Squared Error
  - Peak Signal to Noise Ratio
  - Signal to Noise Ratio
  - Structural Content
  - Maximum Difference
  - Average Difference
  - Normalized Absolute Error
  - R-Averaged Maximum Difference
  - Laplacian Mean Squared Error
- Correlation based
  - Normalized Cross-Correlation
  - Mean Angle Similarity
  - Mean Angle Magnitude Similarity
- Edge Based
  - Total Edge Difference
  - Total Corner Difference
- Spectral Based
  - Spectural Magnitude Error
  - Spectural Phase Error
- Gradient Based
  - Gradient Magnitude Error
  - Gradient Phase Error

1.2 Structural Similarity Measures

- Structural Similarity Index Measures

1.3 InformationTheoretic Measures.

- Visual Information Fidelity
- Reduced Reference Entropic Difference index

2. NO REFERENCE

2.1 Distortion Specific Measures

- JPEG Quality Index

- High-Low Frequency Index

2.2 Training Based Measures.

- Blind Image Quality Index

2.3 Narural Scene Statistics Measures.

- Natural Image Quality Evaluator

ARTIFICIAL NEURAL NETWORK (ANN)

An artificial neural network (ANN), generally called neural network (NN), is a mathematical model or computational model that is inspired by the structure and/or functional aspects of biological neural networks. A neural network contains of an interconnected group of artificial neurons(processing element),working in unison to solve specific problems. ANNs, like people, learn by example. The neuron has two modes of operations. The training/learning mode and the using/testing mode**.** In mainly cases an ANN is an adaptive system that converts its structure based on external or internal information that flows through the network in the learning phase. Recent neural networks are non-linearstatistical data modeling tools. They are generally used to model complex relationships between inputs and outputs or to find patterns in data.

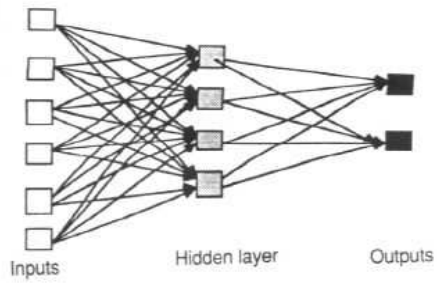
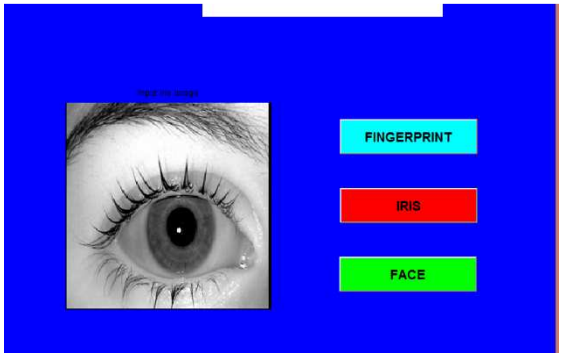


Fig 3: Artificial Neural network

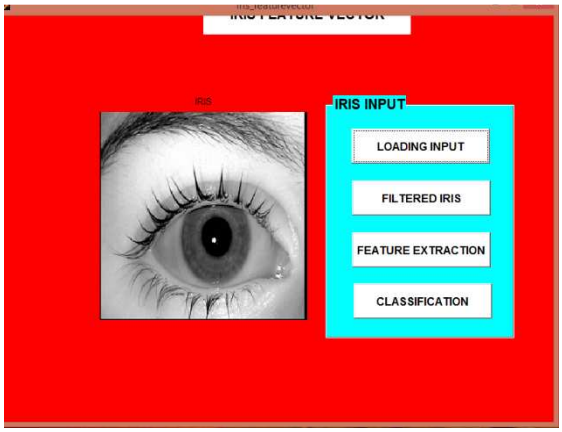
Pattern recognition can be implemented by using a feed-forward neural network that has been trained accordingly. During training, the network is trained to associate outputs with input patterns. When the network is used, it identifies the input pattern and tries to output the associated output pattern. Feed-forward ANNs allow signals to travel one way only; from input to output. There is no feedback (loops) i.e. the output of any layer does not affect that same layer. Feed-forward ANNs tend to be straight forward networks that associate inputs with outputs. They are extensively used in pattern recognition. The features of the images are extracted according to the 25 image quality measures and stored in the database. The ANN Classifier classifies the image into the real or fake according to the image quality features. The classifier check the input image on the basis of the 25 features and not with the single pixel features. As a result classifier can determine which is real and which is fake.

SIMULATION RESULT

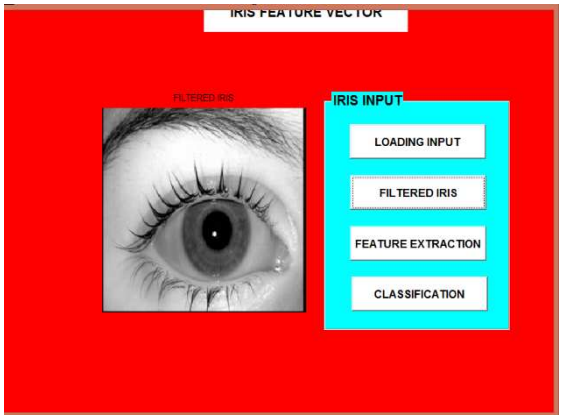
(i) Select the biometric



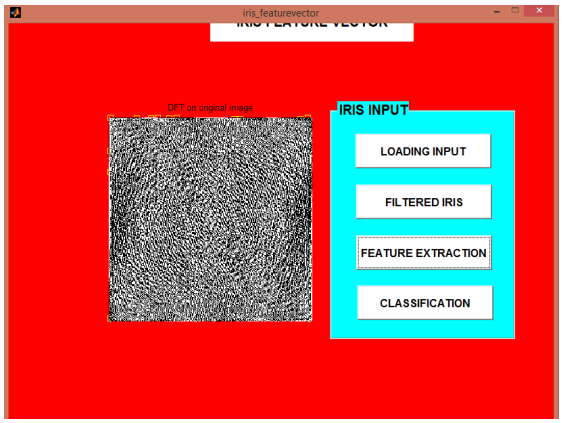
(ii) iris input



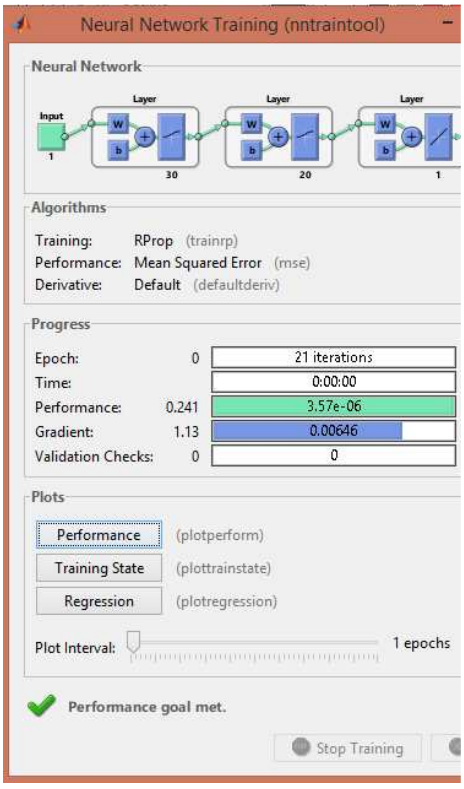
(iii)Filtered Iris



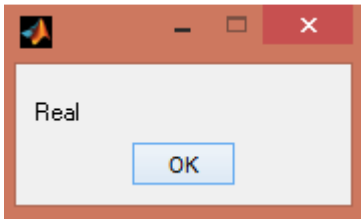
(iv) Feature extraction



(v) Ann classification



(vi) Result



ADVANTAGE OF PROPOSED SYSTEM

The results of the artificial neural network techniques were promisingas, we got 100% for sensitivity, 95% for performance, and97.5% for accuracy.

CONCLUSION:

The study of the vulnerabilities of biometric systems againstdifferent types of attacks has been a very active field of research in recent years. This interest has lead to big advances in the field of security-enhancing technologies for biometric-based applications. Simple visual inspection of an image of a real biometric trait and a fake sample of the same trait shows that the two images can be very similar. In this context, it is reasonable to assume that the image quality properties of real accesses and fraudulent attacks will be different. For this purpose we have considered a feature space of25 complementary image quality measureswhich we havecombined with simple ANN classifiers to detect real and fake accessattempts. The novel protection method has been evaluated onthree largely deployed biometric modalities such as the iris,the fingerprint and 2D face, using publicly available databaseswith well defined associated protocols.

ACKNOWLEDGEMENT

We would like to thank all the faculties and students of Computer Science and Engineering Department, Gnanamani College of Technology for their guidance and support and facilities extended to us.

REFERENCE:

[1] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometricrecognition:Security and privacy concerns," *IEEESecurity Privacy*, vol. 1, no. 2,pp. 33–42, Mar./Apr. 2003.

[2] J. Hennebert, R. Loeffel, A. Humm, and R. Ingold, "Anew forgery scenario based on regaining dynamics ofsignature," in Proc. IAPR ICB,vol. Springer LNCS-4642.2007, pp. 366–375.

[3] T. Matsumoto, "Artificial irises: Importance ofvulnerability analysis," in *Proc. AWB*, 2004.

[4] A. Anjos and S. Marcel, "Counter-measures to photoattacks in face recognition: A public database and abaseline," in *Proc. IEEE IJCB*, Oct. 2011, pp. 1–7.

[5] J. Galbally, R. Cappelli, A. Lumini, G. G. de Rivera, D.Maltoni,J. Fierrez, *et al.*, "An evaluation of direct andindirect attacks using fakefingers generated from ISOtemplates," *Pattern Recognit. Lett.*, vol. 31, no. 8, pp.725– 732, 2010.

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

[7] 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.

[8] 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.

[9] J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, "Iris liveness detection based on quality relatedfeatures," in *Proc. 5th IAPR ICB*, Mar./Apr. 2012, pp. 271–276.