Security Lock System for Fake Traits Based on Image Processing

G.Prathiba
M.Tech.,Assistant professor/ECE, 2.S.Nandhini (M.E.)
P.R. Engineering college
gprathibasubash@gmail,comnandhini002@gmail.com

Abstract-As the number of security issues increased from day to day,we have to improve the security in efficient way.In the biometric signal based security system the major problems is to ensure the actual presence of real trait in contrast toa fake ,self-manufactured,synthetic,reconstructed traits.In this paper we propose a security lock system which provide security with combination of fingerprint,iris and palm images as biometric input.And we also include the authentication system for fake traits like silicon,playdoh,gelatin images by adding liveness assessment in a fast,user-friendly and non-intrusive manner through the image quality assessment method.In this paper we include 25 image quality features extracted from one image to differentiate the legitimate and impostor samples.Its suitable for real time security system in colleges,government sectors,private sectors,etc.This method is very efficient compared to previous state-of-the-art approaches.The cost of the method is very much reduced because the hardware is required to take the input only and the entire system is based on image processing software.The time consumption is also reduced as the recognition system is based on image processing software and we take only one image as input.And the security is very efficient as we take 25 different features in one images like MSE,NAE,AD,MD,etc.

I. INTRODUCTION

In recent years, the increasing interest in the evaluation of biometric systems security has led to the creation of numerous sessions and workshops in biometric-specific and general signal processing conferences [9], the organization of competi-tions focused on vulnerability assessment [10], [11], the acqui-sition of specific datasets [12], [13], the creation of groups and laboratories specialized in the evaluation biometric security [14], or the existence of several European Projects with the biometric security topic as main research interest [15], [16].

All these initiatives clearly highlight the importance given by all parties involved in the development of biometrics (i.e., researchers, developers and industry) to the improvement of the systems security to bring this rapidly emerging technol-ogy into practical use.

Among the different threats analyzed, the so-called *direct* or *spoofing* attacks have motivated the biometric community to study the vulnerabilities against this type of fraudulent actions in modalities such as the iris [2], the fingerprint [17], the face [13], the signature [18], or even the gait [19] and multimodal approaches. In these attacks, the intruder uses some type of synthetically produced artifact (e.g., gummy finger, printed iris image or face mask), or tries to mimic the behaviour of the genuine user (e.g., gait, signature), to fraudulently access the biometric system. As this type of attacks are performed in the analog domain and the interaction with the device is done following the regular protocol, the usual digital protection mechanisms (e.g., encryption, digital signature or watermarking) are not effective.

The aforementioned works and other analogue studies, have clearly shown the necessity to propose and develop specific protection methods against this threat. This way, researchers have focused on the design of specific countermeasures that enable biometric systems to detect fake samples and reject them, improving this way the robustness and security level of the systems.

Besides other anti-spoofing approaches such as the use of multibiometrics or challenge-response methods, special attention has been paid by researchers and industry to the *liveness detection* techniques, which use different physiolog-ical properties to distinguish between real and fake traits. Liveness assessment methods represent a challenging engi-neering problem as they have to satisfy certain demanding requirements [21]: *(i)* non-invasive, the technique should in no case be harmful for the individual or require an excessive contact with the user; *(ii)* user friendly, people should not be reluctant to use it; *(iii)* fast, results very reduced interval as the user cannot be asked to interact with the sensor for a long period of time; *(i v)* low cost, a wide use cannot be expected if the cost is excessively high; *(v)* performance, in addition to having a good fake detection rate, the protection scheme should not degrade the recognition performance (i.e., false rejection) of the biometric system.

Liveness detection methods are usually classified into one of two groups (see Fig. 1): *(i) Hardware-based* techniques, which add some specific device to the sensor in order to detect particular properties of a living trait (e.g., fingerprint sweat, blood pressure, or specific reflection properties of the eye); *(ii) Software-based* techniques, in this case the fake trait is detected once the sample has been acquired with a standard sensor (i.e., features used to distinguish between real and fake traits are extracted from the biometric sample, and not from the trait itself).

The two types of methods present certain advantages and drawbacks over the other and, in general, a combination of both would be the most desirable protection approach to increase the security of biometric systems. As a coarse 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 less intrusive since their implementation is transparent to the user. Furthermore, as they operate directly on the acquired sample (and not on the biometric trait itself), software-based techniques may be embedded in the feature extractor module which makes them potentially capable of detecting other types of illegal break-in attempts not necessarily classified as spoofing attacks. For instance, software-based methods can protect the system against the injection of reconstructed or synthetic samples into the communication channel between the sensor and the feature extractor [22], [23].

Although, as shown above, a great amount of work has been done in the field of spoofing detection and many advances have been reached, the attacking methodologies have also evolved and become more and more sophisticated. As a consequence, there are still big challenges to be faced in the detection of direct attacks. detecting certain type of spoofs (i.e., gummy fingers made out of silicone), but their efficiency drastically drops when they are presented with a different type of synthetic trait (i.e., gummy fingers made out of gelatin). This way, their error rates vary greatly when the testing conditions are modified or if the evaluation database is exchanged. Moreover, the vast majority of current protection methods are based on the measurement of certain specific properties of a given trait (e.g., the frequency of ridges and valleys in fingerprints or the pupil dilation of the eye) which gives them a very reduced interoperability, as they may not be implemented in recognition systems based on other biometric modalities (e.g., face), or even on the same system with a different sensor.

In the present work we propose a novel software-based multi-biometric and multi-attack protection method which targets to overcome part of these limitations through the use of image quality assessment (IQA). It is not only capable of operating with a very good performance under different biometric systems (multi-biometric) and for diverse spoofing scenarios, but it also provides a very good level of protection against certain non-spoofing attacks (multi-attack). Moreover, being software-based, it presents the usual advantages of this type of approaches: fast, as it only needs one image (i.e., the same sample acquired for biometric recognition) to detect whether it is real or fake; non-intrusive; user-friendly (transparent to the user); cheap and easy to embed in already functional systems (as no new piece of hardware is required).

.

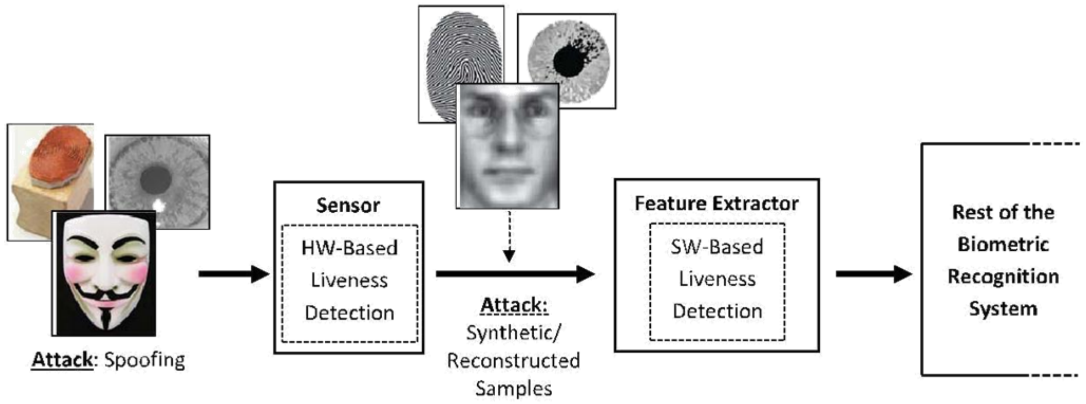
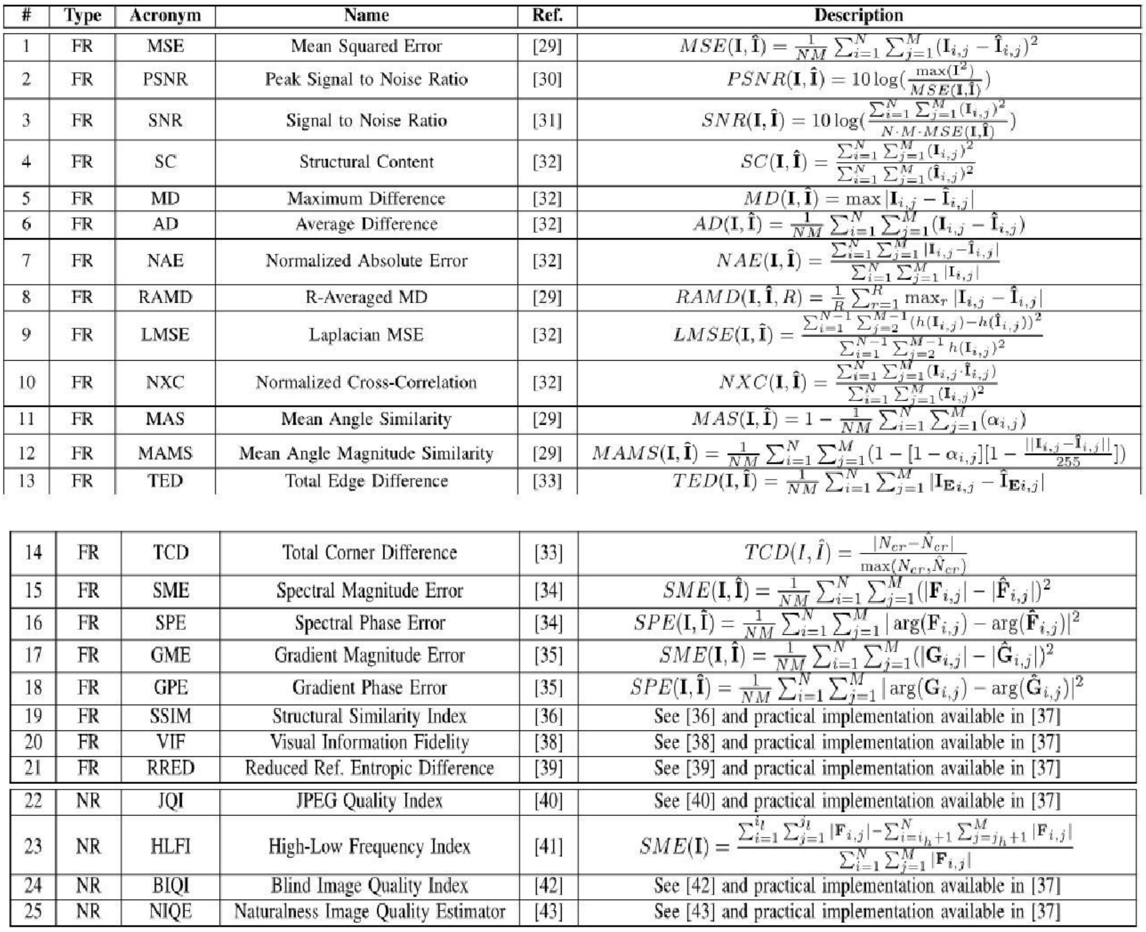

Attack: Spoofing
Sensor
HW-Based Liveness Detection
Attack: Synthetic/ Reconstructed Samples
Feature Extractor
SW-Based Liveness Detection
Rest of the Biometric Recognition System

Fig. 1. Types of attacks potentially detected by hardware-based (spoofing) and software-based (spoofing + reconstructed/synthetic samples) liveness detection techniques.

TABLE I

List of the 25 Image Quality Measures (IQMs) Implemented in The Present Work and Used for Biometric Protection. All the Features Were Either Directly Taken or Adapted from the References Given. In the Table: FR Denotes Full-Reference and NR No-Reference; I Denotes the Reference Clean Image (of Size $N \times M$) and $\hat{\mathbf{I}}$ the Smoothed Version of the Reference Image. For Other Notation Specifications and Undefined Variables or Functions We Refer the Reader to the Description of Each Particular Feature in Section III. Also, for Those Features With No Mathematical Definition, the Exact Details About Their Computation May Be Found in the Given References



#	Type	Acronym	Name	Ref.	Description
1	FR	MSE	Mean Squared Error	[29]	$MSE(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j} - \hat{\mathbf{I}}_{i,j})^2$
2	FR	PSNR	Peak Signal to Noise Ratio	[30]	$PSNR(\mathbf{I},\hat{\mathbf{I}}) = 10\log(\frac{\max(\mathbf{I}^2)}{MSE(\mathbf{I},\hat{\mathbf{I}})})$
3	FR	SNR	Signal to Noise Ratio	[31]	$SNR(\mathbf{I},\hat{\mathbf{I}}) = 10\log(\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}{N \cdot M \cdot MSE(\mathbf{I},\hat{\mathbf{I}})})$
4	FR	SC	Structural Content	[32]	$SC(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}{\sum_{i=1}^{N}\sum_{j=1}^{M}(\hat{\mathbf{I}}_{i,j})^2}$
5	FR	MD	Maximum Difference	[32]	$MD(\mathbf{I},\hat{\mathbf{I}}) = \max\lvert\mathbf{I}_{i,j} - \hat{\mathbf{I}}_{i,j}\rvert$
6	FR	AD	Average Difference	[32]	$AD(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j} - \hat{\mathbf{I}}_{i,j})$
7	FR	NAE	Normalized Absolute Error	[32]	$NAE(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\rvert}{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\mathbf{I}_{i,j}\rvert}$
8	FR	RAMD	R-Averaged MD	[29]	$RAMD(\mathbf{I},\hat{\mathbf{I}},R) = \frac{1}{R}\sum_{r=1}^{R}\max_r\lvert\mathbf{I}_{i,j} - \hat{\mathbf{I}}_{i,j}\rvert$
9	FR	LMSE	Laplacian MSE	[32]	$LMSE(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N-1}\sum_{j=2}^{M-1}(h(\mathbf{I}_{i,j})-h(\hat{\mathbf{I}}_{i,j}))^2}{\sum_{i=1}^{N-1}\sum_{j=2}^{M-1}h(\mathbf{I}_{i,j})^2}$
10	FR	NXC	Normalized Cross-Correlation	[32]	$NXC(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}\cdot\hat{\mathbf{I}}_{i,j})}{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}$
11	FR	MAS	Mean Angle Similarity	[29]	$MAS(\mathbf{I},\hat{\mathbf{I}}) = 1 - \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\alpha_{i,j})$
12	FR	MAMS	Mean Angle Magnitude Similarity	[29]	$MAMS(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(1 - [1 - \alpha_{i,j}][1 - \frac{\lvert\lvert\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\rvert\rvert}{255}])$
13	FR	TED	Total Edge Difference	[33]	$TED(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\mathbf{I}_{\mathbf{E}i,j} - \hat{\mathbf{I}}_{\mathbf{E}i,j}\rvert$
14	FR	TCD	Total Corner Difference	[33]	$TCD(I,\hat{I}) = \frac{\lvert N_{cr}-\hat{N}_{cr}\rvert}{\max(N_{cr},\hat{N}_{cr})}$
15	FR	SME	Spectral Magnitude Error	[34]	$SME(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\lvert\mathbf{F}_{i,j}\rvert - \lvert\hat{\mathbf{F}}_{i,j}\rvert)^2$
16	FR	SPE	Spectral Phase Error	[34]	$SPE(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\arg(\mathbf{F}_{i,j}) - \arg(\hat{\mathbf{F}}_{i,j})\rvert^2$
17	FR	GME	Gradient Magnitude Error	[35]	$SME(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\lvert\mathbf{G}_{i,j}\rvert - \lvert\hat{\mathbf{G}}_{i,j}\rvert)^2$
18	FR	GPE	Gradient Phase Error	[35]	$SPE(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\arg(\mathbf{G}_{i,j}) - \arg(\hat{\mathbf{G}}_{i,j})\rvert^2$
19	FR	SSIM	Structural Similarity Index	[36]	See [36] and practical implementation available in [37]
20	FR	VIF	Visual Information Fidelity	[38]	See [38] and practical implementation available in [37]
21	FR	RRED	Reduced Ref. Entropic Difference	[39]	See [39] and practical implementation available in [37]
22	NR	JQI	JPEG Quality Index	[40]	See [40] and practical implementation available in [37]
23	NR	HLFI	High-Low Frequency Index	[41]	$SME(\mathbf{I}) = \frac{\sum_{i=1}^{i_l}\sum_{j=1}^{j_l}\lvert\mathbf{F}_{i,j}\rvert-\sum_{i=i_h+1}^{N}\sum_{j=j_h+1}^{M}\lvert\mathbf{F}_{i,j}\rvert}{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\mathbf{F}_{i,j}\rvert}$
24	NR	BIQI	Blind Image Quality Index	[42]	See [42] and practical implementation available in [37]
25	NR	NIQE	Naturalness Image Quality Estimator	[43]	See [43] and practical implementation available in [37]

An added advantage of the proposed technique is its speed and very low complexity, which makes it very well suited to operate on real scenarios (one of the desired characteristics of this type of methods). As it does not deploy any trait-specific property (e.g., minutiae points, iris position or face detection), the computation load needed for image processing purposes is very reduced, using only *general* image quality measures fast to compute, combined with very simple classifiers.

It has been tested on publicly available attack databases of iris, fingerprint and 2D face, where it has reached results fully comparable to those obtained on the same databases and following the same experimental protocols by more complex trait-specific top-ranked approaches from the state-of-the-art.

The rest of the paper is structured as follows. Some key concepts about image quality assessment and the rational behind its use for biometric protection is given in Section II. The proposed method is described in Section III. The results for iris, fingerprint and 2D face evaluation experiments appear in Sections IV-A, IV-B, and IV-C. Conclusions are finally drawn in Section V.

II. IMAGE QUALITY ASSESSMENT FOR LIVENESS DETECTION

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.*"

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 fingerprint images 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 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.

Following this "*quality-difference*" hypothesis, in the present research work we explore the potential of *general* image quality assessment as a protection method against different biometric attacks (with special attention to 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. This gives the proposed method a new multi-biometric dimension which is not found in previously described protection schemes.

In the current state-of-the-art, the rationale behind the use of IQA features for liveness detection is supported by three factors:

- Image quality has been successfully used in previous works for image manipulation detection [24], [25] and steganalysis [26], [27] in the forensic field. To a certain extent, many spoofing attacks, especially those which involve taking a picture of a facial image displayed in a 2D device (e.g., spoofing attacks with printed iris or face images), may be regarded as a type of image manipulation which can be effectively detected, as shown in the present research work, by the use of different quality features.

  In addition to the previous studies in the forensic area, different features measuring trait-specific quality properties have already been used for liveness detection purposes in fingerprint and iris applications [5], [28]. However, even though these two works give a solid basis to the use of image quality as a protection method in biometric systems, none of them is general. For instance, measuring the ridge and valley frequency may be a good parameter to detect certain fingerprint spoofs, but it cannot be used in iris liveness detection. On the other hand, the amount of occlusion of the eye is valid as an iris anti-spoofing mechanism, but will have little use in fake fingerprint detection.

  This same reasoning can be applied to the vast majority of the liveness detection methods found in the state-of-the-art. Although all of them represent very valuable works which bring insight into the difficult problem of spoofing detection, they fail to generalize to different problems as they are usually designed to work one specific modality and, in many cases, also to detect one type of spoofingattack.

- Human observers very often refer to

the“different appear-ance” of real and fake samples to distinguish between them. As stated above, the different metrics and methods designed for IQA intend to estimate in an objective and reliable way the perceived appearance of images by humans.

Moreover, as will be explained in Section III, different quality measures present different sensitivity to image arti-facts and distortions. For instance, measures like the mean squared error respond more to additive noise, whereas others such as the spectral phase error are more sensitive to blur; while gradient-related features react to distortions concentrated around edges and textures. Therefore, using a wide range of IQMs exploiting complementary image quality properties, should permit to detect the aforementioned quality differences between real and fake samples expected to be found in many attack attempts (i.e., providing the method with multi-attack protection capabilities).

All these observations lead us to believe that there is sound proof for the “quality-difference” hypothesis and that image quality measures have the potential to achieve success in biometric protection tasks.

III. THE SECURITY PROTECTION METHOD

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 25 general image quality measures.

A general diagram of the protection approach proposed in this work is shown in Fig. 2. 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) 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 stan-dard implementations in Matlab.

• **Pixel Difference measures** :These features compute the distortion between two images on the basis of their pixelwise differences. Here we include:

Mean Squared Error (MSE), Peak Signal to Noise Ratio (PSNR), Signal to Noise Ratio (SNR), Structural Content (SC), Maximum Difference (MD), Average Difference (AD), Normalized Absolute Error (NAE), R-Averaged Maximum Difference (RAMD) and Laplacian Mean Squared Error (LMSE). The formal definitions for each of these features are given in Table I. In the RAMD entry in Table I, maxr is defined as the r -highest pixel difference between two images. For the present implementation, R = 10. In the LMSE entry in Table I, h(Ii, j) = Ii+1, j +Ii−1, j + Ii, j+1 + Ii, j−1 − 4Ii, j .

• **Correlation-based measures** :The similarity between two digital images can also be quantified in terms of the correlation function. A variant of correlation based measures can be obtained by considering the statistics of the angles between the pixel vectors of the original and distorted images. These features include (also defined in Table I): Normalized Cross-Correlation (NXC), Mean Angle Similarity (MAS) and Mean Angle- Magnitude Similarity (MAMS). In the MAS and MAMS entries in Table I, αi, j denotes the angle between two vectors, defined as, αi, j = 2 π arccos Ii, j ,ˆIi, j ||Ii, j ||·||ˆIi, j || , where Ii, j , ˆIi, j denotes the scalar product. As we are dealing with positive matrices I and ˆI, we are constrained to the first quadrant of the Cartesian space so that the maximum difference attained will be π/2, therefore the coefficient 2/π is included for normalization.

• **Edge-based measures:** Edges and other two-dimensional features such as corners, are some of the most informative parts of an image, which play a key role in the human visual system and in many computer vision algorithms including quality assessment applications [33]. Since the structural distortion of an image is tightly linked with its edge degradation, here we have considered two edge-related quality measures: Total Edge Difference (TED) and Total Corner Difference (TCD).

In order to implement both features, which are computed according to the corresponding expressions given in Table I, we use: (i) the Sobel operator to build the binary edge maps IE and ˆIE ;

(i i) the Harris corner detector [48] to compute the number of corners Ncr and Nˆcr found in
I and ˆI.

• **Spectral distance measures.** The Fourier transform is another traditional image processing tool which has been applied to the field of image quality assessment [29]. In this work we will consider as IQ spectral-related features: the Spectral Magnitude Error (SME) and the Spectral Phase

Error (SPE), defined in Table I (where F and ˆF are the respective Fourier transforms of I and ˆI), and arg(F) denotes phase.

• **Gradient-based measures.** Gradients convey important visual information which can be of great use for quality assessment. Many of the distortions that can affect an image are reflected by a change in its gradient. Therefore, using such information, structural and contrast changes can be effectively captured [49]. 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), defined in Table I (where G and Gˆ are the gradient maps of I and ˆI defined as G = Gx+iGy, where Gx and Gy are the gradients in the x and y
directions).

1V. RESULTS.

A. Results**: Iris**

For the iris modality the protection method is tested under two different attack scenarios, namely: i) spoofing attack and ii) 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.

In all cases the final results (shown in Table II) are obtained applying two-fold cross validation. The classifier used for the two scenarios is based on Quadratic Discriminant Analysis (QDA) as it showed a slightly better performance than Linear Discriminant Analysis (LDA), which will be used in the face-related experiments,while keeping the simplicity of the whole system.

1) Results: Iris-Spoofing: The database used in this spoofing scenario is the ATVS-FIr DB which may be obtained from the Biometric Recognition Group-ATVS.1 The database comprises real and fake iris images (printed on paper) of 50 users randomly selected from the BioSec baseline corpus [52]. It follows the same structure as the original BioSec dataset, therefore, it comprises 50 users × 2 eyes × 4 images × 2 sessions = 800 fake iris images and its corresponding original samples. The acquisition of both real and fake samples was carried out using the LG IrisAccess EOU3000 sensor with infrared illumination which captures bmp grey-scale images of size 640 × 480 pixels.

As mentioned above, for the experiments the database is divided into a: train set, comprising 400 real images and their corresponding fake samples of 50 eyes; and a test set with the remaining 400 real and fake samples coming from the other 50 eyes available in the dataset. The liveness detection results achieved by the proposed approach under this scenario appear in the first row of Table II, where we can see that the method is able to correctly classify over 97% of the samples. In the last column we show the average execution time in seconds needed to process (extractWindows7-PC with a 3.4 GHz processor and 16 GB RAM memory, running MATLAB R2012b.

As no other iris liveness detection method has yet been reported on the public ATVS-FIr DB, for comparison, the second row of Table II reports the results obtained on this database by a self-implementation of the anti-spoofing method proposed in [28]. It may be observed that the proposed method not only outperforms the state-of-the-art technique, but also, as it does not require any iris detection or segmentation, the processing time is around 10 times faster.

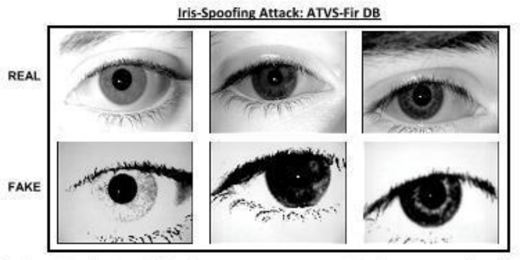


Fig. 4. Typical real iris images (top row) and their corresponding fake samples (bottom row) that may be found in the ATVS-FIr DB used in the iris-spoofing experiments. The database is available at http://atvs.ii.uam.es/.

2) Results: Iris-Synthetic: In this scenario attacks are performed with synthetically generated iris samples which are injected in the communication channel between the sensor and the feature extraction module (see Fig. 1). The real and fake databases used in this case are:

• Real database: CASIA-IrisV1. This dataset is publicly available through the Biometric Ideal Test (BIT) platform of the Chinese Academy of Sciences Institute of Automation (CASIA).2 It contains 7 grey-scale 320×280 images of 108 eyes captured in two separate sessions with a selfdeveloped CASIA close-up camera and are stored in bmp format.

• Synthetic database: WVU-Synthetic Iris DB [23]. Being a database that contains only fully synthetic data, it is not subjected to any legal constraints and is publicly available through the CITeR research center.

The synthetic irises are generated following the method described in [23], which has two stages. In the first stage, a Markov Random Field model trained on the CASIA-IrisV1 DB is used to generate a background texture representing the global iris appearance. In the next stage, a variety of iris features such as radial and concentric furrows, collarette and crypts, are generated and embedded in the texture field. Following the CASIA-IrisV1 DB, this synthetic database includes 7 grey-scale 320 × 280 bmp images of 1,000 different subjects (eyes).

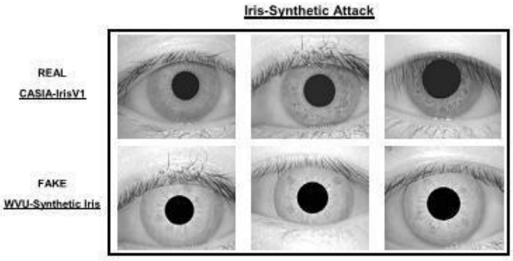
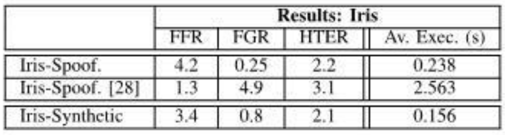


Fig. 5. Typical real iris images from CASIA-IrisV1 (top row) and fake samples from WVU-Synthetic Iris DB (bottom row), used in the iris-synthetic experiments. The databases are available at http://biometrics.idealtest.org and http://www.citer.wvu.edu/.



	Results: Iris			
	FFR	FGR	HTER	Av. Exec. (s)
Iris-Spoof.	4.2	0.25	2.2	0.238
Iris-Spoof. [28]	1.3	4.9	3.1	2.563
Iris-Synthetic	3.4	0.8	2.1	0.156

B. Results: **Fingerprints**

For the fingerprint modality, the performance of the proposed protection method is evaluated using the LivDet 2009 DB [10] comprising over 18,000 real and fake samples. As in the iris experiments, the database is divided into a: train set, used to train the classifier; and test set, used to evaluate the performance of the protection method. 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 irisrelated experiments is used here. 1) Results: Fingerprints-Spoofing LivDet: The LivDet 2009 DB [10] was captured in the framework of the 2009 Fingerprint Liveness Detection Competition and it is distributed through the site of the competition.4 It comprises three datasets of real and fake fingerprints captured each of them with a different flat optical sensor: i) Biometrika FX2000 (569 dpi), ii) CrossMatch Verifier 300CL (500 dpi), and iii) Identix DFR2100 (686dpi). The gummy fingers were generated using three different materials: silicone, gelatin and playdoh, always following a consensual procedure (with the cooperation of the user). As a whole, the database contains over 18,000 samples coming from more than 100 different fingers. Some typical examples of the images that can be found in this database are shown in Fig. 6, where the material used for the generation of the fake fingers is specified (silicone, gelatine or playdoh). The train and test sets selected for the evaluation experiments on this database are the same as the ones used in the LivDet 2009 competition, so that the results obtained by the proposed method based on general IQA may be directly compared to the participants of the contest. The general distribution of the database in the train and test sets is specifiedin Table IV.

Results achieved on this database are shown in the first two rows of Table III. For clarity, only the best results achieved on LivDet09 for each of the individual datasets is given (second row). The best performance obtained by any of the reported methods on each of the three datasets is highlighted in bold in order to facilitate the comparison of the results.

The database has a perfectly defined associated evaluation protocol which considers three totally independent datasets (in terms of users): train, used to tune the parameters of the method; development, to fix the decision threshold; and test, where final results are computed. The protocol is released with the database and has been strictly followed in the present experiments.

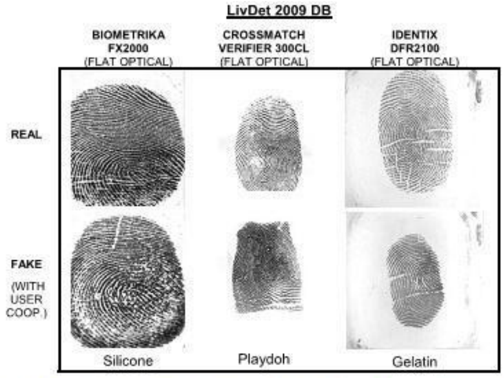

LivDet 2009 DB
BIOMETRIKA FX2000 (FLAT OPTICAL)
CROSSMATCH VERIFIER 300CL (FLAT OPTICAL)
IDENTIX DFR2100 (FLAT OPTICAL)
REAL
FAKE (WITH USER COOP.)
Silicone
Playdoh
Gelatin

Fig. 6. Typical examples of real and fake fingerprint images that can be found in the public LivDet09 database used in the fingerprint anti-spoofing experiments. The database is available at http://prag.diee.unica.it/LivDet09/.

C. Results: **2D Face**

The performance of the IQA-based protection method has also been assessed on a face spoofing database: the REPLAY-ATTACK DB [57] which is publicly available from the IDIAP Research Institute.5 The database contains short videos (around 10 seconds in mov format) of both real-access and spoofing attack attempts of 50 different subjects, acquired with a 320 × 240 resolution webcam of a 13-inch MacBook Laptop. The recordings were carried out under two different conditionswith a uniform background and artificial lighting; adverse, with natural illumination and non-uniform background.

Three different types of attacks were considered: i) print, illegal access attempts are carried out with hard copies of high-resolution digital photographs of the genuine users;ii) mobile, the attacks are performed using photos and videos taken with the iPhone using the iPhone screen; iii) highdef, similar to the mobile subset but in this case the photos and videos are displayed using an iPad screen with resolution 1024 × 768.

In addition, access attempts in the three attack subsets (print, mobile and highdef) were recorded in two different modes depending on the strategy followed to hold the attack replay device (paper, mobile phone or tablet): i) hand-based and ii) fixed-support.Such a variety of real and fake acquisition scenarios And conditions makes the REPLAY-ATTACK DB a unique benchmark for testing anti-spoofing techniques for face-based systems. As a consequence, the print subset was selected as the evaluation dataset in the 2011 Competition on Counter Measures to 2D Facial Spoofing Attacks [11].

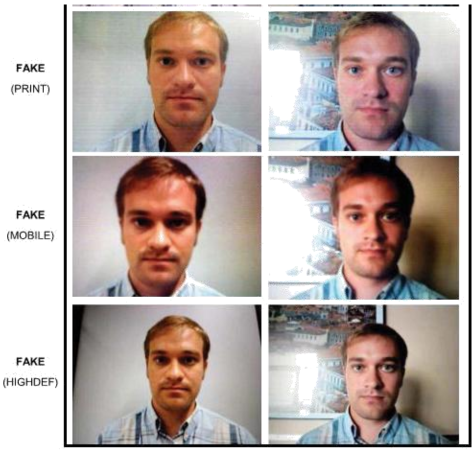


Fig. 7. Typical examples of real and fake (print, mobile and highdef) face

D. Preliminary Feature Individuality Analysis

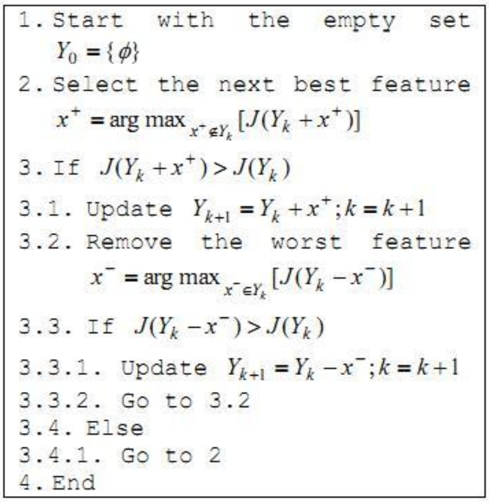
In this section we present a preliminary study of the discriminative power of the different quality features used in the proposed protection method. Although a deeper analysis of the features relevance for each of the considered experimental scenarios would be advisable, such a rigorous examination would represent on its own the topic for a new research work which falls out of the scope of the present contribution.

The Sequential Forward Floating Selection (SFFS) algorithm has been used to determine if certain individual features, or certain subsets of features, present a higher discrimination capability than others under the biometric security experimental framework considered in the work. The SFFS method is a deterministic, single-solution feature selection algorithm, which has shown remarkable performance over other suboptimal selection schemes .

V.SFFS

Feature selection has become the focus of research area for a long time. The purpose of feature selection is to obtain the most minimal sized subset of features [1]. Practical experience has shown that if there is too much irrelevant and redundant information present, the performance of a classifier might be degraded. Removing these irrelevant and redundant features can improve the classification accuracy.

The Sequential Forward Floating Selection (SFFS) method to deal with the nesting problem. In SFFS, Y0 is initialized as the empty set and in each step a new subset is generated first by adding a feature x+, but after that features x– is searched for to be eliminated from Yk until the correct classification rate J(Yk – x–) decreases. The iterations continue until no new variable can be added because the recognition rate J(Yk + x+) does not increase. The algorithm is as below.



```
1. Start with the empty set
   $Y_0 = \{\phi\}$
2. Select the next best feature
   $x^+ = \arg\max_{x^+ \notin Y_k} [J(Y_k + x^+)]$
3. If $J(Y_k + x^+) > J(Y_k)$
3.1. Update $Y_{k+1} = Y_k + x^+; k = k+1$
3.2. Remove the worst feature
     $x^- = \arg\max_{x^- \in Y_k} [J(Y_k - x^-)]$
3.3. If $J(Y_k - x^-) > J(Y_k)$
3.3.1. Update $Y_{k+1} = Y_k - x^-; k = k+1$
3.3.2. Go to 3.2
3.4. Else
3.4.1. Go to 2
4. End
```

The process of searching for the best feature x+ and the worst feature x– within SFFS is repetitive, thus making its results are constants, regardless the number of execution. Therefore, it is only efficient if these results are stored in the memory, rather than having to repeat the process and recalculate every result. By storing these results, CI-SFFS only have to determine whether a feature has been previously calculated. If it hasn't been calculated, then the result will calculated and stored. This process is referred as memory pooling. Thread is the smallest unit of processing that can be scheduled by an operating system. Multithreading allows multiple threads to exist within the context of a single process [45]. These threads share the process' resources but are able to execute independently.

One obvious requirement of multithreading is that the individual threads that make up a process must be switched between at some point. This is necessary because only one thread can have the CPU at a time for execution. Switching between threads can either be cooperative or preemptive. In cooperative task switching, a thread runs until it decides it is done, then lets other thread run,eventually returning to the caller. Preemptive task switching involves a thread that runs until some event (like an interrupt) cause the thread to be suspended and another thread to resume execution.

VI. CONCLUSION

The study of the vulnerabilities of biometric systems against different types of attacks has been a very active field of research in recent years [1]. This interest has lead to big advances in the field of security-enhancing technologies for biometric-based applications. However, in spite of this noticeable improvement, the development of efficient protection methods against known threats has proven to be a challenging task. Simple visual inspection of an image of a real biometric trait and a fake sample of the same trait shows that the two images can be very similar and even the human eye may find it difficult to make a distinction between them after a short inspection. Yet, some disparities between the real and fake images may become evident once the images are translated into a proper feature space. In this context, it is reasonable to assume that the image quality properties of real accesses and fraudulent attacks will be different. Following this ―quality difference‖ hypothesis, in the present research work we have explored the potential of general image quality assessment as a protection tool against different biometric attacks (with special attention to spoofing).For this purpose we have considered a feature space of 25 complementary image quality measures which we have combined with simple classifiers to detect real and fake access attempts. The novel protection method has been evaluated on three largely deployed biometric modalities such as the iris, the fingerprint and 2D face, using publicly available databases

with well defined associated protocols. This way, the results are reproducible and may be fairly compared with other future analogue solutions.

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‖);

ii) The proposed method is able to adapt to different types of attacks providing for all of them a high level of protection (―multi-attack‖);

iii) 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 properties in a practical protection system.

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,‖

[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.

[6] K. A. Nixon, V. Aimale, and R. K. Rowe, ―Spoof detection schemes,‖ Handbook of Biometrics. New York, NY, USA: Springer-Verlag, 2008, pp. 403–423.

[7] ISO/IEC 19792:2009, Information Technology—Security Techniques— Security Evaluation of Biometrics, ISO/IEC Standard 19792, 2009.

[8] Biometric Evaluation Methodology. v1.0, Common Criteria, 2002.

[9] K. Bowyer, T. Boult, A. Kumar, and P. Flynn, Proceedings of the IEEE Int. Joint Conf. on Biometrics. Piscataway, NJ, USA: IEEE Press, 2011.

[10] G. L. Marcialis, A. Lewicke, B. Tan, P. Coli, D. Grimberg, A. Congiu, et al., ―First international fingerprint liveness detection competition— LivDet 2009,‖ in Proc. IAPR ICIAP, Springer LNCS-5716. 2009pp. 12.

[11] M. M. Chakka, A. Anjos, S. Marcel, R. Tronci, B. Muntoni, G. Fadda, et al., ―Competition on countermeasures to 2D facial spoofing attacks,‖ in Proc. IEEE IJCB, Oct. 2011, pp. 1–6.

[12] J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martinez-Diaz, ―Evaluation of direct attacks to fingerprint verification systems,‖ J. Telecommun. Syst., vol. 47, nos. 3–4, pp. 243–254, 2011.

[13] A. 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.

[14] Biometrics Institute, London, U.K. (2011). Biometric VulnerabilitY.

[15] (2012). BEAT: Biometrices Evaluation and Testing [Online]. Available: http://www.beat-eu.org/

[16] (2010). Trusted Biometrics Under Spoofing Attacks (TABULA RASA) [Online]. Available: http://www.tabularasa euproject.org/

[17] 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.

[18] J. Hennebert, R. Loeffel, A. Humm, and R. Ingold, ―A new forgery scenario based on regaining dynamics of signature,‖ .

[19] A. Hadid, M. Ghahramani, V. Kellokumpu, M. Pietikainen, J. Bustard, and M. Nixon, ―Can gait biometrics be spoofed?‖ in Proc. IAPR ICPR, 2012, pp. 3280–3283.