ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

TO ENHANCE THE SECURITY IN BIOMETRIC AUTHENTICATION BY USING ARTIFICIAL NEURAL NETWORK TECHNIQUE

D.Sudha[1], R.Kavitha[2], S.Amsaveni[3], R.Priya[4]
Associate Professor[2], Assistant Professor[134]
Department of Electronics and Communication Engineering[1234]
Bharathiyar Institute of Engineering for Women
Tamil Nadu, India
dsudha.ayyanar@gmail.com[1], kavitharbe@gmail.com[2], amsaece.veni@gmail.com[3], mailmepriya47@gmail.com[4]

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. The information depends on the recent developments in person's identification using Biometric technology method. By using this technology we are to ensure to identify a person weather he/she is real person or a fake person. The objective is to increase the security of biometric reorganization frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive manner. 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, which makes it suitable for real-time applications, using 25 general image quality features extract from one image (i.e., the same acquired for authentication purposes) to differentiate between legitimate and impostor samples. The experimental results, obtained on publicly available data sets of fingerprint, iris, and 2D face, show that the proposed method is highly competitive compared with Classification ANN (Neural Network) approaches and that the analysis of the general image quality of real biometric samples reveals highly valuable information that may be very efficiently used to discriminate them from fake traits using MATLAB.

I. INTRODUCTION

The Digital image processing is the use of computer algorithms to perform image processing on digital images. As a subfield of digital signal processing, digital image processing has many advantages over analog image processing; it allows a much wider range of algorithms to be applied to the input data, and can avoid problems such as the build-up of noise and signal distortion during processing. An image may be defined as a two-dimensional function, f(x, y), where x and y are spatial coordinates, and the amplitude of f at any pair of coordinates (x, y) is called the gray level or intensity of the image at that point. When x, y and the amplitude values of are finite, discrete quantities, we call the image a digital image. The field of digital image processing refers to processing digital images by means of a digital computer. Note that a digital image is composed by a finite number of elements, which everyone has a particular location and value. These elements are referred as picture elements, image elements, pels, and pixels. Pixel is the term most widely used to denote the elements of a digital image. The intent of classification process is to categorize all pixels in a digital image into one of several land cover classes or themes. This classified data may be used to produce thematic maps of the land cover present in an image. Pictures are the most common and convenient means of conveying or transmitting information. A picture is worth a thousand words. Pictures concisely convey information about positions, sizes and inter-relationships between objects. They portray spatial information that we can recognize as objects. Human beings are good at deriving information from such images, because of our innate visual and mental abilities. About 75% of the information received by human is in pictorial form. Thus our discussion will be focusing on analysis of remotely sensed images. These images are represented in digital form. Digital remote sensing data could be analyzed only at specialized remote sensing laboratories. Specialized equipment and trained personnel necessary to conduct routine machine analysis of data were not widely available in digital image processing.

II.THE SECURITY PROTECTION METHOD

Image Quality Assessment technique is used for enable biometric systems to detect fake samples and reject them, improving this way the robustness and security level of the systems. It is not only capable of operating with a very good performance under different biometric systems (multi-biometric) and for diverse spoofing scenarios, but it also provides a very good level of protection against certain non-spoofing attacks (multi-attack). Moreover, being software-based, it presents the usual advantages of this type of approaches: fast, as it only needs one image (i.e., the same sample acquired for biometric recognition) to detect whether it is real or fake; non-intrusive; user-friendly (transparent to the user); cheap and easy to embed in already functional systems. Human observers very often refer to The“different appearance” of real and fake samples to distinguish between them. As stated above, the different metrics and methods designed for IQA intend to estimate in an objective and reliable way the perceived appearance of images by humans. Improvement of the systems security to bring this rapidly emerging technology into practical use Among the different threats analyzed, the so-called direct or spoofing attacks have motivated the biometric community to study the vulnerabilities. To enable biometric systems to detect fake samples and reject them, improving this way the robustness and security level of the systems. Besides other anti-spoofing approaches such as the use of multi biometrics or challenge-response methods, special attention has been paid by researchers and industry to the liveness detection techniques, which use different physiological properties to distinguish between real and fake traits. Liveness assessment methods represent a challenging engineering problem as they have to satisfy certain demanding requirements non-invasive, the technique should in no case be harmful for the individual or require an excessive contact with the user user friendly.

CRITERIA

PERFORMANCE which refers to the achievable recognition accuracy and speed, the resources required to achieve the desired recognition accuracy and speed, as well as the operational and environmental factors that affect the accuracy and speed;

- ACCEPTABILITY which indicates the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives;
- CIRCUMVENTION which reflects how easily the system can be fooled using fraudulent methods.

III. MEASURES

Error Sensitivity Measures : Traditional perceptual image quality assessment approaches are based on measuring the errors (i.e., signal differences) between the distorted and the reference images, and attempt to quantify these errors in a way that simulates human visual error sensitivity features. Widely used methods for IQA as they conveniently make use of many known psychophysical features .Visual system they are easy to calculate and usually have very low computational complexity

Pixel Difference Based Measures : These features compute the distortion between two images on the basis of their pixel difference. These are some of the measures given below:

Mean Square Error (MSE),Peak Signal to Noise Ratio (PSNR), Signal to Noise Ratio (SNR), Structural Content (SC), Maximum Difference (MD), Average Difference(AD), Normalized Absolute Error (NAE), R-Averaged Maximum Difference (RAMD) and Laplacian Mean Squared Error (LMSE).

Edge Based Measures : Edges and other two-dimensional features such as corners are some of the most informative parts of an image, which play a key role in the human visual system. Many computer vision algorithms are including quality assessment applications.

Gradient Based Measures: Gradients convey important visual information which can be of great use for quality assessment. Many of the distortions that can affect an image are reflected by a change in its gradient. Therefore, using such information, structural and contrast changes can be effectively captured.

FR-IQMs:Structural Similarity Measures

Although being very convenient and widely used, the aforementioned image quality metrics based on error sensitivity present several problems which are evidenced by their mismatch (in many cases) with subjective human-based quality scoring systems.In this scenario, a recent new paradigm for image quality assessment based on structural similarity was proposed following the hypothesis that the human visual system is highly adapted for extracting structural information from the viewing field .Therefore, distortions in an image that come from variations in lighting, such as contrast or brightness changes (nonstructural distortions), should be treated differently from structural ones.

NO-REFERENCE IQ MEASURES

Unlike the objective reference IQA methods, in general the human visual system does not require of a reference sample to determine the quality level of an image. Following this same principle, automatic no-reference image quality assessment (NR-IQA) algorithms try to handle the very complex and challenging problem of assessing the visual quality of images, in the absence of a reference. NR-IQA methods generally estimate the quality of the test image according to some pre-trained statistical models.

Distortion-specific approaches : These techniques rely on previously acquired knowledge about the type of visual quality loss caused by a specific distortion.

BLOCK DIAGRAM

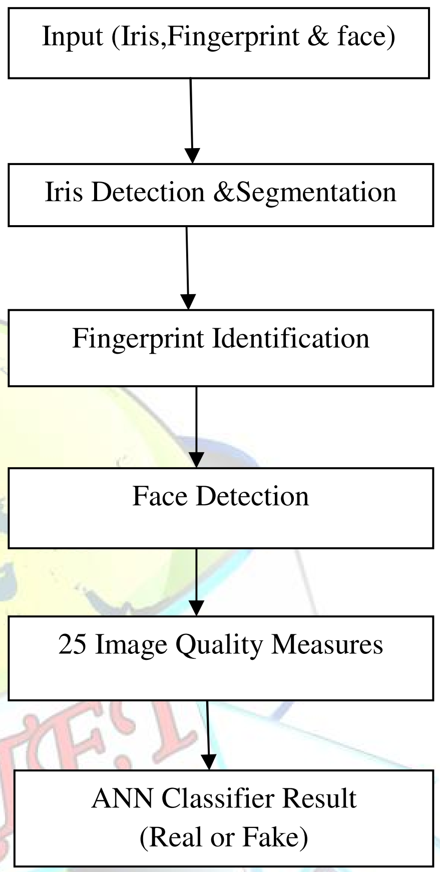
Input (Iris,Fingerprint & face)
Iris Detection &Segmentation
Fingerprint Identification
Face Detection
25 Image Quality Measures
ANN Classifier Result
(Real or Fake)

Fig 1: Image Quality Assessment Process

Inputs are fingerprint,face and iris shown in Fig 3.1. Liveness detection can be performed by simply modifying the algorithm to measure skin properties such as perspiration, elasticity, and deformation. The algorithms can be roughly divided into two groups based on whether they extract static or dynamic features: static approaches compare the features extracted from one or more fingerprint impressions.

IV.RESULTS AND DISCUSSION

FEATURE EXTRACTION:

To extract the features from input image

1.INPUT IMAGE

Select the input image

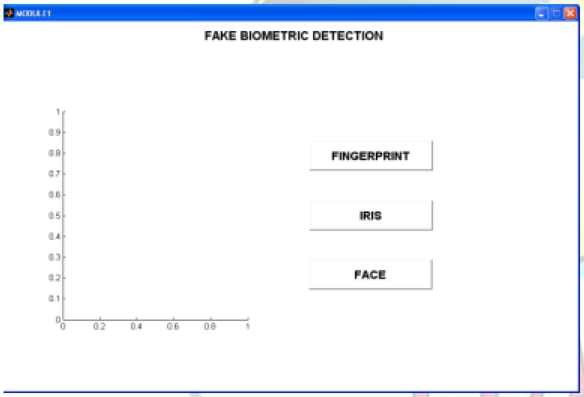

Fig 2: Input image

2.SELECT INPUT FINGERPRINT IMAGE

To select the fingerprint input image is shown as below

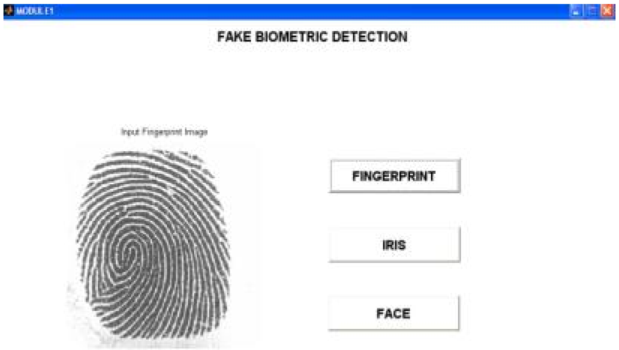

Fig 3 :Input fingerprint image

3. LOADING FINGERPRINT INPUT

To loading the input image is shown as below

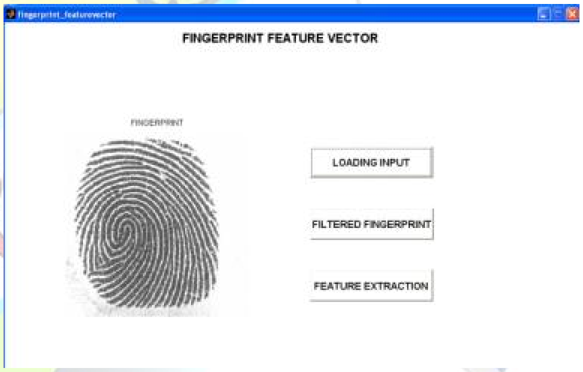

Fig 4: Loading input image

4. FILTERED FINGERPRINT IMAGE

To filtered the fingerprint input image

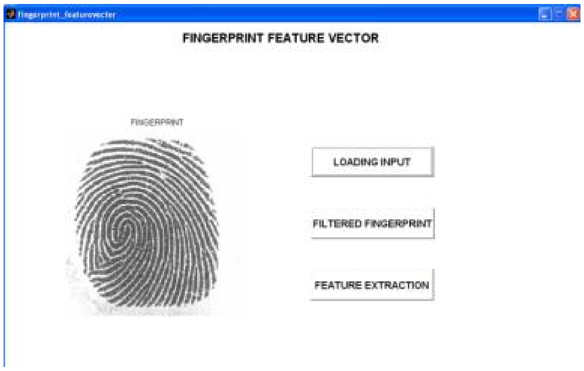

Fig 5: Filterer fingerprint

5. INPUT IRIS IMAGE

To select the input image

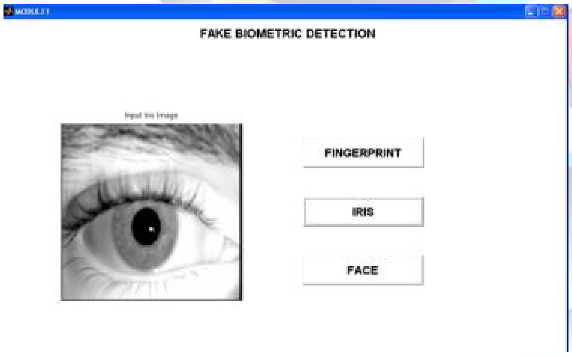

Fig 6: Iris input image

6. LOADING INPUT IRIS IMAGE

To select loading input is shown as below

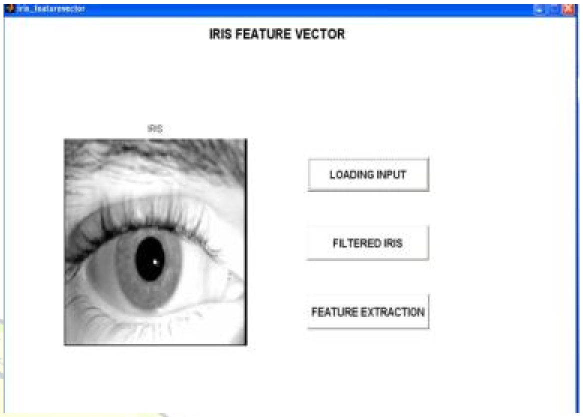

Fig 7: Loading input image

OUTPUT

FEATURE EXTRACTION:

FingerPrint Features for original image

Mean Square Error = 65.0687

Peak Signal to Noise Ratio = 29.9971

MNormalized Cross-Correlation = 0.9912

Average Difference = 0.4114

Structural Content = 1.0162

Maximum Difference = 51

Normalized Absolute Error = 0.0266

FingerPrint Features for fake image

Mean Square Error = 31.1790

Peak Signal to Noise Ratio = 33.1922

MNormalized Cross-Correlation = 0.9919

Average Difference = 0.3139

Structural Content = 1.0151

Maximum Difference = 52

Normalized Absolute Error = 0.0258

Iris Features for original image

Mean Square Error = 6.2052

Peak Signal to Noise Ratio = 40.2032

MNormalized Cross-Correlation = 0.9987

Average Difference = 0.0403

Structural Content = 1.0025

Maximum Difference = 46

Iris Features for fake image

Mean Square Error = 28.0125

Peak Signal to Noise Ratio = 33.6573

MNormalized Cross-Correlation = 0.9963

Average Difference = 0.0880

Structural Content = 1.0068

Maximum Difference = 41

Normalized Absolute Error = 0.0124

V.CONCLUSION

Artificial neural networks method is used for detect the fake samples and reject them and improving this way the robustness and security level of the systems. It is able to consistently perform at a high level for different biometric traits. This method is able to adapt to different types of attacks providing for all of them a high level of protection. The high potential of image quality assessment for securing biometric systems against a variety of attacks. . In order to keep its generality and simplicity, the system needs only one input: the biometric sample to be classified as real or fake (i.e., the same image acquired for biometric recognition purposes). , it does not require an preprocessing steps prior to the computation of the IQ features. This characteristic minimizes its computational load. Linear Discriminant Analysis (LDA) and Quadratic Discriminant Analysis (QDA) classifiers Identification of real or fake. To extracted 25 features from one image using linear discriminant analysis algorithm. In future work extension of the considered 25-features set with new image quality measures using artificial neural networks.

REFERENCES

1. Akhtar Z, .Fumera G and Marcialis G. L,(2012), ‘Evaluation of serial and parallel multi biometric systems under spoofing attacks,’ in Proc. IEEE 5th Int. Conf. BTAS, pp. 283–288.
2. Avcibas I, Memon N and B. Sankur,(2003). ‘Steganalysis using image quality metrics’IEEE Trans. Image Process., vol. 12, no. 2, pp. 221–229.
3. Bayram S, Avcibas I, Sankur B, and Memon M (2003), ‘Image manipulation detection’ J.Electron. Imag., vol. 15, no. 4, pp. 041102-1–041102-17.
4. Jain A.K, Nandakumar K and Nagar A (2008), “Biometric template security,” EURASIP J. Adv. Signal Process., vol. 2008, pp. 113–129.
5. Marcialis G.L, Lewicke A, Tan B,Coli C and Congiu A,(2009)’First international fingerprint liveness detection competition—LivDet 2009,’ in Proc. IAPR ICIAP, Springer LNCS-5716,pp. 12–23.
6. Martini M.G, Hewage C.T and B. Villarini,(2011) ‘Image quality assessment based on edge preservation,’ Signal Process., Image Commun., vol. 27,no. 8, pp. 875–882.
7. Pons A.M, Malo.J, Artigas J.M and P. Capilla, (1999) ‘Image quality metric based on multidimensional contrast perception models,’ Displays J., vol. 20, no. 2, pp. 93–110 .
8. Prabhakar S.Pankanti S and Jain A.K,(2003) ‘Biometric recognition:Security and privacy concerns,’IEEE Security Privacy, vol. 1, no. 2, pp. 33–42.
9. Sheikh H.R and Bovik A.C,(2006) ‘Image information and visual quality’ IEEE Trans. Image Process., vol. 15, no. 2, pp. 430–444.
10. Stamm M.S.(2010) ‘Forensic detection of image manipulation using statistical intrinsic fingerprints,’ IEEE Trans. Inf.