ISSN(Online) :2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

2D Face Based Security System for Fake Biometric Detection Using Image Quality Assessment

Rinu Prakash T[1], Vipin Thomas[2]

P.G. Student, Department of Electronics and Communication Engineering, Ilahia College of Engineering & Technology, Muvattupuzha, India[1]

Assistant Professor, Department of Electronics and Communication Engineering, Ilahia College of Engineering & Technology, Muvattupuzha, India[2]

ABSTRACT: Biometric Identification is the best security system in developing security world. Hackers made a fake biometric in easy way, so it reduce the security accuracy. Biometric security system are hacked by using two types of attack, direct or spoofing attack & indirect attack. So, there is a need to develop a new and efficient protection measure. This protection method uses Image Quality Assessment (IQA) technique. If the image is a real, it checks whether the image belongs to an authorized person or not.Face recognition using Discriminate Power Analysis (DPA) technique is used for detecting authorized person. The objective is to increase the security of biometric recognition framework by adding liveness assessment in fast, non-invasive & user friendly manner. This approach protects the biometric security system from direct and indirect attack. The complexity of the proposed system is very low because it extracts 31 image quality measures from one image.

KEYWORDS: Image quality assessment, Discriminate power analysis, liveness detection.

I. INTRODUCTION

Biometric system are actually computer system or pattern recognition system that is used to identify a person based on their behaviour or physiological characteristic .But nowadays these biometric systems are not at all safe because they are attacked by using fake biometric. Two type of attacks performed by the biometric system are direct or spoofing attack, indirect attack. Direct attack means that biometric features that look similar to the original feature is constructed and using that the attack is performed. Indirect attack means that the biometric features are printed on a paper and using that the attack is performed. So in order to protect biometric security system from these two type of attack a new method is proposed. This is a software based biometric and multi-attack protection method. Multi-attack means that this method protect biometric security system from two type of attack.

II. RELATED WORK

According to Javier Galbally, C.M Sebastien Marcel, Julian Fierrez (2010), the general image quality features extracted from an image to distinguish between the legitimate and imposter samples. Considering that the fake image captured in an attack attempt will have different quality than a real sample acquired in the normal operation scenario. Following this quality difference the authors explored the potential of general image quality assessment as a protection method against different biometric attacks with special attention towards spoofing. As the implemented features do not evaluate any specific property of a given biometric modality or of a specific attack, they may be computed on any image. According to SaptarshiChakraborty, Dhrubajyoti Das (2014), the face liveness detection approaches are categorized based on the various types of techniques used for liveness detection. This categorization helps understanding different spoof attacks scenarios and their relation to the developed solutions. A review of the face liveness detection works is presented. The difference between the live face from not live face, which is a major security issue is presented.

ISSN(Online) :2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

III. IMAGE QUALITY MEASURES

Image quality measures IQMs are used for the evaluation of imaging systems or coding/processing techniques. In this study we consider 31 image quality metrics and their statistical behaviour [1]. The two types of image quality measures are Univariate and Bivariate. Univariate measures-these measures assess the quality of the target image without the explicit use of a reference image. These are also called as Non reference image quality measures. Bivariate measures-these measures use a reference image in-order to identify the quality of an image. These are also called as Full referenceimage quality measures. The 29 image quality measures are selected according to four general criteria. These four selection criteria are: Performance, Complementarity, Complexity and Speed.

A. Bivariate IQ Measures

It is the comparison between input and reference image. A complete reference image is assumed to be known. The bivariate IQM are classified into three: Error sensitivity measures, Structural similarity measures, Information theoretic measures. Error sensitivity measures are classified into 5 categories: Pixel difference measures, Correlation based measures, Edge based measures, Spectral distance measures, and Gradient based measures.

1. Error Sensitivity Measures:

Natural way to assess the quality of an image is to quantify the error between the distorted & reference signal. It measure the errors i.e signal difference between the input and reference images (filtered input image). Error sensitivity measures are classified into 5 types: Difference based, Correlation based, Edge based, Spectral based, Gradient based. In this phase out of five error sensitivity measures two measures are calculated. They are as follow

a. Pixel Difference Measures [2][3][4]:

Pixel difference measures compute the distortion between input & reference image on the basis of their pixel wise difference. Pixel wise difference measures include: Mean Squared Error (**MSE**), Root Mean Square Error (**RMSE**), Peak Signal to Noise Ratio (**PSNR**), Maximum Difference (**MD**), and Signal to Noise Ratio (**SNR**), Structural Content (**SC**), Correlation Quality (**CQ**), Average Difference (**AD**), Normalized Absolute Error (**NAE**), R-Averaged Maximum Difference (**RAMD**) and Laplacian Mean Squared Error (**LMSE**).

b. Correlation Based Measures [5]:

Measures the similarity between two digital images. The three correlation based measures are: Normalized cross-correlation (**NXC**), Image Fidelity (**IF**), Mean angle similarity (**MAS**), Mean angle magnitude similarity (**MAMS).**

c. Edge Based Measures [6]:

These make use of local and global gradient information to provide boundaries to regions of interest, and thus indirectly segment the image. Edge based measures include: Total Edge Difference (**TED**) and Total Corner Difference (**TCD**).

d. Spectral Distance Measures [7]:

In this category, the distortion penalty functions obtained from the complex Fourier spectrum of images are considered. In this study two spectral distance measures are considered: the Spectral Magnitude Error (**SME**) and the Spectral Phase Error (**SPE).**

e. Gradient Based Measures [8]:

These measures convey the important visual information. We use the gradient similarity to measure the change in contrast and structure in images. Two simple gradient-based features included are: Gradient Magnitude Error (**GME**) and GradientPhase Error (**GPE**).

ISSN(Online) :2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

2. *Structural Similarity Measures [9]:*

Natural image signals are highly structured. Their pixels exhibit strong dependencies. Structural Similarity Index Measures (**SSIM)** index is a single-scale approach. It is top down approach. It overcomes super-threshold problem as it does not rely on threshold values.

3. Information Theoretic Measures [10]:

The information theoretic approach attacks the problem of image quality assessment from the viewpoint of information communication and sharing.one important aspect of information theoretic measures is the notation of "information fidelity" as opposed to "signal fidelity". Information fidelity criteria attempt to relate visual quality to the amount of information that is shared between the images being compared. Two information theoretic measures are: the Visual Information Fidelity (**VIF**) and the Reduced Reference Entropic Difference index (**RRED**).

B. Univariate IQ Measures (No-Reference)

A Univariate measure uses a single image. In this input images are only used. The Univariate IQM are classified into three, they are:

1. Distortion-Specific Approaches [11]:

Distortion specific means that the algorithms can assess the quality of an image under the assumption that the image is affected by distortion X, where X could be JPEG compression, blur and so on. It relay on visual quality loss by specific distortion. Two distortion specific approaches used are: JPEG Quality Index (**JQI**), High Low Frequency Index (**HLFI**).

2. Training-Based Approaches [12]:

Here clean and distorted images are used to train the model. Then image quality features are extracted from the test image in order to compute the quality score. Training based approach used here is Blind Image Quality Index **(BIQI).**It identifies the likeliest distortion in the image and quantifies this distortion using an NSS-based approach.

3. Natural Scene Statistic Approaches:

Natural image quality evaluator **(NIQE)** is the natural scene statistic approach used in this work. Natural image quality evaluator is completely blind image quality analyzer, without training any human rated distorted images it only uses measurable deviations observed in natural images

IV. PROPOSED SECURITY SYSTEM

A general diagram of the security approach proposed in this work is shown in Fig 1.This method operates on a single image, it does not require any pre-processing steps (e.g., fingerprint segmentation, iris detection or face extraction) prior to the computation of the IQ features. The block diagram consist of Identification and Authentication phase. Identification phase consist of Input, Image quality measure (IQM) Extraction stage, Classification stage and output. Inthis approach the inputs given are images of fingerprint, iris and 2D face (image and video). The input is then given to the Image quality measure (IQM) Extraction phase. Function of this phase is the extraction of image quality measures from the input image & also it extract the image quality measures from the images available in the data set (real &fake images).In this phase Full-Reference image quality measures(FR-IQMs) and No-Reference image quality measures(NR-IQMs) are calculated. Input image and gaussian filtered input image are the two inputs used for calculating FR-IQMs, for calculating NR-IQMs only input image is needed. The image quality measures obtained from input image are called as test features & those obtained from data set images are called as train features. After the image quality measures has been extracted it is then given to the classification phase. In this phase the first the training of image quality measures obtain from the data set is performed using Artificial Neural Network (ANN), Linear

ISSN(Online) :2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

Discriminant Analysis (LDA) & Quadratic Discriminant Analysis QDA, after this training has been completed it compare the train features with the test features and give the output. The output are whether the input image is real or fake. After identification, if the input images are real then the authentication phase start. Input to the authentication phase is the video of 2D face used in identification phase. In this phase first Discrete cosine transform (DCT) is applied to the face, then the most important features are extracted from the face using Discrimination power analysis(DPA).Training of these features is performed by using Support Vector Machine (SVM) classifier. Output are whether the person accessing the system is an authorized one or not.

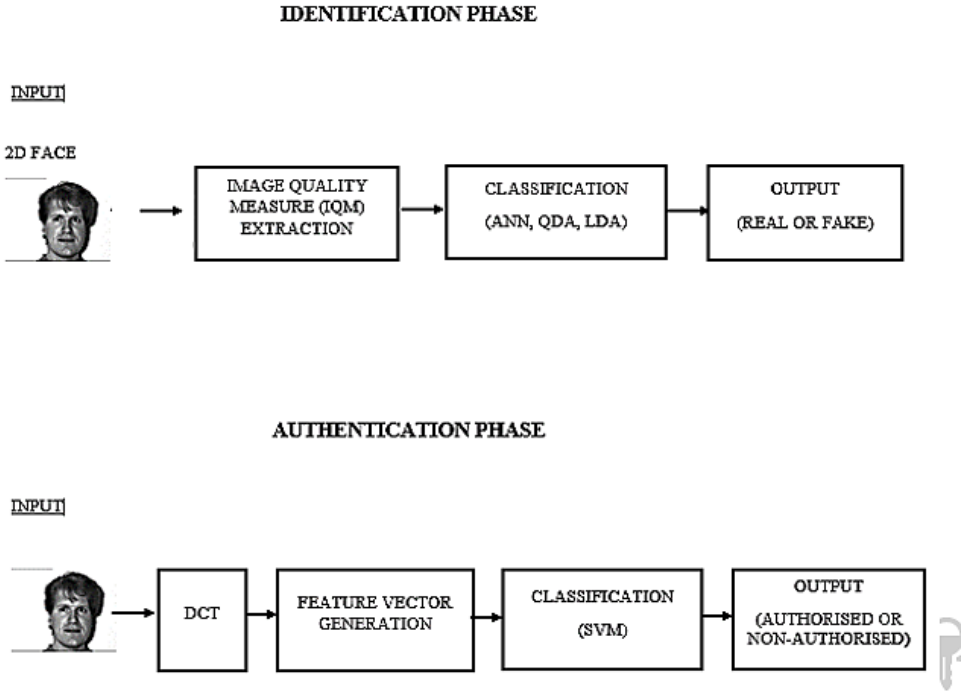

Fig 1.A general diagram of the security system proposed in this work is shown.

V. EXPERIMENTAL RESULTS

Publicly available databases are only used for experiment.29-dimensional simple classifier based on general IQMs are build. Results are calculated in terms of: the False Genuine Rate (FGR), which means number of fake images that are classified as real images and the False Fake Rate (FFR), which means the probability of real images being classified as fake images. Half Total Error Rate (HTER) is calculated as

$$HTER = (FGR + FFR)/2.$$

- *Identification Phase*

A. Results: 2D Face

The REPLAY-ATTACK DB [13] which is available from the IDIAP Research Institute is used for experiment. The database contains short videos captured during attacks. The videos were captured under two different conditions: i) Controlled, with artificial lighting and uniform background .ii) Adverse, with non-uniform background and natural illumination. Different types of attacks are considered are: print, webcam, highdef. Real and fake access are found in REPLAY-ATTACK DB.The classifier used for the two scenarios are Artificial Neural Network (ANN), Quadratic Discriminant Analysis (QDA), Linear Discriminant Analysis (LDA). The results obtained are presented in Table I. The table presents the Comparison between existing (first row) and proposed system (second and third row).

ISSN(Online) :2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

- *Authentication Phase*

In this phase the same replay attack database is used. The calculated values are shown in Table II.

TABLE I
RESULT OBTAINED(IN PERCENTAGE) FOR FACE:

	Results: 2D Face								
	REPLAY ATTACK DB								
	Print			*Webcam*			*Highdef*		
	FFR	**FGR**	**HTER**	**FFR**	**FGR**	**HTER**	**FFR**	**FGR**	**HTER**
IQA-based on QDA	10.3	8.2	9.25	4.2	3.4	3.8	14.6	12.4	13.5
IQA-based on ANN	**5.2**	**2.1**	**3.65**	**1.4**	**1**	**1.2**	**7.6**	**3.2**	**5.4**
IQA-based on LDA	9.2	6.4	7.8	2.4	1.6	2	10.2	8.6	9.4

TABLE II
RESULT OBTAINED IN AUTHENTICATION PHASE:

	Results: Face Recognition		
	Webcam		
	FFR	**FGR**	**HTER**
SVM	**2.2**	**1.1**	**1.65**

VI. CONCLUSION

Biometric systems are becoming increasingly popular both as standalone security systems and as added security largely because of one reason: convenience. People can easily forget a password, but will never forget to bring their finger, iris, face. The main problem that are faced by biometric security system are direct and indirect attack. The proposed system protect biometric security system from these types of attack and thus increase the security level .A novel liveness detection scheme for face based on quality related measures has been presented. Here training of database and classification are done using Artificial Neural Network (ANN), Linear Discriminant Analysis (LDA) and Quadratic Discriminant Analysis (QDA) .Among the three classifier ANN is more efficient and provide accurate result. Image Quality measures are extracted from real and fake images and using these measures vector the classification of image is done.

VII. ACKNOWLEDGMENT

I would like to acknowledge the sincere support provided by Mr. Vipin Thomas (Asst.Professor, ICET) and Mrs. Angel Mathew (Asst.Professor, ICET) in completion of the paper. Words alone cannot express the gratitude i have towards Mr. Jerin K Antony (Scientist/Engineer, QUEST) in teaching; guiding and helping me to accomplish this work successfully.

REFERENCES

[1] Javier Galbally, Sebastien Marcel and Julian Fierrez, "Image quality assessment for fake biometric detection: application to iris, fingerprint and face recognition." *IEEE Trans. Image process*, vol 23, no.2, Feb 2014.
[2] I. Avcibas, B. Sankur, and K. Sayood, "Statistical evaluation of image quality measures," *J. Electron. Imag*, vol. 11, no. 2, pp. 206–223, 2002.
[3] Q. Huynh-Thu and M. Ghanbari, "Scope of validity of PSNR in image/video quality assessment," *Electron. Lett.* vol. 44, no. 13,pp. 800–801, 2008.
[4] S. Yao, W. Lin, E. Ong, and Z. Lu, "Contrast signal-to-noise ratio for image quality assessment," in *Proc. IEEE ICIP*, Sep. 2005, pp. 397–400.

ISSN(Online) :2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2015

[5] A. M. Eskicioglu and P. S. Fisher, "Image quality measures and their performance," *IEEE Trans. Commun.*, vol. 43, no. 12, pp. 2959–2965,Dec. 1995.
[6] M. G. Martini, C. T. Hewage, and B. Villarini, "Image quality assessment based on edge preservation," *Signal Process. Image Commun*, vol. 27, no. 8, pp. 875–882, 2012.
[7] N. B. Nill and B. Bouzas, "Objective image quality measure derived from digital image power spectra," *Opt. Eng.*, vol. 31, no. 4, pp. 813–825, 1992.
[8] A. Liu, W. Lin, and M. Narwaria, "Image quality assessment based on gradient similarity," *IEEE Trans. Image Process.*, vol. 21, no. 4, pp. 1500–1511, Apr. 2012.
[9] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEETrans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004.
[10] H. R. Sheikh and A. C. Bovik, "Image information and visual quality," *IEEE Trans. Image Process.*, vol. 15, no. 2, pp. 430–444, Feb. 2006.
[11] Z. Wang, H. R. Sheikh, and A. C. Bovik, "No-reference perceptual quality assessment of JPEG compressed images," in *Proc. IEEE ICIP*,Sep. 2002, pp. 477–480.
[12] A. K. Moorthy and A. C. Bovik, "A two-step framework for constructing blind image quality indices," *IEEE Signal Process. Lett.* vol. 17, no. 5, pp. 513–516, May 2010.
[13] *LIVE* [Online], Available: http://live.ece.utexas.edu/research/Quality/index.htm.