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

IMAGE QUALITY ASSESSMENT USING BIOMETRIC LIVENESS DETECTION FOR FAKE FINGER PRINT, FACE AND IRIS

Prof. S.Kumar [1] and M.Gomathi [2]
Department of Electronics and Communication Engineering,
Bharathiyar Institute of Engineering for Women

ABSTRACT

Image Quality Assessment (IQA) is one of the geometric techniques used in image processing to determine the biometric model is real or fake. The aim of the system is to improve the biometric detection security. This paper deals with two different measures of IQA. The primary measure is Full-Reference(FR) IQA consists of a 2D image extracting different image quality features using a reference image which is filtered by a technique called Gaussian filtering. The secondary measure is No-Reference (NR) IQA used to approximate the quality level of an image. finally, 26 image quality features are exacted to decrease the degree of density. Feature of test section implies to outcome of the following process of classification based on IQA. The paper introduces the IQA theory and its measures. Results are standard for the preferred real and fake pictures.

Index Terms— Image Quality Assessment (IQA),biometrics, security.

I.INTRODUCTION

Nowadays, estimation of biometric systems security is getting higher so we directed on this major line of work study. Image processing technology was developed to integrate not only with preprocessing steps but also used for feature selection[2], template matching[1] and other applications such as surveillance and security camera systems, underwater research. Various publications make enquiries on assessing biometric liabilities the proposal of Liveness detection (LIVDET) [3],the estimation of blur and noise[4],the detection of high correlation, the suggestion of multi-biometrics[6], the recognition of face datasets[14], the evaluation of face anti-spoofing technique[11], the discovery of different distortion specific experts[10],theexposure of spoofing technique[12], the information of local or global approximation[9], the recognition of iris[8],the exposure of manipulating images[7], the acquaintance of signal power to the noise power[15], the introduction of pattern recognition[13]. For instance, the Windows XP and Vista laptops of Lenovo and Toshiba come with built-in webcams and embedded biometric systems that authenticate users by scanning their faces. The whole inventiveness visibly focused the significance of rising in the biometrics system security leads to use practically in an environment. Among the various threats examined, the *spoofing* attacks have inspired biometric similarity to study the liabilities against various types of fraud access in modalities such as the iris, the fingerprint, the face etc. In these attacks, the impostor uses synthetically manufactured article (e.g., face mask). Usually the digital protection mechanisms such as encryption, watermarking are not operative.

Liveness detection (LIVDET) is a technique to detect anti spoofing approaches in multi-biometrics or challenge-response methods. Thus, the liveness detection method presented has the added advantage over previously studied techniques of needing for different modalities to decide whether it comes from a real or fake image. The advantages i) non-intrusive, specifically not harmful to the contact user; ii)easy to access ;iii)speed, results have to be produced in a small

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

interval; iv)minimize cost ;It limits long period of time to access an image.Liveness detection methods are differentiated into two techniques: i) *Hardware-based*,some special device is added to the sensor in order to estimate specific properties such as blood pressure, reflection of eye etc..ii) *Software-based*, in which the fake modalities are detected once the sample has been acquired with a standard sensor. The two types of methods have some advantages and dis-advantages. So, combination of both approaches is used to enrich the security in biometric recognition.

In the proposed system we present a novel software based multi-biometric and multi-attack protection method which overcome part of the limitations through the use of image quality assessment (IQA). It is capable of functioning with a very high enactment under different biometric systems (multi-biometric) and also provides a very good level of protection against certain non-spoofing attacks(multi-attack).. By using biometric recognition we can solve the problem of user authentication in identity management systems. [5] discussed about Intelligent Sensor Network for Vehicle Maintenance System. Modern automobiles are no longer mere mechanical devices; they are pervasively monitored through various sensor networks & using integrated circuits and microprocessor based design and control techniques while this transformation has driven major advancements in efficiency and safety.

II.IMAGEQUALITY ASSESSMENT FOR LIVENESS DETECTION

Image Quality Assessment (IQA) is a technique used to extract image quality features and compare whether an image is real or fake. During the fraudulent attempts the fake image has various quality compared to real image. Image Quality Measures depends on several criteria i)Performance, ii)Complexity,iii) Speed. Predictable quality feature differences measure of irregularity, level of luminance, blur, noise, gradient, covariance, high relationship, comfortable of information extracted from both type of images will be different. For instance, when comparing real fingerprint image with printed fingerprint image, printed image gives a high blur density. Spoofing attacks will be determined based on estimating different image quality features.

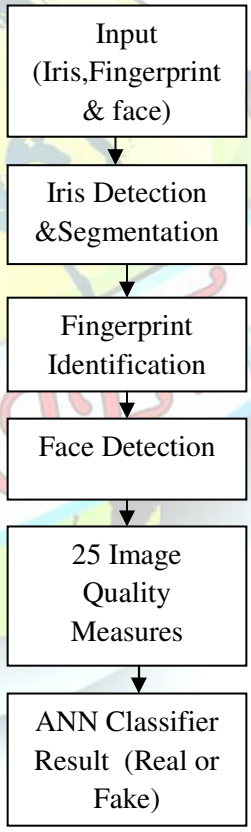

Fig1:Block Diagram

III. FULL REFERENCE IQ MEASURES:

Full-reference (FR) IQA methods are used to estimate the quality of the test sample using a reference image. If reference image is unknown then the image

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

quality will be different compared to a known image. Reference image implies that an image is filtered using Gaussian filtering technique. The input of an image is in grey scale with low pass Gaussian, size of a matrix is N x M. To generate a soft version I^. Then both qualities are computed according to full-reference IQA measures.

1.Error Sensitivity Measures

2.Pixel Difference Based Measures

3.Correlation Based Measures

4.Edge Based Measures

5.Spectral Distance Measures

6.Gradient Based Measures

7.Structural Similarity Measures

8.Information Theoretic Measures

V.NO-REFERENCE IQ MEASURES

Unlike the purpose indication IQA methods, in general the human being visual structure does not involve of a indication sample to create the quality level of an image. Following this same principle, automatic no-reference image quality measurement (NR-IQA) algorithms try to handle the very complex and not easy 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

The methods are coarsely divided into one of three trends

1.Distortion-specific approaches

2.Training-based approaches

3.Blind Image Quality Index

4.Natural Scene Statistic approaches

5.Natural Image Quality Evaluator

V. CLASSIFICATIONt

To get a high presentation when compared with other approaches first approximate the securitymethod of multibiometric width.Then to detect non-spoofing attacks guesstimate the multi-attack aspect of protection method.

ARTIFICIAL NEURAL NETWORKS

Numerous advance have been made in budding quick systems, some motivated by genetic neural networks. Researchers from many controlled discipline are designing artificial neural networks (A"s) to solve a mixture of troubles in sample identification, result, optimization, associative recollection, and power (see the "testing troubles" sidebar). Conventional approaches have been proposed for solving these problems. even though doing well applications can be found in assured well-constrained environments, none is flexible enough to complete well remote its sphere. ANNs provide moving alternatives, and many applications could promote from using them.' This object is for those readers with little or no awareness of ANNs to help them identify with the other articles in this issue of Computer. We converse the motivation last the improvement of A " s , put across the basic genetic neuron and the simulated computational form, outline arrangement architectures and culture processes, and nearby some of the most frequently used ANN models. We conclude with character identification, a doing well ANN application.The long course of advancement has given the creature brain many desirablecharacteristics not present invent Neumann or modern parallel computers. These include

1.substantial Parallelism,

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

2.Circulated Representation And Computation,

3.Knowledge Ability,

4.Generalization Ability,

5.Adaptivity,

6.fault acceptance,

7.Low Energy utilization.

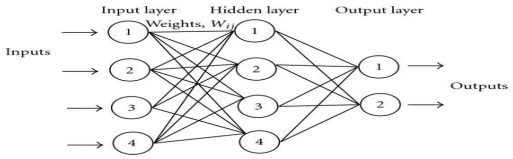

Fig2: Artificial Neural Network configuration.

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

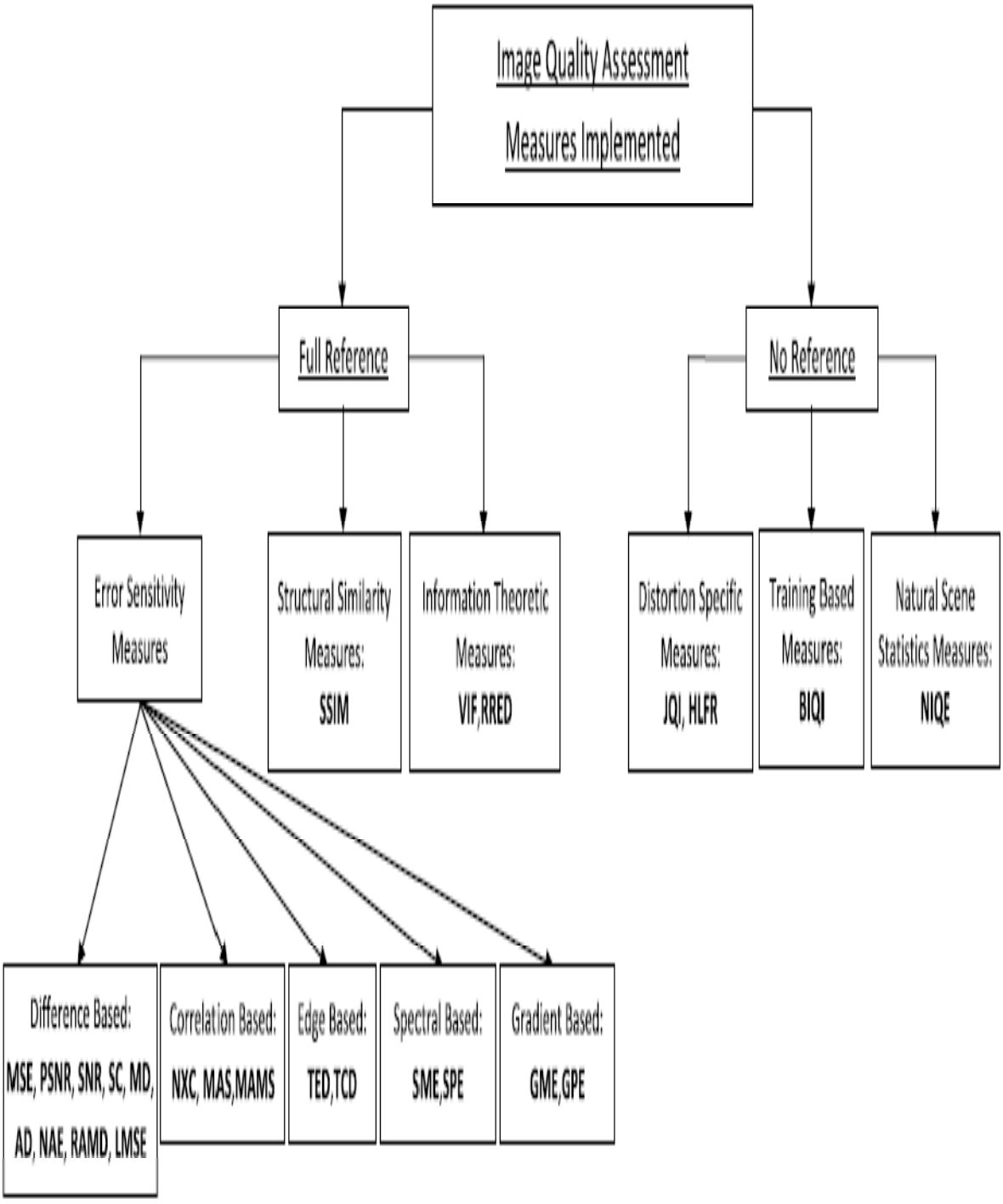

Fig 3: Classification of the 25 image quality measures

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

VI.RESULTS AND DISCUSSION

Fake Biometric Detection appliance offers to present a in half security to your coordination. First the camera will incarcerate the look and transferred to the face is unconstitutional. In the subsequently stage the finger print of the user force be full if the user is formal and then advance the user‟s fingerprint will be tartan for authorization. This two stage security relevance will ensure 100% protection to your system.

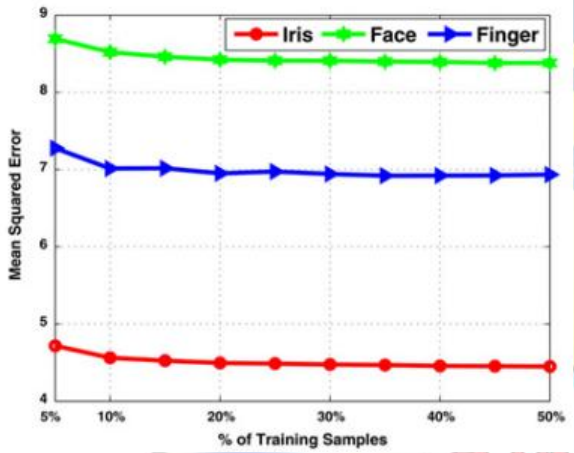

Fig 4: Result

VII.CONCLUSION

Image quality assessment method is used for identify the fake samples and discard them and improving this way the forcefulness and protection level of the systems. It is able to without fail perform at a high level for special 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 likely of image feature 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 confidential as true or false (i.e., the same image acquired for biometric respect purposes). , it does not require an preprocessing steps prior to the division of the IQ features. This characteristic minimizes its computational load. Linear Discriminate 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. Christo Ananth, C.Sudalai@UtchiMahali, N.Ebenesar Jebadurai, S.Sankari@Saranya, T.Archana, “Intelligent sensor Network for Vehicle Maintenance system”, International Journal of Emerging Trends in Engineering and Development (IJETED), Vol.3, Issue 4, May 2014, pp-361-369

6. Martini M.G, Hewage C.T and B. Villarini,(2011) ‘Image quality assessment

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

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,DisplaysJ.,vol.20,no.2,pp.110