Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition

P.KANIMOZHI [#1],

[#1] PG Scholar, Department of MCA,
College, V.S.B Engineering College, Karur, Tamilnadu, India,

Abstract

This paper is based on image processing to ensure the actual presence of a real legitimate trait in contrast to a fake self-manufactured synthetic or reconstructed sample is a significant problem in biometric authentication, which requires the development of new and efficient protection measures. This paper, presents novel software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. The objective of the proposed system is to enhance the security of biometric recognition frameworks, by adding live assessment in a fast. The proposed approach presents a very low degree of complexity, which makes it suitable for real-time applications, using 25 general image quality features extracted from one image besides other anti-spoofing approaches such as the use of multibiometrics or challenge-response methods, special attention has been paid byresearchers and industry to the liveness dtionetec techniques.

I - INTRODUCTION

Expected quality differences between real and fake samples may include: degree of sharpness, color and luminance levels, local artefacts', amount of information found in both type of images (entropy), structural distortions or natural appearance. For example, iris images captured from a printed paper are more likely to be blurred or out of focus due to trembling; face images captured from a mobile device will probably be over- or under-exposed; and it is not rare that fingerprint images captured from a gummy finger present local acquisition artefacts' such as spots and patches. Furthermore, in an eventual attack in which a synthetically produced image is directly injected to the communication channel before the feature extractor, this fake sample will most likely lack some of the properties found in natural images.

II-SYSTEM ANALYSIS

EXISTING SYSTEM

In order to generate totally unbiased results, there is no overlap between both sets (i.e., samples corresponding to each user are just included in the train or the test set). The same QDA classifier already considered in the iris related experiments is used here.

Fingerprints-Spoofing: The DB was captured in the framework of the Fingerprint Liveness Detection Competition and it is distributed through the site of the competition. It comprises three datasets of real and fake fingerprints captured each of them with a different flat optical sensor.

The use of image quality assessment for liveness detection is motivated by the assumption that: "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 was designed."

Disadvantages

- ✓ In the reorganization of Fake detection can be done.
- ✓ Finger print has unrealistic and misintegrate of image is unusual.

PROPOSED SYSTEM

This paper, valuates the "multi-biometric" dimension of the protection method. For this purpose three of the most extended image-based biometric modalities have been considered.The technique used in proposed system is Natural Image Quality Evaluator (NIQE).

This approach is followed by the Natural Image Quality Evaluator (NIQE) used in the present work.The NIQE is a completely blind image quality analyzer based on the construction of a quality aware collection.

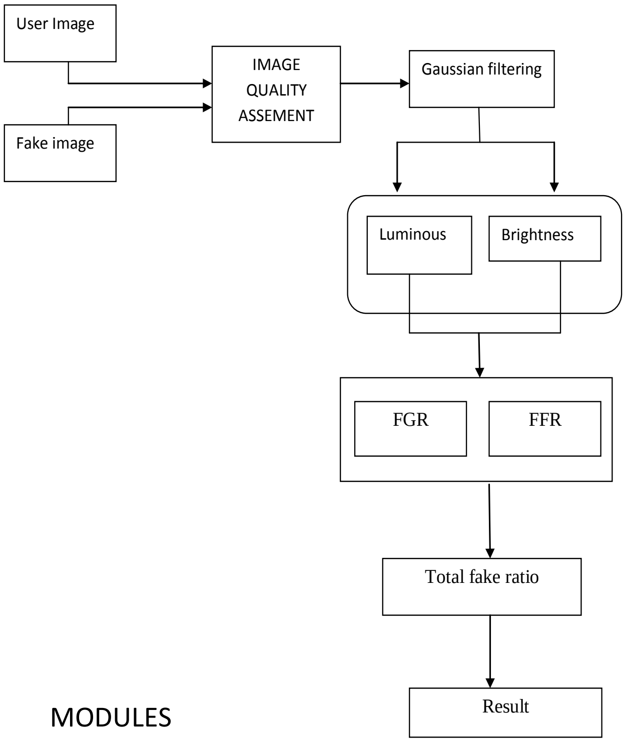
Advantages

- ➢ Time interval is more efficient in JQI and HLFI
- ➢ Model trained on clean images and on images affected by this Particular distortion.

III-SYSTEM TECHNIQUES

NIQE (natural image quality evaluator):

Natural Image Quality Evaluator (NIQE) blind image quality assessment (IQA) is a completely blind image quality analyzer that only makes use of measurable deviations from statistical regularities observed in natural images, without training on human-rated distorted images, and, indeed without any exposure to distorted images. However, all current state-of-the-art general purpose no reference (NR) IQA algorithms require knowledge about anticipated distortions in the form of training examples and corresponding human opinion scores.



MODULES

- IMAGE PREPROCESSING
- FULL REFERENCE IMAGE QUALITY ASSESSMENT
- NO REFERENCE IMAGE QUALITY ASSESSMENT
- FINAL PARAMETERIZATION
- CLASSIFICATION

MODULE DESCRIPTION

IMAGE PREPROCESSING

Pre-processing steps (e.g., fingerprint segmentation, iris detection or face extraction) prior to the computation of the IQ features. This characteristic minimizes its computational load. Once the feature vector has been generated the sample is classified as real (generated by a genuine trait) or fake (synthetically produced), using some simple classifiers. In particular, for our experiments we have considered standard implementations in Mat lab of the Linear Discriminate Analysis.

FULL REFERENCE IMAGE QUALITY ASSESSMENT

Full-reference (FR) IQA methods rely on the availability of a clean undistorted reference image to estimate the quality of the test sample. In the problem of fake detection addressed in this work such a reference image is unknown, as the detection system only has access to the input sample. In order to circumvent this limitation, the same strategy already successfully used for image manipulation detection and for steganalysis is implemented. The input grey-scale image I is filtered with a low-pass Gaussian kernel in order to generate a smoothed version ˆI . Then, the quality between both images (I and ˆI) is computed according to the corresponding full-reference IQA metric this approach assumes that the loss of quality produced by Gaussian filtering differs between real and fake biometric samples.

NO REFERENCE IMAGE QUALITY ASSESSMENT

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.

FINAL PARAMETIRIZATION

Expected quality differences between real and fake samples may include: degree of sharpness, color and luminance levels, local artifacts, amount of information found in both type of images (entropy), structural distortions or natural appearance. For example, iris images captured from a printed paper are more likely to be blurred or out of focus due to trembling.

CLASSIFICATION

For the iris modality the protection method is tested under two different attack scenarios, namely: *i* spoofing attack and *i* attack with synthetic samples. For each of the scenarios a specific pair of real-fake databases is used. Databases are divided into totally independent (in terms of users): train set, used to train the classifier; and test set, used to evaluate the performance of the proposed protection method

IV-FUTURE ENHANCEMENT

The present research also opens new possibilities for future work, including:

i) extension of the considered 25-feature set with new image quality measures;*ii*) further evaluation on other image-based modalities (e.g., palm print, hand geometry, vein); *iii*) inclusion of temporal information for those cases in which it is available.

V-CONCLUSION

Several conclusions may be extracted from the evaluation results presented in the experimental sections of the article: *i*) The proposed method is able to consistently perform at a high level for different biometric traits ("multi-biometric"); *i i*) The proposed method is able to adapt to different types of attacks providing for all of them a high level of protection ("multi-attack"); *i i i*) The proposed method is able to generalize well to different databases, acquisition conditions and attack scenarios; *iv*) The error rates achieved by the proposed protection scheme are in many cases lower than those reported by other trait-specific state-of-the-art anti-spoofing systems which have been tested in the framework of different independent competitions; and *v*) in addition to its very competitive performance, and to its "multi-biometric" and "multi-attack" characteristics, the proposed method presents some other very attractive features such as: it is simple, fast, non-intrusive, user-friendly and cheap, all of them very desirable propertiesin a practical protection system.

VI-REFERENCES

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

[2] T. Matsumoto, "Artificial irises: Importance of vulnerability analysis," in *Proc. AWB*, 2004.

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

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

[5] 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.

fingerprint liveness detection competition—LivDet 2009," in *Proc. IAPR ICIAP*, Springer LNCS-5716. 2009, pp. 12–23.

VII-AUTHOR DETAILS

Ms.P.kanimozhi Received the Bachelor Degree in Computer Application from PGP College of Arts and Science., Nammakal in 2013. Currently I am doing Master of Computer Application at V.S.B Engineering College, Karur under Anna University of Chennai. My research interests include Image Processing and

I participated in several workshops and presented papers.