International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 21 Issue 2 – APRIL 2016.

FORGERY DETECTION SCHEME BIO-SPOOF AND ANTI-SPOOFING

R.Saranya, Prof D Stalin Alex

M.E- Computer Science, CSI College Of Engineering
HOD, CSI College Of Engineering, B.Tech.Information Technology

saranyaramu3@gmail.com

***Abstract*--In recent years, facial biometric systems have received increased deployment in various applications such as surveillance, access control and forensic investigations. However, one of the limitations of face recognition system is the high possibility of the system being deceived or spoofed by non-real faces such as photograph, video clips or dummy faces. In order the Spoofing and anti-spoofing has become a prevalent topic in the biometrics community. This paper introduces novel and appealing techniques for fake biometric detection using liveness detection based on Image Quality assessment (IQA). The key idea of this approach is to present software based multi-biometric and multi-attack protection method that characterize real but not fake ones.**

Keywords- Image quality assessment, fake biometrics, liveness detection.

I. INTRODUCTION

Digital images are usually affected by a wide variety of distortions during acquisition and processing, which results in loss of visual quality. For that reason, image quality assessment (IQA) is applicable to image acquisition, watermarking, compression, transmission, restoration, Enhancement and reproduction. The target of IQA is to calculate the top of quality degradation and is thus used to evaluate/compare the performance of processing systems and/or optimize the choice of parameters in processing. Objective image quality assessment refers to automatically predict the quality of distorted images as would be perceived by an average human. If a naturalistic reference image is supplied against which the quality of the distorted image can be compare, the representation is called full reference (FR) [1].

Conversely, NR IQA models guess that only the distorted images [2], [3] whose quality is being assessed is available. In addition, Image quality assessment (IQA) is related to biometric system. In recent years, the increasing interest in the evaluation of biometric systems security has led to the creation of very diverse initiatives focused on this major field of research [4]: the publication of many research works revealing and evaluating different biometric vulnerabilities [5]. 2D face biometrics (that is identifying individuals based on their 2D face information) is still a major area of research. Wide range of viewpoints, occlusions, aging of subjects and complex outdoor lighting are challenges in face recognition. The vulnerabilities of face biometric systems to spoofing attacks are mostly overlooked.

There are many anti-spoofing techniques such as the use of multibiometrics or challenge-response methods, cancellable biometrics but the liveness detection techniques are the emerging field of research which uses different physiological properties to distinguish between real and fake character. IQA can be used for liveness detection to present a multi-biometric and multi-attack protection method.

II. FACIAL BIOMETRIC LIVENESS DETECTION SYSTEMARCHITECTURE:

The basic block diagram of a face liveness detection system is shown in Figure 1. To use an anti-spoofing system,a user is required to present the relevant biometrics traitto the sensor, which is in this case a camera.

The capturedfacial images is preprocessed into an acceptable form(e.g. such as through normalization and noise removaltechniques) as such distinct ‘live’ facial features can laterbe extracted at the feature extraction module.

Methods:

Liveness assessment methods represent a challenging problem as they have to satisfy certain demanding requirements:

(i) Non-invasive, the technique should not be harmful for the individual or require an excessive contact with the user.

(ii) User friendly, people should not be unwilling to use it.

(iii) Fast, results have to be produced in a very small interval.

(iv) Low cost, a wide use can’t be likely if the cost is excessively high.

(v) Performance, in calculate to have a good fake detection rate and should not degrade false rejection rate of the biometric system.

Liveness Detection Techniques

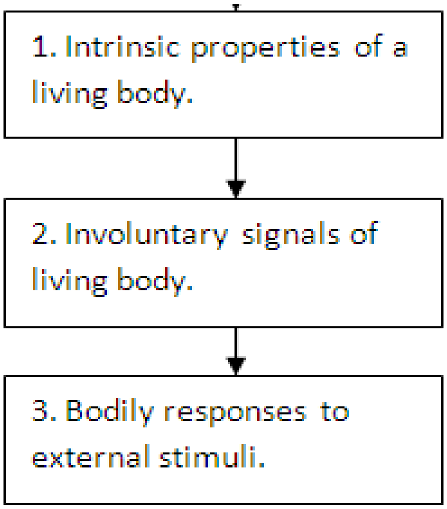

1. Intrinsic properties of a living body.
2. Involuntary signals of living body.
3. Bodily responses to external stimuli.

Fig. 1: Liveness Detection

Real-time liveness detection that uses an undirected conditional random field framework to model the eye-blinking that relaxes the independence assumption of generative modeling and state dependence limitations from hidden Markov modeling. Specific liveness detection measures vary from technology to technology, but all liveness detection technique fall in to three categories (Fig. 1) Although, a great amount of work has been done in the field of spoofing detection still there are big challenges to be faced in the detection of direct attacks.

III. IMAGE QUALITY MEASURES

Image quality measures can be Full Reference or No Reference which can be applied to fake detection. IQMs can be carried out for face detection according to four general criteria that are: Performance:-image quality approaches showing good performance for different applications are considered. Fig 2, complementarilypriority is given to IQMs based on complementary properties of the images (e.g., sharpness, entropy or structure).

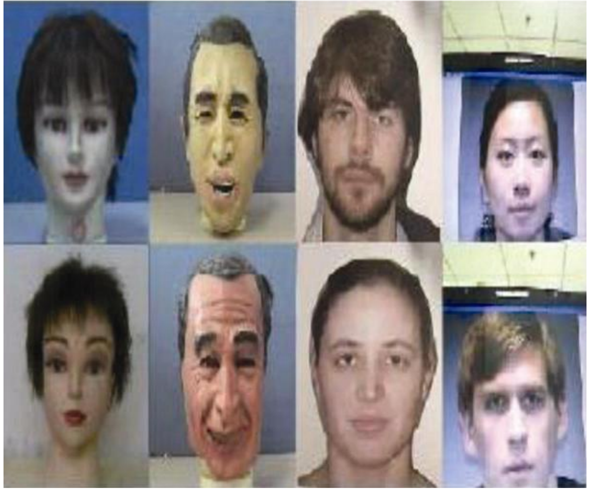


Fig2. Examples of fake facial specimens.

In fake detection Full-Reference IQ Measures consider the input sample as reference image. A. Full-Reference IQ Measures FR IQA method considers a clean undistorted reference image to estimate the quality of the test sample.

In fake detection problem FR IQ Measures consider the input sample as reference image.

1) FR-IQMs.
2) Error Sensitivity Measures.

These features compute the distortion between two images on the basis of their pixel wise differences:

- Peak Signal to Noise Ratio (PSNR),
- Mean Squared Error (MSE),
- Signal to Noise Ratio (SNR),
- Structural Content (SC),
- Maximum Difference (MD),
- Correlation-based measures.

The similarity between two digital images can also be computed in terms of the correlation function.
These features include

- Normalized CrossCorrelation(NXC),
- Mean Angle Similarity (MAS) and
- Mean Angle- Magnitude Similarity (MAMS).

The structural distortion of an image is strongly related with its edge degradation. Edge-related quality measures

- Total Edge Difference (TED) and
- Total Corner Difference (TCD).

IQ spectral-related features are:

- Spectral Magnitude Error (SME) and
- Spectral Phase Error (SPE).

IV. ANTI-SPOOFING MEASURES

Many types of anti-spoofing measures have been used tomake the system robust to spoofing attacks. Smart cards, passwords, enrolling several samples, supervising face
recognition process, multimodal biometric system andliveness detection.

V. LIVENESS DETECTION BASED ON IQA

Liveness detection using image quality assessment based on the “quality difference” hypothesis dictated as: “It is expected that a fake image captured in an attack attempt will have different quality than a real sample acquired in the normal operation scenario for which the sensor be designed.” Quality differences which are expected between real and fake samples may include: measure of sharpness, color and luminance levels, local artifacts, quantity of information found in both category of images, structural distortions or natural appearance. Fake biometric detection problem is a two-class classification problem where an input biometric sample has to be allotted to one of two classes: real or fake.

VI. COMPARITIVE STUDY

In image quality assessment many approaches need for entropy based classification of images.

- Single Stimulus Method:

This method is used for evaluating the IQA algorithms[4,5] i.e. here a set of stimulus is in use one at a time and include a reference image in that set and it is not informed to the observer.

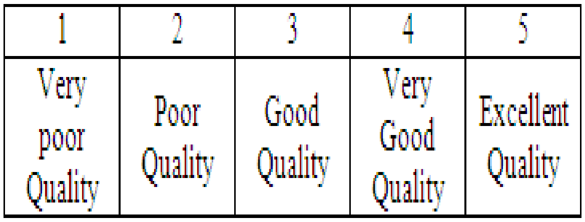
- Quality Ruler Method:

This method is composed of a series of reference images and whose scale is already known and they are closely spaced in quality, but distance a wide range of quality collectively.

- Mean Opinion Score:

Mean opinion score produce the accurate results with small number of scores. It is generated by averaging the results of a set of standard, subjective test and act as an indicator for the perceived image quality [6, 8].Score classes are shown in Table 1.

Table I
Mean Opinion Score Classes



1	2	3	4	5
Very poor Quality	Poor Quality	Good Quality	Very Good Quality	Excellent Quality

- Full Reference Method:

In full reference IQA the reference image is want to be known and predict the visual quality by comparing the distorted signal against the reference image Mean Square error (MSE) and peak signal to noise ratio (PSNR) are mostly used.

- No Reference Method:

The no reference approaches still lags advances in the full reference methods. Many of the blind image quality assessment are distortion specific.

VII. CONCLUSION

Spoofing and anti-spoofing has become a prevalent topic in the biometrics community. It is possible to combat spoofing attacks with liveness detection testing but all of these countermeasures come at certain price often affecting user convenience, hardware prices. Using IQA software based multi-biometric and multi-attack protection method is presented.

REFERENCES

[1] H. R. Sheikh, M. F. Sabir, and A. C. Bovik, "A statistical evaluationof recent full reference image quality assessment algorithms," IEEETrans. Image Process., vol. 15, no. 11, pp. 3440–3451, 2006.

[2] Mittal, A. K. Moorthy, and A. C. Bovik, "No-reference imagequality assessment in the spatial domain," IEEE Trans. Image Process.,2012, to be published.

[3] P. Ye and D. Doermann, "No-reference image qualityassessment usingvisual codebook," in IEEE Int. Conf. Image Process., 2011.

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

[5] J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega- Garcia, "Onthe vulnerability of face verification systems to hill-climbing attacks,"PatternRecognit., vol. 43, no. 3, pp. 1027–1038, 2010.

[6] J. Galbally, R. Cappelli, A. Lumini, G. G. de Rivera, D. Maltoni, J. Fierrez, et al., "An evaluation of direct and indirect attacks using fake fingers generated from ISO templates," Pattern Recognit. Lett., vol. 31,no. 8, pp. 725–732, 2010.

[7] Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: A public database and a baseline," in Proc. IEEE IJCB, Oct. 2011, pp. 1–7.J. Hennebert, R. Loeffel, A. Humm, and R. Ingold, "A new forgery scenario based on regaining dynamics of signature," in Proc. IAPR ICB,vol. Springer LNCS-4642. 2007, pp. 366–375.

[8] Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Evaluation of serial and parallel multibiometric systems under spoofing attacks," in Proc. IEEE 5th Int. Conf. BTAS, Sep. 2012, pp. 283–288.