ISSN No. 0976-5697

Volume 6, No. 1, Jan-Feb 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Detection of Fake Biometric using Liveness Assessment Method

Aditya S. Ambadkar, Prof. Ravi V.Mante, Dr. PrashantN.Chatur
M. Tech. Scholar, Assistant Professor, Head of Department
Government College of Engineering,Amravati, India
ambadkar.aditya@gmail.com, mante.ravi@gmail.com, chatur.prashant@gmail.com

Abstract: The major problem in biometric is to deal with the fake reconstructed sample or self-manufactured synthetic samples. Many biometric system doesn't have that much capability to detect such artificially created input as a fake input. To rectify such problem for detection of fake biometric we use liveness assessment methods using various image quality assessment measures which plays very important role to detect such fake samples and stop them their itself. The Liveness assessment methods using image quality assessment measures is shown to be a good approach for detecting such fake samples in various biometric system like face samples, iris samples, fingerprints samples. Thus, providing a single method multi-detection platform.

Keywords: fake biometric detection, Livenessassessment method, Image quality assessment, face recognition, iris recognition, fingerprint recognition

I. INTRODUCTION

Identity theft is a concern that prevents the mainstream adoption of biometrics as de facto form of identification in commercial systems [1]. Contrary to password-protected systems, our biometric information is widely available and extremely easy to sample.Biometrics recognition addresses the problem of identifying or verifying a person by comparing his biometrics identity with biometrics images stored in the database. Biometric system is nothing but an authentication system that matches the templates generated by the system, with the actual input factors or the images. If the templates are matched then authentication is given otherwise authentication is not given. There is a plenty number of biometric system available in the market, some of them are face recognition system, retina checking system, sound authentication system, heart sound detection system, fingerprints recognition, palm recognition etc. Many major law enforcement departments embraced the idea of first "booking" the Biometrics identity of criminals and storing it in a database (actually, a card file). Later, the leftover (typically, fragmentary) fingerprints or other Biometrics identity (commonly referred to as latents) at the scene of crime could be "lifted" and matched with fingerprints in the database to determine the identity of the criminals.It suffices a small search on the internet to unveil prelabelled samples from users at specialized websites such as Flickr or Facebook. Images can also be easily captured at distance without previous consent. Users cannot trust that these samples will not be dishonestly used to assume their identity before Face biometric recognition systems.

Fingerprint-based biometric systems are rapidly gaining acceptance as one of the most effective technologies to authenticate users in a wide range of applications: from PC logon to physical access control and from border crossing to voter'sauthentication.A typical fingerprint verification system involves two stages: during enrollment, the user's fingerprint is acquired and its distinctive features are extracted and stored as a template; and during verification, a new fingerprint is acquired and compared to the stored template to verify the user's claimed identity.

Gait biometrics aims to recognize people from their way of walking. It is a relatively new biometric modality and has a precious advantage over other modalities, such as iris and voice, in that it can be easily captured from a distance. This makes it an attractive option in video surveillance applications. Gait also works in a non-contact and non-invasive manner.

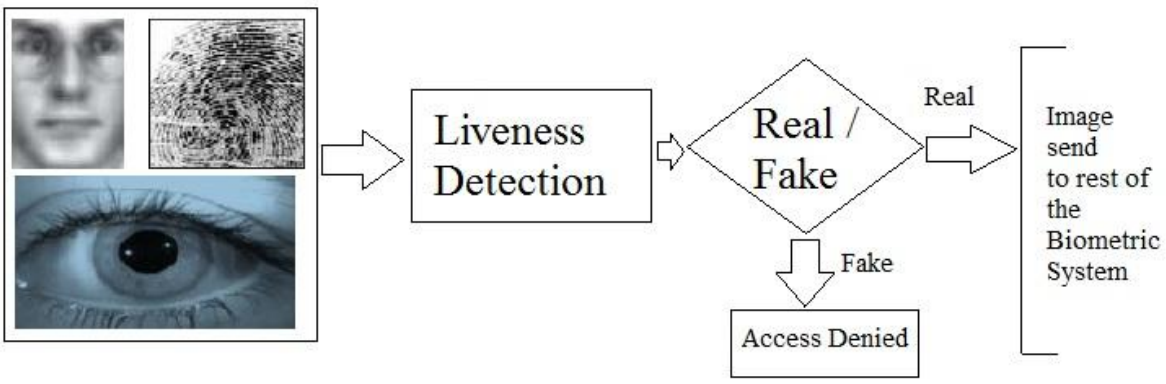

Figure 1. General Process of Detecting Fake Biometric Image

II. LIVENESS DETECTION FOR FACE AND FINGERPRINT RECOGNITION

Despite the fact that solutions exist for spoof prevention using multi-modal techniques [2][3][4][5], it is our belief that research for counter-measures solely based on unimodal 2-D imagery has not yet reached a matured state. There seems to exist no consensus on best practices and techniques to be deployed on attack detection using non-intrusive methods. The number of publications on the subject is small. A missing key to this puzzle is the lack of standard databases to test counter-measures, followed by a set of protocols to evaluate performance and allow for objective comparison. Face recognition systems are known to respond weakly to attacks for a long time and are easily spoofed using a simple photograph of the enrolled person's face, which may be displayed in hard-copy or on a screen. In this short survey, we focus on methods that present counter-measures to such kind of attacks.

The distinctive features used by most fingerprint-based systems are the so- called minutiae, which are local characteristics of the pattern that are stable and robust to fingerprint impression conditions [8]. With the aim of achieving interoperability among different fingerprint-based recognition systems [9], an international standard for minutiae template representation has been recently defined as ISO/IEC 19794-2 [10], which is a minor modification of the earlier ANSI-INCITS 378-2004 [7].

A. Methodology:

Anti-spoofing for 2-D face recognition systems can be coarsely classified in 3 categories with respect to the clues used for attack detection: motion, texture analysis and liveness detection. In motion analysis one is interested in detecting clues generated when two dimensional counterfeits are presented to the system input camera, for example photos or video clips. Planar objects will move significantly differently from real human faces which are 3-D objects, in many cases and such deformation patterns can be used for spoof detection.Texture analysis counter-measures take advantage of texture patterns that may look unnatural when exploring the input image data.

Liveness based technique evaluate on a short sequence of images using a binary detector that evaluates the trajectories of selected parts of the face presented to the input sensor using a simplified optical flow analysis followed by an heuristic classifier.Liveness detection tries to capture signs of life from the user images by analyzing spontaneous movements that cannot be detected in photographs, such as eye- blinks.Fingerprint matching based on minutiae features is a well-studied problem.

These technique often makes assumption that the two fingerprints to be matched are of approximately same size. However, this assumption is not valid in general. For example, matching of partial fingerprints will not bind by this assumption. Even two fingerprints captured using two different scanners may have different size. Matching of two latent fingerprints may face the same problem. Moreover, two images with different orientation may fail to match in minutiae based techniques due to relative change in their minutiae locations.

Liveness detection in Fingerprint matching tries to capture signs of life from the user images by considering different factors from finger like sweat on finger, ECG etc.

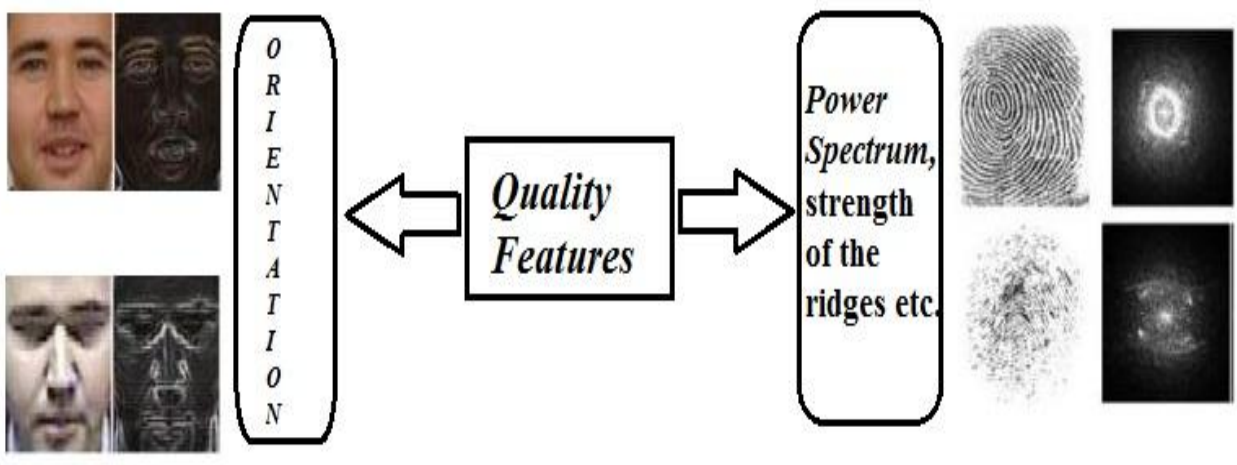

Figure 2. Image Quality Features for Face and Fingerprints Images

III. LIVENESS DETECTION FOR IRIS RECOGNITION

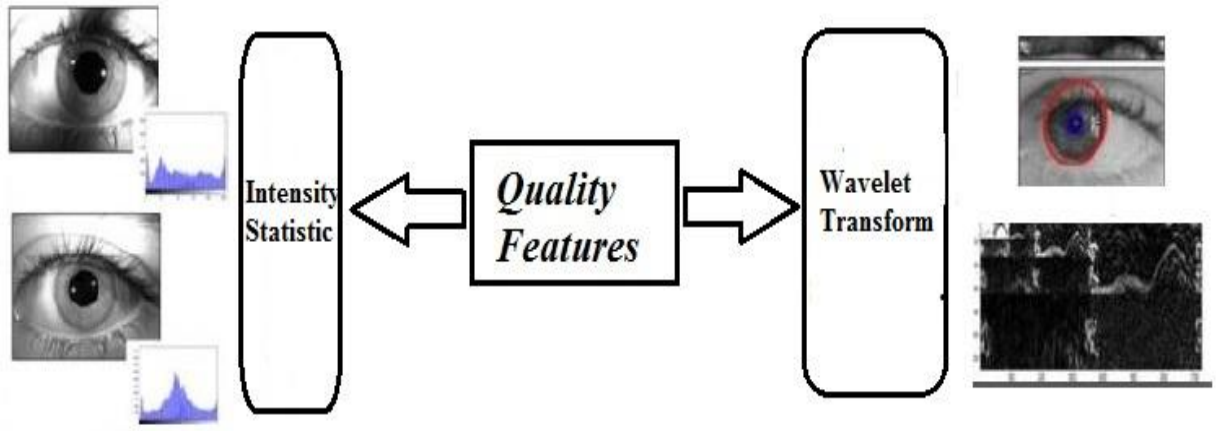

Figure 3. Image Quality Features for Iris image

Iris recognition is an automated method of biometric authentication that uses the mathematical pattern recognition techniques on images of the irises of an individual's eyes, whose complex random patterns are unique and can be seen from some distance. A good biometric is characterized by the use of a feature that is; highly unique – so that the chance of any two people having the same characteristic will be minimal, stable – so that the feature does not change over time, and be easily captured – in order to provide convenience to the user, and prevent misrepresentation of the feature.

A. Methodology:

The use of image quality assessment for liveness detection is motivated by the assumption that: [6] "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."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; face images captured from a mobile device will probably be over- or under-exposed; and it is not rare that fingerprintimages captured from a gummy finger present local acquisition artifacts such as spots and patches. Furthermore, in an eventual attack in which a synthetically produced image is directlyinjected to the communication channel before the feature extractor, this fake sample will most likely lack some of the properties found in natural images.

The problem of fake biometric detection can be seen as a two-class classification problem where an input biometric sample has to be assigned to one of two classes: real or fake. The key point of the process is to find a set of discriminant features which permits to build an appropriate classifier which gives the probability of the image "realism" given the extracted set of features. In the present work we propose a novel parameterization using different general image quality measures.

IV. FLOW OF DATA

The fake biometric detection can be seen as a two-class classification problem in which an input biometric sample is to be classify into one of two classes: real or fake. Here we have to find a set of discriminant features which permits to build an appropriate classifier which gives the probability of the image "realism" given the extracted set of features. To achieve this we can use general image quality measures. In image quality measure we make use of full reference image quality measure and no-reference image quality measure. By using this image quality measure [6] we find quality feature of image and then used to decide whether it is real or fake.A dataflow diagram is shown in fig. 4.

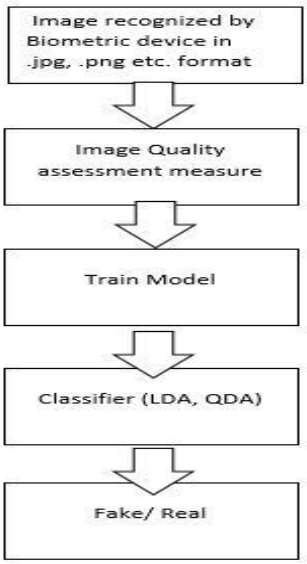

Figure 4. Flow of data for checking fake samples

In image quality measure we use full reference image quality measure like Mean Squared Error, Peak Signal to Noise Ratio, Signal to Noise Ratio, Structural Content, Maximum Difference, Average Difference etc. In no-reference image quality measure we are using JPEG Quality Index, The High-Low Frequency Index, Blind Image Quality Index etc.

The full reference image quality measure has following measure-

Mean Square Error Method

$$MSE(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j} - \hat{I}_{i,j})^2 \text{ [6]}$$

Peak Signal to Noise Ratio Method

$$PSNR(I,\hat{I}) = 10\log\left(\frac{\max(I^2)}{MSE(I,\hat{I})}\right) \text{[6]}$$

Signal to Noise Ratio Method

$$SNR(I,\hat{I}) = 10\log\left(\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j})^2}{N.M.MSE(I,\hat{I})}\right) \text{[6]}$$

Normalised Absolute Error Method

$$NAE(I,\hat{I}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}|I_{i,j} - \hat{I}_{i,j}|}{\sum_{i=1}^{N}\sum_{j=1}^{M}|I_{i,j}|} \text{[6]}$$

As shown in Fig. the input grey-scale image **I** (of size $N \times M$) is filtered with a low-pass Gaussian kernel in order to generate a smoothed version Then, the quality between both images (**I** and **Î**) is computed according to the corresponding full-reference IQA metric.

The No reference image quality measure has following measure-

High Low Frequency index using SME Method

$$SME(I) = \frac{\sum_{i=1}^{i_l}\sum_{j=1}^{j_l}|F_{i,j}| - \sum_{i=i_{h+1}}^{N}\sum_{j=j_{h+1}}^{M}|F_{i,j}|}{\sum_{i=1}^{N}\sum_{j=1}^{M}|F_{i,j}|} \text{[6]}$$

In order to keep its generality and simplicity, the system needs only one input: the biometric sample to be classified as real or fake (i.e., the same image acquired for biometric recognition purposes). Furthermore, as the method operates on the whole image without searching for any trait-specific properties, it does not require any preprocessing steps e.g., fingerprint segmentation, iris detection or face extraction etc. prior to the computation of the IQ features. Thischaracteristic 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. Here we are going to use Linear Discriminant Analysis (LDA) and Quadratic Discriminant Analysis (QDA) classifiers.

V. PROPOSED WORK

To perform liveness assessment using image quality assessment method we need to consider all kind of image details like distortion produced in image, varieties of viewing condition for image, loss of visible feature, the amplification of invisible features, suprathreshold distortions, near threshold distortions, contrast information, structural similarity etc. in grayscale as well as for chrominance image. To deal with such an image quality feature we need to apply some quality measures which should able to extract such features. By using this features we are going to create a classifier which is going to classify the input image sample to one of the class i.e. fake or real.

A. Multi-scale Structural Similarity Index (MS-SSIM)[11]:

Multi-scale structural similarity methodsupplies more flexibility than single-scale methods in incorporating the variations of viewing conditions. It is an image synthesis method to calibrate the parameters that define the relative importance of different scales. It apply the SSIM indexing algorithm for image quality assessment using approach of sliding window. The window moves pixel-by-pixel across the whole image space. In each step, SSIM index iscalculated within the local window. If one of the image being compared is considered to have perfect quality, then the resulting SSIM index map can be viewed as the quality map of the other (distorted) image. Instead of using a square window of any size, a smooth windowing approach is used for local statistics to avoid "blocking artifacts" in the quality map. Finally, a mean SSIM index of the quality map is used to evaluate the overall image quality.

Takingthe reference and distorted image signals as the input, the systemiteratively applies a low-pass filter and downsamples the filteredimage by a factor of 2. We index the original image as Scale 1,and the highest scale as Scale M, which is obtained after M-1iterations. At the j-th scale, the contrast comparison and the structure comparison are calculated and denoted as c_j(x,y) and s_j(x,y), respectively. The luminance comparison is computedonly at Scale M and is denoted as l_m(x,y). The overallSSIM evaluation is obtained by combining the measurement at differentscales using-

$$SSIM(x,y) = [l_m(x,y)]^{\alpha_m}\prod_{j=1}^{m}[c_j(x,y)]^{\beta_j}.[s_j(x,y)]^{\gamma_j}$$

B. Dynamic Range Independent Measure (DRIM):

A novel image quality metric that can compare a pair of images with significantly different dynamic ranges. Its main contribution is a new visible distortion concept based on the visibility of image features and the integrity of image structure. The metric generates a distortion map that shows the loss of reversal of contrast polarity, visible features, amplification of invisible features. All these distortions are considered at various scales and orientations that correspond to the visual channels in the HVS.

C. Most Apparent Distortion (MAD)[12]:

It is an image quality assessment method that attempts to explicitly model two strategies employed by the HVS:

a. a detection based strategy for high-quality images containing near threshold distortions and
b. appearance-based strategy for low-quality images containing clearly suprathreshold distortions.

When viewing and judging the quality of each distorted image, the HVS concentrate on different aspects of the

images. In some of the distorted images just-visible near-threshold distortions can be contained. For these lower quality images, the distortions dominate the overall appearance of each image, and thus visual detection is less applicable.in the high-quality regime, the HVS attempts to look for distortions in the presence of the image and in the low-quality regime, the HVS attempts to look for image content in the presence of the distortions.

Working Steps:

Step 1: Detection-Based Strategy for High-Quality Images
-compute locations at which the distortions are visible
-combine the visibility map with local errors
Step 2: Appearance-Based Strategy for Low-Quality Images
-apply a log-Gabor decomposition
Step 3: Adaptively Combining the Two Strategies
Step 4: Summary of Most Apparent Distortion

D. Feature Similarity Measure (FSIM) [13] and Feature Similarity Measure For Color Images (FSIMC) [13]:

A novel feature-similarity (FSIM) index for full reference IQA is based on the fact that human visual system (HVS)understands an image mainly according to its low-level features. Specifically, the phase congruency (PC) is a dimensionless measure of the significance of a local structure, which is used as the primary feature in FSIM. Considering that PC is contrast invariant while the contrast information does affect HVS perception of image quality, the image gradient magnitude (GM) is employed as the secondary feature in FSIM. Phase congruency and gradient magnitude play complementary roles in characterizing the image local quality. After obtaining the local quality map, we use phase congruency again as a weighting function to derive a single quality score. Although FSIM is designed for grayscale images or the luminance components of color images, the chrominance (color) information can be easily incorporated by means of a simple extension of FSIM to which we call as extension FSIMC.

Phase congruency (PC) is given by-

$$PC_{2D}(x) = \frac{\sum E_{\theta_{j(x)}}}{\epsilon + \sum\sum A_{n,\theta_j}(x)}$$

In Gradient magnitude (GM), the partial derivatives $G_x(X)$ and $G_y(X)$ of the image f(x) along horizontal and vertical directions using the three gradient operators are calculated. The gradient magnitude (GM) of f(x) is then defined as-

$$G = \sqrt{G_x^2 + G_y^2}$$

Suppose that we are going to calculate the similarity between images f1 and f2. Denote by PC1 and PC2 the PC maps extracted from f1 and f2, and G1 and G2 the GM maps extracted from them. It should be noted that for color images, PC and GM features are extracted from their luminance channels. FSIM will be defined and computed based on PC1, PC2, G1 and G2. Furthermore, by incorporating the image chrominance information into FSIM, an IQA index for color images, denoted by FSIMC, will be obtained.

VI. CONCLUSION

The main goal of biometric detection system is to stop the fake synthetic biometric sample to be taken as alegitimate one. The biometric detection system should be robust as well as adequately protect all the communication channels (for example, by encryption and challenge response techniques). It should adopt more effective optimization algorithms and models for estimating the orientation image and should capable for producing faster result so that user did not have to wait longer. The Liveness assessment method has proved its importance in achiving high accuracy to detect fake biometric samples against original one. Quality assessment of biometric samples is an important challenge for the biometrics research community. Existing methodologies have their own advantages with respect to some dependent disadvantages. It is required that a singlebiometric system should be able to detect fake biometric samples for all types of biometrics input like face image, finger image, iris image, palm image etc. as liveness assessment with image quality assessment is doing. The futuristic approach for detecting fake biometric should be multi-biometric multi-attack based intrusion detection and prevention. It is our assertion that quality metrics are an important ingredient in improving the robustness of large real-world biometric systems. In an attempt to demystify the definition and work of biometric quality, several factors that affect a biometric sample are presented. It is imperative that quality assessment entails a notion of fidelity of capture and modality-specific utility as well. Further, the performance of a biometric quality assessment metric in terms of computational complexity must also be discussed more actively in research.

VII. REFERENCES

[1]. S. A. C. Schuckers (2002), “Spoofing and anti-spoofing measures,” Security, vol. 7, no. 4, pp. 56-62.

[2]. R. W. Frischholz and U. Dieckmann (2000), “Bioid: A mul¬timodal biometric identification system,” Computer, vol. 33 issue 2, pp. 64-68.

[3]. I. Pavlidis and P. Symosek (2000), “The imaging issue in an automatic face/disguise detection system,” in IEEE Workshop on Computer Vision Beyond the Visible Spectrum: Methods and Applications.

[4]. N. Eveno and L. Besacier (2005), “Co-inertia analysis for ”liveness” test in audio-visual biometrics,” in Image and Signal Processing and Analysis, 2005. ISPA 2005. Proceedings of the 4th International Symposium on, pp. 257-261.

[5]. K. Kollreider, et al.,(2008), “Verify¬ingliveness by multiple experts in face biometrics,” in IEEE Computer Society Conference on Computer Vi¬sion and Pattern Recognition Workshops, pp. 1-6.

[6]. J. Galbally, et al., (2014),“Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition”, in IEEE, Vol. 23, No. 2,pp.710-724

[7]. Trusted Biometrics Under Spoofing Attacks (TABULA RASA) [Online]. Available: http://www.tabularasa-euproject.org/

[8]. R. Cappelli,et al., (2007), “Fingerprint image reconstruction from standard templates,” IEEE Trans. Pattern Anal.Mach. Intell., vol. 29, no. 9, pp. 1489–1503.

[9]. S. Bayram, et al.,(2006), "Image manipulation detection," J. Electron. Imag., vol. 15, no. 4, pp. 041102-1–041102-17.

[10]. J. Galbally,et al.,(2010), 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.

[11]. Z. Wang, et al.,(2003), "multi-scale structural similarity for image quality assessment", in IEEE, vol. 2,pp. 1398-1402.

[12]. Eric C. LarsonDamon M. Chandler (2010),"Most apparent distortion: full-reference image qualityassessment and the role of strategy", Journal of Electronic Imaging, vol. 19.

[13]. L. Zhang, et al., (2011), "FSIM: A Feature Similarity Index for Image Quality Assessment", inIEEE, Vol. 20, Issue. 8 pp. 2378 – 2386.