Image Quality Assessment for Fake Biometric Detection

Romy Wadhwa[1]
[1]M. Tech Scholar
[1]Department of Computer Science and Applications
[1]Kurukshetra University, Kurukshetra Haryana, India

Abstract— Biometric system plays an important role in authentication but these systems are vulnerable to several attacks. 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, biometrics, 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. Therefore, image quality assessment (IQA) is applicable to image acquisition, watermarking, compression, transmission, restoration, enhancement, and reproduction.

The goal of IQA is to calculate the extent 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 compared, the model is called full reference (FR) [1]. Conversely,

NR IQA models assume that only the distorted images [2], [3] whose quality is being assessed is available.

In addition, Image quality assessment (IQA) are 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. While there is a significant number of works addressing these issues, the vulnerabilities of face biometric systems to spoofing attacks are mostly overlooked.

Among the different threats analyzed, the direct or spoofing attacks have motivated the biometric community to study the vulnerabilities against this type of fraudulent actions in traits such as the fingerprint [6],the face [7] and multimodal approaches [8].

When spoofed, a biometric recognition system is bypassed by presenting a copy of the biometric evidence of a valid user. Spoofing attack is the action of outwitting a biometric. Sensor by presenting a counterfeit biometric evidence of a valid user [9].

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 use different physiological properties to distinguish between real and fake traits.

IQA can be used for liveness detection to present a multi-biometric and multi-attack protection method.

II. LIVENESS DETECTION METHODS

Liveness assessment methods represent a challenging problem as they have to satisfy certain demanding requirements [10]: *(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 addition to having a good fake detection rate and should not degrade false rejection rate of the biometric system.

Liveness detection techniques can be usually categorized into one of two groups (see Fig. 1):

Hardware-based techniques, in this case some specific device are added to the sensor in order to detect particular properties such as fingerprint sweat, blood pressure, or specific reflection properties of the eye of a living trait.

Software-based techniques, in this the sample has been acquired with a standard sensor and features are used to distinguish between real and fake traits.

As a comparison, hardware-based schemes usually present a higher fake detection rate, While software-based techniques are in general less expensive (as no extra device is needed) and their implementation is transparent to the user because it is less intrusive. [11], [12].

Liveness detection is to determine if the biometrics data is being captured from a legitimate , live user who is physically present at the point of acquisition. [13] Explore a technique to estimate liveness based on a short sequence of images using a binary detector that calculates the trajectories of specific parts of the face given to the input sensor using a simplified optical flow analysis followed by heuristic classifier. Introduce a method for fusing scores based on concurrently, the 3-D face motion scheme introduced on the previous work and liveness properties such as eye-blinks or mouth movements.

Real-time liveness detection that uses an undirected conditional random field framework to model the eye-blinking that relaxes the independence assumption of generative modelling and state dependence limitations from hidden Markov modelling.

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.

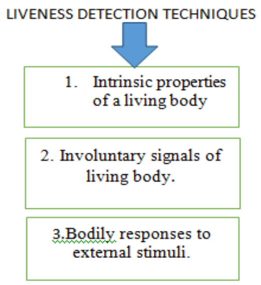
LIVENESS DETECTION TECHNIQUES
1. Intrinsic properties of a living body
2. Involuntary signals of living body.
3.Bodily responses to external stimuli.

Fig. 1: Liveness Detection

One of the shortcomings of anti- spoofing techniques is their lack of generality. If testing conditions or evaluation database is changed then their error rates also get changed. Most of the techniques are based on the certain specific properties of a given trait.

III. Image Quality Measures: Fake Detection

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.

Complementarity:- priority is given to IQMs based on complementary properties of the images(e.g., sharpness, entropy or structure).

Complexity :- Low complexity features are preferred over those which require a high computational load.

Speed:- IQMs having low feature extraction time, which has a very big impact in the overall speed of the fake detection algorithm.

In fake detection Full-Reference [1] IQ Measures consider the input sample as reference image.

A. Full-Reference IQ Measures

FR IQA method consider 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:

Error Sensitivity Measures: Traditional image quality assessment approaches calculates the errors (i.e., signal differences) between the distorted and the reference images, and quantify these errors in a way that simulates human visual error sensitivity features.

Pixel Difference measures [14], [15]. These features compute the distortion between two images on the basis of their pixel wise differences such as Mean Squared Error (MSE), Peak Signal to Noise Ratio (PSNR), Signal to Noise Ratio (SNR), Structural Content (SC), Maximum Difference (MD).

Correlation-based measures[14], [15]. The similarity between two digital images can also be computed in terms of the correlation function. These features include Normalized Cross-Correlation(NXC), Mean Angle Similarity (MAS) and Mean Angle- Magnitude Similarity (MAMS).

Edge-based measures. The structural distortion of an image is strongly related with its edge degradation. Edge-related quality measures are Total Edge Difference (TED) and Total Corner Difference (TCD)

Spectral distance measures. IQ spectral-related features are: the Spectral Magnitude Error (SME) and the Spectral Phase Error (SPE)

Gradient-based measures. Gradients convey important visual information which can be of great use for quality assessment. Two simple gradient-based features are included in the biometric protection system proposed in the present article: Gradient Magnitude Error (GME) and Gradient Phase Error (GPE).

2) FR-IQMs:

Nonstructural Distortions in an image that come from variations in lighting,(contrast or brightness changes) should be treated differently from structural ones. The Structural Similarity Index Measure (SSIM), has the simplest formulation and has gained widespread popularity in a broad range of practical applications [16], [17].

3) FR-IQMs:

Information Theoretic Measures: Under this general framework, image quality measures based on information fidelity exploit the relationship between statistical image information and visual quality. The Visual Information Fidelity (VIF) [18] and the Reduced Reference Entropic Difference index (RRED) [19] are based on the information theoretic perspective of IQA but each of them take either a global or a local approximation to the problem.

B. No-Reference IQ Measures

NR-IQA methods generally estimate the quality of the test image according to some pre-trained statistical models.

Distortion-specific methodologies. These techniques rely on previously acquired knowledge about the type of visual quality loss caused by a specific distortion. The final quality measure is computed according to a model trained on clean images and on images affected by this particular distortion. The JPEG Quality Index (JQI), which evaluates the quality in images affected by the usual block artifacts found in many compression algorithms running at low bit rates such as the JPEG [20].Training-based approaches. In this type of techniques a model is trained using clean and distorted images s affected by different types of distortions. Then, the quality score is computed based on a number of features extracted from the test image and related to the general model [21]

Natural Scene Statistic approaches. These blind IQA techniques use *a priori* knowledge taken from natural scene distortion-free images to train the initial model (i.e., no distorted images are used) based on the hypothesis that undistorted images of the natural world present certain *regular* properties which fall within a certain subspace of all possible images.

IV. Liveness Detection based on Image Quality Assessment

Liveness detection using image quality assessment [22] 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 was designed.”

Quality differences which are expected 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, 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.

The process’s key point is to build an appropriate classifier which gives the probability of the image “realism” based on the extracted set of discriminant features.

This protection approach needs only one input: the biometric sample to be classified as real or fake (i.e., the same image used for biometric recognition purposes). There is no need of preprocessing as the method operates on the whole image without searching for any trait-specific properties, prior to the computation of the IQ features and reduces its computational load. Once the feature vector is known the sample can be classified as real (generated by a genuine trait) or fake (synthetically produced), using some simple classifiers.

V. WHY TO GO FOR IQA FEATURES?

Use of IQA features for liveness detection is supported by three factors.

- In the forensic field, image manipulation detection [23], [24] and steganalysis [25], [26] image quality has been successfully implemented.
- In the previous research works liveness detection techniques are trait specific but using IQA multi-biometric liveness detection techniques are presented.
- Different metrics and methods designed for IQA intend to estimate in an objective and reliable way the perceived appearance of images by humans.

VI. Conclusions

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 a 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 quality assessment usingvisual codebook,” in *IEEE Int. Conf. Image Process.*, 2011.

[4] 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.

[5] J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia, “Onthe vulnerability of face verification systems to hill-climbing attacks,”*Pattern Recognit.*, 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.

[9] K. Nixon, V. Aimale, and R. K. Rowe, “*Spoof detection schemes*,” Handbook of Biometrics, 2008.

[10] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. New York, NY, USA: Springer-Verlag, 2009.

[11] R. Cappelli, D. Maio, A. Lumini, and D. Maltoni, “Fingerprint image reconstruction from standard templates,” *IEEE Trans. Pattern Anal.Mach. Intell.*, vol. 29, no. 9, pp. 1489–1503, Sep. 2007.

[12] S. Shah and A. Ross, “Generating synthetic irises by feature agglomeration,”in *Proc. IEEE ICIP*, Oct. 2006, pp. 317–320.

[13] K. Kollreider, H. Fronthaler, and J. Bigun, "Nonintrusive liveness detection by face images," Image and Vision Computing, vol. 27, no. 3, pp. 233-244, 2009.

[14] Avcibas, B. Sankur, and K. Sayood, “Statistical evaluation of image quality measures,” J. Electron. Imag., vol. 11, no. 2, pp. 206–223, 2002.

[15] M. Eskicioglu and P. S. Fisher, “Image quality measures and their performance,” IEEE Trans. Commun., vol. 43, no. 12, pp. 2959–2965, Dec. 1995.

[16] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, “Image quality assessment: From error visibility to structural similarity,” IEEE Trans. Image Process., vol. 13, no. 4, pp. 600–612, Apr. 2004.

[17] D. Brunet, E. R. Vrscay, and Z. Wang, “On the mathematical properties of the structural similarity index,” IEEE Trans. Image Process., vol. 21, no. 4, pp. 1488–1499, Apr. 2012.

[18] 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.

[19] R. Soundararajan and A. C. Bovik, “RRED indices: Reduced reference entropic differencing for image quality assessment,” *IEEE Trans. Image Process.*, vol. 21, no. 2, pp. 517–526, Feb. 2012.

[20] 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.

[21] 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.

[22] Javier Galbally, Sébastien Marcel, *Member, IEEE*, and Julian Fierrez “Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, And Face Recognition” IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 23, NO. 2, FEBRUARY 2014.

[23] S. Bayram, I. Avcibas, B. Sankur, and N. Memon, “Image manipulation detection,” J. Electron. Imag., vol. 15, no. 4, pp. 041102-1–041102-17, 2006.

[24] M. C. Stamm and K. J. R. Liu, “Forensic detection of image manipulation using statistical intrinsic fingerprints,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 492–496, Sep. 2010.

[25] Avcibas, N. Memon, and B. Sankur, “Steganalysis using image quality metrics,” IEEE Trans. Image Process., vol. 12, no. 2, pp. 221–229, Feb. 2003.

[26] S. Lyu and H. Farid, “Steganalysis using higher-order image statistics,” IEEE Trans. Inf. Forensics Security, vol. 1, no. 1, pp. 111–119, Mar. 2006.